log-concave function of x_d, i.e. $f((1-\lambda)x_d + \lambda y_d) \geq f(x_d)^{1-\lambda} f(y_d)^{\lambda}$ for all $0 \leq \lambda \leq 1$ and $x_d, y_d \in \mathbf{R}$; this is known as *Brunn's inequality*.

3.4.4 Let A be a bounded open set with smooth boundary ∂A, and let B be a ball with the same volume as A. Prove the *isoperimetric inequality* $\mathrm{mes}(\partial A) \geq \mathrm{mes}(\partial B)$. (Hint: Use the Brunn–Minkowski inequality to estimate $\frac{\mathrm{mes}(A+\varepsilon\cdot B)-\mathrm{mes}(A)}{\varepsilon}$ for $\varepsilon > 0$ small, and then let $\varepsilon \to 0$.)

3.4.5 Let A, B be symmetric convex bodies in $\mathbf{R}^d$. Show by examples that there is no upper bound for $\mathrm{mes}(A+B)$ in terms of $\mathrm{mes}(A)$, $\mathrm{mes}(B)$, amd d alone, except in the $d = 1$ case. However, by using Lemma 3.12, show that $\mathrm{mes}(A+B) \leq 4^d \frac{\mathrm{mes}(A)\mathrm{mes}(B)}{\mathrm{mes}(A\cap B)}$.

3.4.6 [282] Let A be a convex body. Use the Brunn's inequality to show that $\mathrm{mes}(A \cap (x+A)) \geq (1-r)^n \mathrm{mes}(A)$ whenever $0 \leq r \leq 1$ and $x \in r \cdot (A-A)$. Conclude that

$$\begin{aligned}\mathrm{mes}(A)^2 &= \int_{A-A} \mathrm{mes}(A \cap (x+A))\, dx \\ &\geq \int_0^1 n(1-r)^{n-1} \mathrm{mes}(A)\mathrm{mes}(r\cdot(A-A))\, dr \\ &= \frac{1}{\binom{2n}{n}} \mathrm{mes}(A)\mathrm{mes}(A-A)\end{aligned}$$

whence one obtains the *Rogers–Shepard inequality* $\mathrm{mes}(A-A) \leq \binom{2n}{n}\mathrm{mes}(A)$. Show that this inequality is sharp when A is a simplex. Use Stirling's formula to compare this inequality with (3.5).

3.4.7 [162] Let A, B be additive sets in $\mathbf{Z}^d$. Use the Brunn–Minkowski inequality to show that $|A+B+\{0,1\}^d| \geq 2^d \min(|A|, |B|)$. (Hint: consider $A + [0,1]^d$ and $B + [0,1]^d$.)

3.4.8 [162] Let A, B be additive sets in $\mathbf{R}^d$. Show that $|A+B+\{0,1\}^d| \geq 2^d \min(|A|, |B|)$. (Hint: partition $\mathbf{R}^d$ into cosets of $\mathbf{Z}^d$, locate the coset with the largest intersection with A or B, and apply the preceding exercise.)

3.4.9 Let A be an open bounded set in $\mathbf{R}^d$. Show that $\mathrm{mes}(A+A) \geq 2^d \mathrm{mes}(A)$, with equality if and only if A is convex. (Hint: $A + A$ contains $2 \cdot A$.)

3.5 Intersecting a convex set with a lattice

In previous sections we have studied lattices, which are discrete but unbounded, and convex sets, which are bounded but continuous. We now study the intersection $B \cap \Gamma$ of a convex set B and a lattice Γ in a Euclidean space $\mathbf{R}^d$, which is then necessarily

a finite set. A model example of such set is the discrete box $[0, N)$ for some $N = (N_1, \dots, N_d)$, which is the intersection of the convex body $\{(x_1, \dots, x_d) : -1 < x_i < N_i \text{ for all } 1 \le i \le d\}$ with the Euclidean lattice $\mathbf{Z}^d$. One of the main objectives of this section shall to show a "discrete John's lemma" which shows that all intersections $B \cap \Gamma$ can be approximated in a certain sense by a discrete box.

We begin with some elementary estimates.

Lemma 3.21 *Let Γ be a lattice in $\mathbf{R}^d$. If $A \subset \mathbf{R}^d$ is an arbitrary bounded set and $P \subset \mathbf{R}^d$ is a finite non-empty set, then*

$$|A \cap (\Gamma + P)| \le |(A - A) \cap (\Gamma + P - P)|. \tag{3.9}$$

If B is a symmetric convex body, then

$$(k \cdot B) \cap \Gamma \text{ can be covered by } (4k + 1)^d \text{ translates of } B \cap \Gamma \tag{3.10}$$

for all $k \ge 1$. If furthermore Γ' is a sub-lattice of Γ of finite index $|\Gamma / \Gamma'|$, then we have

$$|B \cap \Gamma'| \le |B \cap \Gamma| \le 9^d |\Gamma / \Gamma'| |B \cap \Gamma'|. \tag{3.11}$$

Proof We first prove (3.9). We may of course assume that $A \cap (\Gamma + P)$ contains at least one element a. But then $A \cap (\Gamma + P) \subseteq ((A - A) \cap (\Gamma + P - P)) + a$, and the claim follows. Now we prove (3.10). The lower bound is trivial, so it suffices to prove the upper bound. By the preceding argument we can cover $|(\frac{1}{2} \cdot B + x) \cap \Gamma|$ by a translate of $B \cap \Gamma$ for any $x \in \mathbf{R}^d$. But by Corollary 3.15 we can cover $k \cdot B$ by $(4k + 1)^d$ translates of $\frac{1}{2} \cdot B$, and the claim (3.10) follows.

