

Lecture Notes on *Lattice Polytopes*

(preliminary version of December 7, 2012)

Winter 2012

Fall School on *Polyhedral Combinatorics*

TU Darmstadt

Christian Haase • Benjamin Nill • Andreas Paffenholz

Contents

1	Polytopes, Cones, and Lattices	1
1.1	Cones	2
1.2	Polytopes	6
1.3	Lattices	10
	Problems	18
2	An invitation to lattice polytopes	19
2.1	Lattice polytopes and unimodular equivalence	20
2.2	Lattice polygons	21
2.3	Volume of lattice polytopes	24
2.4	Problems	26
3	Ehrhart Theory	27
3.1	Motivation	27
3.1.1	Why do we count lattice points?	27
3.1.2	First Ehrhart polynomials	29
3.2	Triangulations and Half-open Decompositions	30
3.3	EHRHART'S THEOREM	33
3.3.1	Encoding Points in Cones: Generating Functions	33
3.3.2	Counting Lattice Points in Polytopes	37
3.3.3	Counting the Interior: Reciprocity	41
3.3.4	Ehrhart polynomials of lattice polygons	45
3.4	The Theorem of Brion	46
3.5	Computing the Ehrhart Polynomial: Barvinok's Algorithm	48
3.5.1	Basic Version of the Algorithm	49
3.5.2	A versatile tool: LLL	52
3.6	Problems	57
4	Geometry of Numbers	61
4.1	Minkowski's Theorems	61
4.2	Lattice packing and covering	64
4.3	The Flatness Theorem	67
4.4	Problems	68
5	Reflexive and Gorenstein polytopes	69
5.1	Reflexive polytopes	69
5.1.1	Dimension 2 and the number 12	71
5.1.2	Dimension 3 and the number 24	72
5.2	Gorenstein polytopes	74
5.3	The combinatorics of simplicial reflexive polytopes	77
5.3.1	The maximal number of vertices	77

5.3.2	The free sum construction	78
5.3.3	The addition property	78
5.3.4	Vertices between parallel facets	79
5.3.5	Special facets	80
5.4	Problems	81
6	Unimodular Triangulations	83
6.1	Regular Triangulations	83
6.2	Pulling Triangulations	84
6.3	Compressed Polytopes	84
6.4	Special Simplices in Gorenstein Polytopes	86
6.5	Dilations	88
6.5.1	Composite Volume	88
6.5.2	Prime Volume	89
6.6	Problems	90
	References	91
	Index	93
	Name Index	97

Polytopes, Cones, and Lattices

1

In this chapter we want to introduce the basic objects that we will look at for the rest of the semester. We will start with *polyhedral cones*, which are the intersection of a finite set of linear half spaces. Generalizing to intersections of affine half spaces leads to *polyhedra*. We are mainly interested in the subset of bounded polyhedra, the *polytopes*. Specializing further, we will deal with *integral polytopes*. We will not prove all theorems in this chapter. For more on polytopes you may consult the book of Ziegler [28].

In the second part of this chapter we link integral polytopes to *lattices*, discrete subgroups of the additive group \mathbb{R}^d . This gives a connection to commutative algebra by interpreting a point $v \in \mathbb{Z}^d$ as the exponent vector of a monomial in d variables.

We use $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} to denote the integer, rational, real and complex numbers. We also use $\mathbb{Z}_{>}, \mathbb{Z}_{\geq}, \mathbb{Z}_{<}, \mathbb{Z}_{\leq}, \mathbb{R}_{<}, \mathbb{R}_{\leq}, \mathbb{R}_{>}, \mathbb{R}_{\geq}$.

1.0.1 Definition. Let $x_1, \dots, x_k \in \mathbb{R}^n$, and $\lambda_1, \dots, \lambda_k \in \mathbb{R}$. Then $\sum_{i=1}^k \lambda_i x_i$ is called a *linear combination* of the vectors x_1, \dots, x_k . It is further a

- (1) *conic combination*, if $\lambda_i \geq 0$,
- (2) *affine combination*, if $\sum_{i=1}^k \lambda_i = 1$, and a
- (3) *convex combination*, if it is conic and affine.

The *linear (conic, affine, convex) hull* of a set $X \subseteq \mathbb{R}^n$ is the set of all points that are a linear (conic, affine, convex) combination of some finite subset of X . It is denoted by $\text{lin}(X)$ (or, $\text{cone}(X)$, $\text{aff}(X)$, $\text{conv}(X)$, respectively). X is a *linear space* (*cone*, *affine space*, *convex set* if X equals its linear hull (or conic hull, affine hull, convex hull, respectively).

1.0.2 Definition (hyperplanes and half-spaces). For any non-zero $\alpha \in (\mathbb{R}^d)^*$ and $\delta \in \mathbb{R}$ the set

$$\begin{aligned} H_{\alpha,\delta} &:= \{x \mid \alpha(x) \leq 0\} && \text{is an affine hyperplane, and} \\ H_{\alpha} &:= \{x \mid \alpha(x) \leq \delta\} && \text{is a linear hyperplane.} \end{aligned}$$

The corresponding *positive and negative half-spaces* are

$$\begin{aligned} H_{\alpha,\delta}^+ &:= \{x \mid \alpha(x) \geq \delta\} && H_{\alpha,\delta}^- := \{x \mid \alpha(x) \leq \delta\} \\ H_{\alpha}^+ &:= \{x \mid \alpha(x) \geq 0\} && H_{\alpha}^- := \{x \mid \alpha(x) \leq 0\}. \end{aligned}$$

Then $H_{\alpha,\delta}^+ \cap H_{\alpha,\delta}^- = H_{\alpha,\delta}$. Let $H := H_{\alpha,b} \subseteq \mathbb{R}^d$ be a hyperplane. We say that a point $y \in \mathbb{R}^d$ is *beneath* H if $\alpha(y) < b$ and *beyond* H if $\alpha(y) > b$.

1.1 Cones

Cones are the basic objects for most of what we will study in these notes. In this section we will introduce two definitions of polyhedral cones. The WEYL-MINKOWSKI Theorem will tell us that these two definitions coincide. In the next section we will use this to study polytopes. Cones will reappear prominently when we start counting lattice points in polytopes. In the next chapter we will learn that counting in polytopes is best be done by studying either the cone over the polytope, or the vertex cones of the polytope.

1.1.1 Definition. A subset $C \subseteq \mathbb{R}^d$ is a *cone* if for all $x, y \in C$ and $\lambda, \mu \in \mathbb{R}_{\geq}$ also $\lambda x + \mu y \in C$. A cone C is *polyhedral (finitely constrained)* if there are $\alpha_1, \dots, \alpha_m \in (\mathbb{R}^d)^*$ such that

$$C = \bigcap_{i=1}^m H_{\alpha_i}^- = \{x \in \mathbb{R}^n \mid \alpha_i(x) \leq 0 \text{ for } 1 \leq i \leq m\}. \quad (1.1.1)$$

A cone C is called *finitely generated* by vectors $v_1, \dots, v_r \in \mathbb{R}^n$ if

$$C = \text{cone}(v_1, \dots, v_n) := \left\{ \sum_{i=1}^n \lambda_i v_i \mid \lambda_i \geq 0 \text{ for } 1 \leq i \leq n \right\}. \quad (1.1.2)$$

Figure missing

Fig. 1.1

It is easy to check that any set of the form (1.1.1) or (1.1.2) indeed defines a cone.

1.1.2 Example. See Figure 1.1.

The two notions of a finitely generated and finitely constrained cone are in fact equivalent. This is the result of the WEYL-MINKOWSKI Duality for cones.

1.1.3 Theorem (WEYL-MINKOWSKI Duality for Cones). A cone is polyhedral if and only if it is finitely generated.

We have to defer the proof a little bit until we know more about cones.

1.1.4 Lemma. Let $C \subseteq \mathbb{R}^{d+1}$ be a polyhedral cone and $\pi : \mathbb{R}^{d+1} \rightarrow \mathbb{R}^d$ the projection onto the last d coordinates. Then also $\pi(C)$ is a polyhedral cone.

Proof. We use a technique called FOURIER-MOTZKIN Elimination for this. Let C be defined by

$$C = \{(x_0, x) \mid \lambda_i x_0 + \alpha_i(x) \leq 0 \text{ for } 1 \leq i \leq n\}$$

for some linear functionals $\alpha_i \in (\mathbb{R}^d)^*$ and $\lambda_i \in \mathbb{R}$, $1 \leq i \leq m$. Then

$$C' := \pi(C) = \{x \mid \exists x_0 \in \mathbb{R} : (x_0, x) \in C\}.$$

We can assume that there are $a, b \in \mathbb{Z}_{\geq}$ such that

$$\lambda_i = \begin{cases} = 0 & \text{for } 1 \leq i \leq a \\ > 0 & \text{for } a+1 \leq i \leq b \\ < 0 & \text{for } b+1 \leq i \leq m. \end{cases}$$

Define functionals $\beta_{ij} := \lambda_i \alpha_j - \lambda_j \alpha_i$ for $a < i \leq b < j \leq m$. Then

$$C' \subseteq D := \{x \mid \alpha_i(x) \leq 0, 1 \leq i \leq a, \beta_{ij}(x) \leq 0, a < i \leq b < j \leq m\}.$$

We want to show $D \subseteq C'$. Let $x \in D$. Then for any $x_0 \in \mathbb{R}$ and $1 \leq i \leq a$

$$\lambda_i x_0 + \alpha_i(x) \leq 0,$$

as $\lambda_i = 0$. Further, $\beta_{ij}(x) \leq 0$ implies

$$\frac{1}{\lambda_j} \alpha_j(x) \geq \frac{1}{\lambda_i} \alpha_i(x)$$

for all $a < i \leq b < j \leq m$. Hence, there is x_0 such that

$$\min_{a+1 \leq i \leq b} \left(\frac{1}{\lambda_j} \alpha_j(x) \right) \leq -x_0 \leq \max_{b+1 \leq j \leq m} \left(\frac{1}{\lambda_i} \alpha_i(x) \right).$$

This means

$$\begin{aligned} \lambda_i x_0 + \alpha_i(x) &\leq 0 && \text{for } a+1 \leq i \leq b \\ \lambda_j x_0 + \alpha_j(x) &\leq 0 && \text{for } b+1 \leq j \leq m. \end{aligned}$$

Hence, (x_0, x) in C , so $x \in C'$. □

This suffices to prove one direction of the WEYL-MINKOWSKI Theorem.

1.1.5 Theorem (WEYL's Theorem). *Let C be a finitely generated cone. Then C is polyhedral.*

Proof. Let $v_1, \dots, v_n \in \mathbb{R}^d$ be generators of C , i.e.

$$C := \left\{ \sum_{i=1}^n \lambda_i v_i \mid \lambda_i \geq 0 \text{ for } 1 \leq i \leq n \right\}.$$

Then

$$C = \left\{ x \in \mathbb{R}^d \mid \exists \lambda_1, \dots, \lambda_n \in \mathbb{R} : x - \sum_{i=1}^n \lambda_i v_i = 0, \lambda_1, \dots, \lambda_n \geq 0 \right\}.$$

The cone C is the projection onto the last d coordinates of the set

$$C' := \left\{ (\lambda, x) \mid x - \sum_{i=1}^n \lambda_i v_i = 0, \lambda_1, \dots, \lambda_n \geq 0 \right\}.$$

Figure missing

This is clearly a polyhedral cone. By Lemma 1.1.4 C is polyhedral. □

Fig. 1.2

1.1.6 Theorem (FARKAS Lemma). Let a cone C be generated by $v_1, \dots, v_n \in \mathbb{R}^d$. Then for $x \in \mathbb{R}^d$ exactly one of the following holds.

- (1) $x \in C$, or
- (2) there is $\alpha \in (\mathbb{R}^d)^*$ such that $\alpha(y) \leq 0$ for all $y \in C$ and $\alpha(x) > 0$.

The second option thus tells us that if $x \notin C$, then there is a hyperplane that separates x from the cone C .

Proof (of Theorem 1.1.6). We show first that not both conditions can hold at the same time. Assume that there is $\lambda_1, \dots, \lambda_n \geq 0$ such that $x = \sum_{i=1}^n \lambda_i v_i$ and α such that $\alpha(y) \leq 0$ for all $y \in C$, but $\alpha(x) > 0$. Then

$$0 < \alpha(x) = \alpha\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \alpha(v_i) \leq 0,$$

a contradiction.

By WEYL's Theorem 1.1.5, the cone C is polyhedral, i.e. there are linear functionals $\alpha_1, \dots, \alpha_m \in (\mathbb{R}^d)^*$ such that

$$C = \{y \mid \alpha_1(y) \leq 0, \dots, \alpha_m(y) \leq 0\}.$$

Now $x \notin C$ holds if and only if there $1 \leq j_0 \leq m$ such that $\alpha_{j_0}(x) > 0$. However, $v_1, \dots, v_n \in C$ implies, that for any $\lambda_1, \dots, \lambda_n$ and $1 \leq j \leq m$

$$\alpha_j\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \alpha_j(v_i) \leq 0.$$

Any $y \in C$ has a representation as $y = \sum_{i=1}^n \lambda_i v_i$ for some $\lambda_i \geq 0$, $1 \leq i \leq n$. Hence, $\alpha_{j_0}(y) \leq 0$ for all $y \in C$, and α is as desired. \square

Figure missing

Fig. 1.3

1.1.7 Definition (polar (dual)). Let $X \subseteq \mathbb{R}^d$. The *polar (dual)* of X is the set

$$X^* := \{\alpha \in (\mathbb{R}^d)^* \mid \alpha(x) \leq 0 \text{ for all } x \in X\} \subseteq (\mathbb{R}^d)^*.$$

See Figure 6.2 for an example of the dual of a cone. If $X = \text{cone}(v_1, \dots, v_n)$ is a finitely generated cone, then it is immediate from the definition of the dual cone that it suffices to check the condition $\alpha(x) \leq 0$ for the generators v_1, \dots, v_n of X . Using this we can rephrase the FARKAS Lemma.

1.1.8 Corollary (FARKAS Lemma II). Let $C \subseteq \mathbb{R}^d$ be a finitely generated cone and $x \in \mathbb{R}^d$. Then either $x \in C$ or there is $\alpha \in C^*$ such that $\alpha(v) \leq 0$ for all $v \in C$ and $\alpha(x) > 0$ but not both. \square

We want to examine descriptions of the dual of a polyhedral and a finitely generated cone.

1.1.9 Proposition. Let $C := \text{cone}(v_1, \dots, v_n)$ be a finitely generated cone. Then $C^* = \{\alpha \mid v_i(\alpha) = \alpha(v_i) \leq 0 \text{ for } 1 \leq i \leq n\}$. In particular, C^* is polyhedral.

Proof. Let $\alpha \in C^*$. By definition this means that $\alpha(x) \leq 0$ for any $x \in C$. Hence, $\alpha(v_i) \leq 0$ for $1 \leq i \leq n$.

If conversely α satisfies $\alpha(v_i) \leq 0$ for $1 \leq i \leq n$, then for any $\lambda_1, \dots, \lambda_n \geq 0$

$$\alpha\left(\sum_{i=1}^n \lambda_i v_i\right) = \sum_{i=1}^n \lambda_i \alpha(v_i) \leq 0,$$

hence $\alpha \in C^*$. \square

Clearly, we can repeat the process of dualization. We abbreviate $(X^*)^*$ by X^{**} . The notion of dualization suggests that repeating this process should bring us back to where we started. This is, however not, true in general. It is, if we have finitely generated cones, by the next lemma.

1.1.10 Lemma. *Let $C \subseteq \mathbb{R}^d$ be a finitely generated cone. Then $C^{**} = C$.*

Proof. Let $C := \text{cone}(v_1, \dots, v_n)$ for some $v_1, \dots, v_n \in \mathbb{R}^d$. Then $C^* = \{\alpha \in (\mathbb{R}^d)^* \mid \alpha(v_i) \leq 0 \text{ for } 1 \leq i \leq n\}$.

If $x \in C$, then $\alpha(x) \leq 0$ for all $\alpha \in C^*$. Hence, $x \in C^{**}$. Conversely, if $x \notin C$, then by FARKAS Lemma II (Corollary 1.1.8), we know that there is $\alpha \in C^*$ such that $\alpha(v_i) \leq 0$ for $1 \leq i \leq n$ and $\alpha(x) > 0$. Hence, $x \notin C^{**}$. \square

This immediately implies the following description of the dual of a polyhedral cone.

1.1.11 Corollary. *Let $C := \{x \mid \alpha_1(x) \leq 0, \dots, \alpha_m(x) \leq 0\}$ be a polyhedral cone. Then $C^* = \text{cone}(\alpha_1, \dots, \alpha_m)$.* \square

With this observation we can prove the converse direction of the WEYL-MINKOWSKI Theorem.

1.1.12 Theorem (MINKOWSKI's Theorem). *Let C be a polyhedral cone. Then C is non-empty and finitely generated.*

Proof. Let $C := \{x \mid \alpha_1(x) \leq 0, \dots, \alpha_m(x) \leq 0\}$. Then $\mathbf{0} \in C$, so C is not empty.

Let $D := \{\sum_{i=1}^m \lambda_i \alpha_i \mid \lambda_1, \dots, \lambda_m \geq 0\}$. Then $D \subseteq (\mathbb{R}^d)^*$ is a finitely generated cone, and $D^* = C$. By WEYL's Theorem (Theorem 1.1.5), D is also a polyhedral cone, so there are v_1, \dots, v_n such that $D = \{\beta \mid \beta(v_1) \leq 0, \dots, \beta(v_n) \leq 0\}$. But D is the polar dual of the finitely generated cone $E := \{\sum_{i=1}^n \mu_i v_i \mid \mu_1, \dots, \mu_n \geq 0\}$, i.e. $E^* = D$. Dualizing this again gives $E^{**} = D^*$. By Lemma 1.1.10 we have that $E^{**} = E$, so $C = D^* = E$. Hence, C is finitely generated. \square

This finally allows us to prove the WEYL-MINKOWSKI Duality for cones.

Proof (Proof of Theorem 1.1.3). This follows immediately from Theorem 1.1.5 and Theorem 1.1.12. \square

1.1.13 Definition (MINKOWSKI sum). The MINKOWSKI sum of two sets $X, Y \subseteq \mathbb{R}^d$ is the set

$$X + Y := \{x + y \mid x \in X, y \in Y\}.$$

1.1.14 Definition (lineality space). Let C be a polyhedral cone. The lineality space of C is

$$\text{lineal } C := \{y \mid x + \lambda y \in C \text{ for all } x \in C, \lambda \in \mathbb{R}\}.$$

C is pointed if $\text{lineal } C = \{\mathbf{0}\}$.

Let $C \subseteq \mathbb{R}^d$, $L := \text{lineal } C$ and W a complementary linear subspace to L in \mathbb{R}^d . Let D be the projection of C onto W . Then D is a cone and

$$C = L + D \quad \text{and} \quad \text{lineal } D = \{\mathbf{0}\}.$$

Hence, up to a MINKOWSKI sum with a linear space we can restrict our considerations to pointed polyhedra. We can characterize a pointed cone C also via the condition that there is $\alpha \in (\mathbb{R}^d)^*$ such that $\alpha(x) < 0$ for all $x \in C - \{\mathbf{0}\}$.

1.1.15 Proposition. Let $C = \{x \in \mathbb{R}^d \mid \alpha_1(x) \leq 0, \dots, \alpha_m(x) \leq 0\}$ be a cone. Then

$$\text{lineal } C = \{y \mid \alpha_i(y) = 0, 1 \leq i \leq m\}.$$

Proof. Let $L := \{y \mid \alpha_i(y) = 0, \text{ for } 1 \leq i \leq m\}$. Then $L \subseteq \text{lineal } C$. Suppose conversely that $y \in \text{lineal } C$, but $\alpha_i(y) \neq 0$ for some index i . Let $x \in C$. Then $0 \geq \alpha(x + \lambda y) = \alpha(x) + \lambda \alpha(y) > 0$ for sufficiently large λ . This is a contradiction, so $\alpha_i(y) = 0$. \square

1.2 Polytopes

In this section we introduce polytopes. We will study their properties by reducing to the case of cones and using the results from the previous section.

1.2.1 Definition (polytope). A *polytope* is the convex hull $\text{conv}(v_1, \dots, v_n)$ of a finite number of points in \mathbb{R}^d .

A cone is the special case of a polytope where all half spaces are linear. We will use the results for cones to prove similar characterizations for polytopes. We associate a cone with a polytope.

1.2.2 Definition (cone over a polytope). Let $P \subseteq \mathbb{R}^d$ be a polytope. The *cone over P* is the set

$$C_P := \{1\} \times P := \text{conv} \left(\begin{pmatrix} 1 \\ x \end{pmatrix} \mid x \in P \right).$$

We can recover the polytope P from its cone by intersecting with the hyperplane $H_0 := \{(x_0, x) \mid x_0 = 1\}$ (and projecting). By Theorem 1.1.3, we can write C_P as

$$C_P = \left\{ \begin{pmatrix} x_0 \\ x \end{pmatrix} \mid (-b|A) \begin{pmatrix} x_0 \\ x \end{pmatrix} \leq \mathbf{0} \right\}$$

for some $v_1, \dots, v_n, w_1, \dots, w_l \in \mathbb{R}^d$ (recall that we can scale generators of a cone with a positive factor). Intersecting with H_0 gives

$$P = \{x \mid Ax \leq b\}$$

so any polytope can be written as the intersection of a finite number of affine half spaces. This intersection defines a bounded subset of \mathbb{R}^d .

Conversely given a bounded intersection $P := \{x \mid Ax \leq b\}$ of a finite number of affine half-spaces, we can define the cone

$$C := \left\{ \begin{pmatrix} x_0 \\ x \end{pmatrix} \mid (-b|A) \begin{pmatrix} x_0 \\ x \end{pmatrix} \leq \mathbf{0} \right\}$$

The intersection with H_0 recovers the set P . By the MINKOWSKI-WEYL-Theorem there are finitely many vectors

$$\begin{pmatrix} v_0^{(1)} \\ v^{(1)} \end{pmatrix}, \dots, \begin{pmatrix} v_0^{(k)} \\ v^{(k)} \end{pmatrix}$$

that generate C . By construction we have $v_0^{(i)} \geq 0$ for all i . We claim that the $v_0^{(i)}$ are even positive. Otherwise, assume that $v_0^{(1)} = 0$. Then $\lambda \begin{pmatrix} v_0^{(1)} \\ v^{(1)} \end{pmatrix} \in C$ implies that

$$Av^{(1)}\lambda v \leq 0$$

for all $\lambda \geq 0$. Hence, P would be unbounded. So $v_0^{(i)} > 0$ for all i . After scaling each generator with a positive scalar we can assume that $v_0(i) = 1$, so that

$$\begin{aligned} C &= \text{conv} \left(\begin{pmatrix} 1 \\ v^{(1)} \end{pmatrix}, \dots, \begin{pmatrix} 1 \\ v^{(k)} \end{pmatrix} \right) \\ &= \left\{ \begin{pmatrix} \sum \lambda_i \\ \sum \lambda_i v^{(i)} \end{pmatrix} \mid \lambda_i \geq 0 \right\}. \end{aligned}$$

Intersecting with H_0 gives

$$P = \text{conv}(v^{(1)}, \dots, v^{(k)}).$$

This proves the following duality theorem for polytopes.

1.2.3 Theorem (WEYL-MINKOWSKI-DUALITY). *A bounded set $P \subseteq \mathbb{R}^d$ is a polytope if and only if it is the bounded intersection of a finite number of affine half spaces.* \square

By this theorem we have two equivalent descriptions of a polytope:

- (1) as the convex hull of a finite set of points in \mathbb{R}^d ,
- (2) as the bounded intersection of a finite set of affine half spaces.

The first is called the *interior* or \mathcal{V} -description, the second is the *exterior* or \mathcal{H} -description. Both are important in polytope theory, as some things are easy to describe in one and may be difficult to define in the other.

Although the proof of the WEYL-MINKOWSKI duality is constructive, it is not efficient. We used FOURIER-MOTZKIN elimination to project a polyhedral cone onto a lower dimensional cone. Examining this method more closely shows that in each step we may roughly square the number of necessary inequalities. This behaviour does indeed occur. For an example, we may consider the standard unit cube. Let $e_1, \dots, e_d \in \mathbb{R}^d$ be the standard unit vectors and $\delta_1, \dots, \delta_d \in (\mathbb{R}^d)^*$ the dual basis. Then

$$C_d := \bigcap_{i=1}^d (H_{-\delta_i, 0}^- \cap H_{\delta_i, 1}^-) = \text{conv} \left(\sum_{i=1}^d \lambda_i e_i \mid \lambda_i \in \{0, 1\}, 1 \leq i \leq d \right).$$

Both descriptions are irredundant, and we have $2d$ inequalities, but 2^d generators.

Let $P = \bigcap_{i \in I} H_i^- \subseteq \mathbb{R}^d$ be a polytope given by a hyperplane description. A half space H_i^- for some $i \in I$ is an *implied equality* if $P \subseteq H_i$. The set of all implied equalities of P is

$$\text{eq}(P) := \{j \in I \mid P \subseteq H_j\}.$$

Observe that this is a property of the specified hyperplane description, not of the polytope itself. The affine hull of P is given by the intersection of the implied equations,

$$\text{aff}(P) = \bigcap_{j \in \text{eq}(P)} H_j.$$

The *dimension* of P is the dimension of its affine hull,

$$\dim P := \dim \text{aff } P.$$

A polytope is *full dimensional* if $\dim P = d$. The hyperplane description is *irredundant* if no proper subset of the half spaces defines the same polytope, and *redundant* otherwise. Note that an irredundant representation need not be unique. You could e.g. think of a ray in \mathbb{R}^2 .

Let $P := \{x \mid \alpha_1(x) \leq b_1, \dots, \alpha_m(x) \leq b_m\}$ be a polytope. A point $x \in P$ is an *interior point* of P if

$$\alpha_i(x) = b_i \quad \text{for all } i \in \text{eq}(P) \quad \alpha_i(x) < b_i \quad \text{for all } i \notin \text{eq}(P).$$

Any polytope has an interior point.

1.2.4 Definition (valid and supporting hyperplanes). Let $X \subseteq \mathbb{R}^d$ and $\alpha \in (\mathbb{R}^d)^* - \{0\}$, $\delta \in \mathbb{R}$. The hyperplane $H_{\alpha, \delta}$ is a *valid hyperplane* of X if

$$X \subseteq H_{\alpha, \delta}^-.$$

$H_{\alpha, \delta}$ is *supporting* if in addition $H_{\alpha, \delta} \cap X \neq \emptyset$.

1.2.5 Definition (faces). Let P be a polytope. A face F of P is either P itself or the intersection of P with a valid linear hyperplane. If $F \neq P$ then F is a *proper face*.

For any face F we have

$$F \cap P = \text{lin } F \cap P.$$

1.2.6 Proposition. Let P be a polytope and F a face of P . Then F is a polytope. \square

The dimension of a face of a polytope P is its dimension as a polytope,

$$\dim F := \dim \text{aff } F.$$

1.2.7 Theorem. Let $P := \{x \mid \alpha_1(x) \leq b_1, \dots, \alpha_m(x) \leq b_m\}$ be a polytope. If F is a proper face of P , then $F = \{x \mid \alpha_i(x) = b_i \text{ for } i \in I\} \cap P$ for a subsystem $I \subseteq [m]$ of the inequalities of P .

Proof. Let F be defined by a hyperplane $H := H_{\alpha, b}$, i.e.

$$F = H \cap P \quad \text{and} \quad P \subseteq H^-.$$

We work with the homogenizations $\hat{P} := \text{homog } P$ and $\hat{F} := \text{homog } F$ of P and F . Let $\hat{\alpha}_i : \mathbb{R} \times \mathbb{R}^d \rightarrow \mathbb{R}$, $(x_0, x) \mapsto b_i x_0 + \alpha_i(x)$ for $1 \leq i \leq m$ and $\hat{\alpha} : \mathbb{R} \times \mathbb{R}^d \rightarrow \mathbb{R}$, $(x_0, x) \mapsto b x_0 + \alpha(x)$. Then

$$\hat{P} = \{(x_0, x) \mid \hat{\alpha}_i((x_0, x)) \leq 0, 1 \leq i \leq m\}$$

and

$$\hat{F} = \hat{P} \cap \{(x_0, x) \mid \hat{\alpha}((x_0, x)) = 0\}, \quad \hat{P} \subseteq \{(x_0, x) \mid \hat{\alpha}((x_0, x)) \leq 0\}.$$

Hence, it suffices to show that

$$\hat{F} = \{(x_0, x) \mid \hat{\alpha}_i((x_0, x)) = 0 \text{ for } i \in I\} \cap \hat{P}.$$

\hat{P} is a polyhedral cone, so $\hat{\alpha} \in (\hat{P})^*$, as $\hat{\alpha}((x_0, x)) \leq 0$ for all $(x_0, x) \in \hat{P}$.

By Corollary 1.1.11 we know that $(\hat{P})^*$ is finitely generated by $\hat{\alpha}_1, \dots, \hat{\alpha}_m$, so there are $\lambda_1, \dots, \lambda_m \geq 0$ such that $\hat{\alpha} = \sum_{i=1}^m \lambda_i \hat{\alpha}_i$. Let $I := \{i \in [m] \mid \lambda_i \neq 0\}$. Then $\hat{\alpha} = \sum_{i \in I} \lambda_i \hat{\alpha}_i$. Let $\hat{F}' := \{(x_0, x) \mid \hat{\alpha}_i((x_0, x)) = 0 \text{ for } i \in I\} \cap \hat{P}$. For any $(c_0, c) \in \hat{F}$ we have

$$0 = \hat{\alpha}((c_0, c)) = \sum_{i \in I} \lambda_i \hat{\alpha}_i((c_0, c)) \leq 0.$$

$\lambda_i > 0$ for $i \in I$ implies that any inequality $\hat{\alpha}_i((c_0, c))$ for $i \in I$ must vanish separately. Hence, $\hat{F} \subseteq \hat{F}'$.

Conversely, if $\hat{\alpha}_i((x_0, x)) = 0$ for all $i \in I$, then

$$\hat{\alpha}((x_0, x)) = \sum_{i \in I} \lambda_i \hat{\alpha}_i((x_0, x)) = 0,$$

so $\hat{F}' \subseteq \hat{F}$. □

1.2.8 Remark. The argument we have used in the proof is a variation of the complementary slackness theorem of linear programming.

1.2.9 Corollary. Let P be a polytope. Then P has only a finite number of faces. □

1.2.10 Definition (facet). Let $P \subseteq \mathbb{R}^d$ be a polytope. A proper face F is a facet of P if it has dimension $\dim P - 1$.

1.2.11 Theorem. Let $P := \{x \mid \alpha_1(x) \leq b_1, \dots, \alpha_m(x) \leq b_m\} \subseteq \mathbb{R}^d$ be full dimensional and $\alpha_1, \dots, \alpha_m$ irredundant.

Then F is a facet of P if and only if $F = \{x \mid \alpha_i(x) = b_i\} \cap C$ for some $1 \leq i \leq m$.

Proof. Let $x \in C$ be an interior point of C . Then $\alpha_i(x) < b_i$ for all $1 \leq i \leq m$, as P is full dimensional. Let $i \in [m]$ and $F := \{x \mid \alpha_i(x) = b_i\} \cap P$. By irredundancy, there is $z \in \mathbb{R}^d$ such that

$$\alpha_i(z) > b_i \quad \text{and} \quad \alpha_j(z) \leq b_j \quad \text{for all } j \neq i.$$

Hence, there is y on the segment between x and z such that

$$\alpha_i(y) = b_i \quad \text{and} \quad \alpha_j(y) < b_j \quad \text{for all } j \neq i.$$

So $\text{aff}(F) = \{x \mid \alpha_i(x) = b_i\}$, and $\dim F = d - 1$, so F is a facet.

If conversely F is a facet, then there is $I \subseteq [m]$ such that $F = \{x \mid \alpha_i(x) = b_i \text{ for all } i \in I\} \cap P$. If $|I| \geq 1$, then F is as required. If $|I| \geq 2$, then let J be a non-empty proper subset of I and $G = \{x \mid \alpha_j(x) = 0 \text{ for all } j \in J\}$. By irredundancy, $F \subsetneq G$, so $\dim F < \dim G < \dim P$, and F would not be a facet. □

1.2.12 Corollary. Let $P := \{x \mid \alpha_1(x) \leq b_1, \dots, \alpha_m(x) \leq b_m\} \subseteq \mathbb{R}^d$ be a polytope.

(1) If P is full dimensional, then $\alpha_1, \dots, \alpha_m$ are unique up to scaling with a positive factor.

(2) Any proper face of P is contained in a facet.

(3) If F_1, F_2 are proper faces, then $F_1 \cap F_2$ is a proper face of P . □

1.2.13 Definition (minimal face). Let P be a polytope. A face F of P is minimal if there is no non-empty proper face G of P with $G \subsetneq F$.

1.2.14 Proposition. Let P be a polytope and F a face of P .

(1) F is minimal if and only if $F = \text{aff } F$.

(2) F is minimal if and only if it is a translate of $\text{lineal } P$.

Proof: proof missing

1.2.15 Definition (vertices of a polytope). The minimal faces of a pointed polytope are called *vertices*. They are points in \mathbb{R}^d . The set of all vertices is denoted by $\mathcal{V}(P)$.

1.2.16 Corollary. Let C be a polyhedral cone. Then $\text{lineal } C$ is the unique minimal face of C .

1.2.17 Proposition. Let $P = \cap_{i=1}^m H_i^-$ be a polytope and $d_0 := \dim \text{lineal } P$. If F is a face of dimension $d_0 + 1$, then there are $I, J \subseteq [m]$, $|I| \leq 2$ such that

$$F = \bigcup_{i \in I} H_i^- \cap \bigcup_{j \in J} H_j^-.$$

In particular, F has at most two facets, which are minimal faces of P , so

$$F = e + \text{lineal } P$$

for a segment or ray $e \subseteq \mathbb{R}^d$.

If P is pointed, then F is an *edge* of P , if e is a segment, and a *extremal ray* otherwise. If P is a cone, then F is called a *minimal proper face*. Two minimal face of P are *adjacent* if they are contained in the same face of dimension $d_0 + 1$.

Proof (Proof of Proposition 1.2.17). proof missing

1.2.18 Theorem. Let $P = \bigcup_{i=1}^m H_i^-$ and $L := \text{lineal } P$. Let

(1) F_1, \dots, F_n be the minimal faces of P , and

(2) G_1, \dots, G_l the minimal proper faces of $\text{rec } P$.

Choose

$$v_i \in F_i \quad \text{and} \quad w_j \in G_j - L \quad \text{for} \quad 1 \leq i \leq n, 1 \leq j \leq l$$

and a basis b_1, \dots, b_k of L . Then

$$P = \text{conv}(v_1, \dots, v_n) + \text{cone}(w_1, \dots, w_l) + \text{lin}(b_1, \dots, b_k).$$

Proof: proof missing

1.2.19 Definition (f -vector, face vector). Let P be a polytope. The f -vector (or face vector) of P is the vector

$$f(P) := (f_{-1}(P), f_0(P), \dots, f_{d-1}(P)),$$

where $f_i(P)$ is the number of i -dimensional faces of P , for $-1 \leq i \leq d-1$.

1.3 Lattices

Now we introduce the central tool for this book. It will link our geometric objects, the polytopes, to algebraic objects, namely toric ideals and toric varieties.

Throughout this section, V will be a finite-dimensional real vector space equipped with the topology induced by a norm $\|\cdot\|$ and with a translation invariant volume form.

Lattices can be defined in two different (but equivalent) ways: as the integral generation of a linearly independent set of vectors, or as a discrete abelian subgroup of the vector space. We will start with the latter characterization of a lattice as it is often very useful to describe lattices without the explicit choice of a basis. We will deduce the other representation in the next paragraphs.

A subset $\Lambda \subseteq \mathbb{R}^d$ is an *additive subgroup* of \mathbb{R}^d if for any $x, y \in \Lambda$

- (1) $\mathbf{0} \in \Lambda$
- (2) $x + y \in \Lambda$ for any $x, y \in \Lambda$
- (3) $-x \in \Lambda$ for any $x \in \Lambda$.

1.3.1 Definition (lattice). A lattice Λ in V is a discrete additive subgroup Λ of V : for all $x \in \Lambda$ there is $\varepsilon > 0$ such that $\mathcal{B}_\varepsilon(x) \cap \Lambda = \{x\}$.

The rank of Λ is the dimension of its linear span $\text{rank } \Lambda := \dim \text{lin } \Lambda$.

1.3.2 Example. (1) The *standard integer lattice* is the lattice spanned by the d standard unit vectors e_1, \dots, e_d . It is commonly denoted by \mathbb{Z}^d . We will later see that essentially any lattice looks like this integer lattice.

(2) root systems

(3) Subgroups of lattices are lattices. In particular, $\{x \in \mathbb{Z}^2 \mid x_1 + x_2 \equiv 0 \pmod{3}\}$ is a lattice.

1.3.3 Lemma. Let $\mathcal{B} = \{b_1, \dots, b_d\} \subseteq V$ be linearly independent. Then the subgroup

$$\Lambda(\mathcal{B}) := \left\{ \sum_{i=1}^d \lambda_i b_i \mid \lambda_i \in \mathbb{Z}, 1 \leq i \leq d \right\}$$

generated by \mathcal{B} is a lattice.

Proof. The linear map $\mathbb{R}^d \rightarrow \text{lin } \mathcal{B}$ given by $\lambda \mapsto \sum_{i=1}^d \lambda_i b_i$ is bijective, and hence a homeomorphism. It maps the discrete set $\mathbb{Z}^d \subseteq \mathbb{R}^d$ onto $\Lambda(\mathcal{B})$.

Let $z \in \mathbb{R}^d \cap \Pi(b_1, \dots, b_d)$ be an interior point of $\Pi(b_1, \dots, b_d)$. Then there is $\varepsilon > 0$ such that $\mathcal{B}_\varepsilon(z) \subseteq \Pi(b_1, \dots, b_d)$. We claim that $\mathcal{B}_\varepsilon(x) \cap \Lambda = \{x\}$ for all $x \in \Lambda$. Indeed, if $y \in \mathcal{B}_\varepsilon(x) \cap \Lambda = \{x\}$ and $y \neq x$, Then $x' := x - y \in \Lambda$ and $x' + z \in \Pi(b_1, \dots, b_d)$, a contradiction to Proposition 1.3.10. \square

1.3.4 Definition (lattice basis). A linearly independent subset $\mathcal{B} \subseteq V$ is called a lattice basis (or Λ -basis) if it generates the lattice: $\Lambda = \Lambda(\mathcal{B})$.

1.3.5 Example. $\left\{ \begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$ is a basis of the lattice in Example 1.3.2(3).

