Lecture Notes on *Lattice Polytopes*

(**draft of June 28, 2021**)

June 28, 2021

Discrete Geometry III; Summer 2019

TU Berlin

Christian Haase • *Benjamin Nill* • *Andreas Paffenholz*

$\mathbb{R}$ real numbers `\R`
$\mathbb{R}_{>0}$ positive integers `\Rg`
$\mathbb{R}_{\geq 0}$ nonnegative integers `\Rge`
$\mathbb{R}_{<0}$ negative integers `\Rl`
$\mathbb{R}_{\leq 0}$ nonpositive integers `\Rle`
$\mathbb{Q}$ rational numbers `\Q`
$\mathbb{Z}$ integers `\Z`
$\mathbb{Z}_{>0}$ positive integers `\Zg`
$\mathbb{Z}_{\geq 0}$ nonnegative integers `\Zge`
$\mathbb{Z}_{<0}$ negative integers `\Zl`
$\mathbb{Z}_{\leq 0}$ nonpositive integers `\Zle`
$(\mathbb{R}^d)^\star, (\mathbb{Q}^d)^\star, (\mathbb{Z}^d)^\star$ the dual spaces `\Rdual, \Qdual, \Zdual`
$\mathcal{T}$ a triangulation `\triang`
Δ_d a simplex `\simplex`
a the vector with variable name a, all others similar `\va`
$\mathcal{V}(P)$ the vertices of a polytope P `\verts(P)`
$\mathcal{F}(P)$ the facets of a polytope P `\facets(P)`
∂P the boundary (complex) of P `\boundary P`
$\Pi(V)$ the fundamental parallelepiped of V `\fp(V)`
G the integer point generating function`\IntPtGenF`(shortcuts siehe .sty oder Text)
$\widehat{\mathsf{G}}$ the integer point generating series`\IntPtGenS`
$\lfloor a \rfloor$ the largest $z \in \mathbb{Z}$ with $z \leq a$ `\floor`

$\lceil a \rceil$ the smallest $z \in \mathbb{Z}$ with $z \geq a$ `\ceil`
$\{a\}$ the fractional part $a - \lfloor a \rfloor$ of a `\fracpart`
$\mathscr{A}$ a point/vector configuration, usually $P \cap \mathbb{Z}^d$ `\configuration`
ehr the Ehrhart counting function `\ehrcount`
$\widehat{\mathsf{Ehr}}$ the Ehrhart series `\ehrseries`
$\Bbbk$ a field `\kk`
1 the column vector with all entries equal to 1 `\1`
0 the column vector with all entries equal to 1 `\0`
C the cone over a polytope `\pcone`
$C^\star$ the dual cone to C `\dpcone`
$h^\star$ coefficients of the $h^\star$-polynomial `\hstar`
f f-vector entries `\fvec`
$\mathsf{T}_F P$ Tangent cone of a face `\tangentcone{P}{F}`
$\widehat{\mathsf{L}}$ Laurent series`\LaurentS`
L Laurent polynomials`\LaurentP`
Q Laurent quotient`\LaurentQ`
R Laurent rational functions `\LaurentR`
Φ The map onto the rational functions `\LaurentHom`
$F \preceq P$ F is a face of P `\isfaceof`
$C^\star$ `\dual C`
$C^{\star\star}$ `\ddual C`
$C^{\star\star\star}$ `\dddual C`
$\mathcal{C}$ a polyhedral complex `\pcomplex`
$\mathcal{S}$ a subdivision `\psubdiv`
$\mathrm{pull}(\mathcal{S}; v)$ a pulling refinement `\pull{\psubdiv}{\vv}`
$\mathrm{star}(\S; F)$ open star of a face F in a complex $\mathcal{S}$ `\Star{\S}{F}`
$\overline{\mathrm{star}}(\S; F)$ closed star of a face F in a complex $\mathcal{S}$ `\clStar{\S}{F}`
$\mathcal{V}(P)$ vertices of P
$\operatorname{rank} A$ rank of A
$\operatorname{lin} A$ linear space spanned by A
$\operatorname{aff} A$ affine hull of A
$\operatorname{conv} A$ convex hull of A
$\operatorname{cone} A$ conic hull of A
$P \star Q$ the join of P and Q `P \join Q`
vol the (normalized?) volume `\vol`
$\mathrm{nvol}_{\mathbb{Z}^d}$ the normalized volume `\Vol`
$\operatorname{lineal} A$ lineality space of P
$\mathcal{S}_w(V)$ regular subdivision induced by w on V `\regsubdiv{\vw}{V}`
$\mathrm{lift}(w)$ the convex hull of the lift of V by w `\reglift{\vw}{V}`
Ψ_w the convex piecewise linear function `\regfunction{\vw}{V}`
id The identity matrix
The zero matrix
Λ A lattice `\lattice`

$\hat{\Lambda}$ The mother lattice `\lambdahat`
$\mathcal{B}$ A basis of a lattice
$\operatorname{width}(K;a)$ width of convex body K wrt functional $a \in \Lambda^\star$ `\width{K}{\va}`
$\operatorname{width}_\Lambda(K)$ width of convex body K wrt lattice Λ `\lwidth{K}{\lattice}`
$\varrho\,\Lambda$ packing radius of a lattice `\packingradius{\lattice}`
$\mu\,\Lambda$ covering radius of a lattice `\coveringradius{\lattice}`
η_F The unique primitive inner normal of a facet F of a polytope `\innP_F`
u_F The unique primitive inner normal of C_P corresponding to the facet F of a polytope P `\innC_F`
u_P The unique lattice point of the Gorenstein cone C_P satisfying $\langle\, u_P, x \,\rangle = 1$ for any primitive generator of C_P `\innC_P`
$P^\vee$ The Gorenstein polytope dual to P `dualG␣P*fi`
Δ_d The standard simplex $\operatorname{conv}(\mathbf{0}, e_1, \ldots, e_d)$
C_d The unit cube $\{x \in \mathbb{R}^d \mid \mathbf{0} \le x \le \mathbf{1}\} = [0,1]^d$.
$\mathsf{T}_F P$ The tangent cone to P at F `\tangentcone{P}{F}`
$\operatorname{visible}_P(m)$ The complex of faces of P visible from m `\visible{P}{\vm}`

invitation durchlesen, fertig? exercises? B
neuere Resultate zusammenstellen, klassifizieren rein/exercise/notes/raus
– Ehrhart
– GoN
– UT
Struktur sortieren Kap. GoN vs MinkowskiEhrhart; zus"atzliche Themen??
2.3 Lattices streamlinen C
Ch. 2 running examples A
Ch. 3 Ehrhart – Todos
Ch. 4 GoN – gegen Ende gro"se Baustelle (include size?)
Ch. 5 Ehrhart meets Minkowski zu kurz
Ch. 6 Algorithmen schreiben A
Ch. 7 Gorenstein
Ch. 8 UT
somewhere: Cayley-korrespondenz via lattice-point-Zerlegung im dualen Kegel
somehwere: Minkowski-sums and refinement of normal fan, Cayley-Trick

how do we attribute results? in parantheses after “Theorem xy”? In a separate senctence before or after? Do we give a citation, a year? How do we do this for theorems with a name (like *Ehrhart's Theorem*)?

An invitation to lattice polytopes

1

Contents

In this chapter we would like to give the reader a gentle introduction to the main players of this book. For this, we will mainly stick to objects in two dimension, that is, we will consider polygons, their subdivisions into smaller pieces and the lattice of all points with integer coordinates. However, the reader will already encounter many methods and types of results studied in more detail later, among them are triangulations, lattice point counting, estimating volumes, and several classification results.

Our goal is to convey a first impression of the rich flavours of lattice polytope theory. This is a branch of convex-discrete geometry with an algebraic touch and a hint of number theory. It is surprising how many of the interesting features of lattice polytopes already appear in dimensions one, two or three. And there is no shortage of open questions for these seemingly elementary objects.

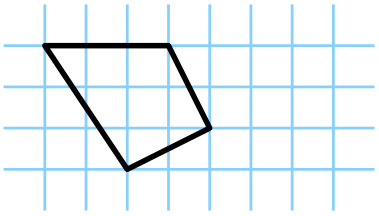


Fig. 1.1: A lattice polygon

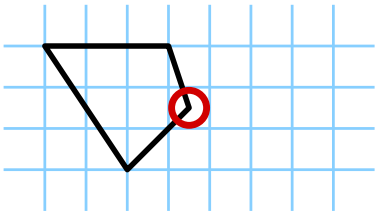


Fig. 1.2: non-lattice

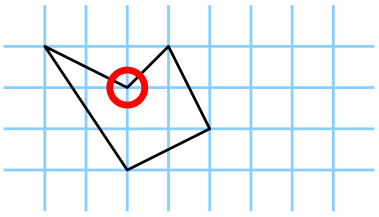


Fig. 1.3: non-convex

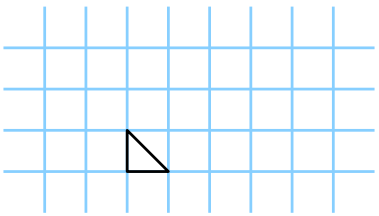


Fig. 1.4: $(b, i, a) = (3, 0, 1/2)$

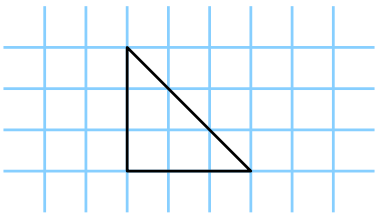


Fig. 1.5: $(b, i, a) = (9, 1, 4.5)$

1.1 Before we begin

Before reading on, we would like to invite the reader to pull out a sheet of graph paper and play with lattice polygons, making one's first own discoveries and building a feeling and an appreceation for the objects and the questions treated in this book.

When we say *lattice polygon*, we mean a closed convex polygon with all vertices at crossing points of your graph paper as in Figure 1.1 (and not as in Figs. 1.2 and 1.3).

For such a polygon, we can record the number b of graph-paper-crossing-points on the boundary, the number i of graph-paper-crossing-points in the interior, and the enclosed area a measured in units of graph-paper-squares. For example, our first polygon above has $(b, i, a) = (6, 5, 7)$.

Your task is now to play with these figures and find out what triples (b, i, a) you can achieve. That is, if I say $(3, 0, 1/2)$, you draw the picture in Figure 1.4, and if I say $(9, 1, 4.5)$, you draw the picture in Figure 1.5. The reader is invited to try realizing the cases $(5, 2, 4)$, $(18, 0, 9)$, $(3, 17, 17.5)$ and $(11, 2, 6.5)$.

1.2 Lattice polygons and isomorphisms

In this section, we formally introduce *lattice polygons*, which are the key player of this chapter, find a famous connection between its lattice points and its volume, and develop the appropriate notion of when to consider two such polygons the same.

Definition 1.1 *A* lattice polygon *is the convex hull in* $\mathbb{R}^2$ *of finitely many points in* $\mathbb{Z}^2$.

Here, the word *lattice* refers to $\mathbb{Z}^2$ whose elements we call *lattice points*. In other words, in dimension 2, lattice points are simply the points on the grid given by the vectors with all coordinates integral. A lattice polygon is the smallest convex set that contains a given finite set of lattice points. Restricting the vertices to lattice points is quite restrictive. In particular, a lattice polygon cannot be arbitrarily small. We bound the volume with the next proposition. We will see that even more is true. Any polygon with this volume will be a triangle, and any such triangles are equivalent to each other in some sense we develop below.

Proposition 1.2 (Pick's Theorem) *Any lattice triangle with only three lattice points (which must be its vertices) has area* $1/2$.

This Proposition may seem unspectacular, at first. But it is remarkable in several ways. First, the corresponding statement is plain wrong in

higher dimensions (see (1.1) below). Second, it is the key ingredient in the proof of Pick's Formula (Theorem 1.8) answering whether or not the triple $(5, 2, 4)$ from Section 1.1 comes from a lattice polygon. Lastly, its proof uses methods we will come across in several places throughout this book, and it leads us to the notion of lattice equivalence that we develop in Definition 1.4.

Proof (of Proposition 1.2). A translation by a lattice vector preserves the number of lattice points as well as the area. Thus, we can assume that our triangle Δ is the convex hull of the origin $\mathbf{0}$ together with two linearly independent lattice vectors v and w.