Finally, we prove (3.11). The lower bound is trivial. For the upper bound, observe that Γ is the union of $|\Gamma / \Gamma'|$ translates of Γ, so it suffices to show that $|B \cap (\Gamma' + x)| \le 9^d |B \cap \Gamma'|$ for all $x \in \mathbf{R}^d$. But by (3.9) and (3.10) we have

$$|B \cap (\Gamma' + x)| \le |(2 \cdot B) \cap \Gamma'| \le 9^d |B \cap \Gamma'|$$

as desired. □

Next, we recall a result of Gauss concerning the intersection of a large convex body with a lattice of full rank.

Lemma 3.22 *Let $\Gamma \subset \mathbf{R}^d$ be a lattice of full rank, let $v_1, \dots, v_d \in \Gamma$ be a set of generators for Γ, and let B be a convex body in $\mathbf{R}^d$. Then for large $R > 0$, we have*

$$|(R \cdot B) \cap \Gamma| = (R^d + O_{\Gamma, B, d}(R^{d-1})) \frac{\mathrm{mes}(B)}{|v_1 \wedge \cdots \wedge v_d|}.$$

Here $|v_1 \wedge \cdots \wedge v_d|$ denotes the volume of the parallelepiped with edges $v_1, \dots, v_d$.

Proof We use a "volume-packing argument". Since Γ has full rank, $v_1, \ldots, v_d$ are linearly independent. By applying an invertible linear transformation we may assume that $v_1, \ldots, v_d$ is just the standard basis $e_1, \ldots, e_d$, so that $\Gamma = \mathbf{Z}^d$. Now let Q be the unit cube centered at the origin. Observe that the sets $\{x + Q : x \in (R \cdot B) \cap \mathbf{Z}^d\}$ are disjoint up to sets of measure zero, and their union differs from $R \cdot B$ only in the $\sqrt{d}$-neighborhood of the surface of $R \cdot B$, which has volume $O_{\Gamma,B,d}(R^{d-1})$. The claim follows. □

Remark 3.23 The task of improving the error term $O_{\Gamma,B,d}(R^{d-1})$ for various lattices and convex bodies (e.g. Gauss' circle problem) is a deep and important problem in number theory and harmonic analysis, but we will not discuss this issue in this book; our only concern is that the error term is strictly lower order than the main term.

If Γ is a lattice, we define a *fundamental parallelepiped* for Γ to be any parallelepiped whose edges $v_1, \ldots, v_d$ generate Γ. From the above lemma we conclude that all fundamental parallelepipeds have the same volume; indeed this volume is nothing more than the covolume $\mathrm{mes}(\mathbf{R}^d/\Gamma)$ of Γ. Thus for instance $\mathrm{mes}(\mathbf{R}^d/\mathbf{Z}^d) = 1$.

By another volume-packing argument we can establish

$$\mathrm{mes}(\mathbf{R}^d/\Gamma)|\Gamma/\Gamma'| = \mathrm{mes}(\mathbf{R}^d/\Gamma') \tag{3.12}$$

whenever $\Gamma' \subseteq \Gamma \subset \mathbf{R}^d$ are two lattices of full rank; see the exercises. In particular we see that the quotient group $|\Gamma/\Gamma'|$ is finite.

Yet another volume-packing argument gives the following continuous and periodic analogue of (2.8).

Lemma 3.24 (Volume-packing lemma) *Let $\Gamma \subset \mathbf{R}^d$ be a lattice of full rank, let V be a bounded open subset of $\mathbf{R}^d$, and let P be a finite non-empty set in $\mathbf{R}^d$. Then*

$$|(V - V) \cap (\Gamma + P - P)| \geq \frac{\mathrm{mes}(V)|P|}{\mathrm{mes}(\mathbf{R}^d/\Gamma)}.$$

In particular, we have

$$|(V - V) \cap \Gamma| \geq \frac{\mathrm{mes}(V)}{\mathrm{mes}(\mathbf{R}^d/\Gamma)}.$$

Proof Let B be the unit ball on $\mathbf{R}^d$, and let $R > 0$ be a large number. Consider the integral of the function

$$f(x) := \sum_{y \in \Gamma \cap (R \cdot B)} \sum_{p \in P} 1_{V+y+p}(x).$$

On the one hand we can compute this integral using Lemma 3.22 as

$$\begin{aligned}\int_{\mathbf{R}^d} f(x)\,dx &= \sum_{y\in\Gamma\cap(R\cdot B)}\sum_{p\in P}\mathrm{mes}(V+y)\\ &= |\Gamma\cap(R\cdot B)||P||\mathrm{mes}(V)|\\ &= (R^d + O_{\Gamma,B,d}(R^{d-1}))|P|\frac{\mathrm{mes}(B)\mathrm{mes}(V)}{\mathrm{mes}(\mathbf{R}^d/\Gamma)}\end{aligned}$$

On the other hand, from (3.9) we have

$$f(x) \le |(x-V)\cap(\Gamma+P-P)| \le |(V-V)\cap(\Gamma+P-P)|.$$

Furthermore, $f(x)$ is only non-zero when x lies in $R\cdot B+V+P\subset(R+O_{V,P}(1))\cdot B$, which has volume $R^d+O_{V,P,d}(R^{d-1})$. Thus

$$\int_{\mathbf{R}^d} f(x)\,dx \le |(V-V)\cap(\Gamma+P-P)|R^d + O_{V,P,d}(R^{d-1}).$$

Combining these inequalities, dividing by R^d, and taking limits as $R\to\infty$, we obtain the result. □

To see the utility of this lemma, let us pause to establish the following classical result in number theory, which we will need later in this book. Let $\|x\|_{\mathbf{R}/\mathbf{Z}}$ denote the distance from x to the nearest integer.