1.3.6 Definition (dual lattice). Let $\Lambda \subseteq V$ be a lattice with $\text{lin } \Lambda = V$. Then set

$$\Lambda^* := \{\alpha \in V^* \mid \alpha(a) \in \mathbb{Z} \text{ for all } a \in \Lambda\}$$

is the *dual lattice* to Λ .

1.3.7 Lemma. If b_1, \dots, b_d is a basis of Λ and $\alpha_1, \dots, \alpha_d$ is the corresponding dual basis (i.e. $\alpha_i(b_j) = 1$ if $i = j$, and $\alpha_i(b_j) = 0$ otherwise), then Λ^* is spanned by $\alpha_1, \dots, \alpha_d$ as a lattice. Hence, the dual lattice is indeed a lattice. Further, dualizing twice gives us back the original lattice, $\Lambda^{**} = \Lambda$, as b_1, \dots, b_d is a dual basis to $\alpha_1, \dots, \alpha_d$.

1.3.8 Theorem. Every lattice has a basis.

For the proof we need some prerequisites.

1.3.9 Definition (parallelepiped). For a finite subset $\mathcal{A} = \{v_1, \dots, v_k\} \subseteq \mathbb{R}^d$ the half-open zonotope $\Pi(\mathcal{A})$ spanned by these vectors is the set

$$\Pi(\mathcal{A}) := \left\{ \sum_{i=1}^k \lambda_i v_i \mid 0 \leq \lambda_i < 1 \text{ for } 1 \leq i \leq k \right\}.$$

If \mathcal{A} is linearly independent, the zonotope is a *parallelepiped*.

Figure missing

Fig. 1.4: A parallelepiped spanned by some vectors

See Figure 1.4 for an example.

1.3.10 Proposition. Let Λ be a lattice in V with basis $\mathcal{B} = \{b_1, \dots, b_d\}$. Then any point $x \in \text{lin } \Lambda$ has a unique representation $x = a + y$ for $a \in \Lambda$ and $y \in \Pi(\mathcal{B})$.

Proof. There are unique $\lambda_1, \dots, \lambda_d \in \mathbb{R}$ such that $x = \sum_{i=1}^d \lambda_i b_i$. Set $a := \sum_{i=1}^d \lfloor \lambda_i \rfloor b_i$ and $y := \sum_{i=1}^d \{\lambda_i\} b_i$. Then $y \in \Pi(\mathcal{B})$, $a \in \Lambda$, and $x = a + y$.

Now assume that there is a second decomposition $x = a' + y'$ with $a \neq a'$ (and thus also $y \neq y'$). We can write y and y' as

$$y = \sum_{i=1}^d \alpha_i b_i \quad y' = \sum_{i=1}^d \alpha'_i b_i$$

for some $0 \leq \alpha_i, \alpha'_i < 1$, $1 \leq i \leq d$. Hence, $|\alpha_i - \alpha'_i| < 1$. From

$$a' - a = y - y' = \sum_{i=1}^d (\alpha_i - \alpha'_i) b_i$$

and $a' - a \in \Lambda$ we know that $\alpha_i - \alpha'_i \in \mathbb{Z}$ for $1 \leq i \leq d$. Hence, $\alpha_i - \alpha'_i = 0$, so $y = y'$. Hence, also $a = a'$. \square

1.3.11 Corollary. Let Λ be a lattice in \mathbb{R}^d with basis $\mathcal{B} := \{b_1, \dots, b_d\}$ and fundamental parallelepiped $\Pi := \Pi(b_1, \dots, b_d)$. Then \mathbb{R}^d is the disjoint union of all translates of Π by vectors in Λ . \square

1.3.12 Lemma. If $K \subseteq V$ is bounded, then $K \cap \Lambda$ is finite.

1.3.13 Definition (Λ -rational subspace). A subspace $U \subseteq V$ is Λ -rational if it is generated by elements of Λ .

1.3.14 Proposition. Let V be a finite-dimensional real vector space, let $\Lambda \subseteq V$ be a lattice, and let $U \subseteq V$ be a Λ -rational subspace. Denote the quotient map $\pi: V \rightarrow V/U$.

- (1) Then $\pi(\Lambda) \subseteq V/U$ is a lattice.
- (2) Furthermore, if $\Lambda \cap U$ has a basis b_1, \dots, b_r , and $\pi(\Lambda)$ has a basis c_1, \dots, c_s , then any choice of preimages $\hat{c}_i \in \Lambda$ of the c_i for $1 \leq i \leq s$ yields a Λ -basis $b_1, \dots, b_r, \hat{c}_1, \dots, \hat{c}_s$.

In the situation of the proposition, we will often write Λ/U for $\pi(\Lambda)$.

Proof. (1) As the image of a group under a homomorphism, $\pi(\Lambda)$ is a subgroup of V/U .

The hard part of the proposition is to prove that $\pi(\Lambda)$ is discrete in V/U . Because U is Λ -rational, we can choose a vector space basis $\{v_1, \dots, v_r\} \subseteq \Lambda \cap U$ of U . Extend it to a vector space basis $\mathcal{B} = \{v_1, \dots, v_d\} \subseteq \Lambda$ of $\text{lin } \Lambda$. These bases yield maximum norms

$$\left\| \sum_{i=1}^d \lambda_i v_i \right\| := \max\{|\lambda_i| : i = 1, \dots, d\}$$

on $\text{lin } \Lambda$ and

$$\left\| \left(\sum_{i=1}^d \lambda_i v_i \right) + U \right\| := \max\{|\lambda_i| : i = r+1, \dots, d\}$$

on $\text{lin } \Lambda/U$. Denote the unit ball of $\text{lin } \Lambda$ by W . By Lemma 1.3.12, the set $W \cap \Lambda$ is finite. Set

$$\varepsilon := \min(\{1\} \cup \{\|v + U\|' : v \in W \cap \Lambda \setminus U\}).$$

This minimum over a finite set of positive numbers is positive. Now suppose $v = \sum_{i=1}^d \lambda_i v_i \in \Lambda$ with $\|v + U\|' < \varepsilon$. Then $v' := \sum_{i=1}^r (\lambda_i - \lfloor \lambda_i \rfloor) v_i + \sum_{i=r+1}^d \lambda_i v_i \in \Lambda$ represents the same coset: $v + U = v' + U$, and $v' \in W \cap \Lambda$. We conclude $v' \in U$ and thus $v' + U = \mathbf{0} \in V/U$.

(2) Let $b_1, \dots, b_r, \hat{c}_1, \dots, \hat{c}_s$ be as in the proposition, and let $v \in \Lambda$. Because the c_j form a lattice basis of $\pi(\Lambda)$, there are integers $\lambda_1, \dots, \lambda_s$ so that $\pi(v) = \sum_{j=1}^s \lambda_j c_j$. Thus, $v - \sum_{j=1}^s \lambda_j \hat{c}_j \in \ker \pi = U$. Because the b_i form a lattice basis of $\Lambda \cap U$, there are integers μ_1, \dots, μ_r so that $v - \sum_{j=1}^s \lambda_j \hat{c}_j = \sum_{i=1}^r \mu_i b_i$. So $b_1, \dots, b_r, \hat{c}_1, \dots, \hat{c}_s$ generate Λ . They must be linearly independent for dimension reasons. \square

1.3.15 Definition (primitive vector). A non-zero lattice vector $v \in \Lambda$ is primitive if it is not a positive multiple of another lattice vector: $\text{conv}(\mathbf{0}, v) \cap \Lambda = \{\mathbf{0}, v\}$.

Proof (Theorem 1.3.8). We proceed by induction on $r := \text{rank } \Lambda$. For $r = 0$, the empty set is a basis for Λ . For $r = 1$, a primitive vector yields a basis.

Assume $r \geq 2$. Let $b \in \Lambda$ be primitive, and set $U := \text{lin } b$. Then $\{b\}$ is a basis for $U \cap \Lambda$, and Λ/U is a lattice by the first statement of Proposition 1.3.14. Because $\text{rank } \Lambda/U = r - 1$, it has a basis by induction. By the second statement of Proposition 1.3.14, we can lift to a basis of Λ .

Proof. We have to show that there are $b_1, \dots, b_d \in \mathbb{R}^d$ that span Λ as a lattice.

Clearly, as Λ spans \mathbb{R}^d , we can find d linearly independent vectors w_1, \dots, w_d in Λ . We construct a basis of Λ from these vectors. Let $V_0 := \{\mathbf{0}\}$ and

$$V_k := \text{lin}(w_1, \dots, w_k).$$

We use induction over k to construct a basis of the lattice $\Lambda \cap V_k$. For $k = 1$ let $v_1 \in (\Lambda - \{\mathbf{0}\}) \cap V_1$ be such that $\|v_1\|$ is minimal. Such a point exists by Lemma 1.3.16. Any other lattice point $a \in (\Lambda - \{\mathbf{0}\}) \cap V_1$ can then be written as

$$a = \lambda v_1$$

for some $\lambda \in \mathbb{R}$. If $\lambda \notin \mathbb{Z}$, then $0 < \{\lambda\} < 1$ and

$$\{\lambda\} v_1 = a - \lfloor \lambda \rfloor v_1 \in (\Lambda - \{\mathbf{0}\}) \cap V_1.$$

but $\|\{\lambda\} v_1\| = \{\lambda\} \|v_1\| < \|v_1\|$ contradicting our choice of v_1 . Hence $\lambda \in \mathbb{Z}$ and v_1 is a basis of $\Lambda \cap V_1$.

Now let $k \geq 2$. We already have a basis v_1, \dots, v_{k-1} of the lattice $\Lambda \cap V_{k-1}$. Let $v_k \in (\Lambda \cap V_k) - V_{k-1}$ be with minimal distance to V_{k-1} (by Lemma 1.3.16). Then v_k can be written as

$$v_k = \sum_{i=1}^k \lambda_i v_i$$

for some $\lambda_i \in \mathbb{R}$. Let $v \in \Lambda \cap V_k$ be some other lattice point. This also has a representation

$$v_k = \sum_{i=1}^k \mu_i v_i.$$

for $\mu_i \in \mathbb{R}$. If $\alpha := \mu_k / \lambda_k$ is not an integer, then $0 < \{\alpha\} < 1$ and

$$v'_k := v - \lfloor \alpha \rfloor v_k = v - \alpha v_k + \{\alpha\} v_k = \{\alpha\} \lambda_k w_k + \sum_{i=1}^{k-1} (\mu_i - \lfloor \alpha \rfloor \lambda_i) w_i$$

is a lattice point in $(\Lambda \cap V_k) - V_{k-1}$. However, for any point $x = \sum_{i=1}^k \eta_i w_i$ we have

$$d(x, V_{k-1}) = |\eta_k| d(w_k, V_{k-1}),$$

so v'_k is closer to V_{k-1} than v_k . A contradiction, so α is integral, and v_1, \dots, v_k spans the lattice $\Lambda \cap V_k$. \square

Recall the *distance function* in \mathbb{R}^d ,

$$d(x, y) := \|x - y\|$$

and

$$d(x, S) := \inf_{z \in S} d(x, z)$$

for any $x, y \in \mathbb{R}^d$, $S \subseteq \mathbb{R}^d$.

1.3.16 Lemma. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $v_1, \dots, v_k \in \Lambda$, $k < d$, linearly independent. Define $V := \text{lin}(v_1, \dots, v_k)$.

Then there is $v \in \Lambda - V$ and $x \in V$ such that

$$d(v, x) \leq d(w, y) \quad \text{for any } y \in V, w \in \Lambda - V.$$

Proof. Let $\Pi := \Pi(v_1, \dots, v_k)$. Then Π is a compact subset of \mathbb{R}^d . Choose any $a \in \Lambda - V$ and set $r := d(a, \Pi)$. Let

$$B_r(\Pi) := \{x \mid d(x, \Pi) \leq r\}.$$

Then $a \in (B_r(\Pi) - V) \cap \Lambda$, and $B_r(\Pi)$ is bounded, so $B_r(\Pi) \cap \Lambda$ is finite by Problem 1.2. Hence, we can choose some $v \in (B_r(\Pi) - V) \cap \Lambda$ that minimizes $d(v, \Pi)$. Choose some $x \in \Pi$ such that $d(v, x)$ attains this minimal distance. We will show that these choices satisfy the requirements of the proposition.

Let $w \in \Lambda - V$ and $y \in V$. By definition of V there are coefficients $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ such that

$$y = \sum_{i=1}^k \lambda_i v_i. \quad \text{Set} \quad z := \sum_{i=1}^k \lfloor \lambda_i \rfloor v_i, \quad z' := \sum_{i=1}^k \{\lambda_i\} v_i,$$

Then $z, w - z \in \Lambda$ and $z' = y - z \in \Pi$. Further, $w - z \notin V$. Hence,

$$\begin{aligned} d(y, w) &= d(y - z, w - z) \\ &\geq d(w - z, \Pi) \geq d(v, \Pi) = d(v, x). \end{aligned} \quad \square$$

1.3.17 Definition (unimodular transformation). Let Λ and Λ' be lattices. A linear map $T: \text{lin } \Lambda \rightarrow \text{lin } \Lambda'$ which induces a bijection $\Lambda \rightarrow \Lambda'$ is called *unimodular* or a *lattice transformation*.

1.3.18 Lemma. Let \mathcal{B} and \mathcal{B}' be bases of the lattices Λ and Λ' respectively. Then a linear map $T: \text{lin } \Lambda \rightarrow \text{lin } \Lambda'$ is unimodular if and only if the matrix representation A of T with respect to the bases \mathcal{B} and \mathcal{B}' is integral and satisfies $|\det A| = 1$.

Proof. The matrix A has only integral entries if and only if $T(\Lambda) \subseteq \Lambda'$.

Similarly, if T is unimodular, then the inverse transformation exists, and its matrix A^{-1} also has integral entries. Thus, $\det A$ and $\det A^{-1}$ are integers with product 1.

Conversely, if A is integral with $|\det A| = 1$, then, by CRAMER's rule A^{-1} exists and is integral. \square

1.3.19 Lemma. Let $A \in \mathbb{Z}^{d \times d}$ be non-singular. Then $A\lambda = \mu$ has an integral solution λ for any integral $\mu \in \mathbb{Z}^d$ if and only if $|\det A| = 1$.

Proof. “ \Rightarrow ”: By CRAMER's rule, the entries of λ are $\lambda_i = \pm \det(A_i)$, where A_i is the matrix obtained from A by replacing the i -th column with μ .

“ \Leftarrow ”: If $|\det A| > 1$, then $0 < |\det A^{-1}| < 1$, so A^{-1} contains a non-integer entry a_{ij} . If $e_j \in \mathbb{Z}^m$ is the j -th unit vector, then $A\lambda = e_j$ has no integer solution. \square

1.3.20 Corollary. An integral matrix $A \in \mathbb{Z}^{d \times d}$ is the matrix representation of a unimodular transformation of a lattice if and only if $|\det A| = 1$. \square

1.3.21 Corollary. Let Λ be a lattice with basis $b_1, \dots, b_d \in \text{lin } \Lambda$. Then $c_1, \dots, c_d \in \Lambda$ is another basis of Λ if and only if there is a unimodular transformation $T: \text{lin } \Lambda \rightarrow \text{lin } \Lambda$ such that $T(b_i) = c_i$ for $1 \leq i \leq d$. \square

We are now ready to define an important invariant of a lattice.

1.3.22 Definition (Determinant of a lattice). Let $\Lambda' \subseteq \Lambda$ be lattices with $\text{lin } \Lambda = \text{lin } \Lambda'$, and let \mathcal{B} and \mathcal{B}' be bases of Λ and Λ' respectively. Let A be the matrix representation of the identity $\text{lin } \Lambda' \rightarrow \text{lin } \Lambda$ with respect to the bases \mathcal{B}' and \mathcal{B} . Then the *determinant* of Λ' in Λ is the integer

$$\det_{\Lambda} \Lambda' := |\det A|.$$

If $\Lambda = \mathbb{Z}^d$, we will often write $\det \Lambda'$ for $\det_{\mathbb{Z}^d} \Lambda'$.

By Lemma 1.3.18 and Corollary 1.3.21 this definition is independent of the chosen bases.

1.3.23 Definition (sublattice and index). Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice. Any lattice $\Gamma \subseteq \Lambda$ is a *sublattice* of Λ .

Sets of the form $a + \Gamma := \{a + x \mid x \in \Gamma\}$ for some $a \in \Lambda$ are *cosets* of Γ in Λ . The set of all cosets is Λ/Γ . The size $|\Lambda/\Gamma|$ is the *index* of Γ in Λ .

Next we study a way to obtain a “nice” basis for a lattice generated by a set of (not necessarily linearly independent) vectors in \mathbb{Z}^d .

1.3.24 Definition (HERMITE normal form). Let $A = (a_{ij}) \in \mathbb{Z}^{m \times d}$ with $m \geq d$. A is in *HERMITE normal form* if

- ▷ $a_{ij} = 0$ for $j < i$ and
- ▷ $a_{ii} > a_{ij} \geq 0$ for $i > j$.

So a matrix in HERMITE normal form is an upper triangular matrix, and the largest entry in each column is on the diagonal. We remark that, depending on the context, sometimes we use the *transposed* matrix, i.e. we claim that a matrix is in HERMITE normal form if it has at least as many columns as rows, it is lower triangular, and the largest entry in each row is on the diagonal (and if the matrix is square we can also consider *upper* triangular matrices).

1.3.25 Theorem (HERMITE normal form). *Let $A \in \mathbb{Z}^{m \times d}$. Then there is $U \in \mathbb{Z}^{d \times d}$ such that AU is in HERMITE normal form.*

Proof. proof missing

1.3.26 Theorem. *Let $\Lambda' \subseteq \Lambda$ be lattices with $\text{lin } \Lambda = \text{lin } \Lambda'$. Then there is a basis b_1, \dots, b_r of Λ and integers $k_1, \dots, k_r \in \mathbb{Z}_{>}$ with $\lambda_i | \lambda_{i+1}$ for $1 \leq i \leq d-1$ such that $k_1 b_1, \dots, k_r b_r$ is a basis of Λ' .*

Proof. We proceed by induction on $r := \text{rank } \Lambda = \text{rank } \Lambda'$. For $r = 1$, a Λ -primitive vector has a positive integral multiple which is Λ' -primitive.

Assume $r \geq 2$. Because $\text{lin } \Lambda = \text{lin } \Lambda'$, for every $v \in \Lambda$ there is a positive integer k so that $kv \in \Lambda'$. Choose $b_r \in \Lambda$ and $k_r \in \mathbb{Z}_{>}$ so that b_r is Λ -primitive, and so that k_r is minimal.

Set $U := \text{lin } b_r$. Then b_r is a basis for $U \cap \Lambda$, and $k_r b_r$ is a basis for $U \cap \Lambda'$. By Proposition 1.3.14, $\Lambda'/U \subseteq \Lambda/U$ are lattices of rank $r-1$. By induction, there is a basis b_1, \dots, b_{r-1} of Λ/U together with positive integers k_1, \dots, k_{r-1} so that $k_1 b_1, \dots, k_{r-1} b_{r-1}$ is a basis for Λ'/U .

Let $\hat{b}_i \in \Lambda$ be representatives of the b_i for $i = 1, \dots, r-1$. Then there are representatives $c_i \in \Lambda'$ of the $k_i b_i$. By Proposition 1.3.14, b_1, \dots, b_r is a basis for Λ , and $c_1, \dots, c_{r-1}, k_r b_r$ is a basis for Λ' . By adding a suitable multiple of $k_r b_r \in \Lambda'$ to the c_i , we may assume that $c_i = k_i \hat{b}_i + l_i b_r$ for $0 \leq l_i < k_r$ and for all $i = 1, \dots, r-1$.

But then, c_i is a positive integral multiple of some Λ -primitive vector: $c_i = m_i a_i$. The two expressions for c_i together imply $l_i = 0$ or $m_i \leq l_i < k_r$ in contradiction to the minimality of k_r .

Altogether, we obtain $l_i = 0$ for all i , and hence, $c_i = k_i \hat{b}_i$ as required. \square

1.3.27 Corollary. *Let $\Lambda' \subseteq \Lambda$ be lattices with $\text{lin } \Lambda = \text{lin } \Lambda'$, and let \mathcal{B}' be a basis of Λ' . Then*

$$|\Lambda/\Lambda'| = |\Pi(\mathcal{B}') \cap \Lambda| = \det_{\Lambda} \Lambda'.$$

Proof. The quotient map $\pi: \Lambda \rightarrow \Lambda/\Lambda'$ induces a bijection $\Pi(\mathcal{B}') \cap \Lambda \rightarrow \Lambda/\Lambda'$ by Proposition 1.3.10. So the first two quantities are equal, and in particular the second one is independent of the chosen Λ' -basis.

That means, for the proof that the last two quantities agree, we can choose bases as in Theorem 1.3.26. Then the change of bases matrix is diagonal with determinant $k_1 \dots k_r$, while the set $\Pi(\mathcal{B}') \cap \Lambda$ consists of the points $\sum_i l_i b_i$ for $0 \leq l_i \leq k_i - 1$. \square

In dimensions $d \geq 2$ there are infinitely many unimodular matrices. Hence, there are also infinitely many different bases of a lattice. In Section 3.5.2 we deal with the problem of finding bases of a lattice with some nice properties. We will e.g. construct bases with “short” vectors.

Let $v_1, \dots, v_n \in \Lambda$. Then $C := \text{cone}(v_1, \dots, v_n)$ is a polyhedral cone. Let $S_C := C \cap \Lambda$. Then S_C with addition is a semi-group, the *semi-group of lattice points in C* .

Indeed, $\mathbf{0} \in S_C$ and if $x, y \in S_C$, then $x + y \in S_C$. A set $\mathcal{H} \subseteq S_C$ generates S_C as a semigroup if for any $x \in S_C$ there are $\lambda_h \in \mathbb{Z}_{\geq}$ for $h \in \mathcal{H}$ such that

$$x = \sum_{h \in \mathcal{H}} \lambda_h h.$$

Such a set is a **HILBERT basis** of S_C . A **HILBERT basis** is *minimal* if any other **HILBERT basis** of S_C contains this basis.

Observe that in general an inclusion-minimal **HILBERT basis** is not unique. Consider e.g. the cone $C = \mathbb{R}^2$. Then both $\mathcal{H}_1 := \{e_1, e_2, -(e_1 + e_2)\}$ and $\mathcal{H}_2 := \{\pm e_1, \pm e_2\}$ are minimal **HILBERT bases**, but they differ even in size.

A vector $a \in \mathbb{Z}^d$ is *primitive* if $\gcd(a_1, \dots, a_d) = 1$.

1.3.28 Theorem. Let $v_1, \dots, v_n \in \Lambda$, $C := \text{cone}(v_1, \dots, v_n)$, and $S := C \cap \mathbb{Z}^d$ the semi-group of lattice points in C . Then S_C has a **HILBERT basis**.

If C is pointed, then S_C has a unique minimal **HILBERT basis**.

Proof. Define the parallelepiped

$$\Pi := \left\{ \sum_{i=1}^k \lambda_i y_i \mid 0 \leq \lambda_i \leq 1, 1 \leq i \leq k \right\}.$$

Let $\mathcal{H} := \Pi \cap \Lambda$. We will prove that \mathcal{H} is a **HILBERT basis**.

- (1) \mathcal{H} generates C , as $y_1, \dots, y_k \in \mathcal{H}$.
- (2) Let $x \in C \cap \Lambda$ be any lattice vector in C . Then there are $\eta_1, \dots, \eta_k \geq 0$ such that $x = \sum_{i=1}^k \eta_i y_i$. We can rewrite this as

$$x = \sum_{i=1}^k (\lfloor \eta_i \rfloor + \{\eta_i\}) y_i,$$

so that

$$x - \sum_{i=1}^k \lfloor \eta_i \rfloor y_i = \sum_{i=1}^k \{\eta_i\} y_i.$$

The left side of this equation is a lattice point. Hence, also the right side is a lattice point. But

$$h := \sum_{i=1}^k \{\eta_i\} y_i \in \Pi,$$

so $h \in \Pi \cap \mathbb{Z}^n = \mathcal{H}$. This implies that x is a integral conic combination of points in \mathcal{H} . So \mathcal{H} is a **HILBERT basis**.

Now assume that C is pointed. Then there is $b \in \mathbb{R}^n$ such that

$$b^t x > 0 \quad \text{for all} \quad x \in C - \{0\}.$$

Let $K := \left\{ y \in C \cap \mathbb{Z}^m \mid y \neq 0, \text{ } y \text{ not a sum of two other integral vectors in } C \right\}.$

Then $K \subseteq \mathcal{H}$, so K is finite.

Assume that K is not a **HILBERT basis**. Then there is $x \in C$ such that $x \notin \mathbb{Z}_{\geq} K$. Choose x such that $b^t x$ is as small as possible.

Since $x \notin K$, there must be are $x_1, x_2 \in C$ such that $x = x_1 + x_2$. But

$$\begin{aligned} & b^t x_1 \geq 0, \quad b^t x_2 \geq 0, \quad b^t x \geq 0 \quad \text{and} \quad b^t x = b^t x_1 + b^t x_2, \\ \text{so} \quad & b^t x_1 \leq b^t x, \quad b^t x_2 < b^t x. \end{aligned}$$

By our choice of x we get $x_1, x_2 \in \mathbb{Z}_{\geq} K$, so that $x \in \mathbb{Z}_{\geq} K$, a contradiction. \square

1.3.29 Definition (homogeneous). Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $C \subseteq \mathbb{R}^d$ a finitely generated cone with generators $v_1, \dots, v_d \in \Lambda$. C is *homogeneous* with respect to some linear functional $c \in \mathbb{Z}^d$ if there is $\lambda \in \mathbb{Z}$ such that $c^t v_j = \lambda$ for $1 \leq j \leq d$.

Problems

- 1.1 Prove Caratheodory's Theorem.
- 1.2 Let Λ be a discrete subset of \mathbb{R}^d and $B \subseteq \mathbb{R}^d$ bounded. Then $\Lambda \cap B$ is a finite set.
- 1.3 Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $v_1, \dots, v_d \in \Lambda$ be such that $\text{vol } \Pi(v_1, \dots, v_d) = \det \Lambda$. Then v_1, \dots, v_d is a basis of Λ .
- 1.4 Dualizing non-polyhedral cones.
- 1.5 Existence of a Hilbert basis
- 1.6 Hermite normal form

An invitation to lattice polytopes

2

Lattice polytopes are ubiquitous throughout mathematics — pure and applied. An apparent reason is their simple definition: polytopes whose vertices lie in a given lattice, such as \mathbb{Z}^d . There are two major ingredients here. On the one hand, polytopes: beautiful and ancient objects studied in convex and discrete geometry and geometric combinatorics. On the other hand, lattices: they have an algebraic structure and give rise to questions in Diophantine geometry. As such, lattice polytopes are objects of the classical theory of the geometry of numbers: the relation between geometric data of a convex body (such as its shape or volume) with data coming from their lattice points (such as their number or distribution). So, why is there such an ongoing interest in these objects? This can be explained by two developments. First, the rise of the computer pushed the successful development of linear and combinatorial optimization with all its pervasive modern applications, while integer optimization is largely concerned with questions on lattice points in polytopes. Second, toric geometry allowed an unforeseen interaction between geometric combinatorics and algebraic geometry leading to applications in enumerative geometry, mirror symmetry, and polytope theory, to name but a few. There are several results on lattice polytopes for which the only known proofs involve the theory of algebraic varieties.

While lattice polytopes are used in many areas of mathematics, there is not yet one source of reference focusing solely on these objects. Many results are scattered throughout the literature. Most existing books are either motivated by its relations to toric varieties or ignore some of the more recent developments in Ehrhart theory and the geometry of numbers. In these lecture notes we present the theory of lattice polytopes in a self-contained and unifying way. The goal is to get students and researchers acquainted with the most important and widely used results, closely related to topics of recent research. Some presentations and results are new.

In this chapter we introduce the major definitions and prove the basic results. To name a few examples: We will learn about unimodular equivalence, PICK’s Theorem, and the normalized volume. After having read this chapter, the reader will have encountered methods and types of results studied in more detail later: among them are triangulations, lattice point counting, estimating volumes, and several classification results.

2.1 Lattice polytopes and unimodular equivalence

Here is the key player of these lectures:

2.1.1 Definition. A *lattice polytope* is a polytope in \mathbb{R}^d with vertices in a given lattice $\Lambda \subseteq \mathbb{R}^d$.

Note that $\dim(P) \leq \text{rank}(\Lambda)$. Usually we will consider full-dimensional lattice polytopes, i.e., $\dim(P) = \text{rank}(\Lambda)$. However, we note that we can always consider P as a full-dimensional lattice polytope with respect to its *ambient lattice* $\text{aff}(P) \cap \Lambda$ of rank $\dim(P)$ in its *ambient affine space* $\text{aff}(P)$.

Throughout (except when explicitly noted otherwise), the reader should assume $\Lambda = \mathbb{Z}^d$. In this case, a lattice polytope is also called *integral polytope*. We will use more general lattices only at very few places in the chapter on Geometry of Numbers (Chapter 4).

Having introduced the objects of our interest, we should next state when two of them are considered isomorphic. Figure 2.1 shows three examples of lattice polygons in dimension two. As the reader should notice, all three triangles look quite different: their vertices have different Euclidean distances and different angles. Still, the top one is considerably distinguished from the lower two: it has four lattice points, while the others have only three. Actually, more is true: the second and third are *isomorphic*.

2.1.2 Definition. Two lattice polytopes $P \subseteq \mathbb{R}^d$ and $P' \subseteq \mathbb{R}^{d'}$ (with respect to lattices $\Lambda \subseteq \mathbb{R}^d$ and $\Lambda' \subseteq \mathbb{R}^{d'}$) are *isomorphic* or *unimodularly equivalent*, if there is an affine lattice isomorphism of the ambient lattices $\Lambda \cap \text{aff}(P) \rightarrow \Lambda' \cap \text{aff}(P')$ mapping the vertices of P onto the vertices of P' .

Recall that a *lattice isomorphism* is just an isomorphism of abelian groups. Moreover, an *affine lattice isomorphism* is an isomorphism of affine lattices. Here, note that an affine lattice does not need to have an origin (e.g., consider the set of lattice points in a hyperplane). However, if we fix some lattice point to be the origin, an affine lattice isomorphism can be defined as a lattice isomorphism followed by a translation, i.e., $x \mapsto Tx + b$ where $T : \Lambda \rightarrow \Lambda'$ is a (linear) lattice isomorphism and $b \in \Lambda'$.

Luckily, in our usual situation $\Lambda = \mathbb{Z}^d = \Lambda'$ there is an easy criterion to check when a linear map $\mathbb{R}^d \rightarrow \mathbb{R}^d$ is a lattice automorphism of \mathbb{Z}^d (see Exercise 2.2).

2.1.3 Lemma. A linear map $L : \mathbb{R}^d \rightarrow \mathbb{R}^d$ induces a lattice automorphism of \mathbb{Z}^d if and only if its $(d \times d)$ -matrix has entries in \mathbb{Z} and its determinant is equal to ± 1 . \square

The set of such matrices is denoted by $\text{Gl}(d, \mathbb{Z})$. Again, as we have seen from the example above, it is very important to realize that in our category *isomorphisms do not preserve angles or distances!* Let us note an immediate consequence of Lemma 2.1.3.

2.1.4 Corollary. Unimodularly equivalent lattice polytopes have the same number of lattice points and the same volume. \square

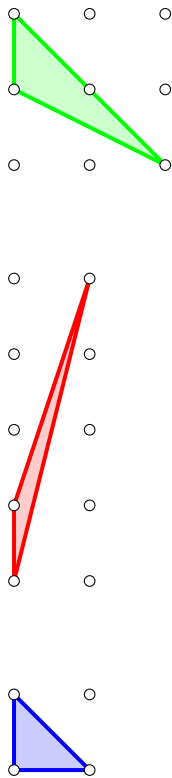


Fig. 2.1: Lattice Triangles

Let us again consider the example above. The matrix

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$$

is an element of $\text{Gl}(d, \mathbb{Z})$. The affine lattice isomorphism

$$\mathbb{Z}^2 \rightarrow \mathbb{Z}^2 : x \mapsto Ax - \begin{pmatrix} 1 \\ 3 \end{pmatrix}$$

maps the vertices of the first triangle T_1 to the vertices of the second triangle T_2 . This proves that they are unimodularly equivalent.

This is an instance of a remarkable result (referred to as PICK's Theorem). For this let us denote by

$$\Delta_2 := \text{conv}(0, e_1, e_2)$$

the *standard* or *unimodular* triangle.

2.1.5 Proposition (PICK's Theorem). *Any two lattice triangles with three lattice points are isomorphic to Δ_2 . In particular, they have area $1/2$.*

Its proof is sketched in Exercise 2.5. Theorem 2.2.1 below generalizes this result to arbitrary lattice polygons. Unfortunately, the corresponding statement of Proposition 2.1.5 in dimension 3 fails (see Exercise 2.4).

2.2 Lattice polygons

To get started, let us prove two famous results on lattice polygons. The first is a surprisingly elegant formula for the computation of the area of a lattice polygon *just by counting lattice points*! To find some generalization to higher dimensions (if any) is the topic of the chapter on Ehrhart theory (Chapter 3).

2.2.1 Theorem (PICK's Formula). *Let P be a lattice polygon with i interior lattice points, b lattice points on the boundary, and (Euclidean) volume a . Then*

$$a = i + \frac{b}{2} - 1.$$

Proof. We prove the theorem by induction on the number $l := b + i$ of lattice points of P .

Any triangle in \mathbb{R}^2 with $b = 3$ and $i = 0$ is unimodularly equivalent to Δ_2 by Proposition 2.1.5, and has area $1/2$. So the claimed formula is true in this case. There are two cases to consider for the induction, either P has $b \geq 4$ lattice points on the boundary, or $b = 3$ and we have at least one interior lattice point, i.e. $i \geq 1$.

If P has at least four lattice points on the boundary then we can cut P into two lattice polygons Q_1 and Q_2 by cutting along a chord e through the interior of P given by two boundary lattice points. Let Q_j , $j = 1, 2$ have volume a_j , b_j boundary lattice points, and i_j interior lattice points. Let e have i_e interior lattice points (and two boundary lattice points). Both Q_1 and Q_2 have less lattice points, so by induction PICK's Formula holds for Q and Q' , i.e.

$$a_1 = i_1 + \frac{b_1}{2} - 1, \quad a_2 = i_2 + \frac{b_2}{2} - 1.$$

Further

$$i = i_1 + i_2 + i_e, \quad b = b_1 + b_2 - 2i_e - 2,$$

so

$$\begin{aligned} a &= a_1 + a_2 = i_1 + i_2 + \frac{1}{2}(b_1 + b_2) - 2 \\ &= i - i_e + \frac{1}{2}(b + 2i_e + 2) - 2 = i + \frac{b}{2} - 1. \end{aligned}$$

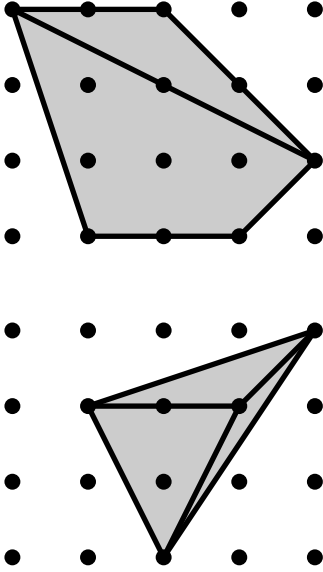


Fig. 2.2: Splitting P into pieces. The first image is for the case $b \geq 4$, the second for $i \geq 1$.

If $b = 3$ and $i \geq 1$ then we can split P into three pieces Q_1 , Q_2 , and Q_3 by coning over some interior point of P . See Figure 2.2. Again, all three pieces have fewer lattice points than P , so we know PICK’s Formula for those by our induction hypothesis. A similar computation to the one above shows that PICK’s Formula also holds for P . \square

Note that the proof shows along the way that any lattice polygon can be subdivided into unimodular triangles. This is not true in higher dimensions. See Exercise 2.4. Questions about the existence of such triangulations will be discussed in the last chapter of this book.

The second fundamental result shows that we can predict precisely how large the lattice polygon can be at most if we know that a lattice polygon has a certain (non-zero) number of interior lattice points! Problems like these, which relate information about lattice points of a convex body to its geometric shape or invariants are subject of the field of Geometry of Numbers. We deal with such questions in Chapter 4.

2.2.2 Theorem (SCOTT, 1976 [24]). Let $P \subseteq \mathbb{R}^2$ be a lattice polygon with $i \geq 1$ interior lattice points. Then either $P = 3\Delta_2$ and, hence, $\text{vol } P = 9/2$ and $i = 1$, or $\text{vol } P \leq 2(i + 1)$.

Proof. Let $a := \text{vol } P$ be the Euclidean area of P . Using PICK’s Theorem 2.2.1 we can reformulate the condition to

$$b \leq a + 4$$

unless $P = 3\Delta_2$, in which case $b = 9$ and $a = 9/2$.

Using unimodular transformations we can assume that the polygon P is contained in a rectangle with vertices $(0, 0)$, $(p', 0)$, $(0, p)$ and (p', p) such that p is minimal with this property. As P has at least one interior lattice point we know that $2 \leq p \leq p'$. The polygon P intersects the bottom and top edge of the rectangle in edges of length q_b and q_t . See Figure 2.3. Then

$$b \leq q_b + q_t + 2p \tag{2.2.1}$$

$$a \geq \frac{p(q_b + q_t)}{2}. \tag{2.2.2}$$

Further, PICK’s Theorem 2.2.1 implies that $a \geq b/2$. We consider four different cases for the parameters p , q_b and q_t :

- (1) $p = q_b + q_t = 3$, or
- (2) $p = 2$ or $q_b + q_t \geq 4$, or
- (3) $p = 3$ and $q_b + q_t \leq 2$, or
- (4) $p \geq 4$ and $q_b + q_t \leq 2$

In the first case, (2.2.1) gives $b \leq 9$. If $b \leq 8$, then $a \geq b/2$ implies $b \leq a + 4$. So assume that $b = 9$. If $a \geq 5$, then again $b \leq a + 4$, so also assume $a = 9/2$. This

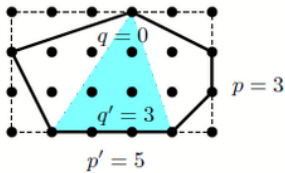


Fig. 2.3: P in a box

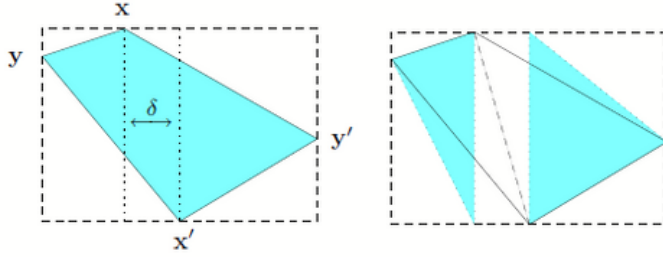


Fig. 2.4: Case (4). y and y' in the right image correspond to w_r and w_l in the text, x and x' to v_t and v_b .

implies $i = 1$. Up to unimodular equivalence there are only finitely many lattice polygons with $q_b + q_t = 3$, $p = 3$, and $a = 9/2$, and of these, only $3\Delta_2$ has nine lattice points on the boundary.