Consider the set

$$\Pi(v, w) \;:=\; \{\lambda v + \mu w \;:\; \lambda, \mu \in [0, 1)\}$$

(cf. Figure 1.6). This is a *half-open parallelogram*, where the segments between the origin and v and w (but not v, w itself!) belong to the set, the other two bounding segments do not.

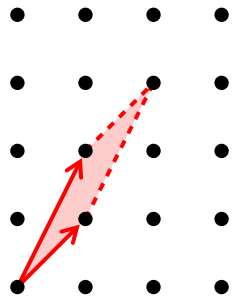


Fig. 1.6: The half-open parallelogram in the proof of Pick's Theorem (Proposition 1.2)

Its area, $|\det[v, w]|$, the absolute value of the determinant of the matrix with columns v and w, equals twice the area of Δ.

We claim that $\Pi(v, w) \cap \mathbb{Z}^2 = \{\mathbf{0}\}$. Suppose $u = \lambda v + \mu w \in \Pi(v, w) \cap \mathbb{Z}^2$. Then either we have $\lambda + \mu \leq 1$ so that u is a lattice point in Δ which leaves only $u = \mathbf{0}$ as $v, w \notin \Pi(v, w)$. Or we have $\lambda + \mu > 1$ so that the reflection $v + w - u$ of u in the parallelogram's center is a lattice point in the interior of Δ; a contradiction.

Now, every lattice point $z \in \mathbb{Z}^2$ can be expressed in terms of v, w:

$$z \;=\; \lambda v + \mu w \;=\; \lfloor\lambda\rfloor v + \lfloor\mu\rfloor w + u$$

where

$$u \;=\; (\lambda - \lfloor\lambda\rfloor)v + (\mu - \lfloor\mu\rfloor)w \;\in\; \Pi(v, w)$$

but also

$$u \;=\; z - \lfloor\lambda\rfloor v - \lfloor\mu\rfloor w \qquad\qquad \in\; \mathbb{Z}^2\,.$$

By the above we must have $u = \mathbf{0}$, that is, z is an integer linear combination of v and w.

If we apply this to the standard basis vectors e_1 and e_2, we obtain integral coefficients fitting into the matrix equation

$$[v, w] \begin{pmatrix} \lambda & \lambda' \\ \mu & \mu' \end{pmatrix} \;=\; \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Because the determinant is multiplicative, the reciprocal of the integer $\det[v, w]$ is an integer. Hence, $\det[v, w] = \pm 1$ and Δ has area $1/2$. □

We will dwell on this proof a little longer. The method of decomposing an arbitrary lattice point z into an integral linear combination of v and w plus a lattice point from the parallelogram is an instance of a general decomposition, Lemma 3.26, which we will use over and over again.

Moreover, this proof shows more than what we set out to prove. It shows that, if $\Delta = \operatorname{conv}(\mathbf{0}, v, w)$ is such a lattice triangle with only three lattice points, then every lattice point is an integral linear combination of v and w and thus the matrix $[v, w]$ has an intergral inverse and its determinant is ± 1. This deserves a definition.

Definition 1.3 *A vector space basis v, w of $\mathbb{R}^2$ is a* lattice basis *of $\mathbb{Z}^2$ if the set of integral linear combinations equals $\mathbb{Z}^2$:*

$$\{\lambda v + \mu w \ : \ \lambda, \mu \in \mathbb{Z}\} \ = \ \mathbb{Z}^2 \, .$$

In other words, a lattice basis of $\mathbb{Z}^2$ consists of two integral vectors so that every other integral vector is an integral linear combination of these two. A change of basis matrix A must have integer entries (Why?), and so must its inverse A^{-1}. We define

$$\mathrm{Gl}_2(\mathbb{Z}) := \{A \in \mathrm{Gl}_2(\mathbb{R}) \ : \ A, \ A^{-1} \in \mathbb{Z}^{2\times 2}\}.$$

A change of lattice basis corresponds to a linear map $\mathbb{R}^2 \to \mathbb{R}^2$ represented by the change of basis matrix in $\mathrm{Gl}_2(\mathbb{Z})$. We do not care which lattice basis we use to coordinatize a given lattice polygon. So we will consider to lattice polygons the same if they are related by such a $\mathrm{Gl}_2(\mathbb{Z})$-map. Also, it should not matter which lattice point we declare to be the origin. Therefore, we also allow translations by lattice vectors, leading us to consider affine maps

$$x \mapsto Ax + b, \quad \text{with } A \in \mathrm{Gl}_2(\mathbb{Z}) \text{ and } b \in \mathbb{Z}^2 \, .$$

We call such maps *affine lattice automorphisms* of $\mathbb{Z}^2$ or *unimodular transformations.*

Definition 1.4 *Two lattice polygons P and P' are* isomorphic *(also called* unimodularly equivalent *or* lattice equivalent*), if there is an affine lattice isomorphism mapping P onto P'.*

Exercise 1.1
Exercise 1.2
Exercise 1.3
Exercise 1.4
Exercise 1.5

A more general definition is given in the next chapter (see Definition 2.74). With the new nomenclature, we can formulate a stronger version of Pick's Theorem (Proposition 1.2) which follows from our proof. For this let us denote by

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

the *standard* or *unimodular* triangle.

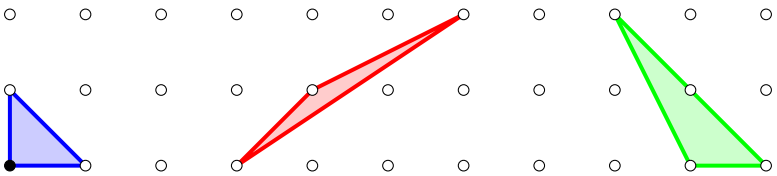


Fig. 1.7: Lattice Triangles

Proposition 1.5 *Any lattice triangle with only three lattice points is isomorphic to* Δ_2.

It is important to build an intuition what these unimodular transformations are, and what they do. Figure 1.7 shows three examples of lattice triangles. The 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. They cannot be lattice equivalent, as unimodular transformations preserve the number of lattice points by design. But the lower two triangles are equivalent by Proposition 1.5. If we pick the filled lattice point as the origin and the other two vertices of the third triangle as basis vectors $(1,0)$ and $(0,1)$. Then the second and third triangles are indeed isomorphic by the following affine lattice isomorphism:

$$\mathbb{Z}^2 \to \mathbb{Z}^2 \colon x \mapsto \begin{pmatrix} -1 & 1 \\ -1 & 2 \end{pmatrix} x + \begin{pmatrix} 1 \\ 4 \end{pmatrix} .$$

There are five more lattice isomorphisms carrying the third triangle to the second. The reader is invited to find them. Exercise 1.6

So angles and Euclidean distances are not preserved by unimodular transformations. But, as we observed at the end of the proof of Pick's Theorem (Proposition 1.2), a change of lattice basis has determinant ± 1 (cf. Exercise 1.7). So unimodular transformations do preserve the area. And there is also a replacement for Euclidean length. Exercise 1.7

Definition 1.6 *The* lattice length *of a lattice segment* $e = \operatorname{conv}(v, w) \subset \mathbb{R}^d$ *is*

$$\operatorname{length}(e) := |e \cap \mathbb{Z}^d| - 1 .$$

As this is the only reasonable notion of length in our context, we often refer to the lattice length of a segment simply as its length. The following is a summary of what we know thus far.

Proposition 1.7 *Equivalent lattice polygons contain the same number of lattice points, they have the same area and the same lattice perimeter.* □

Pick's Theorem (Proposition 1.2) about the area of triangles is at the heart of the proof of Pick's Formula (Theorem 1.8) in the next section. Be

warned, however, that the corresponding version fails in higher dimensions. This is famously shown by the so called *Reeve simplices*:

$$\mathsf{R}_d(m) := \operatorname{conv}\left(\mathbf{0}, e_1, e_2, \ldots, e_{d-1}, \sum_{i=1}^{d-1} e_i + me_d\right) \tag{1.1}$$

Here, d is the dimension of the simplex, and m is a positive integer (its normalized volume, see Definition 2.80 in the next chapter for this notion). Figure 1.8 depicts the 3-dimensional Reeve simplex $\mathsf{R}_3(4)$. As the reader is encouraged to prove in Exercise 1.9, any such simplex has only its vertices as lattice points. This shows that in dimension $d \geq 3$ there are infinitely many lattice simplices containing only $d+1$ lattice points each and which have pairwise different volumes. In particular they are non-isomorphic. As we will discuss later in Section 4.6, this makes life considerably more interesting in higher dimensions, and it highlights once more how remarkable Pick's Theorem (Proposition 1.2) really is.

Exercise 1.9

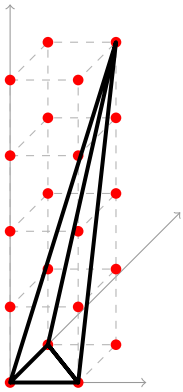


Fig. 1.8: Reeve's Tetrahedron

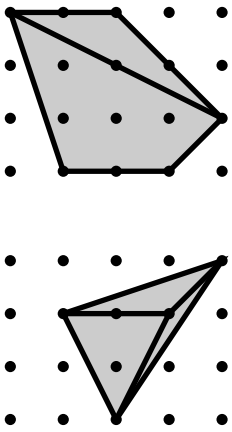


Fig. 1.9: Splitting P into pieces. The first image is for the case $b \geq 4$, the second for $i \geq 1$.

1.3 Triangulations and Pick's formula

The goal of this section is to prove an elegant formula for the computation of the area of a lattice polygon just by counting lattice points. We have seen this miracle already for triangles (Pick's Theorem (Proposition 1.2)) and we will now generalize it to arbitrary lattice polygons. We thus find a first relation among the parameters b, i, a from Section 1.1.

Keep in mind that the Reeve simplices (1.1) exclude a straightforward generalization to higher dimensions. To find some generalization is the topic of Chapter 3 on Ehrhart Theory.

Theorem 1.8 (Pick's Formula) *Let P be a lattice polygon with i interior lattice points, b lattice points on the boundary, and (Euclidean) area a. Then*

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

This shows, for instance, that the triple $(5, 2, 4)$ from Section 1.1 can never come from a lattice polygon.

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

The smallest case $b = 3$ and $i = 0$ is covered by Pick's Theorem (Proposition 1.2). There are two cases to consider for the induction: (1) either P has $b \geq 4$ lattice points on the boundary, or (2) $b = 3$ 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 area a_j, b_j boundary lattice points, and i_j interior lattice points, respectively. Let e have i_e interior lattice points (and two boundary lattice points). Both Q_1 and Q_2 have less than l lattice points, so by induction Pick's Formula holds for Q and Q', i.e.

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

Further

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

so

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

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 1.9.

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 as the one above shows that Pick's Formula also holds for P (see Exercise 1.10). □

The reader is invited to prove that the same relation is true for non-convex lattice polygons in Exercise 1.13. One can also prove that this theorem is equivalent to the Euler relation (see Exercise 1.11). Note that the same induction shows that any lattice polygon can be subdivided into triangles which are isomorphic to Δ_2 (called *unimodular triangles*). As the Reeve simplex shows, this is not true in higher dimensions. Questions about the existence of such unimodular triangulations will be discussed in the last Chapter 8 of this book. See also Exercise 1.12.

The idea of subdiving a convex object into triangles, or simplices in dimensions 3 and above, is quite influential. We will devote a whole chapter to this (Chapter 8).

Definition 1.9 (Triangulation) *Let P be a lattice polygon. A* (lattice) triangulation *of P is a collection $\mathcal{S}$ of lattice triangles such that*

(1) Any two triangles $\Delta_d, simplex' \in \mathcal{S}$ intersect in an edge of both, and (2) the union (as point sets) of all triangles is P.

Figure 1.10 shows two configurations of triangles that are not allowed in a triangulation. In the first, the intersection is not a full edhe in both, in

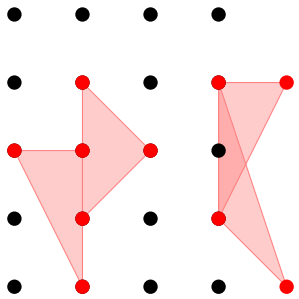


Fig. 1.10: Not allowed in a triangulation

Exercise 1.10

Exercise 1.11

Exercise 1.12

the second, the triangles intersect in more than an edge. A proper lattice triangulation is shown in Figure 1.11.