Corollary 3.25 (Kronecker approximation theorem) *Let $\alpha_1,\ldots,\alpha_d$ be real numbers, and let $0<\theta_1,\ldots,\theta_d\le 1/2$. Then for any $N>0$, we have*

$$|\{n\in(-N,N):\|n\alpha_j\|_{\mathbf{R}/\mathbf{Z}}<\theta_j \text{ for all } j=1,\ldots,d\}| \ge N\theta_1\cdots\theta_d.$$

In particular, if $N\theta_1\cdots\theta_d\le 1$, then there exists an integer $0<n<N$ such that $\|n\alpha_j\|_{\mathbf{R}/\mathbf{Z}}\le\theta_j$ for all $j=1,\ldots,d$.

Proof Apply Lemma 3.24 with $\Gamma:=\mathbf{Z}^d$,

$$V := \{(t_1,\ldots,t_d)+\mathbf{Z}^d : 0<t_j<\theta_j \text{ for all } 1\le j\le d\},$$

and P equal to the arithmetic progression $P=[0,N)\cdot(\alpha_1,\ldots,\alpha_d)$ in $\mathbf{R}^d$. □

Even when B is symmetric, it is possible for $|B\cap\Gamma|$ to be extremely large compared with $\frac{\mathrm{mes}(B)}{2^d\mathrm{mes}(\mathbf{R}^d/\Gamma)}$; consider for instance $\Gamma:=\mathbf{Z}^2$ and $B:=\{(x,y):-1/N^2<x<1/N^2;-N<y<N\}$. However, if $B\cap\Gamma$ has full rank, then we can complement the lower bound (3.14) with an upper bound:

Lemma 3.26 *Let Γ be a lattice of full rank in $\mathbf{R}^d$, and let B be a symmetric convex body in $\mathbf{R}^d$ such that the vectors in $B\cap\Gamma$ linearly span $\mathbf{R}^d$. Then*

$$|B\cap\Gamma| \le \frac{3^d d!\mathrm{mes}(B)}{2^d\mathrm{mes}(\mathbf{R}^d/\Gamma)}. \tag{3.13}$$

This bound is with a factor of $3^d/(2d+1)$ of being sharp, as can be seen by the example where $\Gamma = \mathbf{Z}^d$ and B is (a slight enlargement of) the octahedron with vertices $\pm e_1, \ldots, \pm e_d$. Indeed this example motivates the volume-packing argument used in the proof.

Proof By hypothesis, $B \cap \Gamma$ contains a d-tuple $(v_1, \ldots, v_d)$ of linearly independent vectors. Since $B \cap \Gamma$ is finite, we can choose $v_1, \ldots, v_d$ in order to minimize the volume $\mathrm{mes}(O) = \frac{2^d}{d!}|v_1 \wedge \cdots \wedge v_d|$ of the octahedron with vertices $\pm v_1, \ldots, \pm v_d$. Since B is symmetric and convex, we see that $O \subseteq B$. Also O does not contain any elements of Γ other than $v_1, \ldots, v_d$, since otherwise one could replace one of $v_1, \ldots, v_d$ with this element and reduce the volume of O, a contradiction. Thus we see that the sets $\{x + \frac{1}{2} \cdot O : x \in B \cap \Gamma\}$ are all disjoint and are contained in $B + \frac{1}{2} \cdot O \subseteq \frac{3}{2} \cdot B$. Thus

$$|B \cap \Gamma| \leq \frac{\mathrm{mes}\left(\frac{3}{2} \cdot B\right)}{\mathrm{mes}\left(\frac{1}{2} \cdot O\right)} = \frac{3^d d!}{2^d |v_1 \wedge \cdots \wedge v_d|} \mathrm{mes}(B).$$

Since $|v_1 \wedge \cdots \wedge v_d| \geq \mathrm{mes}(\mathbf{R}^d/\Gamma)$, the claim follows. □

A special case of the volume-packing lemma gives

Lemma 3.27 (Blichtfeld's lemma) *Let $\Gamma \subset \mathbf{R}^d$ be a lattice of full rank, and let V be an open set in $\mathbf{R}^d$ such that $\mathrm{mes}(V) > \mathrm{mes}(\mathbf{R}^d/\Gamma)$. Then there exists distinct $x, y \in V$ such that $x - y \in \Gamma$.*

Now let us apply Lemma 3.24 to the case $V = \frac{1}{2} \cdot B$ and $P = \{0\}$, where B is a symmetric convex body; we obtain the lower bound

$$|B \cap \Gamma| \geq \frac{\mathrm{mes}(B)}{2^d \mathrm{mes}(\mathbf{R}^d/\Gamma)}, \tag{3.14}$$

which is the classical Minkowski's first theorem. The assumption of symmetry is essential. Consider for instance $\Gamma := \mathbf{Z}^2$ and a convex set of the form $B := \{(x, y) : 1/3 < x < 2/3; -N < y < N\}$ for arbitrarily large N.

Theorem 3.28 (Minkowski's first theorem) *Let Γ be a lattice of full rank, and let B be a symmetric convex body such that $\mathrm{mes}(B) \geq 2^d \mathrm{mes}(\mathbf{R}^d/\Gamma)$. Then the closure of B must contain at least one non-zero element of Γ (in fact it contains at least two, by symmetry). If we have strict inequality, $\mathrm{mes}(B) > 2^d \mathrm{mes}(\mathbf{R}^d/\Gamma)$, then we can replace the closure of B with the interior of B in the above statement.*

Proof Apply (3.14) to $(1+\epsilon)B$ and let ϵ go to zero. □

The constant in Minkowski's first theorem is sharp. We may apply an invertible linear transformation to set $\Gamma := \mathbf{Z}^d$, and then the example of the cube $A :=$

$\{(t_1, \ldots, t_d) : -1 < t_j < 1 \text{ for all } j = 1, \ldots, d\}$ shows that the constant 2^d cannot be improved. Nevertheless, it is possible to improve Minkowski's first theorem by generalizing it to a "multiparameter" version as follows.

