A proof of Minkowski's second theorem

Matthew Tointon

Minkowski's second theorem is a fundamental result from the geometry of numbers with important applications in additive combinatorics (see, for example, its application to the proof of Freiman-type theorems in [1, Chapter 3] and [2]). Its statement is as follows; we refer the reader to [1, §3.7] for definitions.

Theorem 1 (Minkowski's second theorem)**.** *Let $K \subset \mathbb{R}^d$ be a centrally symmetric convex body and let Λ be a nodegenerate lattice. Write $\lambda_1 \leq \ldots \leq \lambda_d$ for the successive minima of K with respect to Λ. Then $\lambda_1 \ldots \lambda_d \operatorname{vol}(K) \leq 2^d \det(\Lambda)$.*

The purpose of this note is to present a proof of this result. I hope that it might be of use to those learning it for the first time or teaching it, or even just of interest. It is not intended for publication; in particular, I have not attempted a literature review of the depth that would be required for a published work.

As seems to be standard for proofs of Minlowski's second theorem, the present proof makes use of Blichfeldt's lemma.

Lemma 2 (Blichfeldt)**.** *Suppose that Λ is a nondegenerate lattice and that K is a set containing no pair of distinct points $\mathbf{x}, \mathbf{y}$ with $\mathbf{x} - \mathbf{y} \in \Lambda$. Then $\operatorname{vol}(K) \leq \det(\Lambda)$.*

Proof. The hypothesis implies that the quotient map

$$\varphi : \mathbb{R}^d \to \frac{\mathbb{R}^d}{\Lambda}$$

is injective on K. Letting D be a fundamental domain for Λ and writing ψ for the natural 'unfolding' map $\mathbb{R}^d/\Lambda$, we may consider $\psi \circ \varphi$ as cutting K into (measurable) pieces and then translating these pieces into D. Its injectivity on K implies that it is volume preserving on K, and so we have $\operatorname{vol}(K) \leq \operatorname{vol}(D) = \det(\Lambda)$. □

Upon passing to the interior of K we may assume that K is open. The definition of the successive minima implies that we may fix a linearly independent subset $B = \{\mathbf{b_1}, \ldots, \mathbf{b_d}\}$ of Λ with the property that $\mathbf{b_i} \in \overline{\lambda_i K} \backslash \lambda_i K$, where $\overline{\lambda_i K}$ denotes the closure of $\lambda_i K$.

Write B_i for the vector subspace of $\mathbb{R}^d$ spanned by $\mathbf{b_1}, \ldots, \mathbf{b_i}$, and define

$$\Lambda_i = \Lambda \cap (B_i \backslash B_{i-1}).$$

Set $\Lambda_0 = B_0 = \{0\}$. Note that Λ is the disjoint union of the Λ_i. Then we have the following result.

Proposition 3. *There exist bodies* $K_1 \subset K_2 \subset \ldots \subset K_d = \lambda_d K$ *such that:*

1. *for* $i \le d-1$ *we have* $\mathrm{vol}(K_i) = (\lambda_i/\lambda_{i+1})^i \,\mathrm{vol}(K_{i+1})$*;*
2. *for* $\mathbf{m} \in \Lambda_j$ $(j \ge 1)$ *and* $\mu \in \mathbb{R}$ *satisfying* $|\mu| \ge 2\max\{\lambda_i/\lambda_j, 1\}$ *we have* $K_i \cap (K_i + \mu\mathbf{m}) = \varnothing$.

In particular, Proposition 3 gives the existence of a set K_1 of volume $\mathrm{vol}(K_1) = \lambda_1 \ldots \lambda_d \,\mathrm{vol}(K)$ such that if $\mathbf{m} \in \Lambda\backslash\{0\}$ then whenever $|\mu| \ge 2$ we have $K_1 \cap (K_1 + \mu\mathbf{m}) = \varnothing$. Hence no two distinct points of K_1 differ by an element of $2{\cdot}\Lambda$, and so applying Blichfeldt's lemma to K_1 completes the proof of Theorem 1.

It remains, of course, to prove Proposition 3. We start by proving that if we set $K_d := \lambda_d K$ then K_d satisfies assertion 2 of Proposition 3.