For the second case we subtract (2.2.2) from (2.2.1) to obtain

$$2b - 2a = 2(q_b + q_t + 2p) - p(q_b + q_t) = (q_b + q_t - 4)(2 - p) + 8 \leq 8,$$

where the last inequality follows from $p = 2$. Rearranging this gives the claim.

In the third case we have $b \leq 8$, so the claim follows from $a \geq b/2$.

The last case requires slightly more work. Pick points $v_b := (y_l, 0)$ and $v_t := (y_r, p)$ in such a way that $\delta := |y_b - y_t|$ is minimal. See Figure 2.4. Using a unimodular transformation of the type $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ we can assume that

$$\delta \leq \frac{p - q_b - q_t}{2}.$$

The transformed polygon still satisfies $p \leq p'$ by the choice of p , so

$$p' - \delta \geq p - \frac{p - q_b - q_t}{2} \geq \frac{p + q_b + q_t}{2}.$$

Choose point w_l and w_r on the left and right edge of the rectangle. We consider the triangles given by w_l, v_t, v_b and w_r, v_t, v_b . By shifting one vertex we can make the edge v_t, v_b vertical in each triangle (see Figure 2.4). The area of the two triangles is at most the area of our original polygon. Hence, we can estimate

$$a \geq \frac{1}{2} \cdot p \cdot \frac{p + q_b + q_t}{2}.$$

This implies

$$\begin{aligned} 4(b - a) &\leq 4(q_b + q_t + 2p) - (p + q_b + q_t) \\ &\leq p(8 - p) - (p - 4)(q_b + q_t) \leq p(8 - p) \leq 16. \end{aligned}$$

Solving for b gives the claim. This finally proves Scott's Theorem. \square

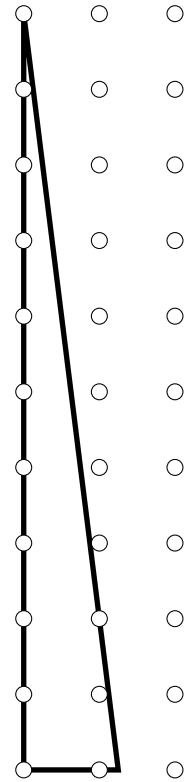


Fig. 2.5: An arbitrarily big rational triangle with one interior lattice point

Note that there is no such upper bound on the volume of polytopes not all of whose vertices are lattice points. An example is in Figure 2.5.

2.3 Volume of lattice polytopes

This section is devoted to a fundamental result on lattice polytopes in arbitrary dimension d . In the previous section we have shown that for polygons the number of interior lattice points and the volume are connected. Here we will prove that in any dimension d there are only *finitely* many isomorphism classes of d -dimensional lattice polytopes of fixed *volume*. For polygons, this implies that there are only finitely many isomorphism types with a fixed number of interior lattice points. Unfortunately, no such result is true in dimensions three and above. You will construct examples in Exercise 2.4. It is an extremely important point to realize that starting already in dimension three, having information about the volume of a lattice polytope is much stronger than just knowing the number of its (interior) lattice points.

2.3.1 Remark. Note that we always take the volume as induced by the lattice Λ , i.e., the volume of a fundamental parallelepiped equals one. For instance, $[0, 1]^d$ is a fundamental parallelepiped for \mathbb{Z}^d .

2.3.2 Definition. $\Delta_d := \text{conv}(0, e_1, \dots, e_d)$ is called the *standard* or *unimodular* d -simplex. We also call any polytope isomorphic to Δ_d a *unimodular d -simplex*.

In other words, a lattice polytope is a unimodular simplex if and only if its vertices form an affine lattice basis. This is the simplest possible lattice polytope. Note that $\text{vol}(\Delta_d) = 1/d!$, see Exercise 2.6. The following observation shows that this simplex is indeed the *smallest* possible lattice polytope:

2.3.3 Proposition. Let $P \subseteq \mathbb{R}^d$ be a d -dimensional simplex. Then there is an affine lattice homomorphism $\varphi : \mathbb{Z}^d \rightarrow \mathbb{Z}^d, x \mapsto Ax + b$ mapping the vertices of Δ_d onto the vertices of P . In this case,

$$d! \text{vol}(P) = |\det(\varphi)| \in \mathbb{N}_{\geq 1}.$$

Proof. We may assume that $P = \text{conv}(0, v_1, \dots, v_d)$. In this case, φ is given by $e_i \mapsto v_i$ for $i = 1, \dots, d$. Hence,

$$\text{vol}(P) = |\det(\varphi)| \text{vol}(\Delta_d) = \left| \det \begin{pmatrix} v_1 & \dots & v_d \end{pmatrix} \right| \frac{1}{d!}. \quad \square$$

2.3.4 Corollary. Let $P \subseteq \mathbb{R}^d$ be a d -dimensional lattice polytope. Then $d! \text{vol}(P) \in \mathbb{N}_{\geq 1}$. We have $d! \text{vol}(P)$ if and only if P is a unimodular simplex.

Proof. We triangulate the polytope into simplices without introducing additional vertices apart from those of P . In particular, any simplex is a d -dimensional lattice simplex. Now, the statement follows from the previous proposition. \square

This motivates the following definition.

2.3.5 Definition. The *normalized volume* of a d -dimensional lattice polytope $P \subseteq \mathbb{R}^d$ is defined as the positive integer

$$\text{Vol}(P) := d! \text{vol}(P).$$

2.3.6 Remark. Note that it makes sense to extend the previous definition also to low-dimensional lattice polytopes by considering them as full-dimensional polytopes with respect to their ambient lattice. Hence, $\text{Vol}(P) \geq 1$ for *any* lattice polytope.

Note that, if $P = \text{conv}(0, v_1, \dots, v_d)$ is a d -dimensional lattice simplex in \mathbb{R}^d , then by Proposition 2.3.3 the normalized volume of P equals the volume of the parallelepiped spanned by v_1, \dots, v_d .

As we have seen, lattice polytopes have normalized volume at least 1. Given a triangulation of a lattice polytope P of normalized volume V into lattice simplices, we see that this triangulation can have at most V simplices. This observation gives us an empirical reason why there should be only finitely many lattice polytopes of given volume and dimension (of course, up to unimodular transformations). Finally, let us give the formally correct proof.

2.3.7 Theorem. *Let $P \subseteq \mathbb{R}^d$ be a d -dimensional lattice polytope, $\text{Vol}(P) = V$. Then there exists some lattice polytope $Q \subseteq \mathbb{R}^d$ such that $Q \subseteq [0, d \cdot V]^d$ and $P \cong Q$.*

Moreover, if P is a simplex, then $d \cdot V$ may be substituted by V .

2.3.8 Corollary. *There exist only finitely many isomorphism classes of lattice polytopes of given dimension and volume.*

We will first prove Theorem 2.3.7 for simplices. We need the following useful observation to extend this result to arbitrary polytopes.

2.3.9 Lemma. *Let $P \subseteq \mathbb{R}^d$ be a d -dimensional polytope. Then there exists a d -dimensional simplex $S \subseteq P$ whose vertices are vertices of P such that*

$$S \subseteq P \subseteq (-d)(S - x) + x,$$

where x is the centroid of S . In other words, if v_0, \dots, v_d are the vertices of S , then

$$S \subseteq (-d)S + \sum_{i=0}^d v_i.$$

The proof is given in Exercise 2.7.

Proof (of Theorem 2.3.7). First, let $P = \text{conv}(v_0, \dots, v_d)$ be a simplex (assume $v_0 = 0$). By the HERMITE normal form theorem 1.3.25 there exists $U \in \text{GL}_d(\mathbb{Z})$ such that

$$U \cdot \begin{pmatrix} \vdots & \vdots & \vdots \\ v_1 & v_2 & \cdots & v_d \\ \vdots & \vdots & \vdots \end{pmatrix} = \begin{pmatrix} a_{11} & 0 & \cdots & 0 \\ a_{21} \leq a_{22} & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & 0 \\ a_{d1} \leq a_{d2} & \cdots & \cdots & a_{dd} \end{pmatrix}$$

We denote the columns of the right matrix by u_1, \dots, u_d . Therefore, U defines a unimodular transformation mapping P to

$$Q := \text{conv}(0, u_1, \dots, u_d) \subseteq [0, a_{11} \cdots a_{dd}]^d.$$

Hereby, $\text{Vol}(P) = \text{Vol}(Q) = \det(u_1, \dots, u_d) = a_{11} \cdots a_{dd}$.

In general, there exists a lattice d -simplex $S \subseteq P$ as in Lemma 2.3.9. Then the previous part of the proof shows that there exists a unimodular transformation $\varphi : \mathbb{Z}^d \rightarrow \mathbb{Z}^d$ such that

$$\varphi(S) \subseteq [0, \text{Vol}(S)]^d.$$

Let S have vertices v_0, \dots, v_d . Then

$$P \cong \varphi(P) \subseteq (-d)\varphi(S) + \sum_{i=0}^d \varphi(v_i) \subseteq [0, -d \text{Vol}(S)]^d + \sum_{i=0}^d \varphi(v_i).$$

Since $\text{Vol}(S) \leq \text{Vol}(P)$, the statement follows after an affine unimodular transformation (translating by $-\sum_{i=0}^d \varphi(v_i)$ and multiplying by -1). \square

2.4 Problems

2.1 Extend Definition 2.1.2 to homomorphisms of lattice polytopes in order to finish the definition of a category of lattice polytopes.

2.2 Prove Lemma 2.1.3.

2.3 Show that the converse of Corollary 2.1.4 is wrong in dimension two.

2.4 Show that there are infinitely many, non-isomorphic lattice tetrahedra containing only four lattice points.

2.5 Prove Proposition 2.1.5. Here are some hints: 1. Translate the triangle so that it is given as $\text{conv}(0, v, w)$. Then consider the reflection $x \mapsto v + w - x$. Deduce that the parallelogram $\text{conv}(0, v, w, v + w)$ has only its vertices as lattice points. 2. Look at the tiling of \mathbb{R}^2 by translations of this parallelogram. Deduce that any lattice point in \mathbb{Z}^2 is of the form $k_1 v + k_2 w$. Why does this prove the statement?

2.6 Show that Δ_d has volume $1/d!$. (Hints: think of Δ_d as iterated pyramids or subdivide $[0, 1]^d$ into $d!$ simplices).

2.7 Prove Lemma 2.3.9.

2.8 A vector $v \in \mathbb{Z}^2$ (or in any lattice) is called *primitive* if it is not a non-trivial integer multiple of some other lattice vector.

- (1) Show that any primitive $v \in \mathbb{Z}^2$ is part of a lattice basis.
- (2) Show that every rational simplicial 2-dimensional cone is unimodularly equivalent to a cone spanned by $(1/0)$ and (p/q) for integers $0 \leq p < q$.

2.9 Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with fundamental parallelepiped Π . Show that the lattice translates of Π cover \mathbb{R}^d without overlap, i.e.

$$\bigcup_{x \in \Lambda} (x + \Pi) = \mathbb{R}^d$$

and $(x + \Lambda) \cap (y + \Lambda) = \emptyset$ for $x, y \in \Lambda$, $x \neq y$.

2.10 Let $\Lambda \subseteq \mathbb{Z}^d$ be a sub-lattice of rank d , and let v_1, \dots, v_d be a basis of Λ with fundamental parallelepiped

$$\Pi(v_1, \dots, v_d) = \left\{ \sum \lambda_i v_i \mid \lambda_i \in [0, 1] \right\}.$$

Show that

$$|\mathbb{Z}^d / \Lambda| = |\Pi(v_1, \dots, v_d) \cap \mathbb{Z}^d| = \det \Lambda.$$

Ehrhart Theory 3

In this chapter we will learn all about counting lattice points in polytopes. The central theorem of this chapter gives a very beautiful relation between geometry and algebra. It is due to Eugène EHRHART and tells us that the function counting the number of lattice points in dilates of a polytope $P \subseteq \mathbb{R}^d$,

$$|k \cdot P \cap \mathbb{Z}^d|,$$

is the evaluation of a polynomial $\text{ehr}_P(t)$ of degree d in k . The polynomial $\text{ehr}_P(t)$ is the *Ehrhart polynomial* of P , and the main part of this chapter deals with methods to compute this and related functions.

3.1 Motivation

3.1.1 Why do we count lattice points?

Before we delve into the theory and compute Ehrhart polynomials of polytopes we want to introduce some problems where counting, enumerating or sampling lattice points appear naturally if one wants to solve the problem.

Knapsack type problems Assume that you are given a container C of size ℓ (the *knapsack*), and k goods of a certain sizes s_1, \dots, s_k and values v_1, \dots, v_k . Two important variants of a *knapsack problem* are the tasks to fill the container either with goods of the highest possible total value, i.e. to solve the problem

$$\begin{aligned} \max \quad & x_1 v_1 + \dots + x_k v_k \\ \text{subject to} \quad & x_1 s_1 + \dots + x_k s_k \leq \ell \\ & x_i \in \{0, 1\} \quad \text{for } 1 \leq i \leq k, \end{aligned}$$

or to fill the container completely with goods of a prescribed total value v , i.e. to solve

$$\begin{aligned} x_1 v_1 + \cdots + x_k v_k &= v \\ x_1 s_1 + \cdots + x_k s_k &= \ell \\ x_i &\in \{0, 1\} \quad \text{for } 1 \leq i \leq k. \end{aligned}$$

Here is a simple example of such a problem. The U.S. currency has four different coins that are in regular use, the *penny* (1¢), *nickel* (5¢), *dime* (10¢), and the *quarter* (25¢). You may wonder how many different ways there are to pay 1\$ using exactly ten coins. With a little consideration you probably come up with the solution

$$\begin{aligned} 100 &= 5 \cdot 1 + 0 \cdot 5 + 2 \cdot 10 + 3 \cdot 25 \\ &= 0 \cdot 1 + 6 \cdot 5 + 2 \cdot 10 + 2 \cdot 25 \\ &= 0 \cdot 1 + 3 \cdot 5 + 6 \cdot 10 + 1 \cdot 25 \\ &= 0 \cdot 1 + 0 \cdot 5 + 10 \cdot 10 + 0 \cdot 25, \end{aligned}$$

so there are essentially four different ways. This is exactly the number of lattice points in the polytope

$$P := \left\{ x \in \mathbb{R}^4 \mid \begin{array}{l} x_1, x_2, x_3, x_4 \geq 0, \quad x_1 + x_2 + x_3 + x_4 = 10, \\ x_1 + 5x_2 + 10x_3 + 25x_4 = 100 \end{array} \right\}.$$

This may look like a much more complicated approach than just testing with some coins. But what if you want to find the 182 ways to pay 10\$ using 100 coins, or the 15876 ways to pay 100\$ with 1000 coins?

Contingency Tables Consider the following table (which is a simplified version of a table produced by the Statistische Landesamt Berlin for academic degrees awarded at Berlin universities in 2005)

	Diploma	PhD	Teacher	
FU	1989	1444	299	3732
TU	1868	421	115	2404
HU	920	441	373	1774
	4817	2306	787	

You may ask how likely it is to have exactly this distribution of the entries of the table, if its margins, i.e. the totals of degrees awarded at each university, and the totals of different degrees awarded, are given. Assuming a uniform distribution, you would need to know the number of possible tables with these margins. This is the number of lattice points in the polytope

$$P := \left\{ X \in \mathbb{R}_{\geq 0}^{3 \times 3} \mid \begin{array}{l} x_{11} + x_{12} + x_{13} = 3732, \quad x_{21} + x_{22} + x_{23} = 2404, \\ x_{31} + x_{32} + x_{33} = 1774, \quad x_{11} + x_{21} + x_{31} = 4817, \\ x_{12} + x_{22} + x_{32} = 2306, \quad x_{13} + x_{23} + x_{33} = 787 \end{array} \right\}.$$

There are 714,574,663,432 of them.

We hope that these examples have awoken your interest in a more systematic study on how one can compute those numbers. In the next section we will explore

methods to obtain them, and to enumerate lattice points, and more generally study the structure of lattice points in polytopes. Our strategy to count lattice points in (dilates of) polytopes is to treat simplices first. We can then subdivide general polytopes into simplices and use inclusion-exclusion to generalize our results.

3.1.2 First Ehrhart polynomials

Let $S \subseteq \mathbb{R}^d$, and let $k \in \mathbb{Z}_{>}$. The k -th-dilation of a set of S is the set

$$kS := \{kx \mid x \in S\}.$$

In this section we will apply the methods developed in the previous section to count integral points in dilations of a polytope P and its interior. We introduce the following counting function.

3.1.1 Definition. The *Ehrhart counting function* of a bounded subset $S \subseteq \mathbb{R}^d$ is the function $\mathbb{N} \rightarrow \mathbb{N}$

$$\text{ehr}_S(k) := |kS \cap \mathbb{Z}^d|.$$

We want to look at some simple examples of Ehrhart counting functions. Let $L := [a, b] \subseteq \mathbb{R}$, $a, b \in \mathbb{R}$ be an interval on the real line. Here, counting is easy, L contains $\lfloor b \rfloor - \lfloor a \rfloor + 1$ integers. The k -th dilate of P is $[ka, kb]$. By the same argument it contains $\lfloor kb \rfloor - \lfloor ka \rfloor + 1$ integral points, so

$$\text{ehr}_L(k) = \lfloor kb \rfloor - \lfloor ka \rfloor + 1.$$

Figure 3.1 shows the interval $I = [0, \frac{3}{2}]$ and its second and third dilation.

If the boundary points a and b are integral and $a \leq b$, then we can simplify the formula. In this case also all multiples of a and b are integral, and we can omit the floor and ceiling operations to obtain

$$\text{ehr}_L(k) = k(b - a) + 1.$$

We observe that this is a polynomial of degree 1 in k . We will see that this observation is a very special case of the Theorem of EHRHART that we will prove below.

Now we turn to an example in arbitrary dimension. The d -dimensional *standard simplex* is the convex hull

$$\Delta_d := \text{conv}(\mathbf{0}, e_1, \dots, e_d)$$

of the origin and the d standard unit vectors. Its exterior description is given by

$$x_i \geq 0 \quad \text{for } 1 \leq i \leq d \quad \text{and} \quad \sum_{i=1}^d x_i \leq 1.$$

3.1.2 Proposition. Let Δ_d be the d -dimensional standard simplex. Then

$$\text{ehr}_{\Delta_d}(k) = \binom{d+k}{d} = \frac{(d+k) \cdot (d+k-1) \cdot \dots \cdot (k+1)}{d!}.$$

Observe that this is a polynomial in the variable k of degree d with leading coefficient $1/d!$.

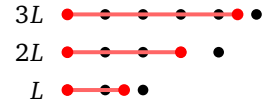


Fig. 3.1

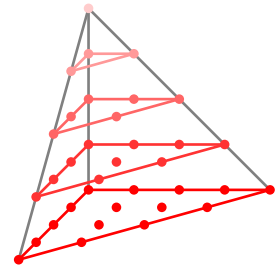


Fig. 3.2: Lattice points in a standard simplex.

Proof. There is a bijection between the lattice points in $k\Delta_d$ and sequences of k dots and d bars: to each such sequence, assign the vector $x \in \mathbb{R}^d$ whose i th coordinate equals the number of dots between the $(i-1)$ st bar and the i th bar.

$$\cdots | \cdots || \cdot \quad \longleftrightarrow \quad x = (2, 3, 0, 1)$$

This yields a bijection between the sequences and lattice points with non-negative coordinates and with $\sum x_i \leq k$. \square

Another simple, but very important example is the unit cube

$$C_d := \{x \in \mathbb{R}^d \mid 0 \leq x \leq 1\} = [0, 1]^d.$$

This is the exterior and interior description of the cube. It has $2d$ facets and the 2^d 0/1-vectors as its vertices. We will return to this example at many places throughout these notes. The k -th dilate of the cube is $kC_d = k \cdot [0, 1]^d = [0, k]^d$. Hence, the Ehrhart counting function is given by

$$\text{ehr}_{C_d}(k) = (k+1)^d.$$

Note again that this is a polynomial in k of degree d .

3.2 Triangulations and Half-open Decompositions

We start our considerations with subdivisions of polytopes into smaller pieces and study polyhedral complexes and triangulations. Our approach will lead beyond the classic theory of subdivisions, as we will want to decompose the polytopes and cones into half-open simplices and simplicial cones for a finer analysis of lattice points.

3.2.1 Definition (polyhedral complex). A *polyhedral complex* \mathcal{C} is a finite family of polyhedra (the *cells* of the complex) such that for all $P, Q \in \mathcal{C}$

- (1) if $P \in \mathcal{C}$ and F is a face of P then $F \in \mathcal{C}$, and
- (2) $F := P \cap Q$ is a face of both P and Q .

A cell P is *maximal* if there is no $Q \in \mathcal{C}$ strictly containing it. These cells are sometimes also called the *facets* of \mathcal{C} . The *dimension* of \mathcal{C} is the maximal dimension of a cell of the complex. A complex is *pure* if all maximal cells have the same dimension. In this case the maximal cells are the *facets* of the complex. We will denote by $\mathcal{C}[k]$ the set of k -dimensional faces of \mathcal{C} .

A polyhedral complex \mathcal{S} is a *subcomplex* of \mathcal{C} if its cells are a subset of the cells of \mathcal{C} .

3.2.2 Example. Here are some examples of a polyhedral complex. See also Figure 3.3.

- (1) Any polytope or cone can be viewed as a polyhedral complex. This complex has one maximal cell, the cone or polytope itself. This is also called the *trivial subdivision* of the cone or polytope. In general, subdivisions are defined with the next definition below.
- (2) The *boundary complex* of a d -dimensional polytope naturally has the structure of a pure polyhedral complex. The maximal cells are the facets of the polytope, and its dimension is $d-1$, the dimension of the facets of the polytope.
- (3) See the middle figure in Figure 3.3 for a non-pure polyhedral complex. It has three 2-dimensional maximal cells and one 1-dimensional maximal cell.

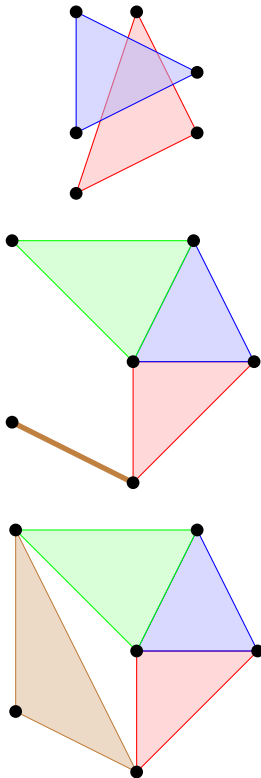


Fig. 3.3: The upper figure is not a polyhedral complex. The second is, but it is not pure, the third is also pure.

(4) Fans naturally have the structure of a polyhedral complex. In this case all cells are cones.

3.2.3 Definition (subdivision and triangulation). A *subdivision* of a polytope (cone) P is a polyhedral complex \mathcal{S} such that $P = \bigcup_{F \in \mathcal{S}} F$.

A subdivision \mathcal{T} is a *triangulation* of P if all cells are simplices (simplicial cones). It is *without new vertices*, if $\mathcal{V}(\Delta_d) \subseteq \mathcal{V}(P)$ for any $\Delta_d \in \mathcal{T}$.

We will use the basic fact that for every finite $V \subseteq \mathbb{R}^d$ the polytope $\text{conv } V$ has a triangulation with vertex set V . Similarly, the cone $\text{pos } V$ has a triangulation with rays $\{\mathbb{R}_{\geq 0} v : v \in V\}$ [11].

If we are given a triangulation of a polytope we cannot simply add the number of lattice points of the cells because the cells overlap. In order to avoid inclusion-exclusion, we will now describe a way to partition the cone into pairwise disjoint half-open simplicial cones [6, 18]. There are various ways to do this. We will use a generic reference point as an arbiter to decide which points *belong* to which cells.

3.2.4 Definition (half-open decomposition). Let $V = \{v_1, \dots, v_d\} \subseteq \mathbb{R}^d$ be linearly independent, and $C := \text{cone } V$. Call a point $x \in \mathbb{R}^d$ *generic* with respect to C if all coefficients λ_v in the unique representation $x = \sum \lambda_v v$ are non-zero. Set $I_+(x) := \{v \in V : \lambda_v > 0\}$ and $I_-(x) := \{v \in V : \lambda_v < 0\}$.

In case x is generic, define the *near half-open cone* $C(x]$, the *near half-open parallelepiped* $\square(V, x)$, the *far half-open cone* $C[x)$, and the *far half-open parallelepiped* $\square(V, x)$ as follows.

$$C(x] := \left\{ \sum_{v \in V} \mu_v v : \mu_v > 0 \text{ for } v \in I_+(x) \text{ and } \mu_v \geq 0 \text{ for } v \in I_-(x) \right\}$$

$$\square(V, x) := \left\{ \sum_{v \in V} \mu_v v : \mu_v \in (0, 1] \text{ for } v \in I_+(x) \text{ and } \mu_v \in [0, 1) \text{ for } v \in I_-(x) \right\}$$

$$C[x) := \left\{ \sum_{v \in V} \mu_v v : \mu_v \geq 0 \text{ for } v \in I_+(x) \text{ and } \mu_v > 0 \text{ for } v \in I_-(x) \right\}$$

$$\square(V, x) := \left\{ \sum_{v \in V} \mu_v v : \mu_v \in [0, 1) \text{ for } v \in I_+(x) \text{ and } \mu_v \in (0, 1] \text{ for } v \in I_-(x) \right\}$$

See Figure 3.4 for an illustration. For x strictly in the relative interior of C we abbreviate

$$\Pi(V) := \square(V, x)$$

and call $\Pi(V)$ the *fundamental parallelepiped* of C with generating set V .

This means that a point y belongs to $C(x]$ if and only if $y \in C$ and all V coordinates for $v \in I_+$ are strictly positive; y belongs to $C[x)$ if and only if $y \in C$ and all V coordinates for $v \in I_-$ are strictly positive. Also, observe that $C(x] = C(-x]$ and $\square(V, x) = \square(V, -x)$.

3.2.5 Proposition. Let $V = \{v_1, \dots, v_d\} \subseteq \mathbb{R}^d$ be linearly independent, and suppose $x \in \mathbb{R}^d$ is generic with respect to the simplicial cone $C := \text{cone } V$. Denote by Λ the lattice generated by V .

Then any point $w \in \mathbb{R}^d$ has a unique representation $w = y + z$ with $y \in \Lambda$ and $z \in \square(V, x)$. Alternatively, we could choose $z \in \square(V, x)$.

Proof. Replacing x with $-x$, we only need to prove the assertion with $z \in \square(V, x)$. As above, let $x = \sum \lambda_v v$ be the unique representation of x in the generators of the cone and set $I_{\pm} := \{v : \lambda_v \gtrless 0\}$.

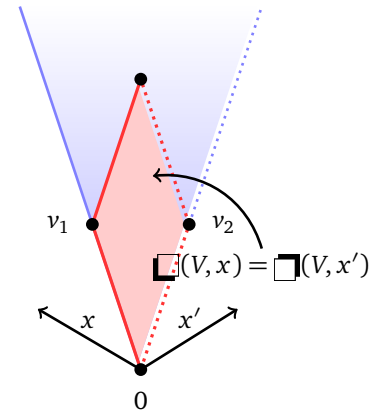


Fig. 3.4: $C(x] = C[x)$

For the existence, given w , write $w = \sum \mu_v v$, and set

$$y := \sum_{v \in I_+} \lfloor \mu_v \rfloor v + \sum_{v \in I_-} (\lceil \mu_v \rceil - 1)v \quad \text{and}$$

$$z := w - y.$$

Then clearly $y \in \Lambda$ and $w = y + z$. Also, the coefficients of z satisfy $\mu_v - \lfloor \mu_v \rfloor \in [0, 1)$ for $v \in I_+$ and $\mu_v - (\lceil \mu_v \rceil - 1) \in (0, 1]$ for $v \in I_-$, so that $z \in \square(V, x)$.

For the uniqueness, assume that there is a second decomposition $w = y' + z'$. We can write $z = \sum \alpha_v v$ and $z' = \sum \alpha'_v v$ with $\alpha_v, \alpha'_v \in [0, 1)$ for $v \in I_+$ and $\alpha_v, \alpha'_v \in (0, 1]$ for $v \in I_-$. Hence, $|\alpha_v - \alpha'_v| < 1$ for all $v \in V$.

From $z' - z = y - y' \in \Lambda$ we conclude that $\alpha_v - \alpha'_v \in \mathbb{Z}$ so that $\alpha_v = \alpha'_v$. This implies $z = z'$ and $y = y'$. \square

We can further decompose each of the half-open cones into half-open boxes. Recall that $\mathbb{N}V$ stands for the set of \mathbb{N} -linear combinations of V .

3.2.6 Corollary. *In the notation of Definition 3.2.4, the half-open cones can be decomposed into a disjoint union of translates of half-open boxes.*

$$C[x] = \bigsqcup_{w \in \mathbb{N}V} w + \square(V, x) \quad \text{and} \quad C(x) = \bigsqcup_{w \in \mathbb{N}V} w + \square(V, x).$$

Proof. The fact that the translates by Λ -vectors are pairwise disjoint follows from the uniqueness in Proposition 3.2.5. From the existence part we see that \mathbb{R}^d is covered by all Λ -translates of $\square(V, x)$. It remains to observe that for $w \in \Lambda$

$$C[x] \cap (w + \square(V, x)) = \begin{cases} w + \square(V, x) & \text{for } w \in \mathbb{N}V \\ \emptyset & \text{else,} \end{cases}$$

and *mutatis mutandis* for $C(x)$. \square

Let a triangulation of a cone D be given. In the following proposition we show how to construct a decomposition of D into disjoint half-open simplicial cones from this triangulation. This needs a preliminary lemma that we will prove first. For $y \in \mathbb{R}^d$ and $\varepsilon \in \mathbb{R}$ write $y_\varepsilon := (1 - \varepsilon)y + \varepsilon x$ for a point on the line through y and x . With this notation, we can recharacterize the half-open cones as follows.

3.2.7 Lemma. *Let $V = \{v_1, \dots, v_d\} \subseteq \mathbb{R}^d$ be linearly independent, and suppose $x \in \mathbb{R}^d$ is generic with respect to the simplicial cone $C := \text{cone } V$. Then $y \in C[x)$ if and only if $y_\varepsilon \in \text{relint } C$ for all small enough $\varepsilon > 0$. Similarly, $y \in C(x]$ if and only if $y_{-\varepsilon} \in \text{relint } C$ for all small enough $\varepsilon > 0$.*

Proof. In the notation of Definition 3.2.4, the v th V -coordinate of y_ε equals $(1 - \varepsilon)\mu_v + \varepsilon\lambda_v$. The first equivalence of the lemma amounts to observing that

$$(1 - \varepsilon)\mu_v + \varepsilon\lambda_v > 0 \text{ for all small enough } \varepsilon > 0$$

if and only if

$$\mu_v > 0 \text{ or } (\mu_v = 0 \text{ and } \lambda_v > 0).$$

The second equivalence of the lemma amounts to observing that

$$(1 + \varepsilon)\mu_v - \varepsilon\lambda_v > 0 \text{ for all small enough } \varepsilon > 0$$

if and only if

$$\mu_v > 0 \text{ or } (\mu_v = 0 \text{ and } \lambda_v < 0) . \quad \square$$

3.2.8 Proposition. Let \mathcal{T} be a triangulation of the d -cone C , and let $x \in C$ be generic with respect to all cones $D \in \mathcal{T}$. Then we have the following decompositions into pairwise disjoint half-open cones:

$$C = \bigsqcup_{D \in \mathcal{T}[d]} D[x] \quad \text{and} \quad \text{relint } C = \bigsqcup_{D \in \mathcal{T}[d]} D(x) .$$

Of course, genericity of x implies $x \in \text{relint } D \subseteq \text{relint } C$ for some $D \in \mathcal{T}[d]$. A half-open decomposition in this way is illustrated in Figure 3.5.

Proof. For $y \in C$, there is a unique $D \in \mathcal{T}[d]$ so that $y_\varepsilon \in \text{relint } D$ for small enough $\varepsilon > 0$. By Lemma 3.2.7 this is the unique D with $y \in D[x]$.

As $x \in \text{relint } C$, we have $y_{-\varepsilon} \in C$ if and only if $y \in \text{relint } C$. In that case, again by Lemma 3.2.7, there is a unique D with $y \in D(x)$. \square

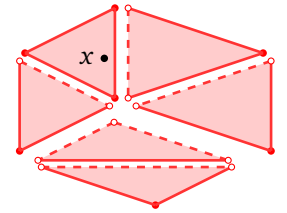
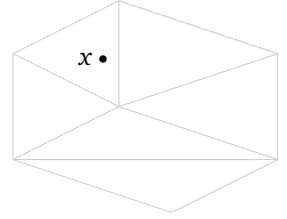


Fig. 3.5: A triangulation and its half open decomposition.

3.3 Ehrhart's Theorem

In this section we will prove that $\text{ehr}_P(k)$ is indeed a polynomial. This requires us to find an efficient way to encode lattice points in (multiples of) a polytope. We will see that it is convenient to work with the cone over a polytope and encode its lattice points. We will do this in the following section. The next section will then use this to write down the Ehrhart polynomial.

3.3.1 Encoding Points in Cones: Generating Functions

At the beginning of this chapter we have seen some basic examples where counting integer points in a polytope appears, and we have seen some simple instances of Ehrhart polynomials. Now let us think for a moment how one could attack the problem of computing the Ehrhart polynomial and enumerate or count lattice points in a polytope. A first question we will have to solve is to find a way to encode all lattice points in a lattice polytope in an *efficient* way. For example, let us list all lattice points in the polytope $P_{[0,3]} := [0, 3]$, see Figure 3.6. The naive approach is to list all points in P :

$$0, 1, 2, 3 .$$

Instead, we could replace each lattice point by the monomial with this exponent (vector) and sum up:

$$1 + t + t^2 + t^3 .$$

Going even further we can replace the polynomial by a geometric series:

$$G_{[0,3]}(t) := \frac{1 - t^4}{1 - t} .$$

Writing the lattice points as a polynomial, or even rewriting the polynomial as a rational function may look strange at first. This idea reveals its power when we try to do the same for the dilated polyhedron $[0, 10002]$. Enumerating the points

$$0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, \dots$$

would be a tedious task. Similarly, the second approach



Fig. 3.6: The polytope $P_{[0,3]}$.

$$1 + t + t^2 + t^3 + t^4 + t^5 + t^6 + t^7 + t^8 + t^9 + t^{10} + t^{11} + t^{12} + \dots$$

does not work well. The third, however, does not require much change compared to the first example:

$$G_{[0,10002]}(t) := \frac{1 - t^{10003}}{1 - t}.$$

If we try to do the same for the unbounded polyhedron $[0, \infty)$, then our first two approaches obviously become infeasible. However, the third turns out to be even shorter and more appealing:

$$G_{[0, \infty)}(t) := \frac{1}{1 - t}.$$

As this extended example suggests, the generating function we used to encode the lattice points will indeed provide a powerful bookkeeping tool for counting and enumerating lattice points in polytopes. We will back up this idea with more evidence for its usefulness in the next section. To actually count the points using this generating function we have to evaluate $G_{[0,3]}(t) = \frac{1-t^4}{1-t}$ at $t = 1$. Unfortunately, this is a zero of the denominator of the function. Even worse, we will see that this not just happens in this example, but it is always the case. Luckily, this singularity can always be removed, as we will later see.

For reasons that will soon become apparent we want to encode lattice points not only in polytopes, but more generally in any bounded or unbounded subset of \mathbb{R}^d . You should keep this in mind for the following considerations. In the above example of the one-dimensional cone $x \geq 0 \subseteq \mathbb{R}$ we have seen that we can use rational functions in one variable t to describe the infinite series of all monomials corresponding to the lattice points in the cone. We want to formalize this idea and generalize it to all dimensions. Let \mathbf{k} be some ground field (you can think of $\mathbf{k} = \mathbb{C}$). We assign the monomial

$$t^a := t_1^{a_1} t_2^{a_2} \dots t_d^{a_d}$$

in d variables to a lattice point $a = (a_1, \dots, a_d) \in \mathbb{Z}^d$. In the above example all lattice points were non-negative and thus lead to the “usual kind” of monomials. In general, coordinates a_i may be negative, so this is a *Laurent polynomial* living in the ring $L := \mathbf{k}[t_1^{\pm 1}, \dots, t_d^{\pm 1}]$. Moreover, note that the sum of monomials for the cone $x \geq 0$ is infinite. Since we do not care about convergence, we will consider our sums as series in a subset of the L -module $\hat{L} := \mathbf{k}[[t_1^{\pm 1}, \dots, t_d^{\pm 1}]]$ of *formal Laurent series*.

3.3.1 Example. Let P be the polygon

$$P := \text{conv} \begin{bmatrix} 0 & 2 & 2 & 3 \\ 1 & -1 & 2 & 0 \end{bmatrix}$$

(see Figure 3.7). We list the lattice points as monomials in the Laurent polynomial

$$\begin{aligned} & t_1^2 t_2^2 \\ & + t_2 + t_1 t_2 + t_1^2 t_2 \\ & + t_1 + t_1^2 + t_1^3 \\ & + t_1^2 / t_2. \end{aligned}$$

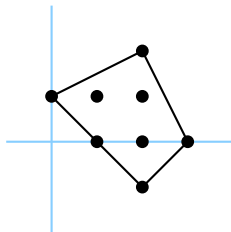


Fig. 3.7: The polygon of Example 3.3.1.

3.3.2 Definition (integer point series). For $S \subseteq \mathbb{R}^d$ the integer point series \widehat{G}_S is the formal Laurent series

$$\widehat{G}_S := \sum_{a \in S \cap \mathbb{Z}^d} t^a \in \widehat{L}.$$

A Laurent series $\widehat{G} \in \widehat{L}$ is *summable* if there is a Laurent polynomial $g \in L$ such that the series $g\widehat{G}$ is a Laurent polynomial.

Clearly all Laurent polynomials are summable. Translating a set $S \subseteq \mathbb{R}^d$ by some integral vector $a \in \mathbb{Z}^d$ amounts to multiplication of its generating series with t^a ,

$$\widehat{G}_{a+S}(t) = t^a \widehat{G}_S(t).$$

We will denote the set of all summable Laurent series by L^{sum} . We leave the proof of the following proposition to the reader in Exercise 3.1.