Definition 3.29 (Successive minima) Let Γ be a lattice in $\mathbf{R}^d$ of rank k, and let B be a convex body in $\mathbf{R}^d$. We define the *successive minima* $\lambda_j = \lambda_j(B, \Gamma)$ for $1 \leq j \leq k$ of B with respect to Γ as

$$\lambda_j := \inf\{\lambda > 0 : \lambda \cdot B \text{ contains } k \text{ linearly independent elements of } \Gamma\}.$$

Note that $0 < \lambda_1 \leq \cdots \leq \lambda_k < \infty$.

Thus, for instance, if $\Gamma = \mathbf{Z}^d$ and B is the box

$$B := \{(t_1, \ldots, t_d) : |t_j| < a_j \text{ for all } j = 1, \ldots, d\}$$

for some $a_1 \geq a_2 \geq \cdots \geq a_d > 0$, then $\lambda_j = 1/a_j$ for $j = 1, \ldots, d$. Note that the assumption that Γ has rank k ensures that the λ_j are both finite and non-zero.

Theorem 3.30 (Minkowski's second theorem) *Let Γ be a lattice of full rank in $\mathbf{R}^d$, and let B be an symmetric convex body in $\mathbf{R}^d$, with successive minima $0 < \lambda_1 \leq \cdots \leq \lambda_d$. Then there exists d linearly independent vectors $v_1, \ldots, v_d \in \Gamma$ with the following properties:*

- *for each $1 \leq j \leq d$, v_j lies in the boundary of $\lambda_j \cdot B$, but $\lambda_j \cdot B$ itself does not contain any vectors in Γ outside of the span of $v_1, \ldots, v_{j-1}$;*
- *the octahedron with vertices $\pm v_j$ contains no elements of Γ in its interior, other than the origin;*
- *we have*

$$\frac{2^d |\Gamma/(\mathbf{Z}^d \cdot (v_1, \ldots, v_d))|}{d!} \leq \frac{\lambda_1 \cdots \lambda_d \mathrm{mes}(B)}{\mathrm{mes}(\mathbf{R}^d/\Gamma)} \leq 2^d; \tag{3.15}$$

in particular, the sub-lattice $\mathbf{Z}^d \cdot (v_1, \ldots, v_d)$ of Γ has bounded index:

$$|\Gamma/(\mathbf{Z}^d \cdot (v_1, \ldots, v_d))| \leq d!. \tag{3.16}$$

One can state (3.15) rather crudely as

$$\lambda_1 \cdots \lambda_d \mathrm{mes}(B) = d^{O(d)} \mathrm{mes}(\mathbf{R}^d/\Gamma)$$

thus relating the successive minima to the volume of the body B and the covolume of the lattice Γ.

Note that if B contains no non-zero elements of Γ then $\lambda_j \geq 1$ for all j, so Minkowski's second theorem implies Minkowski's first theorem. Conversely, we shall see from the proof that Minkowski's second theorem can be obtained from Minkowski's first theorem by a non-isotropic dilation. The basis $v_1, \ldots, v_d$ is

sometimes referred to as a *directional basis* for A with respect to Γ, although one should caution that this basis does not quite generate Γ (the index in (3.16) is bounded but not necessarily equal to 1).

Proof By definition of λ_1, we may find a vector $v_1 \in \Gamma$ such that v_1 lies in the closure of $\lambda_1 \cdot B$, but that $\lambda \cdot B$ contains no non-zero elements of Γ for any $\lambda \leq \lambda_1$. By definition of λ_2, we can then find a vector $v_2 \in \Gamma$, linearly independent from v_1, such that v_2 lies in the closure of $\lambda_2 B$, but that $\lambda \cdot B$ contains no elements of Γ outside of the span of v_1 for any $\lambda \leq \lambda_2$. Continuing inductively we can eventually find a linearly independent set $v_1, \ldots, v_d$ in Γ such that v_j lies in the boundary of $\lambda_j \cdot B$, but $\lambda_j \cdot A$ itself does not contain any vectors in Γ outside of the span of $v_1, \ldots, v_{j-1}$, for all $1 \leq j \leq n$.

The set $v_1, \ldots, v_d$ is a basis of $\mathbf{R}^d$; by applying an invertible linear transformation we may assume it is the standard basis $e_1, \ldots, e_d$ (this changes both B and Γ, but one may easily verify that the conclusion of the theorem remains unchanged). In particular this forces Γ to contain $\mathbf{Z}^d$, hence by (3.12)

$$\mathrm{mes}(\mathbf{R}^d/\Gamma) = \mathrm{mes}(\mathbf{R}^d/\mathbf{Z}^d)/|\Gamma/\mathbf{Z}^d| = 1/|\Gamma/\mathbf{Z}^d| \leq 1. \tag{3.17}$$

Let O^d be the open octahedron whose vertices are $\pm e_1, \ldots, \pm e_d$. We need to verify that O^d contains no lattice points from Γ other than the origin. Suppose for contradiction that $O^d \cap \Gamma$ contained $w = t_1 e_1 + \cdots + t_j e_j$ where $1 \leq j \leq d$ and $t_j \neq 0$. Then $(1+\varepsilon)w$ would be a linear combination of $\pm e_1, \ldots, \pm e_j$ for some $\varepsilon > 0$. All of these points lie in the closure of $\lambda_j \cdot B$, hence w lies in the interior of $\lambda_j \cdot B$, but does not lie in the span of $e_1, \ldots, e_{j-1}$. But this contradicts the construction of $v_j = e_j$. Hence $O^d \cap \Gamma = \{0\}$.