Lemma 4. *Let* $j \in \{1, \ldots, d\}$*, let* $\mathbf{m} \in \Lambda_j$ *and let* $\mu \in \mathbb{R}$ *satisfy* $|\mu| \ge 2\lambda_d/\lambda_j$*. Then* $\lambda_d K \cap (\lambda_d K + \mu\mathbf{m}) = \varnothing$.

Proof. The openness of K and the definition of the successive minima imply that $\mathbf{m} \notin \lambda_j K$, and so by convexity we may define a hyperplane $H_{\mathbf{m}}$ that contains $\mathbf{m}$ but does not meet $\lambda_j K$. By central symmetry we also have that $-H_{\mathbf{m}}$ does not meet $\lambda_j K$, and hence that $\lambda_j K$ is contained in the open slice $S_{\mathbf{m}}$ of $\mathbb{R}^d$ lying between $H_{\mathbf{m}}$ and $-H_{\mathbf{m}}$.

Observe that $-H_{\mathbf{m}} = H_{\mathbf{m}} - 2\mathbf{m}$, which makes it clear that $S_{\mathbf{m}} \cap (S_{\mathbf{m}} + \mu\mathbf{m}) = \varnothing$ for any $\mu \in \mathbb{R}$ with $|\mu| \ge 2$, and in particular that $\lambda_j K \cap (\lambda_j K + \mu\mathbf{m}) = \varnothing$ for any such μ. This in turn means that $\lambda_d K \cap (\lambda_d K + \mu\mathbf{m}) = \varnothing$ whenever $|\mu| \ge 2\lambda_d/\lambda_j$. □

We are now in a position to prove Proposition 3 in full. Define a series of 'compression operations' as follows. If L is any body in $\mathbb{R}^d$ then define $\sigma_i(L)$ to be the result of taking each (i-dimensional) slice of L parallel to B_i and scaling it parallel to B_i by a factor of λ_i/λ_{i+1}, with the scaling centred on the centre of mass[1] of the original slice of L. The operations σ_i are essentially identical to the maps Φ defined in [3, Lemma 3.31].

Note the following three properties of σ_i:

(i) $\mathrm{vol}(\sigma_i(L)) = (\lambda_i/\lambda_{i+1})^i \,\mathrm{vol}(L)$.

(ii) If each slice of L parallel to B_i is convex then, since the scaling is centred on a point of L, we have $\sigma_i(L) \subset L$.

(iii) If each slice of L parallel to B_i is convex then each slice of $\sigma_i(L)$ parallel to B_i is also convex, as is each slice of $\sigma_i(L)$ parallel to B_j for any $j < i$ (although σ_i will not in general preserve convexity of L overall).

Now define the bodies $K_1, \ldots, K_d$ by setting $K_d := \lambda_d K$ and setting $K_i = \sigma_i(K_{i+1})$ for all other i. The convexity of K certainly implies that the slices of K_d parallel to B_{d-1} are convex, and so by repeated application of properties 2 and 3 we have

$$K_i \subset K_{i+1} \tag{1}$$

[1] It does not really matter which point of the slice of L we use here; we specify the centre of mass only for concreteness.

for each $i < d$. Furthermore, property (i) of the σ_i immediately implies property 1 required by Proposition 3.

For arbitrary j, property 2 of Proposition 3 holds for $i = d$ by Lemma 4. For $i < d$ it follows by induction on $d - i$. Indeed, for $i \geq j$ the inductive step is immediate from the definition of σ_i, since each σ_i scales K_{i+1} by λ_i/λ_{i+1} in direction $\mathbf{m}$. For $i < j$ the inductive step follows from (1). This completes the proof of Proposition 3, and hence of Theorem 1. □

References

[1] B. J. Green. *Additive combinatorics*, notes from a Part III lecture course (2009), available at `https://www.dpmms.cam.ac.uk/~bjg23/add-combinatorics.html`.

[2] B. J. Green and I. Z. Ruzsa. Freiman's theorem in an arbitrary abelian group, *J. Lond. Math. Soc.* **75**(1) (2007), 163-175.

[3] T. C. Tao and V. H. Vu. *Additive combinatorics*, Cambridge Univ. Press (2006).