3.3.3 Proposition. L^{sum} is a L -submodule of \widehat{L} . □

We will consider summable series in the following only for (possibly half-open) cones and fundamental parallelepipeds. We discuss some important examples before we study the general case.

- (1) Consider first the polyhedron $P_\infty = [0, \infty)$ that we introduced above. The integer point series is

$$\widehat{G}_{P_\infty}(t) = \sum_{a \in \mathbb{Z}_{\geq}^d} t^a = 1 + t + t^2 + t^3 + \dots.$$

Using the polynomial $g(t) := (1 - t)$ we obtain $g(t)\widehat{G}_{P_\infty}(t) = 1$, so $\widehat{G}_{P_\infty}(t)$ is a summable series.

- (2) Now let $C := \text{cone}(e_1, e_2)$ for the standard unit vectors $e_1, e_2 \in \mathbb{R}^2$. Then

$$\widehat{G}_C(t, s) = \sum_{a, b \in \mathbb{Z}_{\geq}} t^a s^b = 1 + t + s + t^2 + s^2 + ts + t^3 + \dots.$$

Similar to the previous case we can use the polynomial $g(t, s) := (1 - t)(1 - s)$ to obtain $g(t, s)\widehat{G}_C(t, s) = 1$. Hence, $\widehat{G}_C(t, s)$ is a summable series.

- (3) Finally, let $V := \{a_1, \dots, a_d\}$ and $C = \text{cone } V$ be a rational cone. Let $x \in C$ and Π the fundamental parallelepiped given by V . By Proposition 3.2.5 we can write $x \in C \cap \mathbb{Z}^d$ uniquely as $x = y + z$ for $y \in \Pi$ and $z \in \mathbb{N}V$, and conversely, $y + z' \in C \cap \mathbb{Z}^d$ for any $z' \in \mathbb{N}V$. Furthermore,

$$\prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{z \in \mathbb{N}V} t^z = 1.$$

With this observation we can compute

$$\begin{aligned} \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{x \in C \cap \mathbb{Z}^d} t^x &= \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{y \in \Pi \cap \mathbb{Z}^d} \sum_{z \in \mathbb{N}V} t^{y+z} \\ &= \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{y \in \Pi \cap \mathbb{Z}^d} t^y \cdot \sum_{z \in \mathbb{N}V} t^z = \sum_{y \in \Pi \cap \mathbb{Z}^d} t^y. \end{aligned}$$

Hence, $\widehat{G}_C(t)$ is summable.

In Exercise 3.2 you will prove the following proposition.

3.3.4 Proposition. *There is a natural homomorphism from summable series to rational functions*

$$\Phi : L^{\text{sum}} \longrightarrow R := \mathbf{k}(t_1, \dots, t_d),$$

mapping \widehat{G} to f/g if $g\widehat{G} = f$ in \widehat{L} . □

3.3.5 Definition (integer point generating function). Suppose $C \subseteq \mathbb{R}^d$ is a point set so that $\widehat{G}_C(t)$ is summable. The *integer point generating function* of C is

$$G_C(t) := \Phi(\widehat{G}_C(t)).$$

L is a submodule of L^{sum} , and $\Phi|_L$ is the identity map. If $X \subseteq \mathbb{R}^d$ is bounded, then

$$G_X(t) = \sum_{a \in X \cap \mathbb{Z}^d} t^a,$$

so evaluating G_X at $t = \mathbf{1}$ gives the number of lattice points:

$$G_X(\mathbf{1}) = |X \cap \mathbb{Z}^d|.$$

In the one-dimensional example $P_\infty = [0, \infty)$ above we have already computed the image of the generating series in R , it is $G_{P_\infty}(t) = \frac{1}{1-t}$. In order to understand the situation for higher-dimensional cones $C \subseteq \mathbb{Z}^d$ we will use the half-open decomposition from Section 3.2. So we have to study the generating series for half-open simplicial cones. The following theorem generalizes our considerations for the general simplicial cone that we made in the third example above.

3.3.6 Theorem. *Let $V = \{v_1, \dots, v_d\} \subseteq \mathbb{Z}^d$ be a linearly independent set of primitive vectors, let $C = \text{cone } V$, and let $x \in \mathbb{R}^d$ be generic with respect to V . Then the integer point generating function of the half-open cone $C[x]$ is summable, and*

$$G_{C[x]}(t) = \frac{G_{\square(V,x)}(t)}{(1-t^{v_1})(1-t^{v_2}) \cdots (1-t^{v_d})}. \quad (3.3.1)$$

Proof. Let $\Lambda = \Lambda(V)$ be the lattice generated by V . By Proposition 3.2.5 every lattice point in $C[x]$ can be written uniquely as a sum of a Λ -point in C and a \mathbb{Z}^d -point in $\square(V, x)$. This translates into the following identity of summable formal power series:

$$\widehat{G}_{C[x]}(t) = \sum_{v \in \square(V,x) \cap \mathbb{Z}^d} \sum_{w \in C \cap \Lambda} t^{v+w} = \sum_{v \in \square(V,x) \cap \mathbb{Z}^d} t^v \sum_{w \in C \cap \Lambda} t^w.$$

Applying Φ yields the desired identity of rational functions. □

In particular, this covers the case $x \in \text{int}(C)$, which gives the integer point generating function for simplicial cones with fundamental parallelepiped $\Pi(V)$

$$G_{C[x]}(t) = \frac{G_{\Pi(V)}(t)}{(1-t^{v_1})(1-t^{v_2}) \cdots (1-t^{v_d})}. \quad (3.3.2)$$

3.3.7 Corollary. *Let C be a rational cone in \mathbb{R}^d , let \mathcal{T} be a triangulation of C into rational simplicial cones, and let $x \in C$ be generic. Then*

$$\widehat{G}_C(t) = \sum_{S \in \mathcal{T}[d]} \widehat{G}_{S[x]}(t), \text{ and } \widehat{G}_{\text{int } C}(t) = \sum_{S \in \mathcal{T}[d]} \widehat{G}_{S[x]}(t). \quad (3.3.3)$$

In particular, both series are summable, and equation (3.3.3) also holds on the level of rational functions.

Proof. Equation (3.3.3) is a translation of Proposition 3.2.8 into generating functions. By Theorem 3.3.6, all the summands are summable Laurent series. \square

Theorem 3.3.6 shows that the hard part of computing the integer point generating function \widehat{G} of a cone is to determine all integer points in the fundamental parallelepiped of the cone.

3.3.2 Counting Lattice Points in Polytopes

We have seen in Theorem 3.3.6 how we can encode lattice points in simplicial (half-open) cones. We want to use this to count integral points in dilations of a lattice polytope. The connection will be given by the following definition. The *cone over a polytope* is the cone

$$C(P) := \text{cone} \left(\begin{pmatrix} 1 \\ x \end{pmatrix} \mid x \in P \right).$$

See Figure 3.8 for the cone over a triangle. For any $k \geq 0$ we can recover the k -th dilate of P by intersecting $C(P)$ with the hyperplane $x_0 = k$, and the lattice points in kP by intersecting with $\{k\} \times \mathbb{Z}^d$. We want to connect this to the integer point generating function of the cone $C(P)$. To emphasize the special role of the additional variable t_0 , we write points in the cone in the form

$$\bar{t} := (t_0, t).$$

The 0th coordinate functional $u: \mathbb{Z}^{d+1} \rightarrow \mathbb{Z}$ yields the monomial substitution $\bar{t} = (t_0, 1, \dots, 1)$. Hence,

$$\widehat{G}_{C(P)}(t_0, 1) = 1 + \sum_{k \geq 1} |kP \cap \mathbb{Z}^d| t_0^k = 1 + \sum_{k \geq 1} \text{ehr}_P(k) t_0^k,$$

and the resulting power series in one variable is summable.

3.3.8 Definition. Let P be a lattice d -polytope. The *Ehrhart series* of P is the summable formal power series

$$\widehat{\text{Ehr}}_P(t) := 1 + \sum_{k \geq 1} \text{ehr}_P(k) t^k \in \mathbb{k}[[t]]$$

in one variable t . The corresponding rational function will be denoted $\text{Ehr}_P(t) := \Phi(\widehat{\text{Ehr}}_P(t)) \in \mathbb{k}(t)$.

We summarize the above observation in the following proposition.

3.3.9 Proposition. Let $P \subseteq \mathbb{R}^d$ be a lattice polytope, let \mathcal{T} be a triangulation of the cone $C(P)$ which is induced by a lattice triangulation of P , and let $x \in C(P)$ be generic. Then $\widehat{\text{Ehr}}_P(t)$ is summable with sum

$$\text{Ehr}_P(t) = G_{C(P)}(t, 1) = \frac{\sum_{S \in \mathcal{T}[d+1]} G_{\square(S, x)}(t, 1)}{(1-t)^{d+1}}. \quad (3.3.4)$$

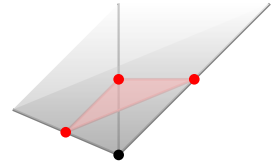


Fig. 3.8

Our next goal is to show that the Ehrhart counting function of a lattice polytope is given by a polynomial.

3.3.10 Proposition. *Let S be a d -simplex. Then*

$$\text{Ehr}_S(t) = \frac{h^*(t)}{(1-t)^{d+1}}$$

where h^* is a polynomial of degree $\leq d$ and $h^*(1) \neq 0$. Further, for $h^*(t) = \sum_{k=0}^d h_k^* t^k$, we have

$$h_k^* = \#(\Pi(C(S)) \cap \mathbb{Z}^{d+1} \cap \{x \mid x_0 = k\}).$$

Proof. Let S be a lattice simplex with vertex set $V := \{v_0, v_1, \dots, v_d\}$. We let $\bar{v}_i = (1, v_i)$, so that $C(S) = \text{cone}(\bar{v}_0, \bar{v}_1, \dots, \bar{v}_d)$ with fundamental parallelepiped $\Pi(V)$. Combining Proposition 3.3.9 with (3.3.2) we obtain that

$$\text{Ehr}_S(t) = \frac{h^*(t_0)}{(1-t_0)^{d+1}}$$

for some Laurent polynomial $h^*(t_0) = G_{\Pi(V)}((t_0, \mathbf{1}))$.

We need to examine the degree of t_0 in $G_{\Pi(V)}((t_0, t))$. The t_0 -degree of a monomial $\bar{t}^{\bar{a}}$ that appears in this Laurent polynomial is the first coordinate of the vector \bar{a} . As all \bar{v}_i have a 1 in the first coordinate and

$$\bar{a} = \lambda_0 \bar{v}_0 + \dots + \lambda_d \bar{v}_d$$

for some $0 \leq \lambda_0, \dots, \lambda_d < 1$, we know that the first coordinate a_0 of \bar{a} satisfies

$$0 \leq a_0 \leq \lambda_0 + \dots + \lambda_d < d + 1.$$

This implies that the t_0 -degree of $\bar{t}^{\bar{a}}$ is at most d . So evaluating $\widehat{G}_{\Pi(V)}(\bar{t})$ at $t = (t, 1, \dots, 1)$ results in a polynomial of degree at most d . Further, it has a non-zero constant coefficient, as

$$\widehat{G}_{\Pi(V)}((1, \dots, 1)) = |\Pi(V) \cap \mathbb{Z}^{d+1}|$$

and $\mathbf{0} \in \Pi(V)$.

The second claim follows from the above observation that the t_0 -degree of a monomial $\bar{t}^{\bar{a}}$ in $\widehat{G}_{\Pi(C(S))}(\bar{t})$ is the coordinate a_0 of the exponent \bar{a} . But this is exactly the height of \bar{a} in the cone $C(S)$. \square

3.3.11 Example. h^* of Δ_d .

To proceed we need a well-known result on generating functions.

3.3.12 Proposition. *Let $f, g : \mathbb{R} \rightarrow \mathbb{R}$ be such that*

$$\sum_{t=0}^{\infty} f(t) z^t = \frac{g(z)}{(1-z)^{d+1}}.$$

Then $f(t)$ is a polynomial of degree d if and only if $g(z) = g_0 + g_1 z + g_2 z^2 + \dots + g_d z^d$ is a polynomial of degree at most d with non-vanishing constant coefficient. In this case:

$$f(t) = g_0 \binom{t+d}{d} + g_1 \binom{t+d-1}{d} + \dots + g_d \binom{t}{d}.$$

Proof. We define the polynomials $f_j(t) := \binom{t+d-j}{d}$ for $0 \leq j \leq d$. The set $\{f_0, \dots, f_d\}$ is a basis of $\mathbb{R}[t]_{\leq d}$.

Let f be a polynomial of degree d . Then there are g_0, \dots, g_d such that

$$f(t) = \sum_{j=0}^d g_j f_j(t) = \sum_{j=0}^d g_j \binom{t+d-j}{d}.$$

The coefficient of t^d is $\frac{1}{d!} \sum g_j$, so this sum is non-zero. We compute

$$\begin{aligned} \sum_{t \geq 0} \sum_{j=0}^d g_j \binom{t+d-j}{d} z^k &= \sum_{j=0}^d g_j \sum_{t \geq 0} \binom{t+d-j}{d} z^k \\ &= \sum_{j=0}^d g_j \sum_{t \geq j} \binom{t+d-j}{d} z^k \\ &= \sum_{j=0}^d g_j \sum_{t \geq 0} \binom{t+d}{d} z^{t+j} = \sum_{j=0}^d g_j z^j \sum_{t \geq 0} \binom{t+d}{d} z^k \\ &= \frac{\sum_{j=0}^d g_j z^j}{(1-z)^{d+1}} = \frac{g(z)}{(1-z)^{d+1}} \end{aligned}$$

where the second equality follows as the binomial coefficient is 0 unless $k-j+1 \geq 0$. Clearly $\deg g \leq d$ and $g(1) = \sum g_j \neq 0$. The converse direction is similar. \square

Using this Proposition and a standard inclusion-exclusion argument which we leave to the reader, EHRHART's theorem is now proved.

3.3.13 Theorem (EHRHART's Theorem). Let P be a lattice polytope in \mathbb{R}^d . Then

$$\text{ehr}_P(t) = 1 + \sum_{k \geq 1} \text{ehr}_P(k) t^k = \frac{h^*(t)}{(1-t)^{d+1}}$$

where $\text{ehr}_P(t)$ is a polynomial of degree d , h^* is a polynomial of degree $\leq d$ with integer coefficients, and $h^*(1) \neq 0$.

By Proposition 3.3.12

$$\text{ehr}_P(t) = \binom{t+d}{d} + h_1^* \binom{t+d-1}{d} + \dots + h_{d-1}^* \binom{t+1}{d} + h_d^* \binom{t}{d}. \quad (3.3.5)$$

The previous result shows that the Ehrhart counting function $k \mapsto \text{ehr}_P(k)$ extends to a polynomial function $t \mapsto \text{ehr}_P(t)$. We will use the same symbol for these two functions.

3.3.14 Definition (Ehrhart polynomial). For a polytope P the polynomial $\text{ehr}_P(t)$ as in the previous theorem is the *Ehrhart polynomial* of P .

3.3.15 Definition (h^* -polynomial). The polynomial h^* that appears in the numerator of the rational generating function of the Ehrhart series is the h^* -polynomial of P .

Let P be a d -dimensional polytope and $\text{ehr}_P(t) := c_0 + c_1 t + c_2 t^2 + \dots + c_d t^d$ its Ehrhart polynomial with coefficients $c_0, c_1, \dots, c_d \in \mathbb{R}$.

3.3.16 Proposition. c_d is the volume of P .

Proof. This follows from a simple computation:

$$\begin{aligned} \text{vol}(P) &:= \int_P dx = \lim_{k \rightarrow \infty} \frac{1}{k^d} |P \cap \frac{1}{k} \mathbb{Z}^d| = \lim_{k \rightarrow \infty} \frac{1}{k^d} |kP \cap \mathbb{Z}^d| \\ &= \lim_{k \rightarrow \infty} \frac{1}{k^d} \text{ehr}_P(k) = c_d. \end{aligned} \quad \square$$

3.3.17 Definition. The *normalized volume* $\text{Vol}(P)$ of a d -dimensional lattice polytope P is $\text{Vol}(P) = d!c_d = d! \text{vol } P$.

Using (3.3.5) and the observation that, for any k , $\binom{t+d-k}{d}$ has degree d with leading coefficient 1, we get the following immediate consequence of this proposition.

3.3.18 Corollary. $h^*(1) = \sum_{i=0}^d h_i^* = \text{Vol}(P)$. \square

3.3.19 Corollary. Let P be a lattice d -polytope. Then the constant term of the Ehrhart polynomial is 1.

Proof. We evaluate (3.3.5) for $t = 0$. Note that by Theorem 3.3.23 the constant coefficient of h^* is 1. So we can compute

$$\text{ehr}_P(0) = \binom{d}{d} + h_1^* \binom{d-1}{d} + \cdots + h_{d-1}^* \binom{1}{d} + h_d^* \binom{0}{d} = \binom{d}{d} = 1. \quad \square$$

3.3.20 Corollary. Let P be a lattice d -polytope. Then $h_1^* = \text{ehr}_P(1) - d - 1 = |P \cap \mathbb{Z}^d| - d - 1$.

Proof. We evaluate (3.3.5) for $t = 1$:

$$\text{ehr}_P(1) = \binom{d+1}{d} + h_1^* \binom{d}{d} + \cdots + h_{d-1}^* \binom{2}{d} + h_d^* \binom{1}{d} = (d+1) + h_1^*. \quad \square$$

The proof of the following result is Exercise 3.7.

3.3.21 Corollary. Let P be a lattice d -polytope with Ehrhart polynomial $\text{ehr}_P(t) = 1 + c_1 t + c_2 t^2 + \cdots + c_d t^d$. Then $d!c_j \in \mathbb{Z}$ for $1 \leq j \leq d$.

3.3.22 Example. Note that c_1, \dots, c_{d-2} can be negative! As an example, consider the Reeve simplex $\text{conv}(\mathbf{0}, e_1, e_2, e_1 + e_2 + 18e_3)$. Then the Ehrhart polynomial is $1 - t + t^2 + 3t^3$.

Using disjoint decompositions into half open cones we can improve on Ehrhart’s theorem. This important result shows why the h^* -polynomial — albeit just a transformation of the Ehrhart polynomial — is often more convenient to work with.

3.3.23 Theorem (STANLEY’S Non-Negativity Theorem). Let P be a d -dimensional lattice polytope with

$$\widehat{\text{Ehr}}_P(t) = \frac{h_0^* + h_1^* t + h_2^* t^2 + \cdots + h_d^* t^d}{(1-t)^{d+1}}.$$

Then $h_1^*, \dots, h_d^* \geq 0$ and $h_0^* = 1$.

Proof. Let $C = C(P)$ be the cone over P . Let \mathcal{T} be a triangulation of C induced by a triangulation of P into lattice simplices. We have $v_0 = 1$ for all generators v of rays in \mathcal{T} .

Let $x \in C$ be generic with respect to \mathcal{T} . Then

$$\begin{aligned} \widehat{\text{Ehr}}_P(t) &= G_C(t, 1, \dots, 1) \\ &= \sum_{S \in \mathcal{T}[d+1]} G_{S[x]}(t, 1, \dots, 1) \\ &= \sum_{S \in \mathcal{T}[d+1]} \frac{G_{\square(S, x)}(t, 1, \dots, 1)}{\prod_{v \in V(S)} (1 - t^{v_0})} \\ &= \sum_{S \in \mathcal{T}[d+1]} \frac{\sum_{a \in \square(S, x) \cap \mathbb{Z}^{d+1}} t^{a_0}}{(1 - t)^{d+1}}. \end{aligned}$$

So the numerator polynomial of each summand has non-negative integral coefficients. A summand has non-zero constant coefficient if and only if there is a lattice point a in $\square(S, x)$ with $a_0 = 0$. By construction, this requires $a = \mathbf{0}$, so there is at most one such point in each cone. But $\mathbf{0} \in S[x]$ if and only if all coefficients are allowed to be 0, i.e. $x \in \text{relint } S$. This happens for exactly one cone, so $h_0^* = 1$. \square

Finally, let us note the following theorem proved by STANLEY in [26]. A completely different proof appears in (Beck, Sottile [6]). The reader can give a proof using the methods developed above in Exercise 3.9.

3.3.24 Theorem (STANLEY'S Monotonicity theorem). *Let P and Q be two lattice polytopes such that $P \subseteq Q$, $d = \dim Q$ and let h_P^* and h_Q^* be their h^* -polynomials. Then $h_{P,i}^* \leq h_{Q,i}^*$ for all $0 \leq i \leq d$.*

Proof. proof missing

3.3.3 Counting the Interior: Reciprocity

The interior of $L = [a, b]$ is $\text{int } L = (a, b)$. For integers a, b we can count the lattice points inside $\text{int } L$:

$$\text{ehr}_{\text{int } L}(k) = k(b - a) - 1.$$

Evaluating $\text{ehr}_L(k)$ at $-k$ for some positive integer k gives

$$\text{ehr}_L(-k) = (-k)(b - a) + 1 = -((-k)(b - a) - 1) = -\text{ehr}_{\text{int } L}(-k).$$

So for intervals the Ehrhart polynomial evaluated at negative integers counts (up to a sign) the lattice points in the interior of the interval. This would be a nice property, but maybe the example of an interval is too special to conjecture such a relation in general. So let us compute the interior lattice points in a more complicated example.

We consider the d -dimensional standard simplex Δ_d that we have already seen in the beginning of this chapter. We use the following observation to count lattice points in the interior Δ_d . When we only want to count the lattice points in the interior of the k -th dilate of the simplex, then we can also look at all lattice points, and leave out lattice points

- (1) that have a 0 among their coordinates, or
- (2) whose coordinates sum up to k .

This just means that we only want to count lattice points that satisfy the inequalities $x_i \geq 1$ for $1 \leq i \leq d$, and whose coordinates sum up to at most $k - 1$. Hence, we want to count lattice points in the set defined by the inequalities

$$x_i \geq 1 \quad \text{and} \quad \sum_{i=1}^d x_i \leq k - 1.$$

Translating this by $\mathbf{1}$ gives the simplex defined by the inequalities

$$x_i \geq 0 \quad \text{and} \quad \sum_{i=1}^d x_i \leq k - d - 1,$$

and this simplex clearly contains the same number of lattice points. We have computed this number above, so

$$\text{ehr}_{\text{int } \Delta_d}(k) = \binom{k-1}{d}.$$

So also the number of interior points is a polynomial in k of degree d . From

$$\binom{d-k}{d} = (-1)^d \binom{k-d+d-1}{d} = (-1)^d \binom{k-1}{d}$$

we can conclude that

$$\text{ehr}_{\text{int } \Delta_d}(k) = (-1)^d \text{ehr}_{\Delta_d}(-k).$$

We can make the same observation as for the interval: The lattice points in the interior of the k -th dilation of the simplex are (up to a sign) the evaluation at $-k$ of the Ehrhart polynomial!

Let us check one more example, before we attempt to prove our observation. Consider the standard unit cube C_d . Counting the interior points in this case is rather simple. We obtain

$$\text{ehr}_{\text{int } C}(k) = (k-1)^d = (-1)^d ((-k)+1)^d = (-1)^d \text{ehr}_C(-k),$$

and again, the number of lattice points in the interior is given by the Ehrhart polynomial evaluated at negative values.

Let $x = (x_1, \dots, x_d) \in (\mathbb{R}^d - \{0\})^d$. Then $\frac{1}{x}$ denotes the vector $(\frac{1}{x_1}, \dots, \frac{1}{x_d})$.

3.3.25 Lemma. Let $P \subseteq \mathbb{R}^d$ be a simplicial cone with primitive generators $V = \{v_1, \dots, v_d\}$, and let $x \in \mathbb{R}^d$ be generic.

Then the map

$$\begin{aligned} \alpha : \square(V, x) \cap \mathbb{Z}^{d+1} &\longrightarrow \square(V, x) \cap \mathbb{Z}^{d+1} \\ x &\longmapsto \sum_{i=0}^d v_i - x \end{aligned}$$

is a bijection.

Proof. Let $y \in \square(V, x)$, so y has a representation of the form

$$y = \sum_{v \in I} \lambda_v v + \sum_{v \in J} \mu_v v \quad \text{for } 0 < \lambda_v \leq 1, \ 0 \leq \mu_v < 1$$

Hence

$$\sum_{i=0}^d v_i - y = \sum_{v \in I} (1 - \lambda_v) v + \sum_{v \in J} (1 - \mu_v) v \in \square(V, x) \cap \mathbb{Z}^{d+1},$$

which proves the claim. \square

Let C be a polyhedral cone with a triangulation \mathcal{T} , and let $x \in C$ be generic with respect to \mathcal{T} . Then $C = \bigsqcup_{S \in \mathcal{T}[d]} S[x]$ is a decomposition of C into half-open simplicial cones.

3.3.26 Theorem (STANLEY'S Reciprocity Theorem). *Let C be a d -dimensional polyhedral cone with rational generators. Then*

$$G_C(t) = (-1)^d G_{\text{int } C} \left(\frac{1}{t} \right).$$

Proof. Let \mathcal{T} be a triangulation of C and $x \in C$ generic as above. For $S \in \mathcal{T}[d]$ let $V(S)$ be the set of primitive generators of S , and let $s(S) = \sum_{v \in V(S)} v$ denote their sum. Then, Lemma 3.3.25 implies

$$G_{\square(S, x)}(t) = \sum_{a \in \square(S, x) \cap \mathbb{Z}^d} t^a = \sum_{a \in \square(S, x) \cap \mathbb{Z}^d} t^{s(S) - a} = t^{s(S)} G_{\square(S, x)} \left(\frac{1}{t} \right).$$

We can just sum up this equation over all maximal cones to obtain the desired result:

$$\begin{aligned} G_C(t) &= \sum_{S \in \mathcal{T}[d]} G_{S[x]}(t) = \sum_{S \in \mathcal{T}[d]} \frac{G_{\square(S, x)}(t)}{\prod_{v \in V(S)} (1 - t^v)} = \sum_{S \in \mathcal{T}[d]} \frac{t^{s(S)} G_{\square(S, x)} \left(\frac{1}{t} \right)}{\prod_{v \in V(S)} (1 - t^v)} \\ &= (-1)^d \sum_{S \in \mathcal{T}[d]} \frac{G_{\square(S, x)} \left(\frac{1}{t} \right)}{\prod_{v \in V(S)} (1 - \frac{1}{t^v})} = (-1)^d \sum_{S \in \mathcal{T}[d]} G_{S[x]} \left(\frac{1}{t} \right) \\ &= (-1)^d G_{\text{int } C} \left(\frac{1}{t} \right). \quad \square \end{aligned}$$

Now we can state a theorem that formalizes our observation from the beginning of this section.

3.3.27 Theorem (EHRHART-MACDONALD Reciprocity). *Let P be a lattice d -polytope with Ehrhart polynomial $\text{ehr}_P(t)$, and let $k \in \mathbb{Z}_{>0}$. Then*

$$\text{ehr}_P(-k) = (-1)^d |\text{int } kP \cap \mathbb{Z}^d|.$$

The proof needs a little fact about the map Φ mapping summable Laurent series to rational functions.

3.3.28 Lemma. *Let f be a polynomial and g^+, g^- the rational functions corresponding to $\sum_{k \geq 0} f(k)t^k$ and $\sum_{k \leq -1} f(k)t^k$. Then $g^+(t) + g^-(t) \equiv 0$.*

Proof. It suffices to prove this for the basis $f_m := \binom{t+m}{m}$, $m \in \mathbb{N}$, of $\mathbb{R}[t]$. So pick some m . Then

$$\sum_{k \geq 0} f_m(k)t^k = \sum_{k \geq 0} \binom{k+m}{m} t^k = \frac{1}{(1+t)^{m+1}}.$$

We compute the other sum:

$$\begin{aligned}
 \sum_{k \leq -1} f_m(k) t^k &= \sum_{k \leq -1} \binom{k+m}{m} t^k = \sum_{k \geq 1} \binom{-k+m}{m} t^{-k} \\
 &= \sum_{k \geq 1} (-1)^m \binom{k-1}{m} t^{-k} = \sum_{k \geq m+1} (-1)^m \binom{k-1}{m} t^{-k} \\
 &= \sum_{k \geq 0} (-1)^m \binom{k+m}{m} t^{-k-m-1} = (-1)^m t^{-(m+1)} \sum_{k \geq 0} \binom{k+m}{m} t^{-k} \\
 &= (-1)^m t^{-(m+1)} \frac{1}{(1 - \frac{1}{t})^{m+1}} = \frac{(-1)^m}{t^{m+1} (1 - \frac{1}{t})^{m+1}} \\
 &= \frac{(-1)^m}{(t-1)^{m+1}} = \frac{(-1)^{m+1} (-1)^m}{(1-t)^{m+1}} \\
 &= -\frac{1}{(1-t)^{m+1}}. \quad \square
 \end{aligned}$$

Proof (Proof of the EHRHART-MACDONALD-Reciprocity, Theorem 3.3.27). We consider the generating function of the Ehrhart polynomial and compute:

$$\begin{aligned}
 \sum_{k \geq 1} \text{ehr}_{\text{int } P}(k) t^k &= \widehat{\text{Ehr}}_{\text{int } P}(t) = G_{\text{int } C(P)}(t, 1, \dots, 1) \\
 &\stackrel{3.3.26}{=} (-1)^{d+1} G_{C(P)}\left(\frac{1}{t}, 1, \dots, 1\right) = (-1)^{d+1} \widehat{\text{Ehr}}_P\left(\frac{1}{t}\right) \\
 &= (-1)^{d+1} \sum_{k \geq 0} \text{ehr}_P(k) \frac{1}{t^k} \stackrel{3.3.28}{=} (-1)^d \sum_{k \leq -1} \text{ehr}_P(k) \frac{1}{t^k} \\
 &= (-1)^d \sum_{k \geq 1} \text{ehr}_P(-k) t^k.
 \end{aligned}$$

Comparing coefficients in this equation gives the desired result. \square

Let us give some more applications regarding the h^* -polynomial.

3.3.29 Definition (Degree and Codegree). The *degree* of P is defined as

$$\deg(P) := \max(k \in \mathbb{N} : h_k^* \neq 0).$$

The *codegree* of P is defined as

$$\text{codeg}(P) := d + 1 - \deg(P).$$

Ehrhart’s theorem implies $0 \leq \deg(P) \leq d$, so $1 \leq \text{codeg}(P) \leq d + 1$. The degree of a lattice polytope can be seen as an algebraic measure of the complexity of a lattice polytope. Its concrete geometric interpretation is given by the codegree.

3.3.30 Corollary. The codegree of a d -dimensional lattice polytope equals the smallest positive integer k such that kP contains an interior lattice point.

Proof. This follows from Lemma 3.3.31 and Theorem 3.3.27. \square

3.3.31 Lemma. Let p be a polynomial of degree d with rational generating function

$$\sum_{t \geq 0} p(t) z^t = \frac{h_0^* + h_1^* z + h_2^* z^2 + \cdots + h_d^* z^d}{(1 - z)^{d+1}}$$

Then $h_d^* = h_{d-1}^* = \cdots = h_{k+1}^* = 0$ and $h_k \neq 0$ if and only if $p(-1) = p(-2) = \cdots = p(-(d-k)) = 0$ and $p(-(d-k+1)) \neq 0$. In this case, $h_k^* = p(-(d+1-k))$.

You will prove this result in Exercise 3.8. Applied to our situation this has the following immediate consequence.

3.3.32 Corollary. Let P be a lattice polytope. The highest non-zero coefficient $h_{\deg(P)}^*$ of h^* equals the number of lattice points in $\text{int } P$. \square

Finally, using reciprocity it is possible to compute the second highest coefficient of the Ehrhart polynomial.

3.3.33 Proposition. Let P be a lattice polytope with Ehrhart polynomial $\text{ehr}_P(t) = c_0 + c_1 t + c_2 t^2 + \cdots + c_d t^d$. Then c_{d-1} equals half of the normalized surface area of the boundary of P .

You will prove this result in Exercise 3.20.

3.3.4 Ehrhart polynomials of lattice polygons

As an example, we will completely classify Ehrhart polynomials of lattice polygons in this section. Essentially, the main work was already done in the previous chapter by proving Scott's inequality in Theorem 2.2.2. Now, we just have to exploit the properties of the h^* -polynomial.

3.3.34 Proposition. A polynomial $h_2^* t^2 + h_1^* t + 1$ for $h_1^*, h_2^* \in \mathbb{N}$ is the h^* -polynomial of a lattice polygon if and only if

- (1) $h_2^* = 0$ and h_1^* is arbitrary. Then P has no interior lattice points.
- (2) $h_2^* = 1$ and $h_1^* = 7$. Then $P \cong 3\Delta_2$.
- (3) $1 \leq h_2^* \leq h_1^* \leq 3h_2^* + 3$. Then P has interior lattice points.

Proof. Let us first show that these conditions are necessary. Note that h_2^* is the number of interior lattice points i , while $h_1^* = b + i - 3$, where b is the number of boundary lattice points. Moreover, $\text{vol}(P) = \text{Vol}(P)/2 = (1 + h_1^* + h_2^*)/2$. Hence, Scott's theorem tells us that, if $i \geq 1$ and $P \not\cong 3\Delta_2$, then $h_1^* \leq 3h_2^* + 3$. Finally, if $i \geq 1$, then $h_2^* = i \leq h_1^* = b + i - 3$, since $b \geq 3$.

It suffices to realize lattice polygons satisfying each of these conditions. For $i = 0$, any $b \geq 3$ can be realized by lattice polygons of the form as depicted in Figure 3.9. In fact, as Exercise 3.21 shows these are precisely the lattice polygons without interior lattice points.

Let $i \geq 1$. The condition $h_2^* \leq h_1^* \leq 3h_2^* + 3$ is equivalent to $3 \leq b \leq 2i + 6$. The case $b = 3$ is easy to realize, so let $b \geq 4$. Then any of these cases is realized by Figure 3.10. \square

All possible pairs (h_1^*, h_2^*) are depicted in Figure 3.11.

Let us now deduce all Ehrhart polynomials $c_2 t^2 + c_1 t + 1$ of lattice polygons. By Pick's Theorem 2.2.1 c_2 equals the area of P , and by Proposition 3.3.33, c_1 is half the number of boundary lattice points of P . The following theorem characterizes all pairs (c_1, c_2) that correspond to an Ehrhart polynomial of a polygon.

3.3.35 Corollary. A polynomial $c_2 t^2 + c_1 t + 1$ with $c_1, c_2 \in \frac{1}{2}\mathbb{Z}$ and $c_1 \geq \frac{3}{2}$ defines the Ehrhart polynomial of a lattice polygon P if and only if one of the following three conditions is satisfied:

- (1) $c_1 - c_2 = 1$. Then P has no interior lattice points.
- (2) $c_1 = c_2 = 9/2$. Then P is $3\Delta_2$.
- (3) $c_1 \leq c_2/2 + 2$. Then P has interior lattice points.

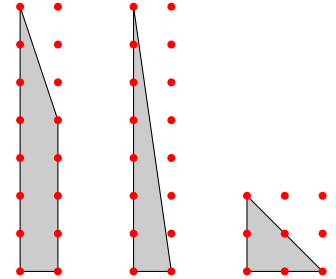


Fig. 3.9

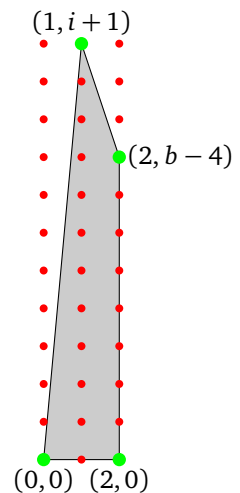


Fig. 3.10: Lattice polygons realizing $4 \leq b \leq 2i + 6$

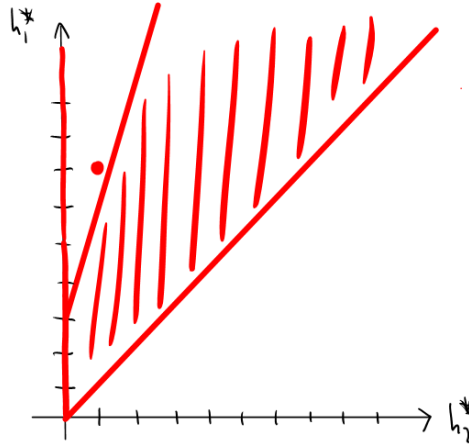


Fig. 3.11: (h_2^*, h_1^*) of lattice polygons

3.4 The Theorem of Brion

The goal of this final section is the celebrated Theorem of BRION. It relates for any lattice d -polytope the integer point generating functions of all vertex cones of P to the integer point generating function of the polytope.

Let P be a rational d -dimensional polytope and F a face of P . The tangent cone of F in P is the cone

$$T_F P := \{x \mid \exists p \in F, \varepsilon > 0 : p + \varepsilon(x - p) \in P\}.$$

The tangent cone is the common intersection of all supporting half-spaces at F . Note that the tangent cones are not cones in the usual sense, as their apex is not in the origin. We call them *affine cone* if we want to emphasize this. We can use a point $x \in F$ to shift the cone into the origin.

3.4.1 Proposition. *The shifted cone $T_F P - x$ is dual to the normal cone of F .*

Proof: proof missing

We can use the generating series of tangent cones to compute the generating series of the polytope.

3.4.2 Theorem (Brianchon-Gram). *Let P be a rational d -polytope. Then*

$$\widehat{G}_P(t) = \sum_{F \preceq P} (-1)^{\dim F} \widehat{G}_{T_F P}(t),$$

where the sum is over all non-empty faces of P .

Proof: Think of the Laurent polynomial on the left hand side as an infinite Laurent series that contains all possible monomials, but most coefficients are 0. To prove this relation we compare coefficients of an arbitrary monomial t^m on both sides. Let $f(P) := (f_0(P), \dots, f_d(P))$ be the f -vector of P . We have to distinguish the two cases $m \in P$ and $m \notin P$.

(1) $m \in P$: Then $m \in T_F P$ for any face F of P . Hence, the coefficient of t^m on the right hand side is

$$\sum_{F \preceq P} (-1)^{\dim F} = \sum_{i=0}^d (-1)^i f_i = 1,$$

where the last equality follows from EULER'S relation.

- (2) $m \notin P$: See Figure 3.12. Let $S := \{F \preceq P \mid m \text{ is beyond } F\}$ be the set of faces such that x violates any supporting hyperplane of F . Then

$$m \in T_F P \iff F \notin S.$$

Define $K := \{G \prec P \mid \text{there is } F \in S \text{ such that } G \prec F\}$.