Next, observe that $\pm v_j = \pm e_j$ lies on the boundary of $\lambda_j \cdot B$ for each $1 \leq j \leq d$. Thus B contains the open octahedron whose vertices are $\pm e_1/\lambda_1, \ldots, \pm e_d/\lambda_d$. This octahedron is easily verified to have volume $\frac{2^d}{d!\lambda_1 \cdots \lambda_d}$; indeed one can rescale to the case when all the λ_j are equal to 1, and then one can decompose the octahedron into 2^d simplices, each of which has volume $1/d!$. This establishes the lower bound in (3.15).

Now we establish the upper bound in (3.15). We need the following lemma.

Lemma 3.31 (Squeezing lemma) *Let K be a symmetric convex body in $\mathbf{R}^d$, let A be an open subset of K, let V be a k-dimensional subspace of $\mathbf{R}^d$, and let $0 < \theta \leq 1$. Then there exists an open subset A' of K such that* $\mathrm{mes}(A') = \theta^k \mathrm{mes}(A)$ *and* $(A' - A') \cap V \subseteq \theta \cdot (A - A) \cap V$.

Note that we do not assume any convexity on A or A'. Indeed the squeezing operation we define in the proof below does not preserve the convexity of A.

Proof Without loss of generality we may take $V = \mathbf{R}^k$, and write $\mathbf{R}^d = \mathbf{R}^k \times \mathbf{R}^{d-k}$. Let $\pi : \mathbf{R}^d \to \mathbf{R}^{d-k}$ be the orthogonal projection map, which restricts to a map $\pi : K \to \pi(K)$. Let $f : \pi(K) \to K$ be any continuous right-inverse of π; thus for instance $f(y)$ could be the center of mass of $\pi^{-1}(y)$.

A point $w \in K$ can be written as $w = (x, y)$, using the decomposition $\mathbf{R}^d = \mathbf{R}^k \times \mathbf{R}^{d-k}$. Consider the map Φ which maps $w = (x, y)$ to $\theta w + (1 - \theta) f(y)$ and set $A' = \Phi(A)$. Since both w and $f(y)$ belong to K and K is convex, it follows that A' is an open subset of K. Furthermore, the second coordinate of $\Phi(w)$ is y as is that of $f(y)$. By applying Cavalieri's principle (or Fubini's theorem) we see that $\mathrm{mes}(A') = \theta^k \mathrm{mes}(A)$ (the map contracts A by a factor θ with respect to $V = \mathbf{R}^k$).

Consider a point $v = \Phi(w) - \Phi(w')$, where $w = (x, y)$, $w' = (x', y')$ are points from A. If $v \in V$, then the second coordinate of v is zero, which means $y = y'$. Then by the definition of Φ, $v = \theta(w - w')$. Thus $v \in \theta \cdot (A - A)$, concluding the proof of Lemma 3.31. □

We apply the squeezing lemma iteratively, starting with $A_0 := \frac{\lambda_d}{2} \cdot B$, to create open sets $A_1, \ldots, A_{d-1} \subseteq A_0$ such that

$$\mathrm{mes}(A_j) = \left(\frac{\lambda_j}{\lambda_{j+1}} \right)^j \mathrm{mes}(A_{j-1})$$

and

$$(A_j - A_j) \cap \mathbf{R}^j \subseteq \frac{\lambda_j}{\lambda_{j+1}} \cdot (A_{j-1} - A_{j-1}) \cap \mathbf{R}^j$$

for all $1 \leq j \leq d - 1$, where $\mathbf{R}^j$ is the span of $e_1, \ldots, e_j$. In every application of the squeezing lemma, A_0 plays the role of the mother set K.

Using the definition of A_0, it is easy to check that

$$\mathrm{mes}(A_{d-1}) = \lambda_1 \cdots \lambda_d 2^{-d} \mathrm{mes}(B). \tag{3.18}$$

Furthermore, by induction one can show

$$(A_{d-1} - A_{d-1}) \cap \mathbf{R}^j \subseteq \frac{\lambda_j}{\lambda_d} \cdot (A_{j-1} - A_{j-1}) \cap \mathbf{R}^j.$$

On the other hand, $A_{j-1} \subset A_0 = (\lambda_d/2) \cdot B$. Since B is symmetric, $\frac{\lambda_d}{2} \cdot B - \frac{\lambda_d}{2} \cdot B = \lambda_d \cdot B$. It follows that

$$(A_{d-1} - A_{d-1}) \cap \mathbf{R}^j \subset \lambda_j \cdot B \cap \mathbf{R}^j$$

for all $1 \leq j \leq d$.