In fact, Pick's Formula (Theorem 1.8) also holds in a non-convex setting. We can generalize it to any (non-convex) lattice polygon with the property, that any vertex is incident to exactly two edges and no edges intersect. You will prove this in Exercise 1.13.

Exercise 1.13

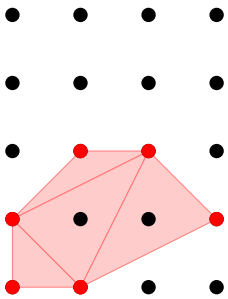


Fig. 1.11: A triangulation

1.4 A Classification of Lattice Polygons

Scott's theorem gives a precise bound on how large a lattice polygon can be, given the number of interior lattice points. It thus provides the answer to all questions (triples) from the end of Section 1.1. Problems like these, which relate information about lattice points of a convex body to its geometry and its invariants are subject of the field of Geometry of Numbers. We deal with such questions again in Chapter 4.

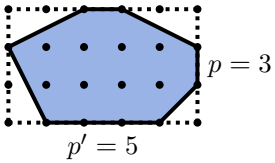


Fig. 1.12: P in a box

Theorem 1.10 (Scott, 1976 [51]) *Let $P \subset \mathbb{R}^2$ be a lattice polygon with $i \geq 1$ interior lattice points and Euclidean volume a. Then either*

(1) $P \cong 3\,\Delta_2$ and hence, $a = 9/2$ and $i = 1$, or
(2) $a \leq 2(i+1)$.

Proof. Let b be the number of boundary lattice points. Using Pick's Formula (Theorem 1.8) we can reformulate the condition to

$$b \;\leq\; a + 4$$

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

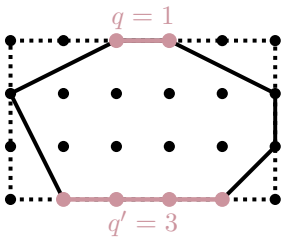


Fig. 1.13: The bottom and top edge of P

Lattice isomorphisms preserve a, b and i, so we can place P tightly into a rectangle $R := [0, p'] \times [0, p]$ and p is the smallest possible among all lattice equivalent P. Then $p \geq 2$ as $i \geq 1$. Exchanging coordinates is a lattice isomorphism, so we have

$$2 \;\leq\; p \;\leq\; p'. \tag{1.2}$$

The polygon P intersects the bottom and top edge of the rectangle in edges of length q and q', see Figure 1.12.

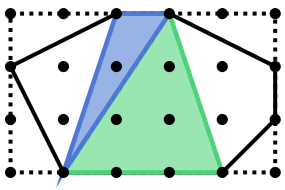


Fig. 1.14: Bounding the volume

At most $2(p-1)$ boundary lattice points of P are not on the two horizontal edges of R, so

$$b \;\leq\; q + 1 + p - 1 + q' + 1 + p - 1 \;=\; q + q' + 2p. \tag{1.3}$$

Subdividing the convex hull of the top edge and the bottom edge into two triangles as in Figure 1.14 we get

$$a \;\geq\; \frac{1}{2}pq + \frac{1}{2}q'p \;=\; \frac{p}{2}(q + q'). \tag{1.4}$$

Using Pick's Formula (Theorem 1.8) and $i \geq 1$ we also know that

$$a \geq b/2\,. \tag{1.5}$$

We split the proof into four cases:

(1) $p = 2$ or $q + q' \geq 4$,
(2) $p = q + q' = 3$,
(3) $p = 3$ and $q + q' \leq 2$,
(4) $p \geq 4$ and $q + q' \leq 3$

For (1) we can combine (1.3) and (1.4) into

$$2b - 2a \;\leq\; 2(q + q' + 2p) - p(q + q') \;=\; (q + q' - 4)(2 - p) + 8\,, \tag{1.6}$$

which is at most 8 as the first summand is at most 0. This implies $b \leq a + 4$ as desired.

For (2) we can use the same inequality to obtain $2b - 2a \leq 9$, *i.e.* $b \leq a + 9/2$. Now, if P has at least one vertex not on the upper or lower edge of R, then (1.4) and hence also (1.6) become strict inequalities, so that in this case $b < a + 9/2$. As $a \in \frac{1}{2}\mathbb{Z}_{\geq 0}$, this implies $b \leq a + 4$. If, on the other hand, all vertices of P are on the upper and lower edge of R, then $a = p(q+q')/2 = 9/2$ and $b \leq a + 9/2 = 9$. If $b < 9$ then $b \leq a + 4$. Otherwise, all vertices are on the upper and lowe redge of R, $b = 9$, $a = 9/2$ and thus $i = 1$. A simple geometric consideration shows that then either $q = 3$ or $q' = 3$ and P must be the triangle $3\,\Delta_2$ (Exercise 1.14). In case (3) the inequlity (1.3) implies $b \leq 8$ and (1.5) shows

$$b - a \;\leq\; b - b/2 \;\leq\; 4\,.$$

Now assume we are in the forth case, so $p \geq 4$ and $q + q' \leq 3$. We choose points $L = (l, 0)$, $U = (u, p)$, $X = (0, x)$, and $Y = (p', y)$ in P such that $\delta := |u - l|$ is minimal. See Figure 1.15. We can assume that $u \leq l$ (otherwise we flip the polygon). Let $L' = (u, 0)$ and $U' = (l, p)$. The triangle S_L spanned by A, L', and U bounds the volume of the triangle spanned by X, L, and U (look at the height over the edge XU). Similarly, the triangle S_U spanned by Y, U' and L bounds the volume of the triangle Y, U, and L from below. Hence,

$$a \;\geq\; \frac{1}{2}p(p' - \delta)\,.$$

The shearing

$$v \;\mapsto\; \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} v$$

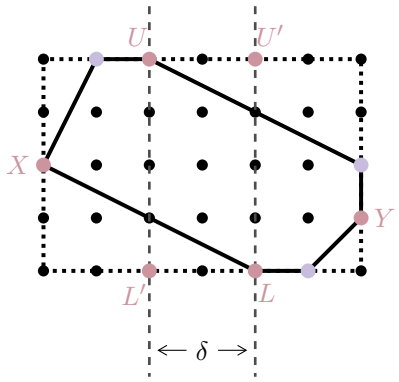


Fig. 1.15: The δ-gap

Exercise 1.14

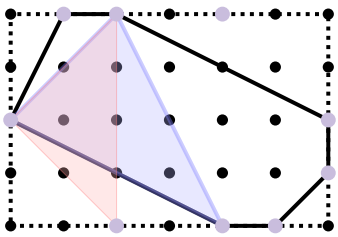
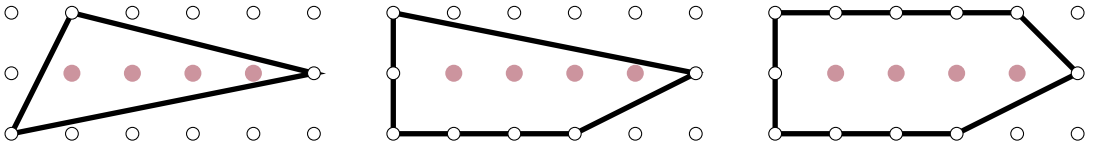


Fig. 1.16: Estimating the area of P from below: The triangle XUL



(a) Realization for $b = 3$ (b) Realization for $4 \leq b \leq i+5$ (c) Realization for $i+5 \leq b \leq 2i+6$

Fig. 1.18: Realizations of pairs (i, b) according to Scott's Theorem

is a lattice isomorphism that, if applied to P, leaves p, q, and q' invariant. Hence, we can transform P such that

$$\delta \leq \frac{1}{2}(p - q - q') . \tag{1.7}$$

As p was chosen to be minimal, we also still have $p \leq p'$ after this transformation. This implies

$$a \geq \frac{1}{4}p(p + q + q') ,$$

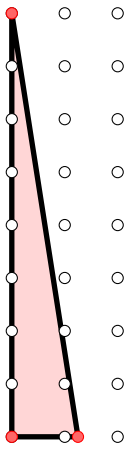


Fig. 1.17: An arbitrarily big rational triangle with one interior lattice point

so that

$$4(b - a) \leq 8p + 4q + 4q' - p(p + q + q') = p(8 - p) - (p - 4)(q + q') .$$

We have $p \geq 4$, so that the left hand side is bounded by 16. This shows $b \leq a + 4$. □

Note that for polygons that are not *lattice* polygons, there is no such upper bound on their areas. Figure 1.17 shows why.

Scott's theorem defines a polyhedral set L given by the inequalities

$$i \geq 1 \qquad a \geq 3/2 \qquad a \leq 2(i-1)$$

such that any pair (a, i) coming from a lattice polygon is either $(a, i) = (9/2, 1)$ or inside L. What about the converse? Is every point

$$(a, i) \in \frac{1}{2}\mathbb{Z} \times \mathbb{Z} \cap L$$

the volume an number of interior lattice points of some lattice polygon? This is easier to answer when we move from the pair (a, i) used in Scott's Theorem to the pair (b, i) using Pick's Theorem. With this transformation our inequalities read

$$i \geq 1 \qquad b \geq 3 \qquad b \leq 2(i+3) .$$

We can indeed realize all of these pairs of integers as the number of lattice points in the interior and the boundary of a lattice polygon. Figure 1.18 shows the construction.

Exercise 1.15

Exercise 1.16

Exercise 1.17

1.5 Dilations

If we know the number of interior and boundary lattice points of a lattice polygon P, then we know its area by Pick's Theorem. Can we also say something about dilates of P, *i.e.* about the number of interior or boundary lattice points of $k \cdot P$ for some $k \in \mathbb{Z}_{\geq 0}$? The interior points cannot just scale: Even for lattice polygons without interior lattice points all sufficiently high multiples will contain a lattice point in their interiors. However, the volume clealy scales with k^2, and the number of boundary lattice points scales with k.

We can plug this into Pick's Theorem to obtain the number $i(k)$ of interior lattice points in $k \cdot P$:

$$i(k) \;=\; ak^2 - \frac{b}{2}k + 1\,.$$

which is a polynomial of degree 2 in k with coefficients a, $-b/2$ and 1. We can reformulate this for the number $l(k) = i(k) + b(k)$ of total lattice points in $k \cdot P$ to obtain

$$l(k) \;=\; i(k) + b(k) \;=\; k^2 a - k\frac{b}{2} + 1 + kb \;=\; ak^2 + \frac{b}{2}k + 1\,,$$

which is again a polynomial of degree 2 in k. Furthermore, we observe that $i(k) = l(-k)$.

We will see that this observation is a special case of two much more general and funcamental theorems, the Theorems of Ehrhart and Ehrhart-Macdonald, which we will study in detail in Chapter 3. The catch is that in any dimension the number of lattice points in the k-th dilate of a polytope is given by a polynomial in k, and that the number of interior lattice polytopes is given (up to sign) by evaluating this same polynomial at $-k$.

1.6 Problems

1.1. Let P be the lattice polygon with the vertices A, B, C, D (and P' respectively with the vertices A', B', C', D') as given in Figure 1.19.
   (1) Compute the areas of P and P'.
   (2) Are P and P' isomorphic? If yes, find an explicit unimodular transformation mapping P to P'.

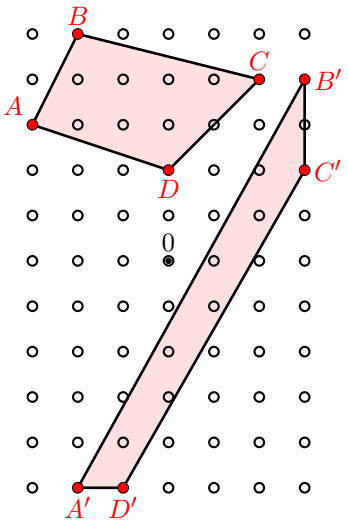


Fig. 1.19: Two lattice polygons

1.2. Exercise 1.18 included on page 8

1.3. included on page 8

included on page 8

included on page 8

1.4.

included on p

1.5.

included on p

1.6. 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 $\begin{pmatrix} 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} p & q \end{pmatrix}$ for integers $0 \leq p < q$.

included on page 9

1.7. Show that an integral matrix $A \in \mathbb{Z}^{2\times 2}$ has an integral inverse if and only if $\det A = \pm 1$, that is,

$$\mathrm{Gl}_2(\mathbb{Z}) = \left\{ A \in \mathbb{Z}^{2\times 2} \ : \ \det A = \pm 1 \right\} .$$

included on page 9

1.8. Show that the converse of Proposition 1.7 is wrong.

included on page 10

1.9. Show that $\mathsf{R}_d(m)$ are d-dimensional simplices of volume $m/d!$ with $d+1$ lattice points.

Hint: projection map.

included on page 11

1.10. Finish the induction in the proof of Pick's Formula (Theorem 1.8) for the missing case $b = 3$ and $i \geq 1$.

included on page 11

1.11. Euler's Formula states that a finite planar graph with v nodes, e edges and f bounded faces satisfies

$$v \ - \ e \ + \ f \ = \ 1$$

Show that this is equivalent to Pick's Formula.

included on page 11

1.12.

included on page 12

1.13. We have seen in Pick's Formula (Theorem 1.8) that there is a simple relation between the area and the lattice points of a *convex* lattice polygon. Prove, that the same relation also holds for *non-convex* lattice polygons, where a non-convex polygon is a connected subset of $\mathbb{R}^2$ bounded by straight noncrossing segments starting and ending in lattice points (the vertices) such that to any vertex there are precisely two incident segments.