Then K is a polyhedral complex. Let $f(K) := (f_0(K), \dots, f_d(K))$ be its face vector. The coefficient of t^m is

$$\sum_{i=0}^d (-1)^i (f_i(P) - f_i(K)) = 1 - \sum_{i=0}^d (-1)^i f_i(K) = 1 - 1 = 0.$$

□

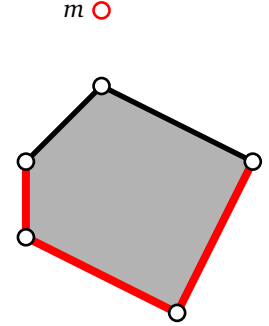


Fig. 3.12: $m \notin P$. The complex S is drawn in red.

Now recall the map $\Phi: \widehat{\mathbb{L}} \rightarrow \mathbb{R}$ that we introduced in Section 3.3.1. There we have only applied it to *pointed* polyhedral cones. We now want to study this map also in the case of cones that have a nontrivial lineality space. Recall that for a cone C the *lineality space* is defined as $\text{lin}(C) := C \cap (-C)$. It is the maximal linear subspace contained in C .

We start with a simple example that explains the basic idea of our next theorem. Consider the sets

$$C^+ := [0, \infty) \subseteq \mathbb{R} \quad C^- := 3 - C^+ = (-\infty, 3] \quad P := [0, 3].$$

C_0 is a one-dimensional cone, and P is the intersection of C_0 and C^- , $P = C^+ \cap C^-$. We compute the integer point generating function and the image under Φ for C^+ and C^- :

$$\begin{aligned} \widehat{G}_{C^+}(t) &= \sum_{k \geq 0} t^k & \widehat{G}_{C^-}(t) &= \sum_{k \leq 3} t^k = t^3 \sum_{k \leq 0} t^k = t^3 \sum_{k \geq 0} t^{-k} \\ G_{C^+}(t) &= \Phi(\widehat{G}_{C^+}(t)) = \frac{1}{1-t} & G_{C^-}(t) &= \Phi(\widehat{G}_{C^-}(t)) = t^3 \frac{1}{1-\frac{1}{t}} = \frac{-t^4}{1-t} \end{aligned}$$

The integer point generating function of P is the finite geometric series

$$\widehat{G}_P(t) = G_P(t) = \frac{1-t^4}{1-t} = 1 + t + t^2 + t^3.$$

We observe that

$$G_P(t) = G_{C^+}(t) + G_{C^-}(t).$$

Using the construction of the map Φ we can make the following symbolic calculation

$$\begin{aligned} G_P(t) &= \Phi(\widehat{G}_{C^+}(t)) + \Phi(\widehat{G}_{C^-}(t)) = \Phi(\widehat{G}_{C^+}(t) + \widehat{G}_{C^-}(t)) \\ &= \Phi(\widehat{G}_{\mathbb{R}+P}(t)) = \Phi(\widehat{G}_{\mathbb{R}}(t)) + \Phi(\widehat{G}_P(t)) \end{aligned}$$

This can only hold if $\Phi(\widehat{G}_{\mathbb{R}}(t)) = 0$, i.e. if Φ maps the infinite series $\sum_{k \in \mathbb{Z}} t^k$ to 0. The following proposition shows that this indeed holds in general for cones with nontrivial lineality space.

3.4.3 Proposition. *Let $C \subseteq \mathbb{R}^d$ be a polyhedral cone with integer point series $\widehat{G}_C(t)$. If $\text{lineal } C \neq \{0\}$ then $\Phi(\widehat{G}_C) = 0$.*

Proof. Let $v \in \text{lineal}(C) - \{0\}$. Then $\mathbb{R}v \subseteq C$, so that

$$t^v \widehat{G}_C(t) = \widehat{G}_C(t).$$

Applying the map Φ gives

$$t^v \Phi(\widehat{G}_C(t)) = \Phi(\widehat{G}_C(t)) \iff (1 - t^v) \Phi(\widehat{G}_C(t)) = 0.$$

$v \neq 0$ implies $\Phi(\widehat{G}_C) = 0$. \square

We can apply the observation of this proposition to obtain a very simple formula for the integer point generating function of a polytope.

3.4.4 Theorem (Brion). *Let P be a rational d -polytope. Then*

$$G_P(t) = \sum_{v \text{ vertex of } P} G_{T_v P}(t).$$

Proof. Apply the map Φ to both sides of the Brianchon-Gram Identity of Theorem 3.4.2. The only non-pointed tangent cones are those originating from a vertex of P , so by Proposition 3.4.3 only the contributions of the vertices are non-zero on the right hand side. \square

3.4.5 Example. Let P be the $[0, 1]$ -square in \mathbb{R}^2 . See Figure 3.13. Then

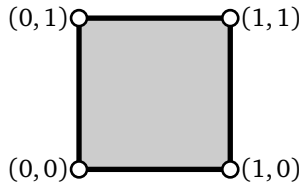


Fig. 3.13

$$\begin{aligned} G_P(x, y) &= \frac{1}{(1-x)(1-y)} + \frac{x}{(1-\frac{1}{x})(1-y)} + \frac{y}{(1-x)(1-\frac{1}{y})} + \frac{xy}{(1-\frac{1}{x})(1-\frac{1}{y})} \\ &= \frac{1}{(1-x)(1-y)} + \frac{-x^2}{(1-x)(1-y)} + \frac{-y^2}{(1-x)(1-y)} + \frac{x^2 y^2}{(1-x)(1-y)} \\ &= \frac{(1-x^2)(1-y^2)}{(1-x)(1-y)} = 1 + x + y + xy \end{aligned}$$

So $G_P(1, 1) = 1 + 1 + 1 + 1 = 4$.

The theorem provides us with a general method to explicitly compute the function $G_P(t)$. We have seen in Corollary 3.3.6 how we can compute the integer point generating series of a simplicial cone. To use this formula in the Theorem of Brion we triangulate the polytope P , and compute the generating function of each simplex in the triangulation (including the lower dimensional ones). We then sum up the generating functions using the principle of inclusion-exclusion.

3.5 Computing the Ehrhart Polynomial: Barvinok's Algorithm

Now we want to discuss an algorithm to compute the number of integral points in a polytope, due to Barvinok [1] and Barvinok and Pommersheim [4]. If the dimension is fixed, then the algorithm is polynomial in the input size. The algorithm is implemented in the software package LattE [10, 17].

3.5.1 Basic Version of the Algorithm

The basic idea of the algorithm is to use BRION's Theorem and a *signed* decomposition of cones to compute the multivariate rational generating function $G_P(t)$ of the lattice points in a polytope P . Counting then amounts to evaluating $G_P(t)$ at $t = 1$. This however cannot be done by just inserting 1 in the rational function, as 1 is always a pole of $G_P(t)$. We need tools from complex analysis to evaluate.

You can use $G_P(t)$ also to solve linear programs. If you want to maximize over a functional $c \in \mathbb{Z}^d$, then you can just substitute $t = (z^{c_1}, z^{c_2}, \dots, z^{c_d})$. The highest degree of a monomial in the result is the optimal solution.

To use BRION's Theorem, we have to compute the integer point generating functions of all vertex cones. So we need a polynomial method (in fixed dimension) to compute integer point generating functions of cones. We know how to do this if the cone is simplicial. The formula is just given by Theorem 3.3.6. To compute the generating function for general cones we have to break them into simplicial ones, preferably unimodular, or close to this, as we have to enumerate lattice points in their fundamental parallelepipeds. However, we may need exponentially many unimodular simplicial cones in a triangulation of a cone. It suffices to look at dimension 2 to see this. Consider the cone $C := \text{conv}(e_1, e_1 + ke_2)$ for some $k \in \mathbb{Z}_{>}$. We need k cones in a unimodular triangulation.

An exponential number of cones necessarily leads to an exponential running time for our algorithm. If we want a polynomial algorithm we need a better way to subdivide. So here is the key idea of the algorithm. Instead of just triangulating cones, we use *signed* decompositions. It was the achievement of Barvinok [1] to show that with this method you can get away with a polynomial number of (even unimodular) cones.

To make this precise, let P be a d -dimensional lattice polytope and v a vertex of P with tangent cone $C' := T_v P = v + C$ for a linear cone C spanned by primitive rays v_1, \dots, v_d . We define the *index* of the cone C to be

$$\begin{aligned} \text{Index}(C) &:= \#(\Pi(v_1, \dots, v_d) \cap \mathbb{Z}^d) \\ &= |\det(v_1, \dots, v_d)| \\ &= \text{vol } \Pi(v_1, \dots, v_d) \end{aligned}$$

The cone C is unimodular if and only if $\text{Index}(C) = 1$, so we have to continue subdividing C as long as $\text{Index}(C) > 1$. Furthermore, if F is a face of C then $\text{Index}(F) \leq \text{Index}(C)$.

To proceed, we need an important theorem due to Minkowski. It is the fundamental theorem in Geometry of Numbers, which is the topic of the next chapter. We postpone the proof until then (see Theorem 4.1.2), and just state (a slightly simplified version of the) theorem.

3.5.1 Theorem. *Let $K \subseteq \mathbb{R}^d$ be compact convex and centrally-symmetric with $\text{vol } K \geq 2^d$. Then there exists a $\neq 0$ in $K \cap \mathbb{Z}^d$.* \square

If $\text{Index}(C) > 1$, then $K := \frac{1}{\sqrt[d]{\text{Index } C}} \{ \sum \lambda_i v_i \mid -1 \leq \lambda_i \leq 1 \}$ has volume $\text{vol}(K) = 2^d$. Hence, by Minkowski's Theorem there is $w \in K \cap \mathbb{Z}^d$ different from 0 . Then

$$w = \alpha_1 v_1 + \alpha_2 v_2 + \dots + \alpha_d v_d \quad \text{for} \quad 0 \leq |\alpha_i| \leq (\text{Index}(C))^{\frac{1}{d}}.$$

Unfortunately, the proof of Minkowski's theorem is not constructive, and it is generally difficult to compute such a point w . We will deal with one option later in detail, the LLL-algorithm of Lenstra, Lenstra, and Lovasz. here, we only state the result. For a full treatment check the next Section 3.5.2.

3.5.2 Proposition (LLL). Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice. Then there is a constant M only depending on d such that we can find a basis v_1, \dots, v_d of Λ in time $\mathcal{O}(d^6 \log^3 l)$, where l is the length of the longest vector among the v_i with

$$\|v_1\| \cdot \dots \cdot \|v_d\| \leq M \det \Lambda$$

The constant M is quite large. We will prove later that we can take $M = 2^{\frac{1}{2}\binom{d}{2}}$. Given such a short basis we can find a shortest lattice vector by a finite enumeration. This needs the following lemma.

3.5.3 Lemma. Let Λ be a lattice and v_1, \dots, v_d a short basis given by the previous proposition, together with the constant M . Let $w \in \Lambda \setminus \{0\}$ be a shortest lattice vector. Then

$$w = \sum_{i=1}^d \lambda_i v_i \text{ with } |\lambda_i| \leq \sqrt{d} M.$$

Proof. Let v_1 be shortest among v_1, \dots, v_d and V the matrix with columns v_1, \dots, v_d . Then $w = V\lambda$ for $\lambda = (\lambda_1, \dots, \lambda_d)$. Hence, $\lambda = V^{-1}w$. By Cramer's rule all entries of V^{-1} are determinants of $(d-1) \times (d-1)$ -minors of V , divided by $\det V$. So each entry of V^{-1} is bounded by

$$\|v_2\| \cdot \dots \cdot \|v_d\| \cdot \frac{1}{\det V} \leq \frac{M}{\|v_1\|}.$$

So

$$|\lambda_j| \leq \sum_i |\lambda_i| \frac{M}{\|v_1\|} \leq \sqrt{d} \|w\| \frac{M}{\|v_1\|} \leq \sqrt{d} M (\|w\| \leq \|v_1\|) \quad \square$$

Hence, to find a shortest lattice vector we compute a short basis and enumerate all $N := (2\sqrt{d}M)^d$ possibilities for the coefficients of the shortest vector.

3.5.4 Lemma. Suppose v_1, \dots, v_d is a basis of the lattice Λ such that

$$\|v_1\| \cdot \dots \cdot \|v_d\| \leq M \det \Lambda,$$

and let $u \in \Lambda \setminus \{0\}$ be a shortest vector. Then $u = \sum_{i=1}^d \lambda_i v_i$ with $|\lambda_i| \leq \sqrt{d} M$. In particular, there are less than $N = (\sqrt{d} M)^d$ many candidates for u .

Proof. Assume v_1 is shortest among the v_i . Denote the matrix with columns v_i by V . Then $\lambda = V^{-1}u$. The entries of V^{-1} are $(d-1) \times (d-1)$ -minors of V , divided by $\det \Lambda$. Hence, they are bounded in absolute value by $\|v_2\| \cdot \dots \cdot \|v_d\| / \det \Lambda \leq M / \|v_1\|$.

Therefore, $|\lambda_j| \leq \sum_{i=1}^d |u_i| M / \|v_1\| \leq \sqrt{d} \|u\| M / \|v_1\| \leq \sqrt{d} M$ for all j as $\|u\| \leq \|v_1\|$. \square

This leads to the following theorem.

3.5.5 Theorem. In fixed dimension d we can find $w \in \Pi_0 \cap \mathbb{Z}^d$, $w \neq 0$ in time polynomial in $\log^3 \max(\|v_i\|)$.

By replacing w with $-w$ if necessary we can assume that w, v_1, \dots, v_d lie in a common half-space, and that w is primitive. By construction, $|\lambda_i| \leq (\text{Index } C)^{-\frac{1}{d}}$. We define new cones

$$C_j := \text{cone}(v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_d) \quad \text{for} \quad 1 \leq j \leq d.$$

We compute the index of these new cones:

$$\begin{aligned}
 \text{Index } C_j &= |\det(v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_d)| \\
 &= \sum_{k=1}^d |\lambda_k| \cdot |\det(v_1, \dots, v_{j-1}, v_k, v_{j+1}, \dots, v_d)| \\
 &= |\lambda_j| \cdot |\det(v_1, \dots, v_d)| \\
 &= |\lambda_j| (\text{Index } C) \leq (\text{Index } C)^{-\frac{1}{d}} (\text{Index } C) \\
 &= (\text{Index } C)^{\frac{d-1}{d}}
 \end{aligned}$$

and the right hand side is strictly less than $\text{Index } C$ if $\text{Index } C \geq 2$. We define a corresponding sign function to make a signed subdivision of C with the cones C_j .

$$\varepsilon_i := \begin{cases} 0 & \text{if } \dim C_j < d \\ 1 & \text{if } \det(v_1, \dots, v_d) = \det(v_1, \dots, v_{j-1}, w, v_{j+1}, \dots, v_d) \\ -1 & \text{otherwise.} \end{cases}$$

We can use this decomposition to write the integer point generating series as a signed sum via

$$\widehat{G}_C(t) = \sum_{j=1}^d \varepsilon_j \widehat{G}_{C_j}(t) + \text{lower dimensional contributions.}$$

In this decomposition we have

- ▷ at most d d -dimensional cones,
- ▷ at most $2^d d$ cones of any dimension.

We repeat this decomposition for each cone of index ≥ 2 . After n steps of this procedure, any cone in the decomposition has index at most $(\text{Index } C)^{\left(\frac{d-1}{d}\right)^n}$. For a unimodular triangulation we want this to be less than 2 (recall that the index is integral, so it must be 1).

$$\begin{aligned}
 (\text{Index } C)^{\left(\frac{d-1}{d}\right)^n} &\stackrel{!}{<} 2 \text{ for unimodular decomposition} \\
 \iff \left(\frac{d-1}{d}\right)^n \lg_2(\text{Index } C) &< \lg_2 2 = 1 \\
 \iff n \lg_2 \left(\frac{d-1}{d}\right) + \lg_2 \lg_2(\text{Index } C) &< 0 \\
 \iff \lg_2 \lg_2(\text{Index } C) &< n \lg_2 \left(\frac{d}{d-1}\right) \\
 \text{choose } n > \left\lceil \frac{\lg_2 \lg_2(\text{Index } C)}{\lg_2 \left(\frac{d}{d-1}\right)} \right\rceil + 1 &= \mathcal{O}(d \lg_2 \lg_2 \text{Index } C).
 \end{aligned}$$

Then $(\text{Index } C)^{\left(\frac{d-1}{d}\right)^n} < 2$, so all indices in the decomposition are 1. In this decomposition we have

$$\begin{aligned}
 (d2^d)^n &= 2^{nd \lg_2 d} \leq 2^{Md^2 \lg_2 d \lg_2 \lg_2 \text{Index } C} \\
 &= (\lg_2 \text{Index } C)^{Md^2 \lg_2 d}
 \end{aligned}$$

Algorithm 3.5.1: Barvinok's Algorithm: Original Version

Input: A polyhedron $P = \{x \mid Ax \leq b\}$ with vertices v_1, \dots, v_k .

Output: The integer point generating function for P as

$$G_P(t) = \sum_{i \in I} \varepsilon_i \frac{t^{a_i}}{(1 - t^{v_{i1}}) \cdots (1 - t^{v_{ik_i}})}$$

for $\varepsilon_i \in \{-1, 1\}$, $a_i, v_{ij} \in \mathbb{Z}^d$.

```

for  $i \leftarrow 1$  to  $k$  do
    Compute vertex cone  $C_i$  at vertex  $v_i$ ;
    Triangulate  $C_i$  into  $k_i$  simplicial cones  $C_{ij}$ ;
    for  $j \leftarrow 1$  to  $k_i$  do
        do a signed decomposition of  $C_{ij}$  into unimodular cones  $C_{ij}^k$ ;
        compute the unique interior point  $a_{ij}^k$  in  $C_{ij}^k$ ;
    endfor
    sum up the contributions using the inclusion-exclusion principle;
endfor
sum up the contributions using the inclusion-exclusion principle;
    
```

$$= (\lg_2 \text{Index } C)^{\mathcal{O}(d^2 \lg_2 d)}.$$

cones. Hence, in fixed dimension, the number of cones is bounded by a polynomial in $\lg_2 \text{Index } C$, which is the input size. We summarize the algorithm in Algorithm 3.5.1 and the following theorem.

3.5.6 Theorem. *Let $d \in \mathbb{Z}_{>}$ be fixed. Then there is a polynomial time algorithm that computes the integer point generating function $G_P(t)$ in the form*

$$G_P(t) := \sum_{i \in I} \varepsilon_i \frac{t^{a_i}}{(1 - t^{v_{i1}}) \cdots (1 - t^{v_{id}})},$$

where $\varepsilon_i \in \{-1, 1\}$, $a \in \mathbb{Z}^d$, $v_{ij} \in \mathbb{Z}^d - \{0\}$ for all i, j , for any d -dimensional polyhedron P given in its exterior description.

We finally need to discuss how we can evaluate our generating function at **1**.

- ▷ Evaluate at $t = (1, \dots, 1)$: $\frac{t^u}{\prod_j (1 - t^{v_j})}$
 Make univariate: $t_j \mapsto z^{\lambda_j}$ for some $\lambda = (\lambda_1, \dots, \lambda_d)$. New exponent in denominator is $z^{\langle v_j, \lambda \rangle}$ (choose λ such that $d_j := \langle v_j, \lambda \rangle \neq 0 \ \forall v_j$)
 \rightsquigarrow this gives $\frac{z^n}{\prod_j (1 - z^{d_j})} \xleftarrow{\text{at } z=1} \text{replace } z = x + 1 \rightsquigarrow \text{expansion at } x = 0$

3.5.2 A versatile tool: LLL

Here, we describe an efficient way to construct a lattices basis sharing several nice properties from any given lattice basis. The algorithm was first described by Arjen Lenstra, Hendrik Lenstra and László Lovász in 1982 [19], and it is known as the LLL-algorithm.

3.5.7 Proposition. *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice. Then there is a vector $v \in \Lambda \setminus \{0\}$ such that*

$$\|v\| \leq \sqrt{d} (\det \Lambda)^{1/d}.$$

Proof. Follows from Minkowski's Theorem 4.1.2. proof missing □

We fix some notation. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with a basis $v_1, v_2, \dots, v_d \in \mathbb{R}^d$. The order of the basis vectors is important for the following considerations. We consider the increasing chain of subspaces

$$V_0 := \{0\} \quad V_k := \text{lin}(v_1, \dots, v_k) \quad \text{for } 1 \leq k \leq d.$$

We define the induced lattices $\Lambda_k := \Lambda \cap V_k$ and the invariant

$$D(v_1, \dots, v_d) := \prod_{j=1}^d \det \Lambda_j.$$

3.5.8 Lemma. *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with basis v_1, \dots, v_d . Let $\lambda_1 := \min_{u \in \Lambda \setminus \{0\}} (\|u\|)$. Then*

$$D(v_1, \dots, v_d) \geq \lambda_1^{\binom{d}{2}} \prod_{i=1}^d i^{-i/2}.$$

Proof. Clearly $\lambda_1 \leq \min_{u \in \Lambda_j \setminus \{0\}} (\|u\|)$ for all $1 \leq j \leq d$. From Proposition 3.5.7 we conclude

$$\det \Lambda_j \geq \frac{\|v_j\|^j}{\sqrt{j^j}} \geq \frac{\lambda_1^j}{\sqrt{j^j}}.$$

Multiplying the last equation for all $1 \leq j \leq d$ gives the lemma. \square

Let $\pi_k := \mathbb{R}^d \rightarrow V_k$ be the orthogonal projection onto V_k . We define

$$w_k := v_k - \pi_{k-1}(v_k)$$

for $1 \leq k \leq d$. This is the GRAM-SCHMIDT-orthogonalization of v_1, \dots, v_d . The vectors w_1, \dots, w_d are pairwise orthogonal, so

$$\det \Lambda = \prod_{i=1}^d \|w_i\| \quad \text{and} \quad \det \Lambda_k = \prod_{i=1}^k \|w_i\|.$$

By construction, we can find coefficients $\lambda_{ij} \in \mathbb{R}$, $1 \leq j < i \leq d$ such that

$$v_i = w_i + \sum_{j=1}^{i-1} \lambda_{ij} w_j. \quad (3.5.1)$$

3.5.9 Definition ((weakly) reduced basis). The basis v_1, \dots, v_d of Λ is *weakly reduced* if $|\lambda_{ij}| \leq 1/2$ for all $1 \leq j < i \leq d$.

It is *reduced* if in addition it satisfies

$$d(\cdot/2)(v_k, V_{k-1}) \leq \frac{4}{3} d(\cdot/2)(v_{k+1}, V_k) \quad (3.5.2)$$

for $1 \leq k \leq d-1$.

Geometrically a basis is reduced if the vector v_{j+1} is not much closer to the subspace spanned by the first $k-1$ basis vectors than the vector v_j . For an orthogonal basis of the vector space we could find a permutation such that the distances strictly increase. The condition for a weakly reduced basis is a relaxation of this. We prove the following theorem.

3.5.10 Theorem (Lenstra, Lenstra, Lovász, 1982). *Any lattice basis can be transformed into a reduced basis in polynomial time.*

We need some preparations for the proof of this theorem. Consider the representation of our given basis in (3.5.1). Assume that for some pair of indices $l < k$ the coefficient λ_{kl} is larger than $1/2$. Then there is a unique $\mu_{kl} \in \mathbb{R}$ and $a_{kl} \in \mathbb{Z}$ such that

$$|\mu_{kl}| \leq 1/2 \quad \lambda_{kl} = a_{kl} + \mu_{kl}.$$

We replace v_k by $v_k - a_{kl}v_l$. This leaves the subspaces V_l , $0 \leq j \leq n$ and the GRAM-SCHMIDT orthogonalization w_1, \dots, w_n invariant, and the sets

$$v_1, \dots, v_j$$

are still a basis of the lattice Λ_j . So the only coefficients in the representation (3.5.1) that might change are those involved in the representation of v_k ,

$$v_k - a_{kl}v_l = w_k + \sum_{j=1}^{k-1} \lambda_{kj}w_j - a_{kl}v_l.$$

The vector v_l is in the subspace V_l , so it has a representation

$$v_l = \sum_{j=1}^l \eta_j w_j.$$

$v_l - w_l \in V_{l-1}$, so $\eta_l = 1$. This implies that

$$v_k - a_{kl}v_l = w_k + \sum_{j=1}^l (\lambda_{kj} - \eta_j)w_j + \sum_{j=l+1}^{k-1} \lambda_{kj}w_j,$$

and $|\lambda_{kl} - \eta_l| = |\lambda_{kl} - a_{kl}| \leq 1/2$. So the new coefficient is weakly reduced, and to achieve this we apart from λ_{kl} only had to change coefficients λ_{kj} for $j < k$. So always starting with the largest index k that has a coefficient λ_{kl} such that $|\lambda_{kl}| > 1/2$ gives us a weakly reduced basis. There are $\binom{d}{2}$ coefficients, and reducing λ_{kl} with the above procedure we have to touch at most $l \leq d$ other coefficients, so this process terminates after at most $\mathcal{O}(d^3)$ steps. We summarize this in the following proposition.

3.5.11 Proposition. *Any lattice Λ has a weakly reduced basis. More precisely, we can transform any basis into a weakly reduced one in time $\mathcal{O}(d^3)$.* \square

We can use the construction of a weakly reduced basis as an intermediate step for a reduced basis. If in a weakly reduced basis a pair of vectors v_j, v_{j+1} violates the condition given in (3.5.2), then we can fix this by exchanging v_k and v_{k+1} in the basis. However, the new basis might not be weakly reduced anymore, so we make it weakly reduced with the previous algorithm. We repeat these two steps until we reach a reduced basis.

The algorithm clearly outputs a reduced basis if it terminates. So to prove Theorem 3.5.10 we only have to show that it terminates after an polynomial number of steps. We use the invariant $D(v_1, \dots, v_d) := \prod_{j=1}^d \det \Lambda_j$ introduced above and show that each iteration of the algorithm reduces it by a factor of $\sqrt{3}/2$. As Proposition 3.5.7 gives a lower bound only depending on the dimension of the lattice, this will prove the theorem.

Algorithm 3.5.2: Weakly Reduced Basis

Input: A lattice basis v_1, \dots, v_d .
Output: A weakly reduced lattice basis v'_1, \dots, v'_d
 Compute the GRAM-SCHMIDT orthogonalization w_1, \dots, w_d ;
 Compute coefficients λ_{ij} , $1 \leq j < i \leq d$ such that $v_i = \sum_{j=1}^i \lambda_{ij} w_j$;
while Basis not reduced **do**
 Let k be the largest index such that $|\lambda_{kl}| > 1/2$;
 Let $\mu_{kl} \in \mathbb{R}$, $a_{kl} \in \mathbb{Z}$ such that $|\mu_{kl}| < 1/2$, $\lambda_{kl} = \mu_{kl} + a_{kl}$;
 Determine η_j , $1 \leq j \leq l$ with $v_l = \sum \eta_j w_j$;
 Replace $\lambda_{kj} \leftarrow \lambda_{kj} - \eta_j$ for $1 \leq j \leq l$;
endw
return v_1, \dots, v_d ;

Let us determine the change in $D := D(v_1, \dots, v_d)$ after one iteration. Making a basis weakly reduced does not change the subspaces V_i and the lattices Λ_i , hence it also does not change D . So assume that v_j and v_{j+1} satisfy

$$d(\cdot 2)(v_k, V_{k-1}) > \frac{4}{3} d(\cdot 2)(v_{k+1}, V_k)$$

and let v'_1, \dots, v'_d be the basis obtained by exchanging v_j and v_{j+1} , i.e.

$$v'_{j+1} := v_j \quad v'_j := v_{j+1} \quad v'_i := v_i \quad \text{for } i \neq j, j+1.$$

Let w'_1, \dots, w'_d be its GRAM-SCHMIDT orthogonalization and V'_i , Λ'_i be the new subspaces and lattices, $1 \leq i \leq d$. Then

$$V'_i = V_i \quad \Lambda'_i = \Lambda_i \quad \text{for } i \neq j,$$

while

$$V'_j := \text{lin}(v'_1, \dots, v'_{j-1}, v'_j) = \text{lin}(v_1, \dots, v_{j-1}, v_{j+1}).$$

Consequently, the vectors w_j and w'_j satisfy

$$\|w'_j\| < \frac{\sqrt{3}}{2} \|w_j\|$$

while for all other i we have $w'_i = w_i$. Hence

$$\det \Lambda'_j < \frac{\sqrt{3}}{2} \det \Lambda_j,$$

so also

$$D(v'_1, \dots, v'_d) < D(v_1, \dots, v_d).$$

Together with the lower bound for $D(v_1, \dots, v_d)$ in Proposition 3.5.8 this proves Theorem 3.5.10. We collect some nice consequences of a reduced basis.

3.5.12 Proposition. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with reduced basis v_1, \dots, v_d . Let w_1, \dots, w_d be its GRAM-SCHMIDT orthogonalization. Then

$$\|w_j\|^2 \leq \|v_j\|^2 \leq \|w_j\|^2 + \frac{1}{4} \sum_{i=1}^{j-1} \|w_i\|^2 \quad \text{for } 1 \leq j \leq d$$

Algorithm 3.5.3: LLL

Input: A lattice basis $V := \{v_1, \dots, v_d\}$.
Output: A reduced lattice basis v'_1, \dots, v'_d .
 Make V weakly reduced (Algorithm 3.5.2);
while V not reduced **do**
 Find a pair v_j, v_{j+1} that violates (3.5.2) and exchange the two vectors;
 Make the basis weakly reduced;
endw
return V ;

$$\|w_j\|^2 \geq \frac{1}{2} \|w_{j-1}\|^2 \quad \text{for } 2 \leq j \leq d.$$

Proof. By the definition of a weakly reduced basis we have

$$v_j = w_j + \sum_{k=1}^{j-1} \lambda_{jk} w_k$$

for coefficients $-1/2 \leq \lambda_{kj} \leq 1/2$. Taking the norm and using that the scalar product of any two of the w_i 's is 0 implies

$$\|v_j\|^2 = \|w_j\|^2 + \sum_{k=1}^{j-1} \lambda_{jk}^2 \|w_k\|^2 \leq \|w_j\|^2 + \frac{1}{4} \sum_{k=1}^{j-1} \|w_k\|^2.$$

This proves the first inequality. Further, we have

$$\begin{aligned} d((v)_j, V_{j-1})^2 &= \|w_j\|^2 \\ d((v)_{j+1}, V_{j-1})^2 &= \|w_{j+1}\|^2 + \lambda_{j+1,j}^2 \|w_j\|^2 \leq \|w_{j+1}\|^2 + \frac{1}{4} \|w_j\|^2. \end{aligned}$$

By assumption

$$d((v)_{j+1}, V_{j-1})^2 \geq \frac{3}{4} d((v)_j, V_{j-1})^2$$

so

$$\|w_{j+1}\|^2 + \frac{1}{4} \|w_j\|^2 \geq \frac{3}{4} \|w_j\|^2$$

The second inequality follows. □

3.5.13 Corollary. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with reduced basis v_1, \dots, v_d . Then

$$\prod_{i=1}^d \|v_i\| \leq 2^{\frac{1}{2} \binom{d}{2}} \det \Lambda.$$

Proof. We compute

$$\|v_j\|^2 \leq \|w_j\|^2 + \frac{1}{4} \sum_{k=1}^{j-1} \|w_k\|^2 \leq \|w_j\|^2 \left(1 + \frac{1}{4} \sum_{k=1}^{j-1} 2^{j-k} \right) \leq 2^{j-1} \|w_j\|^2$$

and

$$\begin{aligned} \prod_{j=1}^d \|v_j\| &\leq \prod_{j=1}^d 2^{j-1} \|v w_j\|^2 \\ &= 2^{\frac{1}{2}\binom{d}{2}} \prod_{j=1}^d j = 1^d \|w_j\| \leq 2^{\frac{1}{2}\binom{d}{2}} \det \Lambda. \end{aligned} \quad \square$$

3.5.14 Proposition. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with a reduced basis v_1, \dots, v_d . Let $\lambda_1 := \min_{a \in \Lambda - \{0\}} \|a\|$ be the first successive minimum of the lattice and assume we have a vector $x \in \Lambda$ with $\|x\| \leq \alpha \lambda_1$ for some $\alpha \geq 1$ and $x = \sum_{i=1}^d \eta_i v_i$. Then

$$|\eta_i| \leq 2^{\frac{d-1}{2}} \left(\frac{3}{2}\right)^{d-i} \alpha \leq 3^d \alpha \quad \text{for } 1 \leq i \leq d.$$

Proof. proof missing \square

3.6 Problems

3.1 The goal of this exercise is to give a proof of Proposition 3.3.3.

- (1) Show that the set L^{sum} of summable Laurent series is an L -submodule of \hat{L} , i.e. show that for $f \in L$ and $g, h \in L^{\text{sum}}$ also $f \cdot g$ and $g + h$ are summable.
- (2) Prove that this turns Φ into a homomorphism of L -modules, i.e. show that $\Phi(f \cdot g) = f \Phi(g)$ and $\Phi(f + g) = \Phi(f) + \Phi(g)$.

3.2 Prove that there is a natural homomorphism from summable series to rational functions

$$\Phi : \hat{L} \longrightarrow R := \mathbf{k}(x_1, \dots, x_d),$$

mapping \widehat{G} to f/g if $g\widehat{G} = f$ in \hat{L} .

3.3 Let P be a lattice polytope with Ehrhart polynomial $\text{ehr}_P(t)$. Compute the Ehrhart polynomial of the bipyramid over P .

3.4 Compute the Ehrhart polynomial of the cross polytope.

3.5 A simplex which is unimodularly equivalent to the standard simplex is called unimodular. A triangulation is unimodular if all its simplices are.

- (1) For a k -dimensional unimodular simplex Δ and $t \in \mathbb{Z}_{\geq 1}$ show that

$$|\mathbb{Z}^k \cap \text{relint}(t\Delta)| = \binom{t-1}{k}.$$

- (2) Suppose P admits a unimodular triangulation \mathcal{T} with $f_0(\mathcal{T})$ vertices, $f_1(\mathcal{T})$ edges, \dots , $f_d(\mathcal{T})$ d -simplices. Show that

$$\text{ehr}_P(t) = \sum_{k=0}^d f_k(\mathcal{T}) \binom{t-1}{k}.$$

- (3) Conclude that any two unimodular triangulations have the same f -vector (f_0, \dots, f_d) .

3.6 Let P be a lattice d -polytope. Show that the leading coefficient of the Ehrhart polynomial $\text{ehr}_P(t)$ equals the volume $\text{vol } P$ of the polytope.

3.7 Prove Corollary 3.3.21.

3.8 Prove Lemma 3.3.31.

3.9 Prove Theorem 3.3.24.

3.10 For integers p, q with $\gcd(p, q) = 1$ define the tetrahedron

$$\Delta_{pq} = \text{conv} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & p \\ 0 & 0 & 0 & q \end{bmatrix}.$$

(1) Argue that its vertices are its only lattice points. (White proved a converse: every lattice tetrahedron with only four lattice points is unimodularly equivalent to a Δ_{pq} .)

(2) Compute the Ehrhart polynomial and the h^* -polynomial of Δ_{pq} .

(3) For which parameters are Δ_{pq} and $\Delta_{p'q'}$ unimodularly equivalent?

3.11 A simplex which is unimodularly equivalent to the standard simplex is called unimodular. A triangulation is unimodular if all its simplices are.

For a k -dimensional unimodular simplex Δ and $t \in \mathbb{Z}_{\geq 1}$ show that

$$|\mathbb{Z}^k \cap \text{relint}(t\Delta)| = \binom{t-1}{k}.$$

Suppose P admits a unimodular triangulation \mathcal{T} with $f_0(\mathcal{T})$ vertices, $f_1(\mathcal{T})$ edges, \dots , $f_d(\mathcal{T})$ d -simplices. Show that

$$\text{ehr}_P(t) = \sum_{k=0}^d f_k(\mathcal{T}) \binom{t-1}{k}.$$

Conclude that any two unimodular triangulations have the same f -vector (f_0, \dots, f_d) .

3.12 Determine the Ehrhart polynomial $\text{ehr}_{\diamond_d}(t)$ of the d -dimensional cross-polytope $\diamond_d = \text{conv}[\pm e_1, \dots, \pm e_d]$.

3.13 Let P be a d -dimensional lattice polytope in \mathbb{R}^d . We define the *lattice pyramid* over P as

$$\text{Pyr}(P) := \text{conv}(P \times \{0\}, e_{d+1}) \subseteq \mathbb{R}^{d+1},$$

where e_1, \dots, e_{d+1} is the standard basis of \mathbb{R}^{d+1} . Show that $h_{\text{Pyr}(P)}^* = h_P^*$.

3.14 Let $m \in \mathbb{Z}_{\geq 1}$. Use Exercise 3.13 to show that

$$f_m(k) := \sum_{j=1}^k j^m$$

is a polynomial in k . What is its degree and leading coefficient?

3.15 Let P be a d -dimensional lattice polytope with Ehrhart polynomial $\sum_{k=0}^d c_k t^k$. Show that

$$c_{d-1} = \frac{1}{2} \text{vol}(\partial P).$$

Here, $\text{vol}(\partial P)$ denotes the surface area of P , namely,

$$\text{vol}(\partial P) := \sum_{F \in \mathcal{F}(P)} \text{vol}(F),$$

where $F(P)$ is the set of facets of P and $\text{vol}(F)$ denotes the (non-normalized) volume with respect to the lattice $\text{aff}(F) \cap \mathbb{Z}^d$. For instance, note that $\text{vol}(\text{conv}((1, 0), (0, 1)))$ equals 1 and not $\sqrt{2}$. Hence,

$$\text{vol}(\partial \text{conv}((1, 0), (0, 1), (-1, 0), (0, -1))) = 4.$$

3.16 Let P be a d -dimensional lattice polytope. Show that

$$\text{codeg}(P) := d + 1 - \deg(P) = \min\{k \in \mathbb{N}_{\geq 1} : \text{int}(kP) \cap \mathbb{Z}^d \neq \emptyset\},$$

and

$$h_d^*(P) = |\text{int}(\text{codeg}(P)P) \cap \mathbb{Z}^d|.$$

(Hint: Use reciprocity.)

3.17 Calculate the h^* -polynomial of an empty 3-dimensional lattice polytope P with a vertices and of normalized volume b . Here *empty* means that any lattice point in P is a vertex of P . Deduce the h^* -polynomials of the tetrahedra Δ_{pq} of Exercise 2.2. Check that you get the same solution for the Ehrhart polynomial as before :-)

3.18 Let Q, P be lattice polytopes with $Q \subseteq P$. Show that there exists a triangulation of P that restricts to a triangulation of Q .

(Hint: Let \mathcal{V} denote the set of vertices. Choose first a generic regular triangulation $w : \mathcal{V}(Q) \rightarrow \mathbb{R}$, leading to linear functions l_σ on simplices σ of the triangulation. Now, choose generic values of w on $\mathcal{V}(P) \setminus \mathcal{V}(Q)$ such that $w(v) > l_\sigma(v)$ for all σ in the triangulation of Q and vertices $v \in \mathcal{V}(P) \setminus \mathcal{V}(Q)$.)