By the definition of the successive minima, $\lambda_j \cdot B \cap \mathbf{R}^j$ does not contain any lattice point in Γ, except for those in $\mathbf{R}^{j-1}$. This implies that $A_{d-1} - A_{d-1}$ does

not contain any point in Γ other than the origin. Applying Blichtfeld's lemma, we conclude that

$$\mathrm{mes}(A_{d-1}) \leq \mathrm{mes}(\mathbf{R}^d / \Gamma),$$

which when combined with (3.18) gives the upper bound in (3.15). □

We now give several applications of this theorem. First we "factorize" a convex body B as the finitely overlapping sum of a subset of Γ and and a dilate of a small convex body B', up to some scaling factors of $O(d)^{O(1)}$:

Lemma 3.32 *Let B be a symmetric convex body in $\mathbf{R}^d$, and let Γ be a lattice in $\mathbf{R}^d$. Then there exists a symmetric convex body $B' \subseteq B$ such that B' contains no non-zero elements of Γ, and such that $B \subseteq O(d^{3/2}) \cdot B' + ((O(d^{3/2}) \cdot B) \cap \Gamma$. In particular, the projection of B in $\mathbf{R}^d / \Gamma$ is contained in the projection of $O(d^{3/2}) \cdot B'$. Furthermore, we have the bounds*

$$\frac{\mathrm{mes}(B)}{O(d)^{5d/2}|B \cap \Gamma|} \leq \mathrm{mes}(B') \leq O(1)^d \frac{\mathrm{mes}(B)}{|B \cap \Gamma|}. \tag{3.19}$$

Proof By using John's theorem and an invertible linear transformation we may assume that $B_d \subseteq B \subseteq \sqrt{d} \cdot B_d$, where B_d is the unit ball. We may assume that the vectors in $B \cap \Gamma$ generate Γ, since otherwise we could replace Γ by the lattice generated by $B \cap \Gamma$.

Let us temporarily assume that Γ has full rank, and thus that the linear span of $B \cap \Gamma$ is $\mathbf{R}^d$. Thus if we let $\lambda_1 \leq \cdots \leq \lambda_d$ be the successive minima of B, then we have $\lambda_j \leq 1$ for all j.

Now we take a directional basis $v_1, \ldots, v_d$ of Γ, and let B' be the open octahedron with vertices $\pm v_j$; this octahedron then contains no non-zero elements of Γ, and is also contained in B (since $\pm v_j/\lambda_j$ already lies on the boundary of B). Observe that $d \cdot B'$ contains a parallelepiped with edges $v_1, \ldots, v_d$, and hence $d \cdot B' + \Gamma = \mathbf{R}^d$. Thus

$$B \subseteq d \cdot B' + ((B - d \cdot B') \cap \Gamma) \subseteq d \cdot B' + (((d+1) \cdot B) \cap \Gamma)$$

as desired (with about $d^{1/2}$ room to spare). In particular we have

$$\mathrm{mes}(B) \leq \mathrm{mes}(d \cdot B')|(d+1) \cdot B \cap \Gamma| \leq (d(4d+5))^d \mathrm{mes}(B')|B \cap \Gamma|$$

thanks to (3.10); this proves the lower bound in (3.19) (with a factor of $d^{d/2}$ to spare). Conversely, the sets $\{x + \frac{1}{2} \cdot B' : x \in B \cap \Gamma\}$ are disjoint (since B' contains no non-zero elements of Γ) and contained in $2 \cdot B$, hence

$$|B \cap \Gamma| \mathrm{mes}\left(\frac{1}{2} \cdot B'\right) \leq \mathrm{mes}(2 \cdot B)$$

which gives the upper bound in (3.19). This concludes the proof when Γ has full rank.

Now suppose that Γ has rank $r < d$, then after a rotation we may assume that Γ is contained in $\mathbf{R}^r \times \{0\} \subset \mathbf{R}^r \times \mathbf{R}^{d-r}$. The point is that the behavior in the $d-r$ dimensions orthogonal to $\mathbf{R}^r$ is rather trivial and can be easily dealt with as follows. Let $\tilde{B} \subset \mathbf{R}^r$ be the intersection of B with $\mathbf{R}^r \times \{0\}$, identifying $\mathbf{R}^r \times \{0\}$ with $\mathbf{R}^r$ in the usual manner. Then by John's theorem we have the inclusions

$$\frac{1}{2} \cdot (\tilde{B} \times B_{d-r}) \subseteq B \subseteq \sqrt{d} \cdot (\tilde{B} \times B_{d-r}).$$

Applying the previous arguments to $\tilde{B}$ to obtain a set $\tilde{B}' \subseteq \tilde{B}$, and then defining $B' := \frac{1}{2} \cdot (\tilde{B}' \times B_{d-r})$, we can verify the claim in this case (losing some additional factors of $d^{1/2}$ and $d^{d/2}$); we omit the details. □

In this theorem, we did not use the full strength of Minkowski's second theorem (in particular we did not need the upper bound). The notion of a directional vector is, however, useful.

As another consequence of Minkowski's second theorem, we show how to find large proper progressions inside sets of the form $B \cap \Gamma$.

Lemma 3.33 *Let B be a convex symmetric body in $\mathbf{R}^d$, and let Γ be a lattice in $\mathbf{R}^d$. Then there exists a proper progression P in $B \cap \Gamma$ of rank at most d such that $|P| \geq O(d)^{-7d/2}|B \cap \Gamma|$.*

Proof Applying John's theorem (Theorem 3.13) and (3.10) followed by a linear transformation, we may reduce to the case where B is the unit ball $B = B_d$ in $\mathbf{R}^d$, provided that we also reduce the $7d/2$ exponent to $3d$. We may assume that $B \cap \Gamma$ spans $\mathbf{R}^d$, since otherwise we may restrict B to the linear span of $B \cap \Gamma$, which is then isomorphic to a Euclidean space of some lower dimension. In particular this means Γ has full rank, and that the successive minima $0 < \lambda_1 \leq \cdots \leq \lambda_d$ of B with respect to Γ cannot exceed 1. Let $v_1, \ldots, v_d \in \Gamma \cap B$ be the corresponding directional basis. Let Q denote the parallelepiped

$$Q := \{t_1 v_1 + \cdots + t_d v_d : 0 \leq t_j < 1/2 \text{ for all } j \in [1, d]\}.$$