Hint: The proof for the convex case essentially works. The part that needs consideration is the induction step, where we assume that we can subdivide our polygon with a diagonal.

1.14. Show that a polygon with volume $9/2$, one interior lattice points, 9 boundary lattice points, and whose vertices are on parallel lines at distance 3 must be the simplex $3\,\Delta_2$.

1.15. Describe as precisely as you can which pairs (b, i) can be realized for lattice polygons.

Hint: Consider long and flat quadrilaterals in which the interior points are lined up on a straight line. We will study this in detail in Chapter 3

included on page 14

1.16. Let P be a lattice polygon, $b(P)$ the number of boundary lattice points, and $i(P)$ the number of interior lattice points. Prove that a given pair (b, i) of nonnegative integers equals the $(b(P), i(P))$ for some lattice triangle P if and only if there exist integers $A, B, C \in \mathbb{Z}$ with $A > 0$ and $0 \leq B < C$ such that $b = A + \gcd(B, C) + \gcd(B - A, C)$ and $i = (AC - b)/2 + 1$. In this case, the triangle with vertices $(0, 0), (A, 0), (B, C)$ can be chosen.

Hint: Move a vertex of the triangle into the origin and use Exercise 1.6.

included on page 14

1.17. Following up on Exercise 1.16 one can plot $(b(P), i(P))$ for all lattice triangles P in a given range, see Figure 1.20. Prove that the region at the bottom, denoted by σ_1°, is given by Scott's theorem (the special point $(9, 1)$ is not visible in the very dense plot). Can you also describe the other prominent regions σ_i° (for $i \geq 1$)?

included on page 15

***1.18.

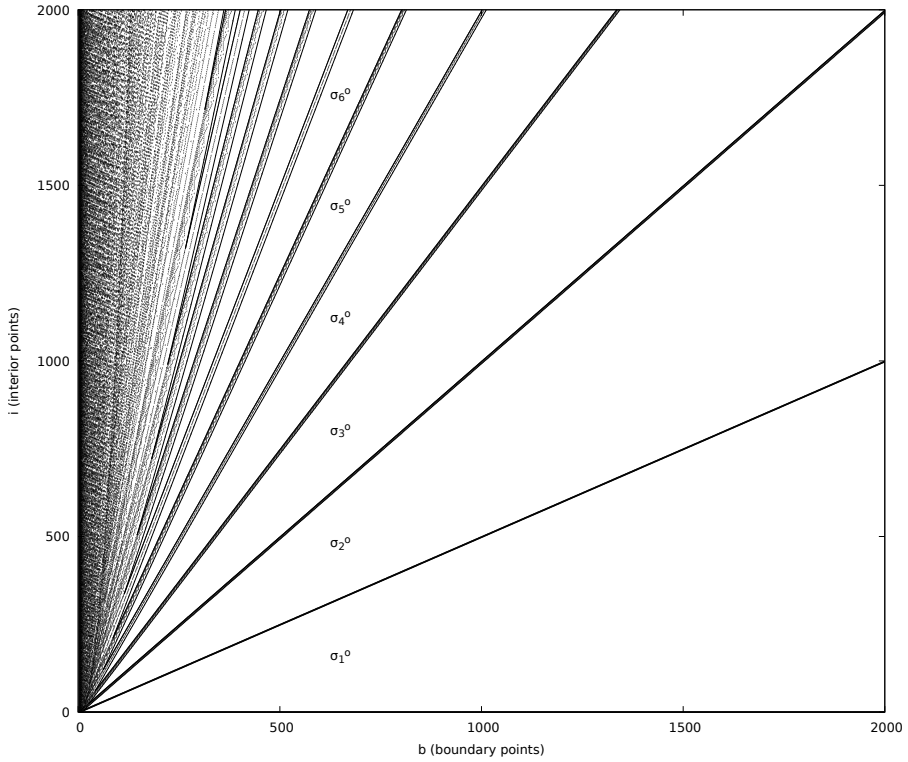


Fig. 1.20: Number of boundary and interior lattice points of lattice triangles

Polytopes and Lattices 2

Contents

You have seen in the previous chapter how polygons and integer points interact nicely and produce some nice and useful classification results. We will show that all these results can, with appropriate modifications,

actually be carried over to general dimensions. However, before we can start with this in the chapter on Ehrhart Theory (Chapter 3) we should take a closer look at the objects we are considering. We will do this in the next sections, but only very briefly. Most of the topics are covered in other courses, and we will give pointers to other books where appropriate.

2.1 Polyhedra

Polyhedral cones 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*.

In the second part of this chapter we link integral polytopes to *lattices*, which are 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.

2.1.1 Cones and Polytopes

We use $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ to denote the integer, rational, real and complex numbers. For $\mathbb{X} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$ we use

$$\mathbb{X}_{>0} := \{x \in \mathbb{X} \mid x > 0\} \qquad \mathbb{X}_{\geq 0} := \{x \in \mathbb{X} \mid x \geq 0\}$$

and similarly $\mathbb{X}_{<0}$ and $\mathbb{X}_{\leq 0}$.

We are mostly concerned with objects that can be defined from a, usually finite, subset $X \subseteq \mathbb{R}^d$. We can study spaces *generated* by such a set. The most commonly studied notion here is the linear span of X.

Definition 2.1 *Let $X \subseteq \mathbb{R}^d$. A* linear combination *of X is a sum*

$$v := \sum_{x \in X} \lambda_x x$$

where $\lambda_x = 0$ for all but finitely $x \in X$. The linear hull *or* linear span *$\operatorname{lin}(X)$ of X is the set of all linear combinations of X,*

$$\operatorname{lin}(X) := \left\{ \sum_{x \in X} \lambda_x x \; : \; \begin{array}{l} \lambda_x \in \mathbb{R} \\ \text{and } \lambda_x = 0 \text{ for all but finitely many } x \end{array} \right\}.$$

The set X is a linear space *if X equals its linear span.*

A linear combination is an affine combination *if addtionally the sum of the coefficients λ_x is 1. The* affine hull *$\operatorname{aff}(X)$ of X is the set of all affine combinations,*

$$\operatorname{aff}(X) := \left\{ \sum_{x \in X} \lambda_x x \; : \; \begin{array}{l} \lambda_x \in \mathbb{R} \text{ with } \sum_{x \in X} \lambda_x = 1 \\ \text{and } \lambda_x = 0 \text{ for all but finitely many } x \end{array} \right\}.$$

The linear span of X is the smallest linear space containing X and the common intersection of all linear spaces containing X. Similarly, the affine hull of X is the smallest affine space containing X and the intersection of all affine spaces containing X. For a matrix $A \in \mathbb{R}^{d\times n}$ with column vectors $a_1, \ldots, a_n$ we also write

$$\operatorname{lin}(A) := \operatorname{lin}(\{a_1, \ldots, a_n\}) \quad \text{and} \quad \operatorname{aff}(A) := \operatorname{aff}(\{a_1, \ldots, a_n\})$$

A set of points X is *linearly* or *affinely independent* if no point of X can be written as a linear or affine combination of the other points.

Linear spaces can always be spanned by a finite subset of X. All minimal such sets, the bases of $\operatorname{lin} X$, have the same size, which is the *dimension* of $\operatorname{lin} X$. The translation of a subset $Y \subseteq \mathbb{R}^d$ by a vector $t \in \mathbb{R}^d$ is

$$Y - t := \{y - t : y \in Y\}$$

For any affine space $A = \operatorname{aff} X$ we can consider its translation by a vector $x \in A$. This is a linear space. The dimension of A is the dimension of $A - x$. Hence, any point in the affine hull of X can be written as an affine combination of at most $d+1$ points in X.

Definition 2.2 *A linear combination is* conic *if all coefficients are non-negative, and it is* convex *if it is conic and affine. The set of all conic combinations of a set X is the* cone *over X, denoted by* $\operatorname{cone}(X)$. *The set of all convex combinations of X is the* convex hull $\operatorname{conv}(X)$. *X is a* cone *if $X = \operatorname{cone}(X)$ and X is a* convex set *if $X = \operatorname{conv}(X)$.*

A polyhedral cone *is the cone of a finite subset of $\mathbb{R}^d$. A* polytope *is the convex hull of finitely many points in $\mathbb{R}^d$.*

The dimension *of a cone is the dimension of its linear span. The* dimension *of a polytope is the dimension of the affine space it spans.*

See Figure 2.1 for an example. Again, we sometimes write $\operatorname{cone}(A)$ and $\operatorname{conv}(A)$ for the conic or convex hull of the set of column vectors of a matrix $A \in \mathbb{R}^{d\times n}$. We are mostly interested in cones and convex sets defined by a finite set X. Clearly, if the dimension of a polytope is less than the dimension of the ambient space, then we can restrict to that affine space. Hence, we may assume that the dimension of our polytopes coincides with the dimension of the space (we will see later that it will be useful to also consider lower dimensional polytopes, though).

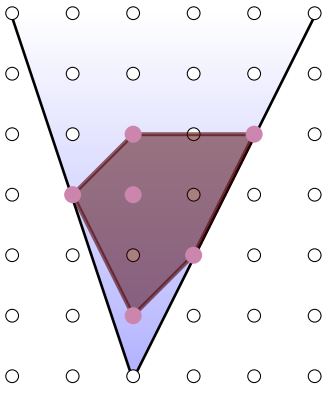


Fig. 2.1: Cone (blue) and Polytope (red) for the point set of the red points.

For polytopes in dimension 2 we have already seen the polygons in the previous chapter. Those are all 2-dimensional polytopes.

We need at least $d+1$ affinely independent points in $\mathbb{R}^d$ to affinely span $\mathbb{R}^d$, so any full-dimensional polytope has at least $d+1$ points in its defining set. Any polytope defined by precisely $d+1$ affinely independent points is called *simplex*. Any two simplices can be identified via a bijective

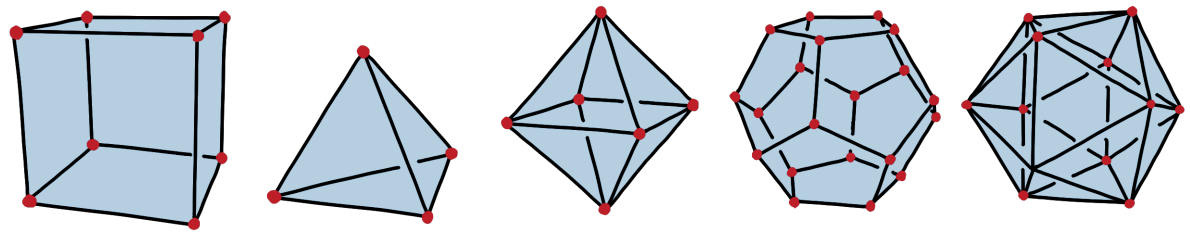


Fig. 2.2: Simplex, Cube, Cross Polytope, Dodecahedron, Icosahedron

affine map (if you translate both simplices such that one point is in the origin this a just a change of basis).

In dimension 3 there are the famous *regular* polytopes, which are the *cube*, the *tetrahedron*, the *octahedron*, the *dodecahedron*, and the *icosahedron*, see Figure 2.2. Three of them can be generalized to higher dimensions. We have seen the simplex above, which is a tetrahedron in dimension 3. The *unit cube* C_d is the convex hull of the set $X := \{0,1\}^d$. The octrahedron can be realized as the special case $d = 3$ of the polytope defined as the convex hull of $\pm e_i$ for $1 \leq i \leq d$, where e_j is the j-th unit vector in $\mathbb{R}^d$. In general, those polytopes are called *cross polytopes*.