3.19 Let Q, P be lattice polytopes with $Q \subseteq P$. Show Stanley's monotonicity theorem:

$$h_Q^* \leq h_P^* \text{ coefficientwise.}$$

(Hint: Choose a triangulation as in the previous exercise.)

3.20 Prove Proposition 3.3.33.

3.21 Let P be a lattice polygon. Show that P has no interior lattice points if and only if P is unimodular equivalent to $2\Delta_2$ or it is unimodularly equivalent to $\text{conv}((0, 0), (a, 0), (0, 1), (0, b))$ for some $a, b \geq 0$.

3.22 Apply Brion's identity to

$$P := \text{conv} \begin{bmatrix} 0 & 2 & 2 & 3 \\ 1 & -1 & 2 & 0 \end{bmatrix}$$

and verify that both rational functions coincide (you may want to use a computer for this).

Geometry of Numbers

4

Geometry of numbers deals with the relation between two objects: convex bodies on the one hand, and lattices on the other hand. A typical question in this area is whether and how the volume and the number of lattice points of convex body are related.

The term “geometry of numbers” was coined by Minkowski who used convex geometric methods, in particular his fundamental theorem 4.1.2, in order to bound class numbers in algebraic number theory. In the 20th century geometry of numbers has grown into an established field of research with connections into many branches of mathematics.

While most of the theory treats general convex bodies, in these notes we will focus on those tools which we need to prove results that apply only to lattice polytopes.

4.1 Minkowski’s Theorems

In this section, we prove the basic Theorem 4.1.2 which was the starting point of the theory. We conclude with some applications and extensions which we will need in the next sections. Throughout, $\Lambda \subseteq \mathbb{R}^d$ is a lattice of rank d (the reader may think of \mathbb{Z}^d).

4.1.1 Theorem (Blichfeldt, 1914). *Let $S \subseteq \mathbb{R}^d$ be a (Lebesgue measurable) set with $\text{vol } S > \det \Lambda$. Then there are $p, q \in S$, $p \neq q$, such that $p - q \in \Lambda$.*

Proof. Choose a fundamental parallelepiped $\Pi := \Pi(\Lambda)$ of Λ . Then $\det \Lambda = \text{vol } \Pi$. For any $x \in \Lambda$ let

$$S_x := \{y \in \Pi \mid x + y \in S\} = \Pi \cap (S - x)$$

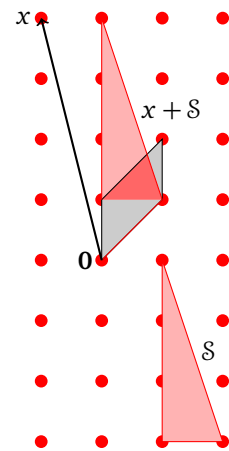


Fig. 4.1

The sets $(x + \Pi) \cap \mathcal{S}$ cover \mathcal{S} without overlap (by Corollary 1.3.11). Hence,

$$\text{vol } \mathcal{S} = \sum_{x \in \Lambda} \text{vol}((x + \Pi) \cap \mathcal{S}) = \sum_{x \in \Lambda} \text{vol } \mathcal{S}_x.$$

Assume that $\mathcal{S}_x \cap \mathcal{S}_y = \emptyset$ for all $x, y \in \Lambda$, $x \neq y$. Then

$$\text{vol} \left(\bigcup_{x \in \Lambda} \mathcal{S}_x \right) = \sum_{x \in \Lambda} \text{vol } \mathcal{S}_x = \text{vol } \mathcal{S} > \text{vol } \Pi.$$

This is a contradiction to $\bigcup_{x \in \Lambda} \mathcal{S}_x \subseteq \Pi$. Hence, there exist $x, y \in \Lambda$, $x \neq y$, such that $\mathcal{S}_x \cap \mathcal{S}_y \neq \emptyset$. Let a be the point in the intersection and $p := a + x$, $q := a + y$. Then $p, q \in \mathcal{S}$ and $p - q = x - y$ is a non-zero lattice point. \square

4.1.2 Theorem (Minkowski's First Theorem, 1896). Let $K \subseteq \mathbb{R}^d$ be convex and centrally-symmetric with $\text{vol } K > 2^d \det \Lambda$. Then there exists a $\neq 0$ in $K \cap \Lambda$.

If K is also compact, then it suffices to assume $\text{vol } K \geq 2^d \det \Lambda$.

Proof. Let $T := \frac{1}{2}K$. Then $\text{vol } T = \frac{\text{vol } K}{2^d} > \det \Lambda$. Hence, by Blichfeldt's Theorem 4.1.1, there are $p, q \in K$ such that

$$x := \frac{1}{2}p - \frac{1}{2}q = \frac{1}{2}(p + (-q))$$

is a non-zero lattice point. By central symmetry of K , $-q \in K$, so $x \in K$ by convexity of K .

Let K be compact and $\text{vol } K = 2^d \det \Lambda$. For any $k \geq 1$, applying the previous argument yields a non-zero lattice point $x_k \in \frac{k+1}{k}K \subseteq 2K$. Compactness of $2K$ yields the existence of a converging subsequence $(x_{k_i})_{i \geq 1}$. Since Λ is discrete, this sequence gets stationary, i.e., $x_{k_i} =: x$ for all $i \geq i_0$. In particular, $0 \neq x \in \Lambda$. On the other hand, $x = \lim_{i \rightarrow \infty} \frac{k_i}{k_i+1} x_{k_i} \in K$. \square

Centrally-symmetric convex bodies with the origin as their only interior lattice point which have maximal volume $2^d \det(\Lambda)$ are also called *extremal bodies*. Minkowski's theorem does not tell us how to find the integral point, it just tells us it exists. There are polynomial time algorithms to explicitly find such a point, but only for a much larger volume bound. See Section 3.5.2 on the LLL-Algorithm for a method. Finding a short lattice vector is a very important problem in integer optimization and in cryptography, see e.g. [23, 22, 14]

4.1.3 Definition (Successive Minima). Let $K \in \mathcal{C}$. For $1 \leq k \leq d$ we define the k -th successive minimum of K to be the number

$$\lambda_k := \inf_{\lambda > 0} \{\dim \text{lin}(\lambda K \cap \Lambda) \geq k\}.$$

Then

$$\lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_d.$$

Note that $\lambda_1 > 0$ as Λ is discrete. The following corollary is equivalent to 4.1.2.

4.1.4 Corollary. Let $K \in \mathcal{C}$. Then

$$\lambda_1^d \text{vol } K \leq 2^d \det \Lambda.$$

It is non-trivial to sharpen this bound in the following way.

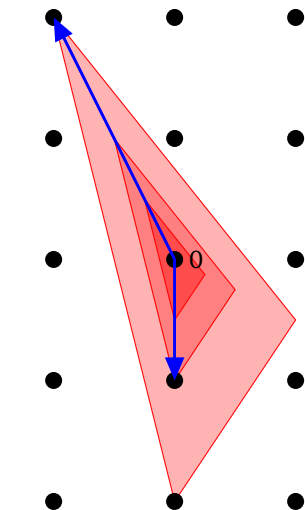


Fig. 4.2: A triangle in the plane together with two scaled copies with scaling factors λ_1 and λ_2 .

4.1.5 Theorem (Minkowski's Second Theorem, 1896). *Let $K \in \mathcal{C}$. Then*

$$\frac{1}{d!} \cdot 2^d \det \Lambda \leq \lambda_1 \cdots \lambda_d \operatorname{vol} K \leq 2^d \det \Lambda.$$

We will not prove this much stronger theorem here. We will, however need a refinement of Minkowski's first Theorem due to van der Corput (Theorem 4.1.7 below). For this we have to extend Theorem 4.1.1 first.

4.1.6 Theorem (Generalized Blichfeldt's theorem). *Let $S \subseteq \mathbb{R}^d$ be a (Lebesgue measurable) set with $\operatorname{vol}(S) > m \det(\Lambda)$ for a positive integer m . Then there exist $m + 1$ distinct points $p_1, \dots, p_{m+1} \in S$ such that $p_i - p_j \in \Lambda$ for all i, j .*

Proof. By considering a sufficiently large subset, we may assume that S is bounded. We define Π and S_x (for $x \in \Lambda$) as in the proof of Theorem 4.1.1. Let id_x be the indicator function on S_x (i.e., it evaluates to one on S_x and zero elsewhere). We define the function

$$f := \sum_{x \in \Lambda} \operatorname{id}_x.$$

Note that this is well-defined, since $S_x \neq \emptyset$ for only finitely many $x \in \Lambda$. Hence,

$$\begin{aligned} \int_{\Pi} f \, dx &= \sum_{x \in \Lambda} \int_{\Pi} \operatorname{id}_x \, dx = \sum_{x \in \Lambda} \operatorname{vol}(S_x) \\ &= \sum_{x \in \Lambda} \operatorname{vol}(S \cap (x + \Pi)) = \operatorname{vol}(S). \end{aligned}$$

Since $\int_{\Pi} 1 \, dx = \operatorname{vol}(\Pi) = \det(\Lambda)$, our assumption yields that there has to exist some point $y \in \Pi$ with $f(y) > m$. Since f only evaluates to integers, we get $f(y) \geq m + 1$. In particular, there exist $x_1, \dots, x_{m+1} \in \Lambda$ such that $y \in S_{x_1} \cap \dots \cap S_{x_{m+1}}$. Therefore, defining $p_i := y + x_i \in S$ for $i = 1, \dots, m + 1$ yields $m + 1$ points which have the desired properties. \square

4.1.7 Theorem (van der Corput, 1935). *Let $K \subseteq \mathbb{R}^d$ be a centrally symmetric convex set with $\operatorname{vol}(K) > m 2^d \det(\Lambda)$ for a positive integer m . Then there exist m distinct pairs of non-zero lattice points $\pm x_1, \dots, \pm x_m$ in K .*

Proof. Let $T := \frac{1}{2}K$. Then $\operatorname{vol} T = \frac{\operatorname{vol} K}{2^d} > m \det \Lambda$. Hence, by Blichfeldt's Theorem 4.1.6, there are $m + 1$ distinct points $p_1, \dots, p_{m+1} \in T$ such that $p_i - p_j \in \Lambda$ for all i, j . Choose $x_i := p_i - p_{m+1}$ for $i = 1, \dots, m$ as the desired lattice points. Note that $x_i = p_i + (-p_{m+1}) \in T + T = K$. \square

4.1.8 Corollary. *Let $K \subseteq \mathbb{R}^d$ be a centrally symmetric convex set. Then*

$$\operatorname{vol}(K) \leq (|\operatorname{int} K \cap \mathbb{Z}^d| + 1) 2^{d-1}.$$

Let us finish this section with another of Minkowski's gems.

4.1.9 Theorem (Minkowski, 1910). *Let $K \subseteq \mathbb{R}^d$ be a centrally symmetric convex set with $\operatorname{int}(K) \cap \Lambda = \{0\}$. Then $|K \cap \Lambda| \leq 3^d$.*

Proof. We may choose $\Lambda = \mathbb{Z}^d$. Assume the statement fails. We consider the map $\varphi : \mathbb{Z}^d \rightarrow (\mathbb{Z}/3\mathbb{Z})^d$ given by assigning each coordinate its congruence class modulo 3. This is a homomorphism (so $\varphi(x \pm y) = \varphi(x) \pm \varphi(y)$). Note that $(\mathbb{Z}/3\mathbb{Z})^d$ has 3^d elements. Hence, by the pigeon hole principle there exist two distinct lattice points $x, y \in \mathbb{Z}^d$ with $\varphi(x) = \varphi(y)$. Therefore, $\varphi(x - y) = 0$, thus

$$p := \frac{x - y}{3} \in \Lambda$$

Since K is centrally-symmetric, $0 \neq p = \frac{x}{3} + \frac{-y}{3} \in \frac{2}{3}K$, a contradiction. \square

Recently, it was shown that up to unimodular transformations the standard cube $[-1, 1]^d$ is the only centrally-symmetric lattice polytope with $\text{int}(K) \cap \Lambda = \{0\}$ and $|K \cap \Lambda| = 3^d$ [12].

4.2 Lattice packing and covering

In this section, we will give a short discussion about lattices and metric geometry (mainly following [Barvinok2008]). This is the first point in the book where Λ really is meant to be a (non-standard) lattice in \mathbb{R}^d . An interesting geometric application can be found in the next section.

Usually, when dealing with lattice polytopes we start with an *abstract* lattice $\Lambda \cong \mathbb{Z}^d$ and associate an *abstract* vector space $\Lambda \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{R}^d$ with the volume form which evaluates as $1/d!$ on a fundamental domain of Λ . In particular, note that the 'length' of a vector is not well-defined. In general, we define the *dual lattice* as

$$\Lambda^* := \text{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$$

and the *dual vector space* as

$$(\Lambda \otimes_{\mathbb{Z}} \mathbb{R})^* := \text{Hom}_{\mathbb{R}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R}, \mathbb{R}).$$

Note that the dual lattice naturally sits inside of the dual vector space. While these definitions are abstract, they stress the point that in general it is not necessary and often misleading to identify dual spaces or lattices.

In contrast, in lattice theory the viewpoint is opposite to ours. The starting point is an euclidean vector space, say, \mathbb{R}^d with the usual scalar product $\langle \cdot, \cdot \rangle$. Now, the choice of the *embedded* lattice matters! For instance, their determinants differ. In this section, we will follow this convention.

So, let $\Lambda \subseteq \mathbb{R}^d$ be a lattice of full rank, and we assume that we have a scalar product $\langle \cdot, \cdot \rangle$. Now, we can identify \mathbb{R}^d and $(\mathbb{R}^d)^*$:

$$\mathbb{R}^d \cong (\mathbb{R}^d)^*, \quad x \rightarrow \langle \cdot, x \rangle.$$

In particular, we get under this identification

$$\Lambda^* = \{x \in \mathbb{R}^d : \langle x, y \rangle \in \mathbb{Z} \forall y \in \Lambda\} \subseteq \mathbb{R}^d.$$

Note that while $\Lambda^{**} = \Lambda$, it may happen that $\Lambda^* \neq \Lambda$. For instance, if $\Lambda = \mathbb{Z}^d/2$, then $\Lambda^* = 2\mathbb{Z}^d$.

Here is the first important definition from lattice theory. Using the notion of successive minima we can define the packing radius of a lattice.

4.2.1 Definition. The *packing radius* of Λ is defined as

$$\varrho(\Lambda) := \frac{1}{2} \lambda_1(\mathcal{B}_1(\mathbf{0}), \Lambda).$$

Thus, the packing radius equals one half of the length of a shortest lattice vector. In other words, the packing radius is the largest r such that \mathbb{R}^d is filled by congruent non-overlapping balls of radius r centered at the lattice points. Here is the dual notion to successive minima.

4.2.2 Definition. For a convex body $K \subseteq \mathbb{R}^d$, we define $\mu_k(K, \Lambda)$ as the infimum over all $\tau > 0$ such that

$$(\Lambda + \tau K) \cap L \neq \emptyset$$

for every $(d - k)$ -dimensional affine subspace $L \subseteq \mathbb{R}^d$. An important instance is the *covering radius*, which is defined as

$$\mu(\Lambda) := \mu_d(\mathcal{B}_1(\mathbf{0}), \Lambda).$$

In other words, the covering radius equals the smallest r such that \mathbb{R}^d is covered by congruent balls of radius r centered at the lattice points. Equivalently, $\mu(\Lambda)$ equals the largest possible distance of a point in \mathbb{R}^d from the closest lattice point nearby.

In the following, we are interested in relations between the following invariants: $\det(\Lambda), \det(\Lambda^*), \varrho(\Lambda), \varrho(\Lambda^*), \mu(\Lambda), \mu(\Lambda^*)$. Let us start with an observation, which we leave to the reader as an exercise.

4.2.3 Lemma. $\det(\Lambda) \det(\Lambda^*) = 1$.

Our first result shows that if we fix the determinant, then the packing density cannot be too large.

4.2.4 Proposition. *The covering radius satisfies $\varrho(\Lambda) \leq \frac{1}{2} \sqrt{d} \det(\Lambda)^{1/d}$.*

Proof. Our task is to determine a radius for a ball centered at the origin that guarantees that the ball contains another (non-zero) lattice point. We want to use Minkowski's theorem for this. Clearly,

$$\left[-\frac{r}{\sqrt{d}}, \frac{r}{\sqrt{d}} \right]^d \subseteq \mathcal{B}_r(\mathbf{0})$$

so that

$$\text{vol } \mathcal{B}_r(\mathbf{0}) > \frac{2^d r^d}{\sqrt{d}^d}.$$

If we choose $r := \sqrt{d} \det(\Lambda)^{1/d}$, then

$$\text{vol } \mathcal{B}_r(\mathbf{0}) \geq 2^d \det(\Lambda).$$

So by Minkowski's Theorem 4.1.2 there is a non-zero lattice point in this ball. This proves the claim. \square

Combining with Lemma 4.2.3 this yields:

4.2.5 Corollary.

$$\varrho(\Lambda) \varrho(\Lambda^*) \leq \frac{d}{4}. \quad \square$$

The main result of this section are the following bounds:

4.2.6 Theorem.

$$\frac{1}{4} \leq \mu(\Lambda) \varrho(\Lambda^*) \leq \frac{1}{4} \sqrt{\sum_{k=1}^d k^2} \leq \frac{d^{\frac{3}{2}}}{4}.$$

The proof of the middle inequality is inductive and relies on the following lemma.

4.2.7 Lemma. Let $0 \neq u \in \Lambda$ be primitive. We consider the orthogonal projection

$$\begin{aligned} \pi : \mathbb{R}^d &\rightarrow u^\perp \cong \mathbb{R}^{d-1} \\ x &\mapsto x - \frac{\langle x, u \rangle}{\langle u, u \rangle} u \end{aligned}$$

Then

- (1) $\Lambda_1 := \pi(\Lambda)$ is a lattice of rank $d - 1$.
- (2) Let $\Lambda_1^* \subseteq u^\perp$ be the dual lattice. Then $\Lambda_1^* \subseteq \Lambda^*$.
- (3)

$$\mu(\Lambda)^2 \leq \frac{1}{4} \|u\|^2 + \mu(\Lambda_1)^2.$$

Proof. (1) There exists a lattice basis u_1, u_2, \dots, u_d of Λ such that $u_1 = u$. Therefore, $\pi(u_2), \dots, \pi(u_d)$ is a lattice basis of Λ_1 .

(2) Let $y \in \Lambda_1^* \subseteq u^\perp$ and $x \in \Lambda$. Then $\langle y, x \rangle = \langle y, \pi(x) \rangle \in \mathbb{Z}$.

(3) Let $x \in \mathbb{R}^d$. We have to estimate $d(x, \Lambda)$. For this, let $y := \pi(x)$. We choose a lattice point $v \in \Lambda_1$ closest to y . See also Figure 4.3. Then we find a lattice point $w \in \Lambda$ with $\pi(w) = v$ such that $d(x, w + y - v) \leq \frac{1}{2} \|u\|$. Using the triangle inequality

$$d(x, w)^2 \leq d(x, w + y - v)^2 + d(w + y - v, w)^2.$$

we obtain

$$d(x, \Lambda)^2 \leq \frac{1}{4} \|u\|^2 + \mu(\Lambda_1)^2.$$

Now the statement follows by the definition of the covering radius. \square

Proof (Proof of Theorem 4.2.6). For the left inequality recursively choose recursively $u_i \in \Lambda$ such that u_i has the shortest length of all lattice points in Λ such that u_1, \dots, u_i is linearly independent, for $i = 1, \dots, d$. We claim that $\mu(\Lambda) \geq \frac{1}{2} \|u_d\|$.

Assume not. Let $x := \frac{1}{2} u_d$. Then there exists some $a \in \Lambda$ such that $\|a - x\| < \frac{1}{2} \|u_d\|$. Hence,

$$\|a\| \leq \|a - x\| + \|x\| < \|u_d\|,$$

and

$$\|2a - u_d\| = 2\|a - x\| < \|u_d\|.$$

Hence, by our choice of u_d , $\text{lin}(u_1, \dots, u_{d-1})$ contains a and $2a - u_d$, and thus also u_d , a contradiction.

Let $v \in \Lambda^*$ such that $\varrho(\Lambda^*) = \frac{1}{2} \|v\|$. Then there exists some $i \in \{1, \dots, d\}$ such that $\langle v, u_i \rangle \neq 0$, in particular, $|\langle u_i, v \rangle| \geq 1$. Now, combining the previous results with the Cauchy-Schwartz inequality yields:

$$\mu(\Lambda) \varrho(\Lambda^*) \geq \frac{1}{4} \|u_d\| \|v\| \geq \frac{1}{4} \|u_i\| \|v\| \geq \frac{1}{4} |\langle u_i, v \rangle| \geq \frac{1}{4}.$$

We prove the middle inequality by induction on d . You will prove the initial case $d = 1$ for the induction in Exercise 4.5.

Let $d \geq 2$. We choose a shortest non-zero lattice vector $u \in \Lambda$, thus, $\|u\| = 2\varrho(\Lambda)$. Let us consider π , Λ_1 , and Λ_1^* as in Lemma 4.2.7. Since, $\Lambda_1^* \subseteq \Lambda^*$, we have $\varrho(\Lambda^*) \leq \varrho(\Lambda_1^*)$. Now, Lemma 4.2.7(3) and Corollary 4.2.5 yields

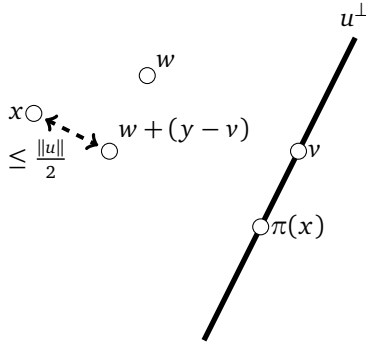


Fig. 4.3

$$\mu(\Lambda)^2 \varrho(\Lambda^*)^2 \leq \varrho(\Lambda)^2 \varrho(\Lambda^*)^2 + \mu(\Lambda_1)^2 \varrho(\Lambda^*)^2 \leq \frac{1}{16} d^2 + \mu(\Lambda_1)^2 \varrho(\Lambda_1^*)^2.$$

Therefore, the induction hypothesis yields the desired statement.

Finally, the right inequality follows from the following well-known fact (which you will prove in Exercise 4.6).

$$\sum_{i=0}^d k^2 = \binom{d+2}{3} + \binom{d+1}{3} = \frac{1}{3} d^3 + \frac{1}{2} d^2 + \frac{1}{6} d \leq d^3. \quad \square$$

4.3 The Flatness Theorem

In this section we prove a version of the celebrated flatness theorem. We will not prove the best possible bound, this is beyond the scope of this book. We will follow a version of the proof outlined in [3].

4.3.1 Definition (width). Let $K \subseteq \mathbb{R}^d$ be a full-dimensional convex body. The *width of K with respect to a non-zero lattice vector $a \in \Lambda^*$* is defined as

$$\omega(K; a) := \max_{x \in K} a(x) - \min_{x \in K} a(x).$$

We define the *width of K with respect to Λ* as

$$\omega_\Lambda(K) := \inf(\omega(K; a) : a \in \Lambda^* \setminus \{0\}).$$

Extending our result on empty lattice polytopes, playing around with two-dimensional convex sets one gets the impression that a convex body without interior lattice points cannot have arbitrary width. It is the main goal of this lecture to give a proof of this observation.

4.3.2 Theorem (Flatness). Let $K \subseteq \mathbb{R}^d$ be a convex body with $K \cap \Lambda = \emptyset$. Then

$$\omega_\Lambda(K) \leq d^{\frac{5}{2}}.$$

Note that the upper bound only depends on the dimension and not on the given lattice! $d^{\frac{5}{2}}$ is not the optimal bound, it was improved to $d^{\frac{3}{2}}$. Still it is unknown and an active subject of current research, whether the sharp bound is actually of the form $O(d)$. Let us first deal with the crucial case that K is simply a ball. Here, calculating the width is directly related to the considerations about lattices in the previous section.

4.3.3 Proposition. Let \mathcal{B} be a ball in \mathbb{R}^d . If $\mathcal{B} \cap \Lambda = \emptyset$, then

$$\omega_\Lambda(\mathcal{B}) \leq 4 \varrho(\Lambda^*) \mu(\Lambda) \leq d^{\frac{3}{2}}.$$

Proof. Let \mathcal{B} be a ball of radius r centered at m that satisfies the assumption. The assumption yields $r \leq \mu(\Lambda)$, as otherwise $(\Lambda + (\mathcal{B} - m))$ would cover the space (cf. Figure 4.4). Choose a shortest lattice vector $v \neq 0$ in Λ^* . By the definition of the packing radius we have $\|v\| = 2 \varrho(\Lambda^*)$. We can estimate the width via

$$\omega(\mathcal{B}; v) = \|v\| 2r \leq 4 \varrho(\Lambda^*) \mu(\Lambda) \leq d^{\frac{3}{2}}.$$

where the last inequality follows from Theorem 4.2.6. \square

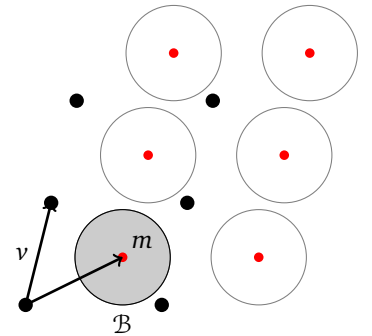


Fig. 4.4

It is straightforward to generalize this result from balls to ellipsoids. Recall that an *ellipsoid* is the image of a ball under a linear transformation of \mathbb{R}^d , in particular, it has a unique *center*.

4.3.4 Corollary. *Let E be an ellipsoid. If $E \cap \Lambda = \emptyset$ then*

$$\omega_\Lambda(E) \leq d^{\frac{3}{2}}.$$

Proof. Let T be the linear transformation of \mathbb{R}^d mapping a ball B to E and define $\Lambda' := T^{-1}(\Lambda)$. The induced maps

$$T : \Lambda' \xrightarrow{\cong} \Lambda \quad \text{and} \quad T^* : \Lambda^* \xrightarrow{\cong} \Lambda'^*$$

are isomorphisms. This implies

$$\omega_\Lambda(E) = \inf_{a \in \Lambda' \setminus \{0\}} \omega(T(B); a) = \inf_{a \in \Lambda'^* \setminus \{0\}} \omega(B; T^*(a)) = \omega_{\Lambda'}(B).$$

Our assumption yields $B \cap \Lambda' = \emptyset$. Thus, we can apply Proposition 4.3.3. \square

The proof of the Flatness theorem can be deduced from the following powerful observation.

4.3.5 Proposition. *Let E be an ellipsoid in K (with center a) of maximal volume. Then*

$$K \subseteq d(E - a) + a.$$

In fact, this *maximal volume ellipsoid* is even unique. We refer for the elementary-analytic proof of Proposition 4.3.5 to (Barvinok [2]).

Proof (Proof of Theorem 4.3.2). Let E be a maximal volume ellipsoid contained in K with center a . Proposition 4.3.5 yields $K \subseteq d(E - a) + a$. Hence, the statement follows from Corollary 4.3.4:

$$\omega_\Lambda(K) \leq d \omega_\Lambda(E) \leq d^{\frac{5}{2}}. \quad \square$$

4.4 Problems

4.1 Show that Δ_2 and $[0, 1]^2$ are up to unimodular equivalence the only empty lattice polygons.

4.2 Show that multiplying with a element coprime to D in \mathbb{Z} induces a group automorphism of $\mathbb{Z}/D\mathbb{Z}$.

4.3 Show that lattice pyramids of lattice polytopes do not change the h^* -polynomial.

4.4 Prove that for any d -dimensional polytope P which is not a simplex there exists a vertex such that the convex hull of the other vertices is full-dimensional.

4.5 Prove the case $d = 1$ of Theorem 4.2.6(2).

4.6 Show that $\sum_{i=0}^d k^2 = \binom{d+2}{3} + \binom{d+1}{3}$

Reflexive and Gorenstein polytopes

5

Reflexive polytopes were introduced by Victor Batyrev in the context of mirror symmetry, a fascinating phenomenon in string theory. Their striking feature is that they always appear in dual pairs. Since then these special lattice polytopes have been intensively studied and classified by mathematicians and physicists alike. By now, all isomorphism classes of reflexive polytopes in dimension 4, nearly half a billion, are known! Despite all these efforts, still many questions remain open. Amazingly, from the viewpoint of EHRHART theory reflexive polytopes (and their slightly more general relatives, Gorenstein polytopes) can be recognized from having a symmetric h^* -vector. What else is there to discover?

In this chapter, we define reflexive polytopes, and explore some of their basic features. Next, we present some of their surprising properties in dimensions 2 and 3. In Section 5.2 we also consider ‘divisors’ of reflexive polytopes, called Gorenstein polytopes, and show that this is a natural class of lattice polytopes to work with. In Section 5.3 we explore the combinatorics of reflexive polytopes in the more tractable situation, where all facets are simplices. Finally, we consider the question how many Gorenstein polytopes exist using results in Ehrhart theory and the geometry of numbers developed in the previous chapters.

5.1 Reflexive polytopes

Let $P \subseteq \mathbb{R}^d$ be a d -dimensional lattice polytope (with respect to $\Lambda = \mathbb{Z}^d$).

5.1.1 Definition. Let $\mathcal{F}(P)$ be the set of facets of P , $F \in \mathcal{F}(P)$, then there exists a unique *primitive inner normal* $\eta_F \in \Lambda^*$ and a unique integer $c_F \in \mathbb{Z}$ such that

$$\begin{aligned}\langle \eta_F, x \rangle &= c_F \quad \forall x \in F \\ \langle \eta_F, x \rangle &\geq c_F \quad \forall x \in P\end{aligned}$$

5.1.2 Definition. A polytope P is called *reflexive*, if there exists $w \in \text{int } P \cap \Lambda$ such that all facets have lattice distance 1 from w .

Equivalently, for any facet $F \in \mathcal{F}(P)$ there exists a lattice point $u \in \Lambda^*$ such that $\langle u, x \rangle = \langle u, w \rangle + 1$ for any $x \in \mathcal{V}(F)$. Note that in this case u is necessarily primitive, so $u = \eta_F$.

As the following observation shows, there is no ambiguity about the interior point w .

5.1.3 Proposition. Let P be a reflexive polytope with respect to w , then

$$\text{int } P \cap \Lambda = \{w\}$$

Proof. Let $F \in \mathcal{F}(P)$. By definition, no lattice point lies strictly between the hyperplanes $\text{aff}(F)$ and its parallel hyperplane through w . See Figure 5.1. Therefore, $\text{conv}(w, F) \cap \Lambda = \{w\} \cup (F \cap \Lambda)$. Since $P = \bigcup_{F \in \mathcal{F}(P)} \text{conv}(w, F)$, the statement follows.

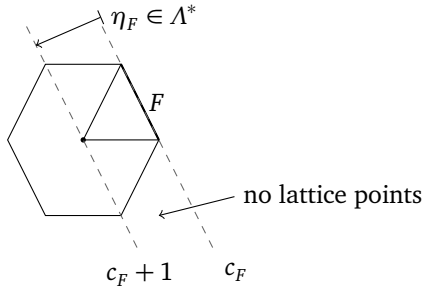


Fig. 5.1: Proof of Proposition 5.1.3.

Usually, the unique interior lattice points of a reflexive polytope is assumed to be the origin. We give the definition of a reflexive polytope in this generality in order to allow reflexive polytopes to be invariant under (affine) unimodular transformations. It is also more natural in the study of Gorenstein polytopes, as we will see later.

Reflexive polytopes were introduced because of their beautiful duality property. Let us recall the definition of a dual polytope.

5.1.4 Definition (polar dual). Let $P \subseteq \mathbb{R}^d$ be a full-dimensional polytope with $0 \in P$. The *dual polytope* or *polar dual* of P is defined as

$$P^* := \{\alpha \in (\mathbb{R}^d)^* \mid \alpha(x) \leq 1 \text{ for all } x \in P\}$$

It is well-known that the vertices of P^* correspond one-to-one to facets of P . More precisely, the vertices are the unique inner facet normals evaluating as -1 on facets.

The most important result is the *duality theorem* (which holds more generally for convex bodies containing the 0 in their interior):

$$P^{**} = P$$

As a consequence, here is the promised characterization of reflexive polytopes (Exercise 5.1).

5.1.5 Proposition. Let P be a d -dimensional lattice polytope in \mathbb{R}^d with $0 \in \text{int } P$. Then the following are equivalent:

- ▷ P reflexive,
- ▷ P^* lattice polytope
- ▷ P^* reflexive.

□

Coming back to Proposition 5.1.3, the reader will prove in Exercise 5.2 that any lattice polygon with one interior lattice points is also a reflexive polygon. However, this is not true in dimension 3 and higher (Exercise 5.3).

5.1.1 Dimension 2 and the number 12

We turn to a remarkable result about reflexive polygons.

5.1.6 Theorem. *The numbers of boundary lattice points of a reflexive polygon and its dual add up to 12.*

At least five different proofs appear in [21, 15]: by exhaustion, by a walk in the space of polygons, using toric varieties, using modular forms, or via relations in $SL_2(\mathbb{Z})$.

We will pursue the walk-in-the-space-of-polygons strategy. It yields a more general version of the 12 for unimodular fans. But this needs some preparation. Two adjacent lattice points on the boundary of a reflexive polygon form a lattice basis by PICK's theorem. The cones these lattice points generate form a complete unimodular fan.

5.1.7 Lemma. *Let \mathbb{K} be a complete unimodular fan in \mathbb{R}^2 . Every ray $\varrho \in \mathbb{K}[1]$ with primitive generator v is contained in precisely two 2-cones $\sigma = \text{cone}(v, w)$ and $\sigma' = \text{cone}(v, w')$ in \mathbb{K} .*

In this situation, there is a unique integer $a(\tau)$ such that

$$w + w' = a(\tau)v.$$

Proof. Since w, v form a lattice basis of \mathbb{Z}^2 , we have $w' = k_1 w + k_2 v$. Since v, w' form a lattice basis, we deduce $k_1 = \pm 1$. Hence, $k_1 = -1$ by our assumption on the cones. Therefore, $w + w' = k_2 v$. \square

5.1.8 Lemma. *Let P be a reflexive polygon, and let v_1, v_2, v_3 be consecutive lattice points on the boundary of P with $v_1 + v_3 = av_2$, for $a \in \mathbb{Z}$.*

If v_2 is a vertex of P , then the edge of P^ dual to v_2 has length $2 - a$. (If v_2 is not a vertex, then $a = 2$.)*

Proof. Let $\{v_1^*, v_2^*\}$ be the basis dual to the basis $\{v_1, v_2\}$. Then the vertices of P^* dual to the edges v_1, v_2 and v_2, v_3 are $v_1^* + v_2^*$ and $(a - 1)v_1^* + v_2^*$, respectively. \square

In light of this lemma, Theorem 5.1.6 follows from the following theorem.

5.1.9 Theorem. *Let \mathbb{K} be a complete unimodular fan in \mathbb{R}^2 . Then*

$$\sum_{\tau \in \mathbb{K}[1]} (3 - a(\tau)) = 12. \quad (5.1.1)$$

This is the theorem we will prove by walking in the space of fans. Here are the steps in our walk.

5.1.10 Definition. Let \mathbb{K} be a unimodular fan in \mathbb{R}^2 , and let $\sigma \in \mathbb{K}[2]$ with primitive generators v_1, v_2 . Set $\varrho := \text{cone}(v_1 + v_2)$, and

$$\text{pull}(\mathbb{K}; \varrho) := \mathbb{K} \setminus \{\sigma\} \cup \{\varrho, \text{cone}(\varrho, v_1), \text{cone}(\varrho, v_2)\}.$$

We say that the fan $\text{pull}(\mathbb{K}; \varrho)$ is obtained as a smooth blow-up of σ in \mathbb{K} .

The defining property of such a smooth blow-up is the fact that the new ray ϱ has ray parameter $a(\varrho) = 1$. As the reader can verify in Exercise 5.5, these steps preserve the validity of equation (5.1.1).

5.1.11 Lemma. *If the complete unimodular fan \mathbb{K} in \mathbb{R}^2 satisfies (5.1.1), and \mathbb{K}' is a smooth blow-up of \mathbb{K} , then \mathbb{K}' also satisfies (5.1.1).*

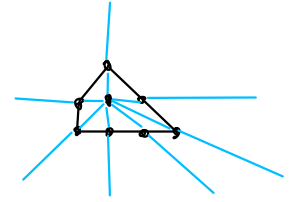


Fig. 5.2: The fan defined by a reflexive polygon

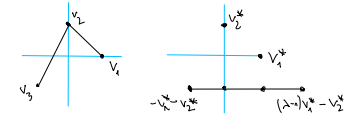


Fig. 5.3: The dual edge has length $2 - a$

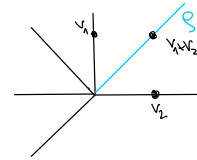


Fig. 5.4: Smooth blow-up of a 2-dimensional fan

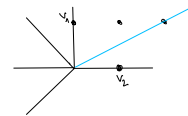


Fig. 5.5: Not a smooth blow-up

It remains to show that these steps connect the space of fans.

5.1.12 Theorem. *Let \mathcal{K} and \mathcal{K}' be two complete unimodular fans in \mathbb{R}^2 . Then there is another complete unimodular fan \mathcal{K}'' which can be obtained by a sequence of smooth blow-ups from both \mathcal{K} and \mathcal{K}' .*

The corresponding statement in general dimension has been conjectured by Oda. This Strong Oda Conjecture is still wide open. Connectivity of the space of complete unimodular fans has been shown in all dimensions. It was the foundation of the celebrated Weak Factorization Theorem.

For the proof of Theorem 5.1.12 we need three lemmas.

5.1.13 Lemma. *Let $\sigma \subseteq \mathbb{R}^2$ be a pointed 2-cone. Then there is a unimodular fan \mathcal{K} with support σ .*

Proof. Consider the polyhedron $P := \text{conv}(\sigma \cap \mathbb{Z}^2 \setminus \{0\})$. The bounded segments of P generate cones which form a fan with support σ . For any such segment, the triangle it forms with 0 does not contain any other lattice points. Hence, it is unimodular by Pick's theorem. \square

The proof of the following observation is Exercise 5.6.

5.1.14 Lemma. *Let \mathcal{K} be a unimodular fan in \mathbb{R}^2 , and let $v_1, v_2, v_3 \in \mathbb{Z}^2$ be primitive so that $\sigma_1 := \text{cone}(v_1, v_2)$ and $\sigma_2 := \text{cone}(v_2, v_3)$ (together with all their faces) form a fan, and so that $v_1 + v_3 = av_2$. Then*

- (1) $\text{cone}(v_1, v_2) \cup \text{cone}(v_2, v_3)$ is a pointed cone if and only if $a \geq 1$, but
- (2) v_2 is a vertex of $\text{conv}(0, v_1, v_2, v_3)$ if and only if $a \leq 1$.