By (3.16), Since each translate of $Q - Q$ is a fundamental domain for $\mathbf{Z}^d \cdot (v_1, \ldots, v_d)$, it contains at most $d!$ elements of Γ. By Lemma 2.14, we can cover B by at most $\frac{\mathrm{mes}(B+Q)}{\mathrm{mes}(Q)}$ translates of $Q - Q$, and thus

$$|B| \leq d! \frac{\mathrm{mes}(B+Q)}{\mathrm{mes}(Q)}.$$

Since the $v_1, \ldots, v_d$ lie in the unit ball B, we see that $Q \subseteq \frac{d}{2} \cdot B$ and hence $B + Q \subseteq (\frac{d}{2} + 1) \cdot B$. Crudely bounding $d! = O(d^d)$, we thus conclude that

$$|B \cap \Gamma| \leq O(d)^{2d} / \mathrm{mes}(Q).$$

From (3.15) we have

$$\lambda_1 \cdots \lambda_d \leq O(1)^d \mathrm{mes}(\mathbf{Z}^d / \Gamma) \leq O(1)^d \mathrm{mes}(Q)$$

and thus

$$|B \cap \Gamma| \leq O(d)^{2d} / \lambda_1 \cdots \lambda_d.$$

The claim now follows by setting $P := [-N, N] \cdot (v_1, \ldots, v_d)$, where $N_j := 1/2d\lambda_j$ for $j \in [1, d]$; note that one can easily verify that P is contained in $B \cap \Gamma$. □

We now give an alternative approach that gives results similar to Lemma 3.33. We first need a lemma to modify the directional basis given by Minkowski's second theorem (which only spans a sub-lattice of Γ, see (3.16)) into a genuine basis.

Theorem 3.34 (Mahler's theorem) *Let Γ be a lattice of full rank in $\mathbf{R}^d$, and let B be an symmetric convex body in $\mathbf{R}^d$, with successive minima $0 < \lambda_1 \leq \cdots \leq \lambda_d$. Let $v_1, \ldots, v_d$ be a directional basis for Γ. Then there exists a basis $w_1, \ldots, w_d$ of Γ such that w_1 lies in the closure of $\lambda_1 \cdot B$, and w_i lies in the closure of $\frac{i\lambda_i}{2} \cdot B$ for all $2 \leq i \leq d$. Furthermore, if V_i is the linear span of $v_1, \ldots, v_i$, then $w_1, \ldots, w_i$ forms a basis for $\Gamma \cap V_i$.*

The basis $w_1, \ldots, w_d$ is sometimes known as a *Mahler basis* for Γ.

Proof We choose $w_1 := v_1$; clearly w_1 forms a basis for $\Gamma \cap V_1$. Now suppose inductively that $2 \leq i \leq d$ and $w_1, \ldots, w_{i-1}$ have already been chosen with the desired properties. The lattice $\Gamma \cap V_i$ has one higher rank than $\Gamma \cap V_{i-1}$ and hence there exists a vector w_i in $\Gamma \cap (V_i \backslash V_{i-1})$ which, together with $\Gamma \cap V_{i-1}$, generates $\Gamma \cap V_i$; in particular, $w_1, \ldots, w_i$ will generate $\Gamma \cap V_i$. Since $v_1, \ldots, v_i$ linearly span V_i, we may write $w_i = t_1 v_1 + \cdots + t_{i-1} v_{i-1} + t_i v_i$ for some real numbers $t_1, \ldots, t_i$ with $t_i \neq 0$. Since v_i lies in $\Gamma \cap V_{i-1} + W$, we must have $t_i = \pm 1/n$ for some integer n. If $|t_i| = 1$, then $\Gamma \cap V_i$ is generated by $\Gamma \cap V_{i-1}$ and v_i, and we can take $w_i := v_i$. Thus we may assume $|t_i| \leq 1/2$. Also, by subtracting integer multiples of $v_1, \ldots, v_{i-1}$ from w_i if necessary (which will not affect the fact that $\Gamma \cap V_i$ is generated by $\Gamma \cap V_{i-1}$ and w_i) we may assume that $|t_j| \leq 1/2$ for all $1 \leq j < i$. But since each v_j lies in the closure of $\lambda_j \cdot B$ and hence $\lambda_i \cdot B$, we conclude by convexity that w_i lies in the closure of $\frac{i\lambda_i}{2} \cdot B$, and so we can continue the iterative construction. Setting $i = d$ we obtain the remaining claims in the theorem. □

As an application we give

Corollary 3.35 *Let Γ be a lattice of full rank in $\mathbf{R}^d$. Then there exists linearly independent vectors $w_1, \ldots, w_d \in \Gamma$ which generate Γ, and such that*

$$\mathrm{mes}(\mathbf{R}^d/\Gamma) = |w_1 \wedge \cdots \wedge w_d| \geq \Omega(d^{-3d/2})|w_1| \cdots |w_d|. \tag{3.20}$$

Proof Let $w_1, \ldots, w_d$ be a Mahler basis for Γ with respect to the unit ball B, and let $\lambda_1, \ldots, \lambda_d$ be the successive minima. Then by Theorem 3.34 we have

$$|w_1| \cdots |w_d| \leq \lambda_1 \prod_{i=2}^{d} \frac{i\lambda_i}{2}.$$

Applying (3.15) we obtain

$$|w_1| \cdots |w_d| \leq \frac{2d!}{\mathrm{mes}(B)} \mathrm{mes}(\mathbf{R}^d/\Gamma).$$

On the other hand, from (3.8) we have

$$\mathrm{mes}(B) = \frac{\Gamma(3/2)^d 2^d}{\Gamma(d/2+1)} = (2\pi e + o(1))^{d/2} d^{-d/2}.$$

Crudely bounding $d! = O(d^d)$, the claim follows. □

As a consequence, we can give a "discrete John's theorem" to characterize the intersection of a convex symmetric body with a lattice.