Let us also look at a slightly more complicated, but highly intersting group of polytopes, the *hypersimplices*. The hypersimplex $h(d,k) \subset \mathbb{R}^d$ for $1 \leq k \leq d-1$ is most easily defined as a polytope of one dimension less than its ambient space. It is the convex hull of all vertices of the unit cube whose coordinates sum up to k:

$$\begin{aligned} h(d,k) &:= \operatorname{conv}\left(x \in \{0,1\}^d \,:\, \sum_{i=1}^{d} x_i = k\right) \\ &= C_d \cap \left\{x \in \mathbb{R}^d \,:\, \sum_{i=1}^{d} x_i = k\right\}. \end{aligned}$$

For $k = 1$ and $k = d-1$ we obtain a $(d-1)$-dimensional simplex. You can of course extend the definition to $k = 0$ and $k = d$, but these are just single points in $\mathbb{R}^d$.

Definition 2.3 (boundary and interior points) *Let K be a convex set. A point $x \in K$ is an* interior point *of K if there is some $\varepsilon > 0$ such that $\mathcal{B}_x(\varepsilon) \subseteq K$. Otherwise x is a* boundary point*.*

$x \in K$ is a relative interior point *of K if it is an interior point of K if considered as a subset of* aff *K.*

See also Figure 2.3.

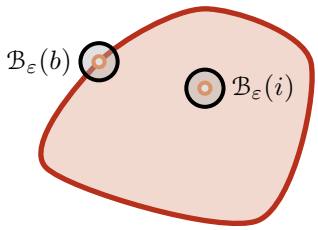


Fig. 2.3: An interior point i and a boundary point b.

Similar to the linear and affine spaces above any point x in a cone can be written as the conic generation of at most d elements of X, and a point in the convex hull as the convex combination of at most $d+1$ elements of X. Diffently from above, however, the choice of these points

depends on x. The followinf theorem, whose proof ist left as Exercise 2.1, makes this precise.

Theorem 2.4 (Carathéodory's Theorem) *Let $X \subseteq \mathbb{R}^d$, $C = \operatorname{cone}(X)$, and $y \in C$. Then there are $x_1, x_2, \ldots, x_d \in X$ and $\lambda_1, \lambda_2, \ldots, \lambda_d \geq 0$ such that*

$$y \;=\; \sum_{i=1}^{d} \lambda_i x_i \;.$$

Similarly, for $P = \operatorname{conv}(X)$ and $z \in P$ there are $x_0, x_1, \ldots, x_d \in X$ and $\lambda_0, \lambda_1, \ldots, \lambda_d \geq 0$ such that

$$z \;=\; \sum_{i=0}^{d} \lambda_i x_i \qquad \text{and} \qquad \sum_{i=0}^{d} \lambda_i \;=\; 1 \;.$$

See also Figure 2.4

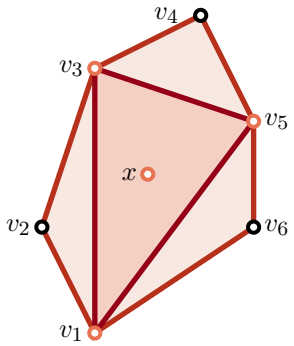


Fig. 2.4: x can be written as a convex combination of v_1, v_3 and v_5.

Exercise 2.1

2.1.2 Convex hulls and half-spaces

There is a second definition of a polytope that we want to introduce now.

Definition 2.5 (hyperplanes and half-spaces) *For any non-zero functional $a \in (\mathbb{R}^d)^\star$ and $\beta \in \mathbb{R}$ the set*

$$H \;:=\; \{x \mid \langle a, x \rangle \leq \beta\}$$

is the affine hyperplane *defined by a and β. An affine hyperplane is a* linear hyperplane *if $\beta = 0$. The* (negative) half-space *corresponding to an affine hyperplane is*

$$H^- \;:=\; \{x \mid \langle a, x \rangle \leq \beta\} \;.$$

We say that a point $y \in \mathbb{R}^d$ is beneath *H if $\langle a, y \rangle < \beta$ and* beyond *H if $\langle a, y \rangle > \beta$.*

Note that $\lambda a, \lambda\beta$ for any $\lambda \neq 0$ defines the same hyperplane as a, β, and the same affine half space if $\lambda > 0$. Hence, the defining functional for a hyperplane or half space is unique only up to a non-zero and positive factor, respectively.

Definition 2.6 *A* polyhedron *P is the intersection of finitely many affine half spaces,*

$$P \;=\; \bigcap \{x \mid \langle a_i, x \rangle \leq \beta_i\} \;=\; \{x \mid \langle a_1, x \rangle \leq \beta_1, \ldots, \langle a_m, x \rangle \leq \beta_m\}$$

for $a_i \in \mathbb{R}^d$ and $\beta_i \in \mathbb{R}$ and $1 \leq i \leq k$. This is often written in the more consise form

$$P \;=\; \{\, x \;\mid\; Ax \le b \,\}$$

where $A \in \mathbb{R}^{k\times d}$ *whose rows are the functionals* $a_1, a_2, \ldots, a_k$ *and* b *is the vector with entries* $\beta_1, \beta_2, \ldots, \beta_k$.

Example 2.7 *We look at some simple examples.*

(1) The unit cube C_d *is defined by the inequalities*

$$x_i \;\ge\; 0 \qquad\qquad x_i \;\le 1 \qquad\qquad \text{for } 1 \le i \le d\,.$$

(2) The inequalities

$$x_1 \;\ge\; 0 \quad x_1 - x_2 \;\le\; 2 \quad x_1 + 3x_2 \;\le\; 10 \quad 3x_1 - x_2 \;\ge\; 0$$

define a polygon with vertices

$$\begin{bmatrix}0\\0\end{bmatrix} \qquad \begin{bmatrix}2\\0\end{bmatrix} \qquad \begin{bmatrix}4\\2\end{bmatrix} \qquad \begin{bmatrix}1\\3\end{bmatrix}.$$

see Figure 2.5.

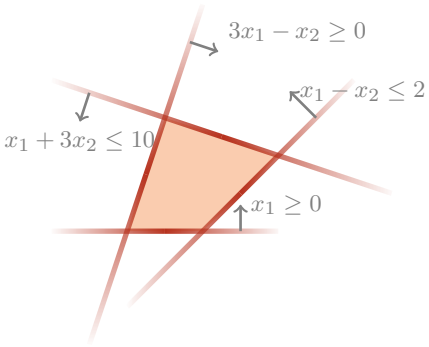


Fig. 2.5: The polygon of Example 2.7(2)

Definition 2.8 *A polyhedron* P *is a* (polyhedral) cone *if all defining inequalities are linear, that is,*

$$P \;=\; \bigcap H^-_{a_i,0} \tag{2.1}$$

for some $a_1, a_2, \ldots, a_k \in (\mathbb{R}^d)^\star$.

We have already defined a *cone over a set* X as the set of all conic combinations in the previous section. We will see below that this and the newly defined notion of a polyhedral cone coincide if X is a finite set, *i.e.* any polyedral cone can equally be described as the cone over some suitably chosen finite set X, and any cone over a finite set is polyhedral.

We will not encounter non-polyhedral cones, that is, cones defined as the set of conic combinations over an infinite set X, in this book. Therefore, we will often omit the word polyhedral and just speak of cones in the text, and only stress this restriction in definitions and theorems.

The *dimension* of such a polyhedron defined by half spaces is again defined as the dimension of its affine hull. We sometimes use the notion *d-polytope* for a d-dimensional polyhedron. A polyhedron is *full dimensional* if $\dim P = d$.

Definition 2.9 *Let* $P = \bigcap H^-_{a_i,\beta_i}$ *be a polyhedron. The* recession cone *and* lineality space *of* P *are*

$$\operatorname{rec} P \;=\; \bigcap H^-_{a_i,0} \qquad \textit{and} \qquad \operatorname{lineal} P \;=\; \bigcap H_{a_i,0}\,.$$

A polytope is pointed *if* $\operatorname{lineal} P = \varnothing$.

Example 2.10

We can associate a cone to each polyhedron $P \subseteq \mathbb{R}^d$ that esssentially has the same combinatorial and geometric properties. This is the *homogenization* of P or just the *cone over* P defined by

$$C(P) \;:=\; \operatorname{cone}(\{1\} \times P) \;\subseteq\; \mathbb{R}^{d+1}\,, \tag{2.2}$$

so if $P := \{x \mid \langle a_1, x\rangle \le \beta_1, \ldots, \langle a_m, x\rangle \le \beta_m\} \subseteq \mathbb{R}^d$ with $a_i \in (\mathbb{R}^d)^\star$, $\beta_i \in \mathbb{R}$ for $i \in [m]$ then

$$C(P) \;=\; \{(x_0, x) \mid -\beta_1 x_0 + \langle a_1, x\rangle \le 0, \ldots, -\beta_m x_0 + \langle a_m, x\rangle \le 0\}\,.$$

It is often convenient to look at the homogenization of the polyhedron instead of the polyhedron itself as it is defined by linear instead of affine inequalities. We can recover the polyhedron by intersecting the cone with the hyperplane $x_0 \equiv 1$ (and projecting).

Definition 2.11 (Minkowski sum) *The* Minkowski sum *of two sets $X, Y \subseteq \mathbb{R}^d$ is the set*

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

A set X is *finitely generated* if it can be written as a Minkowski sum of a polytope, a cone, and a linear space, that is, there are $v_i \in \mathbb{R}^d$, $i = 1, \ldots, r$, $r_j \in \mathbb{R}^d$, $j = 1, \ldots, s$, $vb_k \in \mathbb{R}^d$, $k = 1, \ldots, t$ such that

$$X \;=\; \left\{ \sum_{i=1}^{r} \lambda_i v_i + \sum_{j=1}^{s} \mu_i r_i + \sum_{k=1}^{r} \nu_i b_i \;:\; \begin{array}{c} \lambda_i, \mu_j, \nu_k \in \mathbb{R}, \\ \lambda_i, \mu_j \ge 0, \sum_{i=1}^{r} \lambda_i = 1 \end{array} \right\}. \tag{2.3}$$

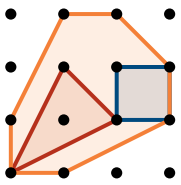


Fig. 2.6: The orange polygon is the Minkowski sum of the red and blue polygons

Theorem 2.12 (Weyl-Minkowski Theorem) *Let $P \subseteq \mathbb{R}^d$. Then P is a polyhedron if and only if it is finitely generated.*

A proof of this theorem can be found in [50]. Projections of polyhedra are again polyhedra, finitely generated by the projections of the generators.

Example 2.13 *In the notation of Weyl-Minkowski Theorem (Theorem 2.12) we can define a polyhedron with*

$$v_1 := \begin{bmatrix} 1 \\ 3 \end{bmatrix} \quad v_2 := \begin{bmatrix} 1 \\ 2 \end{bmatrix} \quad v_3 := \begin{bmatrix} 2 \\ 1 \end{bmatrix} \quad r_1 := \begin{bmatrix} 1 \\ 3 \end{bmatrix} \quad r_2 := \begin{bmatrix} 3 \\ 1 \end{bmatrix},$$

see Figure 2.7. It is defined by the inequalities

$$3x_1 - x_2 \;\ge\; 3 \qquad x_1 \ge 1 \qquad x_1 + x_2 \;\ge\; 3 \qquad x_1 - 3x_2 \;\le\; -1\,.$$

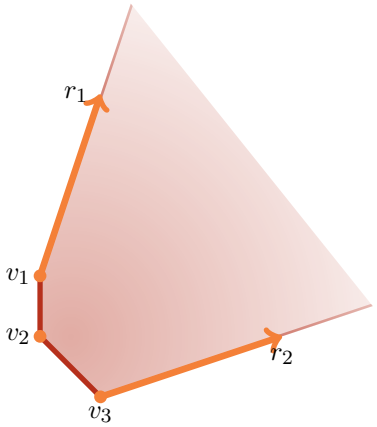


Fig. 2.7: The polyhedron of example Example 2.13

The Minkowski sum of a polytope with a cone C or a linear space L is unbounded if C or L have positive dimension. Hence, we can deduce the following duality for polytopes from the Weyl-Minkowski Theorem.