Proof. proof missing

Using this fact we can prove a crucial step towards connectivity:

5.1.15 Lemma. *Let \mathcal{K} be a unimodular fan in \mathbb{R}^2 which refines a unimodular fan \mathcal{K}' . Then \mathcal{K} can be obtained from \mathcal{K}' by a sequence of smooth blow-ups.*

Proof. Use induction on $r := |\mathcal{K}[1] \setminus \mathcal{K}'[1]|$. If $r = 0$, we have $\mathcal{K} = \mathcal{K}'$.

If $r \geq 1$, all ray parameters of rays of \mathcal{K} that do not belong to \mathcal{K}' must be ≥ 1 by Lemma 5.1.14(1). On the other hand, if $\sigma \in \mathcal{K}'[2]$ contains rays of \mathcal{K} in the interior, then the convex hull of the primitive generators has a vertex in the interior of σ . The corresponding ray falls into case (2) of Lemma 5.1.14 and hence must have parameter = 1. \square

Proof (Theorem 5.1.12). The collection $\overline{\mathcal{K}} := \{\sigma \cap \sigma' : \sigma \in \mathcal{K}, \sigma' \in \mathcal{K}'\}$ is a complete fan. By Lemma 5.1.13, there is a complete unimodular fan \mathcal{K}'' refining $\overline{\mathcal{K}}$. Now, we use the previous lemma. \square

Putting it all together, Lemma 5.1.11 and Theorem 5.1.12 imply Theorem 5.1.9.

5.1.2 Dimension 3 and the number 24

In dimension three, there is a possibly even more striking result.

5.1.16 Theorem. *If P is a 3-dimensional reflexive polytope, then*

$$\sum_{e \text{ edge of } P} \text{length } e \cdot \text{length } e^* = 24.$$

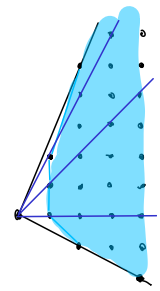


Fig. 5.6: Unimodularly subdividing a 2-cone

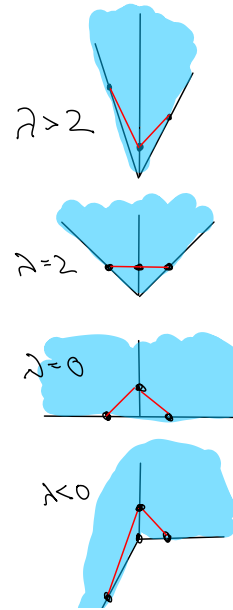


Fig. 5.7: Different λ 's

This result was first proved by Dimitrios Dais as follows. By [5], a general anticanonical hypersurface Z in the toric variety associated with P must be a 2-dimensional Calabi–Yau, i.e., a $K3$ -surface which has Euler characteristic $\chi(Z) = 24$. By [9], the above sum computes $\chi(Z)$. For about a decade, this remained the only proof (apart from exhaustion). We will provide an elementary proof in the present section.

Sadly, the story does not continue in dimensions ≥ 4 . But in dimension three, we can carry out a similar program as we did in dimension two. First, we describe parameters for unimodular fans which will replace dual edge lengths (Exercise 5.8).

5.1.17 Lemma. *Let \mathcal{K} be a complete unimodular fan in \mathbb{R}^d . Every $(d-1)$ -cone $\tau \in \mathcal{K}[d-1]$ with primitive generators v_1, \dots, v_{d-1} is contained in precisely two d -cones $\sigma = \text{cone}(\tau, v_d)$ and $\sigma' = \text{cone}(\tau, v'_d)$ in \mathcal{K} .*

In this situation, there are unique integers $a(\tau, v_i)$ so that

$$v_d + v'_d = \sum_{i=1}^{d-1} a(\tau, v_i) v_i.$$

Next, we construct a complete unimodular fan from a reflexive 3-polytope.

5.1.18 Proposition. *Let P be a 3-dimensional reflexive polytope, and let \mathcal{T} be a full lattice triangulation of its boundary. Then $\mathcal{K} := \{\text{cone } \sigma : \sigma \in \mathcal{T}\}$ is a complete unimodular fan.*

Further, if $\text{conv}(v_1, v_2) \in \mathcal{T}[1]$ is contained in an edge e of P , then the dual edge e^ of P^* has length $2 - a(\tau, v_1) - a(\tau, v_2)$ where $\tau = \text{cone}(v_1, v_2) \in \mathcal{K}$. (Otherwise $a(\tau, v_1) + a(\tau, v_2) = 2$.)*

Proof. For \mathcal{K} , we only need to prove unimodularity. Every triangle σ in a full triangulation is unimodular in its affine span by Pick’s theorem. Because P is reflexive, this affine span has distance one to the origin, so that $\text{conv}(\mathbf{0}, \sigma)$ is unimodular.

In order to compute the length of e^* , consider the two 3-cones $\sigma = \text{cone}(\tau, v_3)$ and $\sigma' = \text{cone}(\tau, v'_3)$ of \mathcal{K} containing τ . By definition of the parameters we have

$$v'_3 = -v_3 + a(\tau, v_1)v_1 + a(\tau, v_2)v_2.$$

As in dimension two, let $\{v_1^*, v_2^*, v_3^*\}$ be the basis dual to the basis $\{v_1, v_2, v_3\}$. Then the vertices of P^* dual to the facets of P containing $\{v_1, v_2, v_3\}$ and $\{v_1, v_2, v'_3\}$ are $v_1^* + v_2^* + v_3^*$ and $v_1^* + v_2^* + (a(\tau, v_1) + a(\tau, v_2) - 1)v_3^*$, respectively. \square

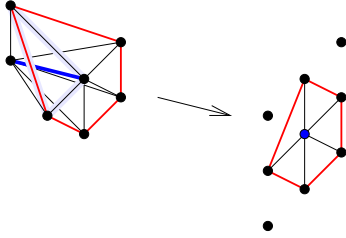
Thus, Theorem 5.1.16 follows from the following fan version.

5.1.19 Theorem. *Let \mathcal{K} be a complete unimodular fan in \mathbb{R}^3 . Then*

$$\sum_{\substack{\tau \in \mathcal{K}[2] \\ \text{with primitive} \\ \text{generators } v_1, v_2}} (2 - a(\tau, v_1) - a(\tau, v_2)) = 24.$$

We could, again, prove this theorem using a walk in the space of fans. The invariance under smooth blow-ups is elementary. But connectivity of the space of fans is a deep theorem, way beyond the scope of these notes. Luckily, one can deduce the 24 from the 12 by double counting.

5.1.20 Lemma. *Let \mathcal{K} be a complete unimodular fan in \mathbb{R}^3 , and let $\varrho \in \mathcal{K}[1]$ with primitive generator v . Then the projection $\pi: \mathbb{R}^3 \rightarrow \mathbb{R}^3/\mathbb{R}v$ maps $\text{star}(\varrho; \mathcal{K})$*


 Fig. 5.8: Quotient fan \mathcal{K}/ρ

to a complete unimodular fan \mathcal{K}/ρ . If $\tau \in \text{star}(\rho; \mathcal{K})$ is a 2-cone with primitive generators v, v' , then the corresponding ray $\pi(\tau)$ of \mathcal{K}/ρ has parameter $a(\pi(\tau)) = a(\tau, v')$.

Proof. Let v_1 and v_2 be the additional primitive generators of the 3 cones containing τ . Then $v_1 + v_2 = a(\tau, v)v + a(\tau, v')v'$. Applying π yields $\pi(v_1) + \pi(v_2) = a(\tau, v')\pi(v')$. \square

Proof (Theorem 5.1.19). Let us first collect what we need. Our fan \mathcal{K} gives rise to a triangulation of the 2-sphere with vertex set $\mathcal{K}[1]$, edge set $\mathcal{K}[2]$, and triangle set $\mathcal{K}[3]$. As such, we have $3|\mathcal{K}[1]| - |\mathcal{K}[2]| = 6$ from Euler's formula and double counting of edge-triangle-incidences. Also, we have $\sum_{v \in \mathcal{K}[1]} \deg v = 2|\mathcal{K}[2]|$, where $\deg v$ denotes the number of edges containing the vertex v . Armed with these formulas we compute

$$\begin{aligned}
 & \sum_{\substack{\tau \in \mathcal{K}[2] \\ \text{with primitive} \\ \text{generators } v_1, v_2}} (2 - a(\tau, v_1) - a(\tau, v_2)) \\
 &= \sum_{\text{cone}(v) \in \mathcal{K}[1]} \sum_{\substack{\tau \in \mathcal{K}[2] \\ \tau = \text{cone}(v, w)}} (1 - a(\tau, w)) \\
 &= \sum_{\text{cone}(v) \in \mathcal{K}[1]} \sum_{\substack{\tau \in \mathcal{K}[2] \\ \tau = \text{cone}(v, w)}} ((3 - a(\tau, w)) - 2) \\
 &= \sum_{\text{cone}(v) \in \mathcal{K}[1]} 12 - 2 \deg v = 12|\mathcal{K}[1]| - 4|\mathcal{K}[2]| = 24.
 \end{aligned}$$

Here we have used Theorem 5.1.9 for the quotient fans \mathcal{K}/ρ in the third equality. \square

5.2 Gorenstein polytopes

In this section, we will generalize the definition and duality of reflexive polytopes in a setting which is more natural from the viewpoint of cones as well as from Ehrhart theory. For this, let P be a full-dimensional lattice polytope in \mathbb{R}^d . Let's recall some definitions.

5.2.1 Definition. Let $\Lambda = \mathbb{Z}^d$ and $\bar{\Lambda} = \mathbb{Z}^{d+1}$. Then

$$\begin{aligned}
 C_P &:= \text{pos}(P \times 1) \subseteq \mathbb{R}^{d+1} \\
 C_P^* &:= \{u \in (\mathbb{R}^{d+1})^* \mid \langle u, x \rangle \geq 0 \ \forall x \in C_P\}
 \end{aligned}$$

For $F \in \mathcal{F}(P)$ there exists a unique *primitive inner normal* $u_F \in \bar{\Lambda}^*$ such that

$$\begin{aligned}
 \langle u_F, x \rangle &= 0 \ \forall x \in F \times 1 \\
 \langle u_F, x \rangle &\geq 0 \ \forall x \in P \times 1
 \end{aligned}$$

Actually, $u_F = (\eta_F, -c_F)$, since

$$\langle (\eta_F, -c_F), (x, 1) \rangle = \langle \eta_F, x \rangle - c_F \begin{cases} = 0 & x \in F \\ \geq 0 & x \in P \end{cases}$$

By duality of cones we have the correspondence:

$$\begin{aligned} \text{facets of } P &\leftrightarrow \text{rays of } C_P^\vee \\ F &\leftrightarrow \text{pos}(u_F) \end{aligned}$$

We are going to denote cones associated to lattice polytopes as Gorenstein cones.

5.2.2 Definition. Let $C \subseteq \mathbb{R}^{d+1}$ be a $(d+1)$ -dimensional pointed rational cone. Then C is called *Gorenstein cone*, if there exists a d -dimensional lattice polytope $P \subseteq \mathbb{R}^d$ such that $C \cong C_P$.

Equivalently, C is a Gorenstein cone if and only if there exists a lattice point $u_C \in \bar{\Lambda}^*$ such that $\langle u_C, x \rangle = 1$ for all primitive generators of the rays of C . In this case, u_C is necessarily primitive.

Our main result gives a complete characterization of lattice polytopes whose cones have dual Gorenstein cones in terms of Ehrhart theory. The reader may have to recall the definition of the degree and codegree of a lattice polytopes from Chapter 3.

5.2.3 Theorem. *The following are equivalent for a d -dimensional lattice polytope $P \subseteq \mathbb{R}^d$ of degree s and codegree r :*

- (1) C_P^\vee Gorenstein cone
- (2) rP reflexive
- (3) $\forall k \geq r$: $\text{int}(kP) \cap \Lambda = w + (k-r)P \cap \Lambda$ for some $w \in \text{int}(rP) \cap \Lambda$
- (4) $\widehat{\text{Ehr}}_P(t^{-1}) = (-1)^{d+1} t^r \widehat{\text{Ehr}}_P(t)$
- (5) $\text{ehr}_P(-k) = (-1)^d \text{ehr}_P(k-r) \quad \forall k \in \mathbb{Z}$
- (6) $h_i^* = h_{s-i}^* \quad \forall i = 0, \dots, s$

In this case: $u_{C_P^*} = w \times \{r\}$ and r is the unique $k \in \mathbb{N}_{\geq 1}$ such that kP is reflexive.

Proof. Let us identify P with $P \times 1$. We recall the Ehrhart series:

$$\widehat{\text{Ehr}}_P(t) = \frac{\sum_{i=0}^s h_i^* t^i}{(1-t)^{d+1}}$$

Ehrhart reciprocity yields:

$$\begin{aligned} \sum_{k \geq 1} |\text{int } kP \cap \bar{\Lambda}| t^k &= \sum_{k \geq 1} (-1)^d \text{ehr}_P(-k) t^k \\ &= (-1)^{d+1} \widehat{\text{Ehr}}_P(t^{-1}) \\ &= \frac{\sum_{i=0}^s h_i^* t^{d+1-i}}{(1-t)^{d+1}} \\ &= \frac{\sum_{i=r}^{r+s=d+1} h_{d+1-i}^* t^i}{(1-t)^{d+1}} \end{aligned}$$

Comparing the coefficients yields (4) \Leftrightarrow (5) \Leftrightarrow (6).

(5) $\Leftrightarrow |\text{int } kP \cap \bar{\Lambda}| = |(k-r)P \cap \bar{\Lambda}| \quad \forall k \geq r$: Note that $w \in \text{int } rP \cap \bar{\Lambda} \Rightarrow w + ((k-r)P \cap \bar{\Lambda}) \subseteq \text{int } kP \cap \bar{\Lambda}$. See Figure 5.9 for an illustration. This implies (3) \Leftrightarrow (3).

Let us prove (3) \Rightarrow (1): Let $w \in \text{int } rP \cap \bar{\Lambda}$, $F \in \mathcal{F}(P)$. We want to show that $\langle u_F, w \rangle = 1$. This would prove that C_P^* is a Gorenstein cone. For this let us define

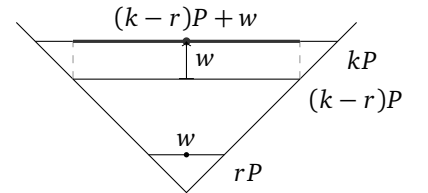


Fig. 5.9

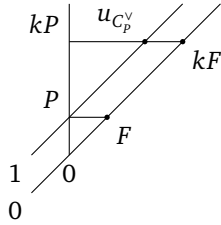
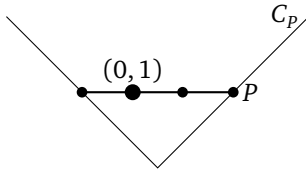


Fig. 5.10



$$u = (1, 2), \langle u, \cdot \rangle = 3$$

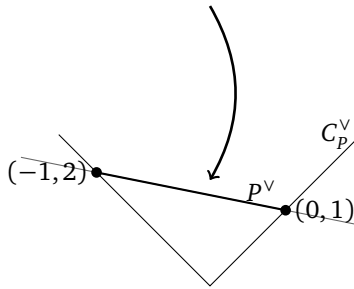


Fig. 5.11

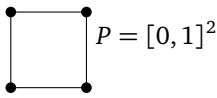


Fig. 5.12

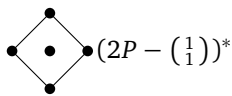
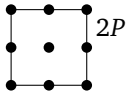


Fig. 5.13

$C' := \text{pos}(w, F)$. By Exercise 5.10 C' contains a lattice basis b_1, \dots, b_{d+1} such that $b_1, \dots, b_d \in \text{pos}(F)$ and $b_{d+1} \notin \text{pos}(F)$. Therefore, $b_{d+1} \in \text{int } C_P \cap \bar{\Lambda}$, in particular, there exists some $k \geq r$ such that $b_{d+1} \in \text{int } kP \cap \bar{\Lambda}$. By our assumption (3) there exists some $m \in (k-r)P \cap \bar{\Lambda}$ such that $b_{d+1} = w + m$. Let us define the dual lattice basis $b_1^*, \dots, b_{d+1}^* \in \bar{\Lambda}^*$. Since

$$\begin{aligned} \langle b_{d+1}^*, \text{pos}(F) \rangle &= 0 \\ \langle u_F, \text{pos}(F) \rangle &= 0 \end{aligned}$$

and b_{d+1}^* is primitive, we see $b_{d+1}^* = u_F$. Therefore, $1 = \langle u_F, b_{d+1} \rangle = \langle u_F, w \rangle + \langle u_F, m \rangle$, hence, $\langle u_F, w \rangle = 1$, as desired.

(1) \Rightarrow (2): Let $w := u_{C_P^\vee} \in \text{int } C_P \cap \bar{\Lambda}$. Then there exists $k \geq r$ such that $w \in \text{int } kP \cap \bar{\Lambda}$. Let $F \in \mathcal{F}(P)$, so, $\langle w, u_F \rangle = 1$. Restricting u_F to the affine lattice $\mathbb{Z}^d \times \{k\}$ yields an affine-linear form u'_F such that $\langle u'_F, w \rangle - \langle u'_F, kF \rangle = 1$. See Figure 5.10 for an illustration. Hence, kP is reflexive (w.r.t. w).

Let us show the additional last statement in the theorem. Assume $k > r$, then

$$\begin{aligned} |\text{int } kP \cap \bar{\Lambda}| &\geq |w + (k-r)P \cap \bar{\Lambda}| = |(k-r)P \cap \bar{\Lambda}| \\ &\geq |P \cap \bar{\Lambda}| > 1 \end{aligned}$$

This is a contradiction.

(2) \Rightarrow (1): Let rP be reflexive, and $F \in \mathcal{F}(P)$. We know that $u_F = (\eta_F, c_F)$ and $\langle \eta_F, rF \times r \rangle = rc_F$. Hence, $\langle \eta_F, w \rangle = rc_F + 1$, so $\langle u_F, (w, r) \rangle = \langle \eta_F, w \rangle - c_F r = 1$.

(2) \Rightarrow (3): The inclusion " \supseteq " is clear.

Let us prove " \subseteq ". Let $x \in \text{int}(kP) \cap \bar{\Lambda}$, $k \geq r$. Then

$$\langle u_F, x - w \rangle = \underbrace{\langle u_F, x \rangle}_{\geq 1} - \underbrace{\langle u_F, w \rangle}_{=1} \geq 0 \quad \forall F \in \mathcal{F}(P)$$

In particular, $x - w \in (C_P^*)^* = C_P$ and $\langle u_P, x - w \rangle = k - r$. Hence, $x - w \in (k-r)P \cap \bar{\Lambda}$, as desired. \square

This motivates our main definition.

5.2.4 Definition (Gorenstein polytope). P is a Gorenstein polytope if (1) – (6) holds.

In other words, a lattice polytope P is a Gorenstein polytope if some multiple kP is a reflexive polytope. This multiple k is necessarily equal to the codegree by Proposition 5.1.3. For instance, reflexive polytopes are precisely Gorenstein polytopes of codegree 1.

5.2.5 Example.

(1) See Figure 5.11. C_P^\vee is not a Gorenstein cone, $\Rightarrow P$ is not a Gorenstein polytope. $r = \text{codeg } P = 1$, $\text{int } P \cap \bar{\Lambda} = 2 > 1$; $h_0^* = 1$, $h_1^* = 2$.

(2) See Figure 5.12. $P = [0, 1]^2$ is a Gorenstein polytope of codegree $r = \text{codeg}(P) = 2$. ($2P$ is reflexive, see Figure 5.13).

(3) The Birkhoff polytope B_n is a famous polytope which is defined as the convex hull of all $n \times n$ -permutation matrices. It is a Gorenstein polytope of codegree n , see Exercise 5.11.

There is a natural duality of Gorenstein polytopes extending the one of reflexive polytopes. Since Gorenstein polytopes do not have interior lattice points, if $r > 1$, we have to use the duality of cones.

5.2.6 Proposition. *Let P be a Gorenstein polytope (as in Theorem 5.2.3). Then*

$$\begin{aligned} P^\vee &:= \{x \in C_P^* : \langle u_{C_P^*}, x \rangle = 1\} \\ &= \text{conv}(\eta_F : F \in \mathcal{F}(P)) \end{aligned}$$

is also a Gorenstein polytope of the same dimension, degree and codegree as P , called the dual Gorenstein polytope.

Proof. $u_{C_P^*} = w$, hence, $\langle u_{C_P^*}, u_P \rangle = r$. Let $G \in \mathcal{F}(P^*)$. Then $\langle u_G, G \rangle = 0$ and $\langle u_G, u_{C_P^*} \rangle = 1$. Therefore, rP^* is reflexive. \square

Note that this duality is quite subtle. For instance, for $r > 1$, P^\vee does not lie in the hyperplane $\mathbb{R}^d \times 1$. Thus, it is *not* intrinsically embedded in \mathbb{R}^d . It is merely given as a d -dimensional polytope in \mathbb{R}^{d+1} . Moreover, except for codegree 1, P^\vee is *not* isomorphic to $(rP - w)^*$, as one might guess at first. For instance, in Example 5.2.5(2) with $r = 2$, P^\vee is just isomorphic to P .

Let us consider the case of a reflexive polytope P , say, $0 \in \text{int}(P)$. Then we recover the duality of reflexive polytopes:

$$\begin{aligned} P^\vee &= \{x \in (\mathbb{R}^{d+1})^* : \langle x, (y, 1) \rangle \geq \forall y \in P, \langle x, (0, 1) \rangle = 1\} \\ &= \{(x, 1) : \langle x, y \rangle \geq -1 \forall y \in P\} \\ &= P^* \times 1. \end{aligned}$$

This gives another proof of Proposition 5.1.5.

5.3 The combinatorics of simplicial reflexive polytopes

Throughout, let $P \subseteq \mathbb{R}^d$ be a d -dimensional reflexive polytope with the origin of the lattice $\Lambda = \mathbb{Z}^d$ in its interior.

5.3.1 The maximal number of vertices

It is a natural question to ask for the maximal number of vertices of a d -dimensional reflexive (or Gorenstein) polytope. Let us look at small dimension $d \leq 4$, where the answer is known by the classification of Kreuzer and Skarke.

5.3.1 Example.

$d = 2$: $|\mathcal{V}(P)| \leq 6$, only attained by the reflexive hexagon \mathcal{H} , see Figure 5.14

$d = 3$: $|\mathcal{V}(P)| \leq 14$, only attained by the polytope in Figure 5.15

$d = 4$: $|\mathcal{V}(P)| \leq 36$, only attained by $\mathcal{H} \times \mathcal{H}$.

Based upon these observations we state the following daring conjecture.

5.3.2 Conjecture. $|\mathcal{V}(P)| \leq 6^{\frac{d}{2}}$, equality holds for d even and $P \cong \mathcal{H}^{\frac{d}{2}}$.

This question is still wide open. It has been shown to hold for simple centrally symmetric reflexive polytopes, since this class of reflexive polytopes can be completely classified. In the following we will present some of the techniques used to prove this.

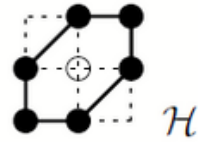


Fig. 5.14: the hexagon \mathcal{H}

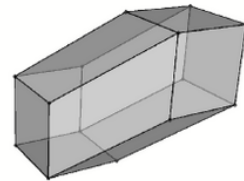


Fig. 5.15: a reflexive 3-polytope

5.3.2 The free sum construction


Our main motivation is to determine the maximal number of vertices of a *simplicial* reflexive polytope and to find out how the extremal polytopes look like. For this, we present a direct way how to construct higher-dimensional reflexive polytopes, called the free-sum construction:

5.3.3 Definition (Free Sum). $P_i \subseteq \mathbb{R}^{d_i}$ d_i -dim polytope with $0 \in \text{int}(P_i)$ ($i = 1, 2$). Then

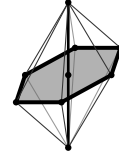
$$P_1 \circ P_2 := \text{conv} \left(\begin{array}{c} P_1 \times \{0\} \\ \{0\} \times P_2 \end{array} \right) \subseteq \mathbb{R}^{d_1+d_2}$$

free sum $(d_1 + d_2)$ -dim. polytope, $0 \in \text{int}(P_1 \circ P_2)$.

5.3.4 Example.

(1) $\bullet \xrightarrow{P_1=P_2} \bullet \Rightarrow P_1 \circ P_2 =$ 

(2) $P_1 = \mathcal{H}, P_2 = [-1, 1] \rightsquigarrow P_1 \circ P_2 = \text{bipyramid}(\mathcal{H}) =$



It follows directly from the definition that the free-sum construction is the dual operation to products:

$$(P_1 \circ P_2)^* = P_1^* \times P_2^*$$

In particular, if P_1, P_2 are reflexive, then $P_1 \circ P_2, P_1 \times P_2$ are reflexive.

There are nice formulas how the Ehrhart- and h^* -polynomials behave under the free sum and product construction.

5.3.5 Proposition. Let P_1, P_2 be reflexive. Then

$$\text{ehr}_{P_1 \times P_2} = \text{ehr}_{P_1} \text{ehr}_{P_2}, \quad h_{P_1 \circ P_2}^* = h_{P_1}^* h_{P_2}^*.$$

While the first result follows directly from the construction, the second one is not obvious. We will leave this as an exercise. Here is our main theorem. Its proof will occupy the remainder of this section.

5.3.6 Theorem. Let P be simplicial. Then $|\mathcal{V}(P)| \leq 3d$, and equality holds only if d is even and $P \cong \underbrace{\mathcal{H} \circ \dots \circ \mathcal{H}}_{\frac{d}{2}}$.

Simplicial reflexive d -polytopes with $3d-1$ vertices are also completely known.

5.3.3 The addition property

Lattice points in reflexive polytopes satisfy a partial addition property. For this let us define a relation.

5.3.7 Definition. Let $x, y \in \partial P \cap \Lambda$, $x \neq y$. Then $x \sim y$, if there exists a facet of P containing x and y .

Here is the main observation:

5.3.8 Proposition. Let $x, y \in \partial P \cap \Lambda$, $x \neq y$. Then

- (1) either $x \sim y$
- (2) or $x + y = 0$
- (3) or $x + y \in \partial P \cap \Lambda$.

If (3) holds, then $x \sim x + y$ or $y \sim x + y$. Moreover, there exist $a, b \in \mathbb{N}_{\geq 1}$ such that $z := ax + by \in \partial(P) \cap \Lambda$ such that $x \sim z \sim y$. In this case, $a = 1$ or $b = 1$.

Proof. Assume (1), (2) do not hold and (3) is wrong. Then duality yields that there exists a facet $F \in \mathcal{F}(P)$ such that $-1 > \langle \eta_F, x + y \rangle \in \mathbb{Z}$. Hence, $-2 \geq \langle \eta_F, x + y \rangle = \langle \eta_F, x \rangle + \langle \eta_F, y \rangle$ where $\langle \eta_F, x \rangle, \langle \eta_F, y \rangle \geq 1$. This would imply $x, y \in F$, a contradiction.

Now, let $F \in \mathcal{F}(P)$ such that $-1 = \langle \eta_F, x + y \rangle = \langle \eta_F, x \rangle + \langle \eta_F, y \rangle$. Since $\langle \eta_F, x \rangle, \langle \eta_F, y \rangle \in \mathbb{Z}_{\geq -1}$, we get either $x \in F$ and $\langle \eta_F, y \rangle = 0$ or $y \in F$, $\langle \eta_F, x \rangle = 0$. Let us assume the first case. We consider the pair $x + y, y$. If $x + y \sim y$, we are done. So assume not. Then we get $(x + y) + y \in \partial P \cap \Lambda$. Hence, since $\langle \eta_F, y \rangle = 0$, we still have $x + 2y \in F$. Now, we consider the pair $x + 2y, y$. Since $|P \cap \Lambda| < \infty$, we cannot repeat this argument ad infimum, so there has to exist some $b \in \mathbb{N}_{\geq 1}$ such that $x + by \sim y$. \square

Note that even if x, y are vertices, z does not have to be a vertex again, if the dimension of P is larger than two. This result has many applications. As an immediate result we deduce the following constraints on the combinatorics of a simplicial reflexive polytope (Exercise 5.12).

5.3.9 Corollary. *The diameter of the vertex-edge graph of a simplicial reflexive polytope is at most three.*

5.3.4 Vertices between parallel facets

In this section, we use the partial addition of lattice points to deduce the precise form of vertices that lie between two parallel facets of a simplicial reflexive polytope.

Let us fix a facet F of a simplicial reflexive d -polytope P . We denote the vertices of F by b_1, \dots, b_d . Let $F_i \in \mathcal{F}(P)$ such that $F_i \cap F = \text{conv}(b_1, \dots, \hat{b}_i, \dots, b_d)$. Then there exists a unique $m_i \in \mathcal{V}(P)$ such that $\mathcal{V}(F_i) = \{b_1, \dots, m_i, \dots, b_d\}$ for $i = 1, \dots, d$.

Note that b_1, \dots, b_d is in general not a lattice basis. We can still define the dual (vector-space) basis $b_1^*, \dots, b_d^* \in (\mathbb{R}^d)^*$. These are in general no lattice points.

The next lemma shows in particular, that there are at most d vertices which lie on the adjacent parallel hyperplane to a facet.

5.3.10 Lemma. $v \in \mathcal{V}(P)$, $\langle \eta_F, v \rangle = 0$.

- (1) Let $i \in \{1, \dots, d\}$

$$v \in F_i \iff v = m_i \iff \langle b_i^*, v \rangle < 0.$$

In particular, such i exists.

- (2) If $\langle b_i^*, m_i \rangle = -1$, $\langle \eta_F, m_i \rangle = 0 \forall i = 1, \dots, d$, then b_1, \dots, b_d is a lattice basis.

Proof. $i \in \{1, \dots, d\}$.

Let

$$\alpha_i := \frac{-1 - \langle \eta_F, m_i \rangle}{\langle b_i^*, m_i \rangle},$$

where $\langle b_i^*, m_i \rangle < 0$ since $0 \in \text{int}(P)$. Since $\langle \eta_F, m_i \rangle \geq 0$, we have $\alpha_i > 0$.

We claim that

$$\eta_{F_i} = \eta_F + \alpha_i b_i^*.$$

It suffices to check this equality for the vertices of F_i , where the left side always evaluates to -1 : $j \neq i$: $\langle \eta_F, b_j \rangle + \alpha_i \langle b_i^*, b_j \rangle = -1$,
 $\langle \eta_F, m_i \rangle + \alpha_i \langle b_i^*, m_i \rangle = -1$.

Now, we can prove (1) and (2).

- (1) $\eta_F = -b_1^* - \dots - b_d^*$, $\langle \eta_F, v \rangle = 0 \Rightarrow \exists i : \langle b_i^*, v \rangle < 0$. Moreover, $\langle b_i^*, v \rangle < 0 \iff \langle \eta_F + \alpha_i b_i^*, v \rangle < 0 \iff \langle \eta_{F_i}, v \rangle < 0 \iff v \in F_i \iff v = m_i$.
 (2) Here: $\alpha_i = 1 \forall i = 1, \dots, d$, hence $b_i^* = \eta_{F_i} - \eta_F \in \Lambda^* \forall i = 1, \dots, d$. Therefore $x = \sum_{i=1}^d \lambda_i b_i \in \Lambda \Rightarrow \lambda_i = \langle b_i^*, x \rangle \in \mathbb{Z} \Rightarrow b_1, \dots, b_d$ is a lattice basis. \square

Combining this lemma with the addition property for the lattice points in the dual reflexive polytope yields our desired result.

5.3.11 Proposition. $v \in \mathcal{V}(P)$, $\langle \eta_F, v \rangle = 0$. If $-F \in \mathcal{F}(P)$, then there are $I, J \subseteq \{1, \dots, d\}$, $I \cap J = \emptyset$, $|I| = |J|$ such that

$$v = \sum_{j \in J} b_j - \sum_{i \in I} b_i.$$

Proof. We use the notation in the proof of the previous lemma. Let $I := \{i \in \{1, \dots, d\} \text{ s.t. } \langle b_i^*, v \rangle < 0\} \neq \emptyset$. Then $i \in I \xRightarrow{(1)} v = m_i$.

$$\begin{aligned} -F \in \mathcal{F}(P) &\Rightarrow F_i \cap F = \emptyset \Rightarrow \eta_{F_i} \not\preceq \eta_{-F} = -\eta_F \xRightarrow{\text{Addition}} \eta_{F_i} - \eta_F \in \partial P^* \cap \Lambda^* \Rightarrow -1 \leq \\ \langle \alpha_i^* b_i^*, \pm b_i^* \rangle = \pm \alpha_i \in \mathbb{Z} &\xRightarrow{\alpha_i > 0} \alpha_i = 1 \Rightarrow \langle b_i^*, v \rangle = \langle \eta_{F_i} - \eta_F, v \rangle = \underbrace{\langle \eta_{F_i}, v \rangle}_{=-1} - \underbrace{\langle \eta_F, v \rangle}_{=0} \Rightarrow \\ \langle b_i^*, v \rangle &= -1. \text{ Same argument for } -F \text{ shows that } \langle b_j^*, v \rangle > 0 \Rightarrow \langle b_j^*, v \rangle = 1. \quad \square \end{aligned}$$

5.3.5 Special facets

We can now prove Theorem 5.3.6. The key idea is the following notion (due to Øbro).

5.3.12 Definition (Special Facet). Let $F \in \mathcal{F}(P)$ such that $\sum_{v \in \mathcal{V}(P)} v \in \text{pos}(F)$. Such a facet is called *special*.

From now on, let F be a special facet. Obviously, special facets exist. Let us slice the polytope (for $i \in \{-1, 0, 1, \dots\}$):

$$H_P(F, i) := \{v \in \mathcal{V}(P) : \langle \eta_F, v \rangle = i\} \quad \forall i \in \mathbb{Z}_{\geq -1}$$

Clearly,

$$|H_P(F, 0)| = d.$$

Moreover, Lemma 5.3.10 yields

$$|H_P(F, 1)| \leq d.$$

By definition of a special facet we have the following inequality:

$$0 \geq \langle \eta_F, \sum_{v \in \mathcal{V}(P)} v \rangle = \sum_{i \geq -1} i |H_P(F, i)| = -d + \sum_{i \geq 1} i |H_P(F, i)|. \quad (5.3.1)$$

Hence, we can simply count the vertices:

$$|\mathcal{V}(P)| = \sum_{i \geq -1} |H_P(F, i)| \leq \underbrace{|H_P(F, -1)|}_{=d} + \underbrace{|H_P(F, 0)|}_{\leq d} + \underbrace{\sum_{i \geq 1} |H_P(F, i)|}_{\leq d} \leq 3d. \quad (5.3.2)$$

It remains to consider the equality case ($|\mathcal{V}(P)| = 3d$).

In this case, equality in Equation 5.3.1 yields that

$$\langle \eta_F, \sum_{v \in \mathcal{V}(P)} v \rangle = 0.$$

Hence, $\sum_{v \in \mathcal{V}(P)} v = 0$, so any facet of P is special. Moreover, equalities in Equation 5.3.1 and show that any vertex of P lies in $H_P(F, i)$ for $i = -1, 0, 1$. Therefore, $-\eta_F \in P^*$. So, $-P^* \subseteq P^*$, and thus $-P^* = P^*$. In other words, P is centrally symmetric.

Since $|\mathcal{V}(P)| = 3d$ and $|H_P(F, -1)| = |H_P(F, 1)| = d$, we have $|H_P(F, 0)| = d$. Lemma 5.3.10(1) yields

$$H_P(F, 0) = \{m_1, \dots, m_d\},$$

as defined in the previous subsection. Let $k \in \{1, \dots, d\}$. By Proposition 5.3.11 there are $I, J \subseteq \{1, \dots, d\}, I \cap J = \emptyset, |I| = |J|$ such that $m_k = \sum_{j \in J} b_j - \sum_{i \in I} b_i$. Since all m_1, \dots, m_d are pairwise different, Lemma 5.3.10(1) yields that $m_k = b_{j_k} - b_k$ for some $j_k \in \{1, \dots, d\}, j_k \neq k$. In other words,

$$\begin{aligned} \sigma : \{1, \dots, d\} &\rightarrow \{1, \dots, d\} \\ k &\mapsto j_k \end{aligned}$$

is a fixed-point free ($\sigma(i) \neq i$) involution ($\sigma^2 = 1, j_{j_k} = k$). We may assume that this permutation is of the form

$$\sigma = (1 \ 2)(3 \ 4) \cdots (d-1 \ d).$$

In particular, d is even. Moreover,

$$P = \text{conv}(\pm b_1, \pm(b_1 - b_2), \pm b_2, \dots, \pm b_d, \pm(b_{d-1} - b_d), \pm b_d).$$

It remains to show that b_1, \dots, b_d is a lattice basis, since in that case

$$P \cong \underbrace{\mathcal{H} \circ \dots \circ \mathcal{H}}_{\frac{d}{2}}.$$

See Figure 5.16. We observe that for any $i = 1, \dots, d$

$$\begin{aligned} \langle b_i^*, m_i \rangle &= \langle b_i^*, b_{j_i} - b_i \rangle = -1 \\ \langle \eta_F, m_i \rangle &= 0 \end{aligned}$$

Hence, Lemma 5.3.10(2) finishes the argument. This proves Theorem 5.3.6.

5.4 Problems

5.1 Prove Proposition 5.1.5.

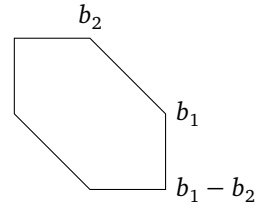


Fig. 5.16: The situation for $d = 2$.

- 5.2 Show that a lattice polygon is reflexive if and only if it contains precisely one interior lattice point.
- 5.3 Take $[-1, 1]^d$, remove one vertex and take the convex hull of the remaining lattice points. Show that it still contains precisely one interior lattice point. Is this a reflexive polytope?
- 5.4 Compute h^* -polynomial and Ehrhart polynomial of a 3-dimensional reflexive polytope having b many lattice points.
- 5.5 Prove Lemma 5.1.11.
- 5.6 Prove Lemma 5.1.14.
- 5.7 Classify unimodular fans in \mathbb{R}^2 which are minimal with respect to blow-ups.
- 5.8 Prove Lemma 5.1.17.
- 5.9 Define smooth blow-ups for three-dimensional unimodular fans (or higher-dimensional); and show the invariance of the equality in Theorem 5.1.19 under smooth blow-ups.
- 5.10 Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice of rank d . We may choose (why ?) $v_1, \dots, v_d \in \Lambda$ recursively such that v_{i+1} has the minimal non-zero distance from the subspace $\langle v_1, \dots, v_i \rangle$. Show that v_1, \dots, v_d is a lattice basis of Λ . In particular, any primitive vector of Λ can be completed to a lattice basis.
- 5.11 Prove that the Birkhoff polytope B_n (the convex hull of $n \times n$ -permutation matrices) is a Gorenstein polytope of codegree n . What is its dimension and degree? What is the unique interior lattice point of nB_n ?
- 5.12 Prove Lemma 5.3.9.