Lemma 3.36 (Discrete John's theorem) *Let B be a convex symmetric body in $\mathbf{R}^d$, and let Γ be a lattice in $\mathbf{R}^d$ of rank r. Then there exists a r-tuple $w = (w_1, \ldots, w_r) \in \Gamma^r$ of linearly independent vectors in Γ and and a r-tuple $N = (N_1, \ldots, N_r)$ of positive integers such that*

$$(r^{-2r} \cdot B) \cap \Gamma \subseteq (-N, N) \cdot w \subseteq B \cap \Gamma \subseteq (-r^{2r}N, r^{2r}N) \cdot w.$$

Notice that the fact $(-N, N) \cdot w \subseteq B \cap \Gamma$ is similar to the conclusion of Lemma 3.33. However, the generalized arithmetic progression in Lemma 3.33 has higher density.

Proof We first observe, using John's theorem and an invertible linear transformation, that we may assume without loss of generality that $B_d \subseteq B \subseteq d \cdot B_d$, where B_d is the unit ball in $\mathbf{R}^d$. We may assume that Γ has full rank $r = d$, for if $r < d$ then we may simply restrict B to the linear span of Γ, which can then be identified with $\mathbf{R}^r$. We may assume $d \geq 2$ since the claim is easy otherwise.

Now let $w = (w_1, \ldots, w_d)$ be as in Lemma 3.35. For each j, let L_j be the least integer greater than $1/d|w_j|$. Then from the triangle inequality we see that $|l_1 w_1 + \cdots + l_d w_d| < 1$ whenever $|l_j| < L_j$, and so $(-L, L) \cdot w$ is contained in B_d and hence in B.

Now let $x \in B \cap \Gamma$. Since w generates Γ, we have $x = l_1 w_1 + \cdots + l_d w_d$ for some integers $l_1, \ldots, l_d$; since $B \subseteq d \cdot B_d$, we have $|x| \leq d$. Applying Cramer's rule to solve for $l_1, \ldots, l_d$ and (3.20), we have

$$\begin{aligned} |l_j| &= \frac{|x \wedge w_1 \cdots w_{j-1} \wedge w_{j+1} \wedge w_d|}{|w_1 \wedge \cdots \wedge w_d|} \leq \frac{|x||w_1| \cdots |w_d|}{|w_j||w_1 \wedge \cdots \wedge w_d|} \\ &= \frac{|x| \operatorname{mes}(\mathbf{R}^d/\Gamma)}{|w_j|} \leq \frac{2d \cdot d!}{|w_j|}, \end{aligned}$$

which is certainly at most $d^{2d} L_j$. It follows that $x \in (-d^{2d} L, d^{2d} L) \cdot w$, which is what we wanted to prove. A more-or-less identical argument gives the inclusion $(d^{-2d} \cdot B) \cap \Gamma \subseteq (-L, L) \cdot w$. □

It would be of interest to see if the constant r^{2r} could be significantly improved here, for instance to $e^{O(r)}$ or even $r^{O(1)}$. Progress on this issue may well have applications to improvements for Freiman's theorem (see Chapter 5), which can be viewed as a variant of the above theorem in which the set $B \cap \Gamma$ is replaced by a more general set of small doubling.

Exercises

3.5.1 Prove (3.12).

3.5.2 Let α be an irrational number, and let I be any open interval in $\mathbf{R}$. Show that $\mathbf{Z} \cdot \alpha$ and $I + \mathbf{Z}$ have non-empty intersection. (In other words, the integer multiples of α are dense in $\mathbf{R}/\mathbf{Z}$.)

3.5.3 Let Γ be a lattice in $\mathbf{R}^d$, and let A be a convex body (possibly asymmetric). Show that $\sigma[A \cap \Gamma] \leq O(1)^d$.

3.5.4 Let $v_1, \ldots, v_d$ be any vectors in a lattice $\Gamma \subset \mathbf{R}^d$ of full rank. Show that $|v_1 \wedge \cdots \wedge v_d|$ is an integer multiple of the covolume $\operatorname{mes}(\mathbf{R}^d/\Gamma)$.

3.5.5 Let Γ be a lattice of full rank in $\mathbf{R}^d$, let B be a symmetric convex body, and let $v_1, \ldots, v_d$ be a directional basis with successive minima $\lambda_1 \leq \cdots \leq \lambda_d$. Let O be the open octahedron with vertices $\pm v_j/\lambda_j$. Show that $O \subseteq B \subseteq O(d)^d \cdot O$. Thus Minkowski's second theorem can be used to give a rather weak version of John's theorem.

3.5.6 Let Γ be a lattice of full rank in $\mathbf{R}^d$, let B be a symmetric convex body, and let $\lambda_1 \leq \cdots \leq \lambda_d$ be the successive minima of B. Establish the bounds

$$O(d)^{-O(d)} \prod_{1 \leq i \leq d} \max\left(1, \frac{1}{\lambda_i}\right) \leq |B \cap \Gamma| \leq O(d)^{O(d)} \prod_{1 \leq i \leq d} \max\left(1, \frac{1}{\lambda_i}\right). \tag{3.21}$$

3.5.7 Generalize Lemma 3.32 and Lemma 3.36 to the case when B is an asymmetric convex body.