Corollary 2.14 (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.* □

From this theorem we obtain 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.

2.1.3 The face lattice

Throughout this section let $P := \{x \mid \langle a_1, x\rangle \leq \beta_1, \ldots, \langle a_m, x\rangle \leq \beta_m\}$ be a polyhedron defined by $a_i \in (\mathbb{R}^d)^\star$, $\beta_i \in \mathbb{R}$ for $i \in [m]$. We have seen in the examples above that some intersections of the hyperplanes distinguish lower dimensional subsets of a polyhedron. We want to formalize this observation in this section.

A hyperplane $H := \{x \mid \langle a, x\rangle \leq \beta\}$ for some $a \in (\mathbb{R}^d)^\star$ and $\beta \in \mathbb{R}$ defines a *valid hyperplane* if P is contained in the negative half space of H, that is, if $\langle a, x\rangle \leq \beta$ for all $x \in P$. A valid hyperplane is *supporting* if $P \cap H$ is non-empty.

Definition 2.15 (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.

Observe that the empty set is also a face of P. For any face F we have

$$F \cap P = \operatorname{aff} F \cap P\,,$$

so faces of polyhedra are again polyhedra and a face of a face of the polyhedron is a face of the polyhedron. The *dimension of a face* of a polyhedron P is its dimension as a polyhedron,

$$\dim F := \dim \operatorname{aff} F\,.$$

We sometimes use the notion *k-face* for a k-dimensional face of a polytope P. If for a polyhedron P and a functional $a \in (\mathbb{R}^d)^\star$ the value β of

$$\max\{\langle a, x\rangle \mid x \in P\}$$

is finite then $H := \{x \mid \langle a, x \rangle \leq \beta\}$ is a supporting hyperplane of P and $P \cap H$ is a face of P, the *face defined by* a. The functionals defining a face are exactly those in the negative dual of the recession cone.

Any functional a_i in the definition of P for some $i \in [m]$ is an *implied equality* if $\langle a, x \rangle = \beta_i$ for all $x \in P$. The set of all implied equalities of P is

$$\operatorname{eq}(P) := \{j \in \{1, \ldots, m\} \mid \langle a_j, x \rangle = \beta_j \text{ for all } x \in P\}.$$

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

$$\operatorname{aff}(P) = \bigcap_{j \in \operatorname{eq}(P)} \{x \mid \langle a_j, x \rangle = \beta_j\}.$$

The hyperplane description is *irredundant* if no proper subset of the half spaces defines the same polytope, and *redundant* otherwise. Let $P :=$ be a polyhedron. A point $x \in P$ is a *relative interior point* of P if

$$\langle a_i, x \rangle = \beta_i \quad \text{for all } i \in \operatorname{eq}(P) \qquad \langle a_i, x \rangle < \beta_i \quad \text{for all } i \notin \operatorname{eq}(P).$$

Any polytope of dimension $d \geq 1$ has a relative interior point. Observe that this notion of relative interior points coincides with the one given in Definition 2.3. So we have two different ways to check whether a point is in the realitve interior of a polyhedron.

If F is a proper face of P, then $F = \{x \mid \langle a_i, x \rangle = \beta_i \text{ for } i \in I\} \cap P$ for a subsystem $I \subseteq [m]$ of the inequalities of P. In particular, P has only a finite number of faces. A proper face F of P is a *facet* if it has dimension $\dim P - 1$.

Now assume that P is full dimensional and the defining functionals $\alpha_1, \ldots, \alpha_m$ are irredundant. Then F is a facet of P if and only if $F = \{x \mid \prod a_i x = \beta_i\} \cap P$ for some $i \in [m]$. Furthermore, if P is full dimensional, then $a_1, \ldots, a_m$ are unique up to scaling with a positive factor. Also, any proper face of P is contained in a facet, and if F_1, F_2 are proper faces, then $F_1 \cap F_2$ is a proper face of P. A face F of P is *minimal* if there is no non-empty proper face G of P with $G \subsetneq F$. F is minimal if and only if $F = \operatorname{aff} F$ if and only if it is a translate of $\operatorname{lineal} P$. The minimal faces of a pointed polyhedron are called *vertices*. They are points in $\mathbb{R}^d$. The set of all vertices is denoted by $\mathcal{V}(P)$. 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 vertices of P are *adjacent* if they are contained in the same edge. Faces of a polyhedron are ordered by inclusion. Hence, the set $\operatorname{faces}(P)$ of all faces of P (including the empty set and P itself) is a poset, which is actually an Eulerian lattice, the *face*

lattice of P. A k-face F and a j-face G of P are *incident* if either F is a face of G or vice versa. The *f-vector* (or *face vector*) of P is the vector

$$\mathsf{f}(P) \;:=\; (\mathsf{f}_0(P), \ldots, \mathsf{f}_{d-1}(P))\,,$$

where $\mathsf{f}_i(P)$ is the number of i-dimensional faces of P, for $0 \le i \le d-1$.

Exercise 2.5

Exercise 2.6

Let $P \subseteq \mathbb{R}^d$ be a full-dimensional polyhedron with $\mathbf{0} \in \operatorname{int} P$. The *polar dual* of a polytope P is

Theorem 2.16 *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with $\mathbf{0} \in \operatorname{int} P$ and vertices $v_1, \ldots, v_m$. Then $P^\star$ is defined by the inequalities*

$$P^\star := \left\{ a \in (\mathbb{R}^d)^\star \;:\; \langle\, a, v_1 \,\rangle \le 1, \ldots, \langle\, a, v_m \,\rangle \le 1 \right\}$$

and its vertices are $1/b_j a_j$ for each facet defining inequality $\langle\, a_j, x \,\rangle \le b_j$ of P. □

You will show in Exercise 2.7 that dualizing twice gives back the original polytope.

Exercise 2.7

Corollary 2.17 *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with $\mathbf{0} \in \operatorname{int} P$. Then we have a bijective correspondence between k-faces of P and $(d-1-k)$-faces of $P^\star$ for $0 \le k \le d-1$ and if a k-face F of P is contained in a $(k+1)$-face G of P, then the face corresponding to G in $P^\star$ is contained in the face corresponding to F in $P^\star$.* □

Corollary 2.18 *If $\mathsf{f} = (\mathsf{f}_1, \ldots, \mathsf{f}_{d-1})$ is the f-vector of P and $\mathsf{f}' = (\mathsf{f}'_{d-1}, \ldots, \mathsf{f}'_0)$ that of $P^\star$ then*

$$\mathsf{f}_i \;=\; \mathsf{f}'_{d-1-i} \qquad \text{for} \qquad 0 \le i \le d-1\,.$$ □

For the next observations we switch to the interior description of a polytope. Let $\varphi : \mathbb{R}^d \to \mathbb{R}^e$ be an affine map and $P = \operatorname{conv}(v_1, \ldots, v_n) + \operatorname{cone}(w_1, \ldots, w_l)$ a polyhedron for some $v_1, \ldots, v_n, w_1, \ldots, w_l \in \mathbb{R}^d$. Then

$$\varphi\left(\sum_{i=1}^{d} \lambda_i v_i + \sum_{j=1}^{l} \mu_j w_j \right) \;=\; \sum_{i=1}^{d} \lambda_i \varphi v_i + \sum_{j=1}^{l} \mu_j \varphi w_j\,,$$

so φP is again a polyhedron.

Definition 2.19 (affine equivalence) *Let $P \subseteq \mathbb{R}^d$ and $Q \subseteq \mathbb{R}^e$ be two polytopes. P and Q are* affinely equivalent *if there are affine maps $\varphi : \mathbb{R}^d \to \mathbb{R}^e$ and $\psi : \mathbb{R}^e \to \mathbb{R}^d$ such that*

$$\varphi P = Q \qquad\qquad \psi Q = P\,.$$

A polytope is *simplicial* if all faces are simplices. It is *simple* if all k-dimensional faces are incident to exactly $\dim P - k$ faces. It suffices to check this condition for the vertices. Simplicial and simple are dual notions, that is, the dual of a full dimensional simplicial polytope is simple, see Exercise 2.8.

f-vectors of simplicial polytopes have been completely charecterized in the g-Theorem of Billera, Lee [12] and Stanley [55] following a conjecture of McMullen [39]. This theorem can best be described with a linear transformation of the f-vector, which we introduce now. We can write the f-vector as a polynomial in the form

$$f(t) \;:=\; (t-1)^d + \sum_{i=1}^{d} f_{i-1}(t-1)^{d-i}\,.$$

Writing this polynomial in the basis $1, t, t^2, \ldots, t^d$ gives the h-polynomial

$$f(t) \;=\; \sum_{j=0}^{d} h_j t^j\,.$$

We also need the following notion of an M-sequence. For any integers $n, k \geq 1$ there is a unique way to express n in the form

$$n \;=\; \binom{a_k}{k} + \binom{a_{k-1}}{k-1} + \cdots + \binom{a_i}{i}$$

with $a_k \geq a_{k-1} \geq \ldots \geq a_i \geq i \geq 1$. We define

$$n^{\langle k \rangle} \;:=\; \binom{a_{k-1}}{k-1} + \binom{a_{k-2}}{k-2} + \cdots + \binom{a_{i-1}}{i-1}$$

and $0^{\langle 0 \rangle} = 0$. A nonnegative sequence $(m_0, m_1, m_2, \ldots)$ is an *M-sequence* if $m_0 = 1$ and $m_k^{\langle k \rangle} \leq m_{k-1}$ for all $k \geq 2$. With this notion we have the following theorem.

Theorem 2.20 (g-Theorem) *A sequence $h = (h_0, \ldots, h_d)$ is the h-vector of a simplicial polytope if and only if*

(1) $h_i = h_{d-i}$ for $i = 0, \ldots, \lfloor d/2 \rfloor$
(2) $(g_0, g_1, \ldots, g_{\lfloor d/2 \rfloor})$ is an M-sequence, where $g_0 = h_0$ and $g_i = h_i - h_{i-1}$ for $i = 1, \ldots, \lfloor d/2 \rfloor$.

Example 2.21

2.2 Decompositions of Polytopes

We start our considerations with subdivisions of polytopes into smaller pieces and study polyhedral complexes and triangulations.

2.2.1 Polyhedral Complexes

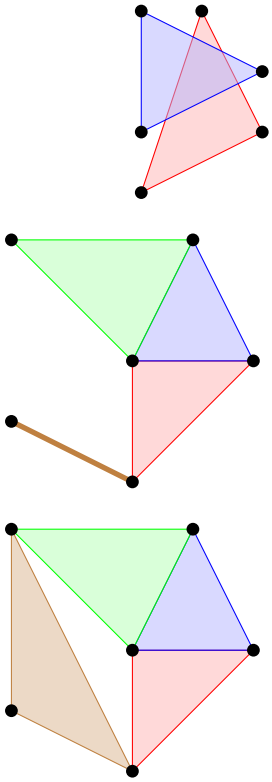


Fig. 2.8: The upper figure is not a polyhedral complex. The second is, but it is not pure, the third is also pure.