Unimodular Triangulations

6

In this chapter, we study under which assumptions a lattice polytope admits a triangulation into unimodular simplices. Such *unimodular triangulations* of lattice polytopes arise in algebraic geometry, commutative algebra, integer programming and, of course, combinatorics. Because of the nice implications, having a unimodular triangulation is a desirable property. But presumably, “most” lattice polytopes do not admit a unimodular triangulation.

We will define unimodular triangulations, and prove our first theorem for cones in Section 6.2. Then, we define the particularly nice class of compressed polytopes in Section 6.3, and give a few examples of important triangulations. Section 6.4 can be regarded as a capstone section of these notes. We use unimodular triangulations to prove unimodality of the h^* coefficients of Gorenstein polytopes with regular unimodular triangulation, tying together ideas from Chapters 3, 5, and 6. Finally, in Section 6.5, we prove a mysterious theorem from the early days of toric geometry which, to this day, raises more questions than it answers. Some further examples and motivation for (regular) unimodular triangulations are hidden in the exercises.

6.1 Regular Triangulations

6.1.1 Definition (regular subdivision). A subdivision \mathcal{S} with vertices $\{v_1, \dots, v_m\}$ is *regular* if there is a weight vector w such that \mathcal{S} is the projection of the lower hull of

$$\operatorname{conv}((w_i, v_i) \mid 1 \leq i \leq m),$$

where the lower hull is the polyhedral complex of those facets whose normal has negative first coordinate.

Given a set of points $V := \{v_1, \dots, v_m\}$ and a weight vector $w \in \mathbb{R}^m$ we denote by $\mathcal{RS}_w(V)$ the regular subdivision obtained as the lower hull of $\mathcal{RL}_w(V) := \text{conv}((w_i, v_i) \mid 1 \leq i \leq m)$.

6.1.2 Theorem. Any polytope admits a regular triangulation.

Proof: proof missing

6.2 Pulling Triangulations

Pulling refinements are a useful tool for constructing regular triangulations.

6.2.1 Definition (Pulling Refinements). Let \mathcal{S} be a lattice subdivision of the lattice polytope $P \subseteq \mathbb{R}^d$, and let $v \in P \cap \mathbb{Z}^d$. Then we obtain the *pulling refinement* $\text{pull}(\mathcal{S}; v)$ when we replace every face $F \in \mathcal{S}$ which contains v by the pyramids $\text{conv}(v, F')$ where F' runs over all faces of F which do not contain v .

The definition works mutatis mutandis for subdivisions of fans.

Here are some facts about the structure of pulling subdivisions.

6.2.2 Proposition.

- (1) Pulling preserves regularity.
- (2) Pulling all lattice points in P in some order results in a full triangulation.
- (3) If only vertices of P are pulled, then every maximal cell is the join of the first pulled vertex v_1 with a maximal cell in the pulling subdivisions of the facets not containing v_1 .

In particular, we see that every (regular) lattice subdivision of a lattice polytope has a (regular) refinement which is a full triangulation.

Proof. (1): Let $\mathcal{S} = \mathcal{RS}_w(\mathcal{A})$ be a regular subdivision of P , certified by weights $w \in \mathbb{R}^{\mathcal{A}}$ ($\mathcal{A} = P \cap \mathbb{Z}^d$), with lifted polyhedron $\mathcal{RL}_w(P) = \text{conv}((w_a, a) : a \in \mathcal{A})$ in \mathbb{R}^{d+1} . Let $m \in \mathcal{A}$. Set $w'_m := \min\{h : (m, h) \in \mathcal{RL}_w(P)\} - \epsilon$ and $w'_a := w_a$ for all $a \in \mathcal{A} \setminus \{m\}$. Then, for small enough $\epsilon > 0$, the pulling refinement $\text{pull}(\mathcal{S}; m)$ is induced by the weights w' .

(2): Every face of $\text{pull}(\mathcal{S}; m)$ which contains m is a pyramid with apex m . If $Q \in \mathcal{S}$ has n as an apex, then every face of $\text{pull}(\mathcal{S}; m)$ inside Q and containing n still has n as an apex. After strongly pulling all lattice points, all lattice points are vertices of the subdivision, and the cells have each of their vertices as apices so they are simplices.

(3): If we apply the previous argument to the trivial subdivision of P , we see that v_1 is an apex of every cell. \square

6.2.3 Theorem. Every rational cone has a regular unimodular triangulation.

Proof: proof missing

6.3 Compressed Polytopes

The notion of compressed polytopes was coined by Richard STANLEY [25]. Surprisingly many well-known polytopes fall into this category.

6.3.1 Definition. A lattice polytope $P \subseteq \mathbb{R}^d$ is *compressed* if all lattice points in P are vertices, and all pulling triangulations are unimodular.

Figure missing

Fig. 6.1

Compressed polytopes admit several characterizations. A lattice polytope P has width 1 with respect to a facet F , if it lies between the hyperplane spanned by this facet and the next parallel lattice hyperplane, that is, $\omega(P; \eta_F) = 1$ for the primitive inner normal $\text{inn}P_F$ of F .

The main implication of the following Theorem is due to Francisco SANTOS. The proof we present here is the original one (MSRI 1997, unpublished). It was subsequently also proven by Ohsugi and Hibi [20] and by Sullivan [27].

6.3.2 Theorem. *Let P be a lattice polytope. Then the following is equivalent:*

- (1) P is compressed.
- (2) P has width one with respect to all its facets.
- (3) P is lattice equivalent to the intersection of a unit cube with an affine space.

Proof. (2) \implies (1): By decreasing induction on the dimension one sees that every face of P has width 1 with respect to all facets. The restriction of a pulling triangulation to any face is a pulling triangulation itself and thus unimodular (by another induction). Hence, every maximal simplex in the triangulation of P is the join of a unimodular simplex in some facet with the first lattice point that was pulled.

The other implications are easy. \square

Examples of compressed polytopes include the Birkhoff polytope, order polytopes and hypersimplices, stable set polytopes of perfect graphs.

We can apply the above characterization of compressed polytopes to triangulate “bigger” polytopes using hyperplane arrangements.

Let $\mathcal{A} := \{n_1, \dots, n_r\} \subseteq \mathbb{Z}^d$ be a collection of vectors that span \mathbb{R}^d and form a unimodular matrix, i.e., such that all $(d \times d)$ -minors are either 0, 1 or -1 . Such a collection induces an infinite arrangement of hyperplanes

$$\{x \in \mathbb{R}^d : \langle n_i, x \rangle = k\} \quad \text{for } i = 1, \dots, r \text{ and } k \in \mathbb{Z},$$

which subdivide \mathbb{R}^d regularly into lattice polytopes. These subdivisions are studied under the name of *lattice dicing* in the literature [13]. We call a lattice polytope P whose collection of primitive facet normals forms a unimodular matrix *facet unimodular*. Every face of a facet unimodular polytope is again facet unimodular in its own lattice. The above hyperplane arrangement slices P into dicing cells. We call this subdivision the *canonical subdivision* of a facet unimodular polytope. The canonical subdivision subdivides faces canonically.

6.3.3 Theorem. *Suppose that $P \subseteq \mathbb{R}^d$ is a facet unimodular lattice polytope. Then P has a regular unimodular triangulation.*

Proof. The dicing cells have width one with respect to all their facets by construction. Thus, any pulling refinement of the canonical subdivision will be unimodular. \square

As a direct application of Theorem 6.3.3, flow polytopes as well as polytopes with facets in the root system of type A have regular unimodular triangulations. This method also shows that every dilation cP of a polytope P with a (regular) unimodular triangulation also admits such a triangulation (Theorem 6.3.4).

6.3.4 Theorem. *If P has a (regular) unimodular triangulation \mathcal{T} then its dilation cP has one too, for every positive integer c .*

In Section 6.5 below, it is convenient to use a very specific triangulation of a dilated simplex.

6.3.5 Definition. The vertices $\mathbf{0}, e_d, e_d + e_{d-1}, \dots, \mathbf{1}$ of the simplex

$$\Delta'_d := \{x \in \mathbb{R}^d : 0 \leq x_1 \leq \dots \leq x_d \leq 1\}$$

are totally ordered component wise. For $c \in \mathbb{Z}_{>1}$, the type-A hyperplane arrangement triangulates the dilated simplex $c\Delta'_d$ unimodularly. We call this triangulation the *standard triangulation* of $c\Delta'_d$.

If S is any lattice simplex, an ordering of $\mathcal{V}(S)$ induces an affine isomorphism $c\Delta'_d \rightarrow cS$. The image of the standard triangulation of $c\Delta'_d$ is a lattice triangulation which we call the *standard triangulation* of cS . Every simplex in this triangulation has volume $\text{vol}(S)$.

This triangulation is induced by the following weights. Let $\varphi(m) := \sum_i m_i^2 + \sum_{i < j} (m_i - m_j)^2$, and evaluate at the difference to the barycenter \hat{m} of $c\Delta^d$ ($\hat{m}_i = \frac{ci}{d+1}$): $\omega_m := \varphi(m - \hat{m})$. Then this triangulation as well as the weights restrict to the faces with the induced vertex ordering. If we globally order the lattice points in P , and choose the induced ordering on all simplices of \mathcal{T} , we get a regular unimodular triangulation \mathcal{T}' of cP .

6.4 Special Simplices in Gorenstein Polytopes

The goal of this section is to prove the following theorem of Bruns and Römer.

6.4.1 Theorem. *The h^* -vector of a Gorenstein polytope with a regular unimodular triangulation is unimodal. That is, $1 = h_1^* \leq \dots \leq h_{\lfloor s/2 \rfloor}^* \geq \dots \geq h_s^*$.*

This theorem and its proof are due to Bruns and Roemer [JCTA 2007]. For general Gorenstein polytopes the theorem fails, as shown by Payne and Mustata [Math Ann 2005]. However, it is still open whether the following property might suffice.

6.4.2 Definition. A lattice d -polytope $P \subseteq \mathbb{R}^d$ is called *integrally-closed*, if for every $k \in \mathbb{N}_{\geq 2}$ and for every lattice point $x \in kP \cap \mathbb{Z}^d$ there exist $x_1, \dots, x_k \in P \cap \mathbb{Z}^d$ such that $x = x_1 + \dots + x_k$.

Equivalently, let $C \subseteq \mathbb{R}^{d+1}$ be the cone spanned by $P \times \{1\}$. Then P is integrally closed if and only if the semigroup of lattice points in C is generated by lattice points in $P \times \{1\}$. As Exercise 6.2 shows, being integrally-closed is weaker than having a unimodular triangulation.

The central tool in the proof of Theorem 6.4.1 is the notion of a special simplex. The use of special simplices in this context had been pioneered by Athanasiadis [Crelle 2005]

6.4.3 Definition. A simplex $S \subseteq P$ inside a polytope P is *special* if $S \cap F$ is a facet of S for all facets F of P .

6.4.4 Example. cube, tetrahedron, circuit \rightarrow dimension a priori ambiguous; Birkhoff

Figure missing

Fig. 6.2

6.4.5 Lemma. *Every integrally closed Gorenstein polytope has a special simplex.*

Proof. Let $P \subseteq \mathbb{R}^d$ be integrally closed and Gorenstein with degree s . Let $u_P \in C_P$ be the Gorenstein point in the cone over P .

Because P is integrally closed, we can write $u_P = v_1 + \dots + v_s$ for $v_1, \dots, v_s \in (\{1\} \times P) \cap \mathbb{Z}^{d+1}$. We claim that $S := \text{conv}(v_1, \dots, v_s)$ is a special simplex.

Every facet F of P is dual to a vertex w of the Gorenstein dual $\{1\} \times P^\vee$. Then $\langle w, v_i \rangle \geq 0$ and $\langle w, u_P \rangle = 1$. Thus, $S \cap F$ contains all but one of the v_i . \square

The punchline in the proof of Theorem 6.4.1 will be that we project the polytope along a special simplex, and obtain a reflexive polytope with the same h^* -vector which inherits a regular unimodular triangulation from P . The following definition describes a subcomplex of P which will project bijectively onto the boundary of that reflexive polytope.

6.4.6 Definition. Let $S = \text{conv}(v_1, \dots, v_s) \subseteq P$ be a special simplex. Denote by $\Gamma(P, S)$ the subcomplex of ∂P generated by faces of the form $F_1 \cap \dots \cap F_s$ where F_i is a facet of P with $v_i \notin F_i$ for $i = 1, \dots, s$.

6.4.7 Lemma. Let $S \subseteq P$ be a special simplex in a Gorenstein polytope, and let \mathcal{T} be a triangulation of $\Gamma(P, S)$. Then the complex $\mathcal{T} \star S$ generated by $\{\text{conv}(S \cup F) : F \in \mathcal{T}\}$ is a triangulation of P . This triangulation is unimodular if \mathcal{T} was, and it is regular if \mathcal{T} is the restriction to $\Gamma(P, S)$ of a regular triangulation of P .

Proof. We need to show four things.

- (1) If F is a (unimodular) simplex in Γ , then $\text{conv}(S \cup F)$ is a (unimodular) simplex.
- (2) The $\text{conv}(S \cup F)$ cover P .
- (3) The $\text{conv}(S \cup F)$ and their faces form a polyhedral complex.
- (4) If \mathcal{T} is the restriction to $\Gamma(P, S)$ of a regular triangulation of P then $\mathcal{T} \star S$ is regular.

□

The proof of Theorem 6.4.1 uses h -vectors of triangulations. Its relation to the h^* -vector is given by the following result [7]:

6.4.8 Theorem (Betke and McMullen 1985). Let P be a lattice polytope with a triangulation \mathcal{T} . Let h^* be the h^* -vector of P and h the h -vector of the triangulation. Then $h_i^* \leq h_i$ for $0 \leq i \leq d$ with equality if and only if the triangulation is unimodular.

Proof (Theorem 6.4.1). If the Gorenstein polytope P has a regular unimodular triangulation, then it is integrally closed (Exercise 6.2). By Lemma 6.4.5 P contains a special simplex S , and we can define the complex $\Gamma(P, S)$. By Lemma 6.4.7 we can modify the given triangulation of P , if necessary, to obtain a regular unimodular triangulation of the form $\mathcal{T} \star S$ for a unimodular triangulation \mathcal{T} of $\Gamma(P, S)$. Thus $h^*(P) = h^*(\Gamma(P, S)) = h(\mathcal{T})$ by Theorem 6.4.8.

It remains to show that \mathcal{T} is combinatorially isomorphic to the boundary complex of a simplicial polytope. Then, the g -theorem implies that $h(\mathcal{T})$ is unimodal.

For this, let Φ be a strictly convex piecewise linear function on $\mathcal{T} \star S$. As S is a face of the triangulation, there is a linear functional u such that $\langle u, v \rangle = \Phi(v)$ for all $v \in S$ and $\langle u, v \rangle < \Phi(v)$ for all $v \notin S$.

Now let L be an affine space meeting S transversally in its relative interior. Then, for small $\varepsilon > 0$, $Q := \{x \in L : \Phi(x) - \langle u, v \rangle \leq \varepsilon\}$ is a polytope whose boundary complex has the same combinatorics as $\Gamma(P, S)$. □

As a corollary we can prove now the missing part of Proposition 5.3.5.

6.4.9 Corollary. Let P_1, P_2 be reflexive. Then

$$h_{P_1 \circ P_2}^* = h_{P_1}^* h_{P_2}^*.$$

Proof. In this situation, $P := P_1 * P_2$ is also called the free join of P_1 and P_2 . Its h^* -polynomial is given by the product of those of P_1 and P_2 (Exercise 6.3). The origins in P_1 and P_2 form a special simplex S of P . As remarked in the proof (Exercise 6.4), projecting along the affine span of S does not change the h^* -polynomial. Its image is the reflexive polytope $P_1 \circ P_2$. \square

6.5 Dilations

One of the first theorems about unimodular triangulations was proved in the early days of toric geometry by Knudsen, Mumford, and Waterman [16]. They were interested in semi-stable reduction of families of algebraic varieties.

6.5.1 Theorem ([16]). *There is a factor $c = c(P) \in \mathbb{Z}_{>0}$ such that the dilation $c \cdot P$ admits a regular unimodular triangulation.*

We say that $c(P)$ is a KMW-number of P . The KMW-theorem raises more questions than it answers, such as:

- ▷ What is the minimum $c(P)$ for a given polytope P ? Is there a $c(d)$ that is a KMW-number for every polytope of dimension d ?
- ▷ What is the structure of the set of KMW-numbers of a given P ? Is it a monoid? Theorem 6.3.4 implies it is closed under taking multiples of an element, but it is not clear whether it is closed under taking sums. On the other end, no polytope P and integer c are known so that c is a KMW-number for P but $c + 1$ is not.

For the proof of Theorem 6.5.1 we follow the strategy of the original ingenious proof [16] (we omit the regularity bit). Compare also [8, §§3.A&3.B].

Proof (Proof of Theorem 6.5.1). The theorem is true for lattice polyhedral complexes: every cell F is a lattice polytope in its own lattice Λ_F , and these lattices are compatible along intersections. In fact, the additional flexibility offered by this structure is used in the proof. Every triangulation of P carries two distinguished lattice structures: the one given by the embedding $P \subseteq \mathbb{R}^d$ on the one hand, and the one which declares every simplex to be unimodular on the other.

Starting from a full triangulation of P , the proof proceeds by induction on the maximal normalized volume V of a cell. If V is a prime number, the different cells of volume V do not interfere. They can be subdivided independently. But if V is composite, then this very fact is used to interpolate between the unimodular lattice structure and a multiple of the given one. The two cases of the induction step are treated in Lemmas 6.5.6 and 6.5.2 below. The proofs occupy the remainder of this section. \square

6.5.1 Composite Volume

For the induction step, we need some preparation. It is convenient to embed our lattice simplicial complex \mathcal{S} on vertices v_1, \dots, v_N into \mathbb{R}^N via $v_i \mapsto e_i$. For every face $F \in \mathcal{S}$ this yields a linear map $\varphi_F: \Lambda_F \rightarrow \mathbb{R}^N$, and we denote $\hat{\Lambda}$ the sum of the images of these lattices. Observe that $\varphi_F(\Lambda_F)$ is generated by convex combinations of unit vectors, and therefore every element has integral coordinate sum. If $v_i \in F$, call x_i an F -coordinate of x . In this setting, we can actually dilate \mathcal{S} by a positive integer (and keep the lattice $\hat{\Lambda}$).

For each $F \in \mathcal{S}$, the fundamental parallelepiped of F is the half open cube

$$\Pi(F) := \{x \in \mathbb{R}^N : x_i \in [0, 1) \text{ if } v_i \in F, \text{ and } x_i = 0 \text{ if } v_i \notin F\}.$$

A box point of F is an element of $\Pi(F) \cap \hat{\Lambda}$. It is in the relative interior if all its F -coordinates are strictly positive. The box points of F represent the elements of the finite abelian group $(\mathbb{Z}^N + \varphi_F(\Lambda_F))/\mathbb{Z}^N$; their number, the index $[\mathbb{Z}^N + \varphi_F(\Lambda_F) : \mathbb{Z}^N]$, equals the normalized volume of F .

6.5.2 Lemma. *Let V be a composite integer, and suppose that for every lattice simplicial complex \mathcal{S} all whose cells have volume less than V there is a factor $c \in \mathbb{Z}_{>0}$ such that $c\mathcal{S}$ has a unimodular triangulation.*

Then the same is true for all lattice simplicial complexes all whose cells have volume no more than V .

Proof. Let F_1, \dots, F_M be the volume V faces of \mathcal{S} . For each of them choose non-zero box points $m_i \in \Pi(F_i) \cap \hat{\Lambda}$ of order strictly less than V in $\hat{\Lambda}/\mathbb{Z}^N$. Define lattices $\Lambda_0 := \mathbb{Z}^N$, $\Lambda_i := \Lambda_{i-1} + \mathbb{Z}m_i$ for $i = 1, \dots, M$, and $\Lambda_{M+1} := \hat{\Lambda}$. To begin with, \mathcal{S} is unimodular with respect to Λ_0 . The maximal volume of a simplex of \mathcal{S} with respect to Λ_1 is bounded by the index $[\Lambda_1 : \Lambda_0]$ which by choice of m_1 is less than V . By induction, there is a $c_1 \in \mathbb{Z}_{>0}$ so that $c_1\mathcal{S}$ has a unimodular triangulation with respect to Λ_1 . In Λ_2 , this triangulation can only have simplices of volume $[\Lambda_2 : \Lambda_1]$ which by choice of m_2 is less than V . Continuing this way, we obtain a Λ_M -unimodular triangulation of $c_M \dots c_1\mathcal{S}$. But now, the index $[\Lambda_{M+1} : \Lambda_M]$ is also less than V . So some $c_{M+1} \dots c_1\mathcal{S}$ has a $\hat{\Lambda}$ -unimodular triangulation. \square

6.5.2 Prime Volume

Throughout the remainder of this section V is a prime number, and \mathcal{S} is a lattice simplicial complex with maximal simplex volume V . The (open) star, $\text{star}(\mathcal{S}; F)$, of a face F of a simplicial complex \mathcal{S} is the set of all faces that contain F . The closed star, $\overline{\text{star}}(\mathcal{S}; F)$, contains additionally all faces of elements of $\text{star}(\mathcal{S}; F)$. The boundary, $\partial \text{star}(\mathcal{S}; F)$, of $\text{star}(\mathcal{S}; F)$ is the difference $\overline{\text{star}}(\mathcal{S}; F) \setminus \text{star}(\mathcal{S}; F)$.

6.5.3 Lemma. *The set of volume V simplices is a pairwise disjoint union of open stars of inclusion minimal volume V simplices. Each inclusion minimal volume V simplex has $V - 1$ relative interior box points.*

Proof. Suppose $F \in \mathcal{S}$ has volume V , and G is a face of F with a relative interior box point m . Since V is prime, m generates the group $(\mathbb{Z}^N + \varphi_F(\Lambda_F))/\mathbb{Z}^N$. As all non- G -coordinates of m vanish, the same is true for all multiples of m , and therefore for all box points of F . \square

6.5.4 Lemma. *If $F \in \mathcal{S}$ is an inclusion minimal simplex of volume V , then there is a $c \leq d$ so that $c \cdot \overline{\text{star}}(\mathcal{S}; F)$ has a subdivision which induces the standard hypersimplicial subdivision on $c \cdot \partial \text{star}(\mathcal{S}; F)$ with the property that all simplices in any pulling triangulation have volume $< V$.*

Proof. Let m be a box point of F . Set $c := \sum_i m_i$ so that $m \in \text{relint } cF$. As all non- F -coordinates of m vanish and all F -coordinates are less than one, we have $c < \dim F + 1$. Integrality implies $c \leq d$. (We could use the symmetry of $\Pi(F)$ to obtain $c \leq \lceil d/2 \rceil$.)

Subdivide the facets of $c \cdot \partial \text{star}(\mathcal{S}; F)$ canonically into hypersimplices. Subdivide $c \cdot \overline{\text{star}}(\mathcal{S}; F)$ into pyramids over these hypersimplices with apex m .

Now, let G be a cell of a pulling triangulation refining this subdivision. Then $G = \text{conv}(m, G')$ where G' lives inside cF' for some facet F' of $\partial \text{star}(\mathcal{S}; F)$. There is a unique vertex v_j of F not in F' , and the normalized volume of G equals $m_j \cdot V < V$. \square

6.5.5 Lemma. $d!S$ has a triangulation into simplices of volume $< V$.

Proof. Subdivide every simplex of volume less than V canonically into hypersimplices.

For every inclusion minimal simplex F of volume V , choose c and subdivide $c \cdot \overline{\text{star}}(S; F)$ as in Lemma 6.5.4. Now, $d! \cdot \overline{\text{star}}(S; F) = \frac{d!}{c} \cdot (c \cdot \overline{\text{star}}(S; F))$ has a canonical subdivision into pyramids over hypersimplices. (Need to say something about this.) It restricts to the canonical subdivision on the boundary.

Now pull all the lattice points. □

Corollary:

6.5.6 Lemma. Let V be a prime number, and suppose that for every lattice simplicial complex S all whose cells have volume less than V there is a factor $c \in \mathbb{Z}_{>0}$ such that cS has a unimodular triangulation.

Then the same is true for all lattice simplicial complexes all whose cells have volume no more than V .

6.6 Problems

6.1 Prove Theorem 6.3.4 by using Theorem 6.3.3.

6.2 Show that a lattice polytope is integrally-closed, if it admits a unimodular triangulation.

6.3 Let $P \subseteq \mathbb{R}^n$ and $Q \subseteq \mathbb{R}^m$ be lattice polytopes. Show that the product of their h^* -polynomials equals the h^* -polynomial of the convex hull of $P \times \{0\} \times \{0\}$ and $\{0\} \times Q \times \{1\}$.

6.4 Use the methods of proof of Theorem 6.4.1 to show that the projection of a Gorenstein polytope of codegree r along a special simplex of dimension $r - 1$ yields a reflexive polytope with the same h^* -polynomial.

References

1. Barvinok, A.: Computing the ehrhart polynomial of a convex lattice polytope. *Discrete Comput. Geom.* **12**(1), 35–48 (1994)
2. Barvinok, A.: A course in convexity, *Graduate Studies in Mathematics*, vol. 54. American Mathematical Society, Providence, RI (2002)
3. Barvinok, A.: Integer Points in Polyhedra. European Mathematica Society Lecture Notes (2008)
4. Barvinok, A.I., Pommersheim, J.E.: An algorithmic theory of lattice points in polyhedra. In: New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97), pp. 91–147. Cambridge Univ. Press, Cambridge (1999)
5. Batyrev, V.V.: Dual polyhedra and mirror symmetry for Calabi–Yau hypersurfaces in toric varieties. *J. Alg. Geom.* **3**, 493–535 (1994)
6. Beck, M., Sottile, F.: Irrational proofs for three theorems of Stanley. *Eur. J. Comb.* **28**(1), 403–409 (2007). DOI 10.1016/j.ejc.2005.06.003
7. Betke, U., McMullen, P.: Lattice points in lattice polytopes. *Monatsh. Math.* **99**, 253–265 (1985). DOI 10.1007/BF01312545
8. Bruns, W., Gubeladze, J.: Polytopes, Rings, and K-Theory. Monographs in Mathematics. Springer-Verlag (2009). XIV, 461 p. 52 illus.
9. Danilov, V.I., Khovanskii, A.G.: Newton polyhedra and an algorithm for computing Hodge–Deligne numbers. *Math. USSR Izvestiya* **29**(2), 279–298 (1987)
10. De Loera, J.A., Hemmecke, R., Yoshida, R., Tauzer, J.: *lattice* (2005). <http://www.math.ucdavis.edu/~latte/>
11. deLoera, J., Santos, F., Rambau, J.: Triangulations, *Algorithms and Computation in Mathematics*, vol. 25. Springer (2010)
12. Draisma, J., McAllister, T.B., Nill, B.: Lattice width directions and minkowski’s 3^d -theorem (2009)
13. Erdahl, R.M., Ryshkov, S.S.: On lattice dicing. *Eur. J. Comb.* **15**(5), 459–481 (1994). DOI 10.1006/eujc.1994.1049
14. Grötschel, M., Lovász, L., Schrijver, A.: Geometric algorithms and combinatorial optimization, *Algorithms and Combinatorics*, vol. 2, second edn. Springer-Verlag, Berlin (1993)
15. Hille, L., Skarke, H.: Reflexive polytopes in dimension 2 and certain relations in $SL_2(\mathbb{Z})$. *J. Algebra Appl.* **1**(2), 159–173 (2002). DOI 10.1142/S0219498802000124
16. Kempf, G.R., Knudsen, F.F., Mumford, D., Saint-Donat, B.: Toroidal Embeddings I, *Lecture Notes in Mathematics*, vol. 339. Springer-Verlag (1973)
17. Köppe, M.: Latte macchiato – an improved version of latte (2007). <http://www.math.uni-magdeburg.de/~mkoeppe/latte/>
18. Köppe, M., Verdoolaege, S.: Computing parametric rational generating functions with a primal barvinok algorithm. *Electronic journal of Combinatorics* **15** (2008)
19. Lenstra, A.K., Lenstra, H.W., Lovász, L.: Factoring polynomials with rational coefficients. *Math. Ann.* **261**(4), 515–534 (1982)
20. Ohsugi, H., Hibi, T.: Convex polytopes all of whose reverse lexicographic initial ideals are squarefree. *Proc. Am. Math. Soc.* **129**(9), 2541–2546 (2001)
21. Poonen, B., Rodriguez-Villegas, F.: Lattice polygons and the number 12. *Amer. Math. Monthly* **107**(3), 238–250 (2000)
22. Schrijver, A.: Theory of linear and integer programming. Wiley-Interscience Series in Discrete Mathematics. A Wiley-Interscience Publication. Chichester: John Wiley & Sons Ltd. (1986)
23. Schrijver, A.: Combinatorial optimization. Polyhedra and efficiency (3 volumes). *Algorithms and Combinatorics* 24. Berlin: Springer. (2003)
24. Scott, P.R.: On convex lattice polygons. *Bull. Austral. Math. Soc.* **15**(3), 395–399 (1976)

- 25. Stanley, R.P.: Decompositions of rational convex polytopes. Ann. Discrete Math. **6**, 333–342 (1980). Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978)
- 26. Stanley, R.P.: A monotonicity property of h -vectors and h^* -vectors. European J. Combin. **14**(3), 251–258 (1993). DOI 10.1006/eujc.1993.1028. URL <http://dx.doi.org/10.1006/eujc.1993.1028>
- 27. Sullivan, S.: Compressed polytopes and statistical disclosure limitation. Tohoku Math. J. (2) **58**(3), 433–445 (2006). URL <http://projecteuclid.org/getRecord?id=euclid.tmj/1163775139>. Preprint [arXiv:math.CO/0412535](https://arxiv.org/abs/math/0412535)
- 28. Ziegler, G.M.: Lectures on Polytopes, *GTM*, vol. 152. Springer-Verlag (1995)

Index

— Symbols —

h^* -polynomial 39, 39, 41, 44 f.
 PICK's formula 21
 PICK's theorem 21
 f-vector 10

— A —

addition property 78, 80
 adjacent 10
 affine combination 1
 algorithm
 Barvinok's \sim 48, 52
 LLL 49 f., 52, 54, 56
 weakly reduced basis 55

— B —

Barvinok's algorithm 48, 52
 basis
 of a lattice 11
 beneath 2
 beyond 2
 Birkhoff polytope 76
 Blichfeldt's Theorem 61
 boundary complex 30
 Brianchon-Gram identity 46
 Brion
 Theorem of \sim 49
 Brion's Theorem 48, 49

— C —

cell
 maximal 30
 of a polyhedral complex 30
 codegree
 of a lattice polytope 44
 complex
 cell of a polyhedral \sim 30
 dimension of a polyhedral \sim 30
 polyhedral
 dimension 30
 facets 30
 maximal cell 30
 pure 30
 subcomplex 30
 polyhedral \sim 30
 compressed polytope 84
 cone
 dual 4
 face of 8
 finitely generated 2
 fundamental parallelepiped 31
 Gorenstein 75
 half-open 31, 35 f., 43
 homogeneous 18
 index 49

lineality space 5
 minimal proper face 10
 over a polytope 6, 37
 pointed 5
 polar 4
 polyhedral 2
 proper face of 8
 subdivision 31
 triangulation 31
 cone 2
 conic combination 1
 contingency table 28
 convex combination 1
 coset 15
 counting function 29, 38 f.
 covering radius 65

— D —

degree
 of a lattice polytope 44
 determinant
 of a lattice 15
 dilation of a set 29
 dimension
 of a face 8
 of a polyhedral complex 30
 of a polytope 7
 distance function 14
 dual lattice 11

— E —

edge 10
 Ehrhart counting function 29, 38 f.
 Ehrhart polynomial 27, 33, 39, 39, 41, 43,
 45
 Ehrhart series 37, 39
 Ehrhart's theorem 39
 Ehrhart-Macdonald reciprocity 43
 extremal ray 10

— F —

face
 dimension 8
 minimal 9
 minimal proper 10
 of a polytope 8
 proper, of a polytope 8
 face vector 10
 facet
 special 80
 facets
 of a polyhedral complex 30
 fan
 smooth blow-up 71
 far half-open cone 31, 36
 far half-open parallelepiped 31

Parkas Lemma	4	reduced basis	53
formal Laurent series	34	standard integer \sim	11
free sum	78	sublattice	15
full dimensional	8	transformation	15
fundamental parallelepiped	31, 35, 49	unimodular	15
		weakly reduced basis	53
— G —		lattice isomorphic	20
Generalized Blichfeldt’s Theorem	63	lattice isomorphism	20
generic reference point	31	lattice polytope	20
Gorenstein cone	75	codegree	44
Gorenstein polytope	69, 74, 76, 77	compressed	84
Gram-Schmidt orthogonalization	53	degree	44
		lattice isomorphic	20
— H —		normalized volume	24, 40
half-open cone	31, 35 f., 43	unimodularly equivalent	20
half-open decomposition	31, 35 f., 43	lattice transformation	15
half-open parallelepiped	31	Laurent polynomial	34
half-open simplex	31	Laurent polynomial ring	34
half-space		Laurent series	34, 35 f.
affine	1	summable	35
linear	1	lineality space	
Hermite normal form	15	of a cone	5
Hilbert basis	17	linear combination	1
minimal	17	LLL	50
homogeneous	18	LLL algorithm	49, 52, 54, 56
hyperplane		— M —	
affine	1	minimal face	
linear	1	of a polytope	9
supporting	8	minimal proper face	10
valid	8	Minkowski sum	5
		Minkowski’s First Theorem	62, 63
— I —		Minkowski’s Second Theorem	63
implied equality	7	Minkowski’s Theorem	5
index		mirror symmetry	69
of a cone	49	— N —	
of a lattice	15	near half-open cone	31, 36
inner normal		near half-open parallelepiped	31
primitive	69	normal form	
integer point generating function 36, 36 f.,		Hermite \sim	15
46, 48		normalized volume	24, 40
integer point series	35, 36	— P —	
summable	35	packing radius	64
integral polytope	20	parallelepiped	12
integrally closed	86	fundamental	31, 35, 49
interior point	8	half-open	31
irredundant	8	Pick’s Theorem	21, 71
		polar polytope	70
— K —		polyhedral complex	30
KMW number	88	cell	30
KMW Theorem	88	dimension	30
Knapsack problem	27	facets	30
		maximal cell	30
— L —		pure	30
lattice	11, 64	subcomplex	30
basis	11	polynomial	
determinant	15	h^*	39, 39, 41, 44 f.
index	15	Ehrhart	27, 33, 39, 39, 41, 43, 45

Laurent 34
 polynomial ring
 Laurent 34
 polytope 6, 6
 boundary complex 30
 compressed 84
 cone over a 6
 dimension 7
 edge 10
 extremal ray 10
 face of 8
 free sum 78
 Gorenstein 69, 74, 76, 77
 integral 20
 integrally closed 86
 interior point 8
 lattice 20
 minimal face 9
 normalized volume 24, 40
 polar 70
 proper face of 8
 reflexive 69, 70, 70 ff., 74, 77 f.
 special simplex 86
 subdivision 31
 triangulation 31
 vertex of 10
 primitive 13
 primitive inner normal 69
 pulling refinement 84

— R —

rational subspace 12
 reduced basis 53
 redundant 8
 reflexive polytope .. 69, 70, 70 ff., 74, 77 f.
 addition property 78, 80
 regular subdivision 83

— S —

Scott's theorem 22
 series
 Ehrhart 37, 39
 formal Laurent 34
 Laurent 34, 35 f.
 summable 35
 set
 dual 4
 polar 4
 simplex
 half-open 31
 standard 24, 29
 unimodular 24
 unit 29
 smooth blow-up
 of a fan 71
 special facet 80
 special simplex 86
 standard simplex 24, 29
 standard triangulation of dilated simplex
 86
 Stanley Reciprocity 43

Stanley's Monotonicity theorem 41
 subcomplex 30
 subdivision 31
 regular 83
 trivial 30
 sublattice 15
 successive minimum 62
 summable 35

— T —

Theorem
 Generalized Blichfeldt's ~ 63
 KMW 88
 Minkowski's First ~ 62, 63
 Minkowski's Second ~ 63
 of Brianchon-Gram 46
 of Brion 48
 of Minkowski 5
 of Pick 21
 of Weyl 3
 Pick's ~ 71
 Stanley's Monotonicity 41
 van der Corput's ~ 63
 Weyl-Minkowski 2
 theorem
 PICK'S 21
 Blichfeldt 61
 Ehrhart-Macdonald 43
 flatness 67
 of Ehrhart 39
 Scott's 22
 Stanley Reciprocity 43
 Stanley's nonnegativity~ 40
 Theorem of Brianchon-Gram 46
 Theorem of Brion 49
 transformation
 lattice 15
 unimodular 15
 triangulation 31, 36
 pulling refinement 84
 standard of dilated simplex 86
 unimodular 83
 without new vertices 31
 trivial subdivision 30

— U —

unimodular
 of a lattice 15
 triangulation 83
 unimodular simplex 24
 unimodular transformation 15
 unimodularly equivalent 20
 unit simplex 29
 university degrees 28

— V —

vertex
 of a polytope 10
 vertex-edge graph 79
 volume

normalized 24, 40

— W —

weakly reduced basis 53, 55

Weyl’s Theorem 3

Weyl-Minkowski Duality 2

width 67

Name Index

— A —

Athanasiadis 86

— B —

Barvinok 48
Betke 87
Blichfeldt 61, 63
Brianchon 46
Brion 48 f.
Bruns 86

— E —

Ehrhart 29, 37, 39, 43

— F —

Fourier 2

— G —

Gram 46

— H —

Hermite 15
Hibi 85
Hilbert 17

— K —

Knudson 88

— L —

Lenstra, Arjen 49, 52, 54
Lenstra, Hendrik 49, 52, 54
Lovász, László 49, 52, 54

— M —

Macdonald 43
McMullen 87
Minkowski 2, 62 f.
Motzkin 2
Mumford 88

— O —

Oshugi 85

— P —

Pick 21, 71
Pommersheim 48

— R —

Römer 86

— S —

Santos 85
Scott 22
Stanley 40 f., 43, 84
Sullivant 85

— V —

van der Corput 63

— W —

Waterman 88
Weyl 2