Definition 2.22 (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. 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* $\mathcal{C}$*.*

Example 2.23 *Here are some examples of a polyhedral complex. See also Figure 2.8.*

(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 2.8 for a non-pure polyhedral complex. It has three 2*-dimensional maximal cells and one* 1*-dimensional maximal cell.*

Definition 2.24 (face vector) *The* face vector *of a pure* d*-dimensional polyhedral complex* $\mathcal{C}$ *is the vector*

$$\mathsf{f}(\mathcal{C}) = (\mathsf{f}_{-1}, \mathsf{f}_0, \ldots, \mathsf{f}_d)$$

where f_k *counts the number of* k*-dimensional faces of* $\mathcal{C}$*.*

Observe that this is completely analogous to our earlier definition of the face vector of a polytope. Further, f_{-1} corresponds to the empty face, hence, $f_{-1} = 1$ for any polyhedral complex. We will see later that the entries of the face vector satisfy a linear relation, the Euler equation. The *Euler characteristic* of the complex $\mathcal{C}$ is

$$\chi(\mathcal{C}) := -\mathsf{f}_{-1} + \mathsf{f}_0 - \mathsf{f}_1 + \ldots + (-1)^d \mathsf{f}_d\,.$$

This satisfies some addition formula. Let $\mathcal{C}$ and $\mathcal{C}'$ be two polyhedral complexes such that $\mathcal{C} \cap \mathcal{C}'$ is a subcomplex of both. Then there union is also a polyhedral complex and

$$\chi(\mathcal{C}) + \chi(\mathcal{C}') = \chi(\mathcal{C} \cup \mathcal{C}') - \chi(\mathcal{C} \cap \mathcal{C}') \,. \tag{2.4}$$

Definition 2.25 (fan) *A* fan *is a pure connected polyhedral complex such that all cells of the complex are cones.*

Definition 2.26 (normal cone) *The* normal cone $\mathsf{N}_P(F)$ *of a face F of a polytope P is the set of linear functionals a such that there is some β with $\langle a, F \rangle = \beta$ and $\langle a, P \rangle \leq \beta$.*

Proposition 2.27 *The normal cone is a polyhedral cone spanned by the facet normals defining the face F.* □

Definition 2.28 (normal fan) *The* normal fan *of a polytope P is the collection of all normal cones of proper faces of P.*

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

Definition 2.29 (tangent cone) *Let P be a d-polytope and F a face of P. The* tangent cone $\mathsf{T}_F P$ *of F is the cone*

$$\mathsf{T}_F P := \{p + v \in \mathbb{R}^d \mid p \in F,\, p + \varepsilon v \in P \text{ for some } \varepsilon > 0\} \,.$$

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 $w \in F$ to shift the cone into the origin. The following proposition is proved in Exercise 2.9.

Proposition 2.30 *The shifted cone $\mathsf{T}_F P - w$ is dual to the normal cone of F.*

Exercise 2.9

Exercise 2.10

2.2.2 Regular Subdivisions and Triangulations

Often it is useful to subdivide a polytope into smaller pieces and look at the pieces separately. It will turn out that the most useful subdivisions are those where all pieces are simplices. Such subdivisions are called *triangulations* of the polytope. The next definition formalizes this notion.

Definition 2.31 (Subdivision and Triangulation) *A* subdivision *of a polytope P is a pure polyhedral complex $\mathcal{S}$ such that $P = \bigcup_{C \in \mathcal{S}} C$.*

A subdivision is a triangulation *of P if all cells are simplices.*

Example 2.32

A subdivision or triangulation 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 $V \subset \mathbb{R}^d$ the polytope $\operatorname{conv} V$ has a triangulation with vertex set V. Similarly, the cone $\operatorname{pos} V$ has a triangulation with rays $\{\mathbb{R}_{\geq 0} v \ : \ v \in V\}$ [19].

Definition 2.33 (regular subdivision) *A subdivision $\mathcal{S}$ of a polytope with vertices $\{v_1, \ldots, v_m\}$ (of the subdivision) 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 $V := \{v_1, \ldots, v_m\}$ and a weight vector $w \in \mathbb{R}^m$ we denote by $\mathcal{S}_w(V)$ the regular subdivision obtained as the lower hull of $\operatorname{lift}(w) := \operatorname{conv}((w_i, v_i) \mid 1 \leq i \leq m)$.

You will show in Exercise 2.11 that all subdivisions of a polygon using only the vertices of the polygon are regular. WISHLIST: convex piecewise linear function $\Psi_w(x) = \min\{h \ : \ (h, x) \in \operatorname{lift}(w)\}$

Exercise 2.11

Definition 2.34 (polyhedral sphere, polyhedral ball)

Theorem 2.35 *Every d-polytope P has a regular triangulation using only the vertices of the polytope.*

Proof. Let $V := \mathcal{V}(P)$ be the vertices of the polytope. We can assume that P is full dimensional. We claim that any sufficiently generic vector w induces a regular triangulation.

The subdivision induced by w is a triangulation if and only if for each facet of the lower hull of $\operatorname{lift}(w)$ is a d-simplex, i.e. if at most $d+1$ of the points

$$(w_1, v_1), \ldots, (w_d, v_d)$$

lie on a common hyperplane. For any $(d+2)$-tuple

$$(w_{i_1}, v_{i_1}), \ldots, (w_{i_{d+2}}, v_{i_{d+2}})$$

being on a common hyperplane means that the determinant

$$\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ w_{i_1} & w_{i_2} & \cdots & w_{i_{d+2}} \\ v_{i_1} & v_{i_2} & \cdots & v_{i_{d+2}} \end{pmatrix}$$

vanishes. We can view this determinant as a linear functional in the entries of w. There are $\binom{m}{d+2}$ different such functionals, hence, the complement Z^c of the union of the zero sets of these functionals is not empty. Choosing any $w \in Z^c$ satisfies our requirements. □

It is important to realize that not all triangulations of a polytope are regular. See e.g. Figure 2.9 for a simple example. You will prove that it is indeed not regular in Exercise 2.12

(1) intersections
(2) refinements

Corollary 2.36 *Every pointed cone C can be triangulated into simplicial cones without introducing new generators.*

Proof. If C is pointed, then there is a functional u such that

$$u^t x > 0 \qquad \text{for all } x \in C\,.$$

Then $P := C \cap \{x \mid u^t x = 1\}$ is a polytope, and C is the cone over P. By the previous Theorem 2.35 P has a regular triangulation $\mathcal{T}$ without new vertices. The cones over the cells in this triangulation give a triangulation of the cone C without using new generators. □

Exercise 2.12

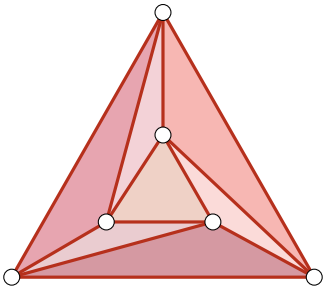


Fig. 2.9: A non-regular subdivision

2.3 Lattices

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 $\|\,.\,\|$ and with a translation invariant volume form.

2.3.1 Discrete Subgroup and Lattice Bases

Lattices can be defined in two different (but equivalent) ways. On the one hand as the integral generation of a linearly independent set of vectors, on the other hand as a discrete abelian subgroup of the vector space. We will start with the latter characterization of a lattice, This is often very useful to describe lattices without the explicit choice of a basis. We will deduce the other representation in a sequence of propositions that introduce some interesting structure ofr lattices.

Recall that a subset $\Lambda \subseteq V$ is an *additive subgroup* of V if

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

Definition 2.37 (lattice, rank) *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, that is,* $\operatorname{rank} \Lambda := \dim \operatorname{lin} \Lambda$.

Exercise 2.13

Exercise 2.14

Note that this notion of a lattice is not connected to the *face lattices* that we looked at earlier. You will show in Exercise 2.15 that this definition is independent of the chosen norm, and in Exercise 2.16 that one can choose the same ε for all $x \in \Lambda$.

Exercise 2.15

Exercise 2.16

Example 2.38 *(1) The* standard integer lattice *is the lattice spanned by the* d *standard unit vectors* $e_1, \ldots, e_d$*. It is commonly denoted by* $\mathbb{Z}^d$*. We will later see that essentially any lattice looks like this integer lattice. See Figure 2.10.*

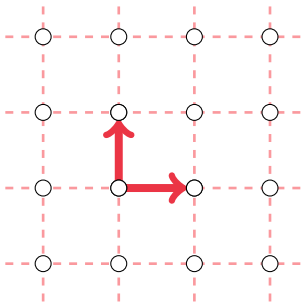


Fig. 2.10: The lattice $\mathbb{Z}^2$

(2) Root systems are a famous class of lattices. We introduce some of them here, and you can explore more in the exercises.

a) We can identify $\mathbb{R}^d$ *with the linear subspace*

$$L := \left\{ x \in \mathbb{R}^{d+1} : \sum_{i=0}^{d} x_i = 0 \right\}.$$

The set $\mathrm{A}_d := L \cap \mathbb{Z}^{d+1}$ *is a lattice in* L*.* A_d *is clearly discrete, as it is a subset of a discrete set, and the addition of any two elements in* A *stays in* L*, as this is a linear subspace. The same is true for the multiplication by* -1*. This is the* root lattice A_d*. See Figure 2.11.*

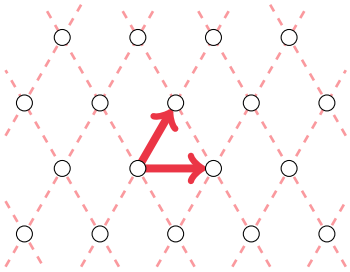


Fig. 2.11: The lattice A_2

b) Let D_d *be the set*

$$\mathrm{D}_d := \left\{ x \in \mathbb{Z}^d : \sum_{i=1}^{d} x_i \text{ is even} \right\}. \tag{2.5}$$

Again, this is a discrete set and addition and multiplication by -1 *stay inside the set. This is the* root lattice D_d*.*

(3) Subgroups of lattices are again lattices. To make a concrete example for this, the set

$$\Lambda_{2;3} := \{x \in \mathbb{Z}^2 : x_1 + x_2 \equiv 0 \mod 3\}$$

is a lattice.

(4) Let Λ *be a lattice and* $L \subset V$ *be a proper linear subspace of* V*. Then* $\Lambda \cap L$ *is a lattice in* L*.*

Exercise 2.17

For a set $\mathcal{B} = \{b_1, \ldots, b_d\} \subset V$ of linearly independent vectors we define the subgroup

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

Definition 2.39 (lattice basis) *A linearly independent subset $\mathcal{B} \subset V$ is called a lattice basis (or Λ-basis) if it generates the lattice: $\Lambda = \Lambda(\mathcal{B})$.*

Example 2.40 $\mathcal{B} := \left\{ \begin{bmatrix} 3 \\ 0 \end{bmatrix}, \begin{bmatrix} -1 \\ 1 \end{bmatrix} \right\}$ *is a basis of the lattice in Example 2.38(3).*

Definition 2.41 (parallelepiped) *For a finite subset $\mathscr{A} = \{v_1, \ldots, v_k\} \subset \mathbb{R}^d$ the* half-open zonotope $\Pi(\mathscr{A})$ *spanned by these vectors is the set*

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

If $\mathscr{A}$ is linearly independent, the zonotope is a parallelepiped.

Here is one of the most fundamental definitions for lattices.

Definition 2.42 (fundamental parallelepiped) *Let Λ be a lattice with basis $\mathcal{B} = \{b_1, \ldots, b_d\}$. The parallelepiped $\Pi(\mathcal{B})$ is the* fundamental parallelepiped *of the lattice with basis $\mathcal{B}$.*

See Figure 2.12 for an example. Clearly, the fundamental parallelepiped depends on the chosen basis. However, its volume, the *determinant* of the lattice, does not, and we obtain a very nice representation of points in the underlying vector space with the following proposition.

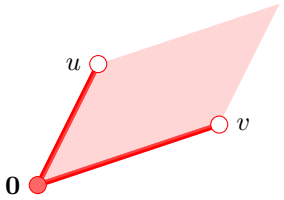


Fig. 2.12: A parallelepiped spanned by some vectors

Proposition 2.43 *Let Λ be a lattice in V and assume it has a basis $\mathcal{B} = \{b_1, \ldots, b_d\}$. Then any point $x \in \operatorname{lin} \Lambda$ has a unique representation $x = a + y$ for $a \in \Lambda$ and $y \in \Pi(\mathcal{B})$.*

Proof. There are unique $\lambda_1, \ldots, \lambda_d \in \mathbb{R}$ 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

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

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 $a = a'$. □

From this theorem it follows immediately that the parallelepipeds of a lattice with basis $\mathcal{B}$ tile the space, see also Exercise 2.18.

Corollary 2.44 *Let Λ be a lattice in $\mathbb{R}^d$ and assume it has a basis $\mathcal{B} := \{b_1, \ldots, b_d\}$ and let $\Pi := \Pi(b_1, \ldots, b_d)$ be the fundamental parallelepiped. Then $\mathbb{R}^d$ is the disjoint union of all translates of Π by vectors in Λ.* □

Exercise 2.18

We now show that any set $\mathcal{B}$ of linearly independent vectors actually generates a lattice with basis $\mathcal{B}$.

Lemma 2.45 *Let $\mathcal{B} = \{b_1, \ldots, b_d\} \subset V$ be linearly independent. Then the subgroup*

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

generated by $\mathcal{B}$ is a lattice.

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

Let $z \in \mathbb{R}^d \cap \Pi(b_1, \ldots, b_d)$ be an interior point of $\Pi(b_1, \ldots, b_d)$. Then there is $\varepsilon > 0$ such that $\mathcal{B}_\varepsilon(z) \subseteq \Pi(b_1, \ldots, b_d)$. 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 $x' + z \in \Pi(b_1, \ldots, b_d)$, a contradiction to Proposition 2.43. □

Theorem 2.46 *Every lattice has a basis.*

For the proof we need some prerequisites. The following lemma is immediate from the definition.

Lemma 2.47 *If $K \subset V$ is bounded, then $K \cap \Lambda$ is finite.* □

Definition 2.48 (Λ-rational subspace) *A subspace $U \subseteq V$ is Λ-rational if it is generated by elements of Λ.*

Proposition 2.49 *Let V be a finite-dimensional real vector space, let $\Lambda \subset V$ be a lattice, and let $U \subseteq V$ be a Λ-rational subspace. Denote the quotient map $\pi\colon V \to V/U$.*

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

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

Proof. (1) $\pi(\Lambda)$ is the image of a group under a homomorphism. Hence, it is a subgroup of V/U. The hard part of the proposition is to prove that $\pi(\Lambda)$ is discrete in V/U.
The space U is Λ-rational. So we can choose a vector space basis $\{v_1, \ldots, v_r\} \subset \Lambda \cap U$ of U. We can extend this basis to a vector space

basis $\mathcal{B} = \{v_1, \ldots, v_d\} \subset \Lambda$ of $\operatorname{lin}\Lambda$. These bases yield maximum norms

$$\left\| \sum_{i=1}^{d} \lambda_i v_i \right\| \;:=\; \max\left(\{|\lambda_i| \;:\; i = 1, \ldots, d\}\right)$$

on $\operatorname{lin}\Lambda$ and

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

on $\operatorname{lin}\Lambda/U$. Denote the unit ball of $\operatorname{lin}\Lambda$ by W. By Lemma 2.47, the set $W \cap \Lambda$ is finite. Set

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

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

$$v' \;:=\; \sum_{i=1}^{r} (\lambda_i - \lfloor \lambda_i \rfloor) v_i + \sum_{i=r+1}^{d} \lfloor \lambda_i \rfloor v_i \;\in\; \Lambda$$

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 $b_1, \ldots, b_r, \hat{c}_1, \ldots, \hat{c}_s$ be as in the proposition, and let $v \in \Lambda$. Because the c_j form a lattice basis of $\pi(\Lambda)$, there are integers $\lambda_1, \ldots, \lambda_s$ 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 $\mu_1, \ldots, \mu_r$ so that $v - \sum_{j=1}^{s} \lambda_j \hat{c}_j = \sum_{i=1}^{r} \mu_i b_i$. So $b_1, \ldots, b_r, \hat{c}_1, \ldots, \hat{c}_s$ generate Λ. They must be linearly independent for dimension reasons. □

Definition 2.50 (primitive vector) *A non-zero lattice vector $v \in \Lambda$ is primitive if it is not a positive multiple of another lattice vector, i.e.* $\operatorname{conv}(\mathbf{0}, v) \cap \Lambda = \{\mathbf{0}, v\}$.

Proof (of Theorem 2.46). We proceed by induction on $r := \operatorname{rank}\Lambda$. 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 $U := \operatorname{lin} b$. Then $\{b\}$ is a basis for $U \cap \Lambda$, and Λ/U is a lattice by the first statement of Proposition 2.49. Because $\operatorname{rank}\Lambda/U = r - 1$, it has a basis by induction. By the second statement of Proposition 2.49, we can lift to a basis of Λ. □

Exercise 2.19

Definition 2.51 (unimodular transformation) *Let Λ and Λ' be lattices. A linear map $\mathsf{T}\colon \operatorname{lin}\Lambda \to \operatorname{lin}\Lambda'$ which induces a bijection $\Lambda \to \Lambda'$ is called* unimodular *or a* lattice transformation. *T is a* lattice isomorphism *if $\Lambda = \Lambda'$.*

Definition 2.52 (sublattice and index) *Let $\Lambda \subset \mathbb{R}^d$ 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 $|\Gamma/\Lambda|$ is the* index *of Γ in Λ.*

Theorem 2.53 *Let $\Lambda' \subseteq \Lambda$ be lattices with $\operatorname{lin}\Lambda = \operatorname{lin}\Lambda'$. Then there is a basis $b_1, \dots, b_r$ of Λ and integers $k_1, \dots, k_r \in \mathbb{Z}_{>0}$ with $\lambda_i | \lambda_{i+1}$ for $1 \le i \le d-1$ such that $k_1 b_1, \dots, k_r b_r$ is a basis of Λ'.*

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

Assume $r \ge 2$. Because $\operatorname{lin}\Lambda = \operatorname{lin}\Lambda'$, for every $v \in \Lambda$ there is a positive integer k so that $kv \in \Lambda'$. Choose $b_r \in \Lambda$ and $k_r \in \mathbb{Z}_{>0}$ so that b_r is Λ-primitive, and so that k_r is minimal.

Set $U := \operatorname{lin} b_r$. Then b_r is a basis for $U \cap \Lambda$, and $k_r b_r$ is a basis for $U \cap \Lambda'$. By Proposition 2.49, $\Lambda'/U \subseteq \Lambda/U$ 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 2.49, $b_1, \dots, b_r$ 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 $0 \le l_i < k_r$ 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 $m_i \le l_i < k_r$ 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. □

Exercise 2.20

Exercise 2.21

Corollary 2.54 *Let $\Lambda' \subseteq \Lambda$ be lattices with $\operatorname{lin}\Lambda = \operatorname{lin}\Lambda'$, and let $\mathcal{B}'$ be a basis of Λ'. Then*

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

Proof. The quotient map $\pi\colon \Lambda \to \Lambda/\Lambda'$ induces a bijection $\Pi(\mathcal{B}') \cap \Lambda \to \Lambda/\Lambda'$ by Proposition 2.43. 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 2.53. Then the change of bases matrix is diagonal with determinant $k_1 \cdot \ldots \cdot k_r$, while the set $\Pi(\mathcal{B}') \cap \Lambda$ consists of the points $\sum_i l_i b_i$ for $0 \leq l_i \leq k_i - 1$. □

In dimensions $d \geq 2$ there are infinitely many unimodular matrices. Hence, there are also infinitely many different bases of a lattice. In Section 6.4 we deal with the problem of finding bases of a lattice with some nice properties. We will e.g. construct bases with "short" vectors.

Exercise 2.22
Exercise 2.23
Exercise 2.24
Exercise 2.25
Exercise 2.26
Exercise 2.27
Exercise 2.28
Exercise 2.29

Definition 2.55 (dual lattice) *Let $\Lambda \subset V$ be a lattice with $\operatorname{lin}\Lambda = V$. Then set*

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

is the dual lattice *to* Λ.

If $b_1, \ldots, b_d$ is a basis of Λ and $\alpha_1, \ldots, \alpha_d$ is the corresponding dual basis (i.e. $\alpha_i(b_j) = 1$ if $i = j$, and $\alpha_i(b_j) = 0$ otherwise), then $\Lambda^\star$ is spanned by $\alpha_1, \ldots, \alpha_d$ as a lattice. Hence, the dual lattice is indeed a lattice. Further, dualizing twice gives us back the original lattice, $\Lambda^{\star\star} = \Lambda$, as $b_1, \ldots, b_d$ is a dual basis to $\alpha_1, \ldots, \alpha_d$. The following observation is left to the reader as as Exercise 2.32.

Exercise 2.30
Exercise 2.31
Exercise 2.32

Lemma 2.56 $\det(\Lambda)\det(\Lambda^\star) = 1$.

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

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

and

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

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

Lemma 2.57 *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $v_1, \ldots, v_k \in \Lambda$, $k < d$, linearly independent. Define $V := \operatorname{lin}(v_1, \ldots, v_k)$. Then there is $v \in \Lambda - V$ and $x \in V$ such that*

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

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

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

Then $a \in (B_r(\Pi) - V) \cap \Lambda$. Further, $B_r(\Pi)$ is bounded, so $B_r(\Pi) \cap \Lambda$ is finite by Lemma 2.47. Hence, we can choose some $v \in (B_r(\Pi) - V) \cap \Lambda$ that minimizes $\mathrm{d}(v, \Pi)$. Choose some $x \in \Pi$ such that $\mathrm{d}(v, x)$ 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 $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ such that

$$y = \sum_{i=1}^{k} \lambda_i v_i \,.$$

Set $$z := \sum_{i=1}^{k} \lfloor \lambda \rceil_i \, v_i \,, \text{and} \quad z' := \sum_{i=1}^{k} \{\lambda\}_i \, v_i \,,$$

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

$$\mathrm{d}(y, w) \;=\; \mathrm{d}(y - z, w - z) \;\geq\; \mathrm{d}(w - z, \Pi) \geq \mathrm{d}(v, \Pi) \;=\; \mathrm{d}(v, x) \,. \qquad \square$$

We obtain a second proof that any lattice has a basis. For this, let $v_1, \ldots, v_d \in \Lambda$ be any linearly independent set in Λ. We consider the chain of subspaces

$$L_0 \;:=\; \{\mathbf{0}\} \qquad \text{and} \qquad L_i \;:=\; \mathrm{lin}\,(v_1, \ldots, v_i)$$

$$L_0 \;\subsetneq\; L_1 \;\subsetneq\; \ldots \;\subsetneq\; L_d \,.$$

By Lemma 2.57 we can find $b_1 \in L_1$ closest to $\mathbf{0}$. Let w be any other lattice vector in L_1. Then there is λ such that $w = \lambda b_1$, and

$$0 \;\leq\; \|w - \lfloor \lambda \rceil b_1\| \;<\; 1 \,.$$

By our choice of b_1 now $\lambda \in \mathbb{Z}$.

Now assume by induction that we habe a lattice basis of L_{k-1}. Choose any $b_k \in Ł_k \setminus L_{k-1}$ closest to L_{k-1} via Lemma 2.57. Let $w \in \Lambda \cap L_k$. Then there are $\mu_i, \eta_i \in \mathbb{R}$ for $1 \leq i \leq k$ such that

$$b_k \;:=\; \sum \mu_i v_i \qquad \text{and} \qquad w \;:=\; \sum \eta_i v_i \,.$$

Potentially flipping b_k we can assume than $\mu_k > 0$. We can find some $\ell \in \mathbb{Z}$ such that $0 \leq \eta'_k := \eta_k - \ell\mu_k < \mu_k$. Then

$$\mathrm{d}(w - \ell b_k, L_{k-1}) \;=\; \mathrm{d}(\eta'_k v_k, L_{k-1}) \;<\; \mathrm{d}(\mu_k v_k, L_{k-1}) \;=\; \mathrm{d}(b_k, L_{k-1}) \,.$$

Hence, by our choice of b_k we conclude that $w - \ell b_k \in L_{k-1} - cap\Lambda$, so that $\ell \in Z$. As we already know a lattice basis $b_1, \ldots, b_{k-1}$ of L_{k-1} we ontain an integral representation of w in $b_1, \ldots, b_k$. Hence, wen we habe reached L_d, then we have constructed a lattice basis of Λ. This reproves Theorem 2.46.

So far, we have considered lattices in *linear* spaces. We can shift all definitions to *affine* spaces.

Definition 2.58 (affine lattice) *Let Λ be a subset of an affine space A. Λ is an* affine lattice *if for some $x \in \Lambda$ the set $\Lambda - x$ is a lattice. A subset $\mathcal{B} \subseteq \Lambda$ is an* affine lattice basis *of Λ if $\mathcal{B} - x$ is a lattice basis of $\Lambda - b$. An* affine lattice isomorphism *is a map on Λ that comes from a lattice isomoprhism on $\Lambda - x$.*

2.3.2 Coordinates and Normal Forms

So far, all our considerations about lattices did not depend on a particular basis and a representation of transformations in coordinates *w.r.t.* to such a basis. However, sometimes, in particular for explicit computations in examples, it is more convenient to consider lattices and transformations in a given basis. We now reconsider some notions in the presence of a basis and introduce the Hermite and Smith normal form. Those allow us to compute bases and reprove Theorem 2.53.

Lemma 2.59 *Let $\mathcal{B}$ and $\mathcal{B}'$ be bases of the lattices Λ and Λ' respectively. Then a linear map $\mathsf{T}\colon \operatorname{lin}\Lambda \to \operatorname{lin}\Lambda'$ 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 $\mathsf{T}(\Lambda) \subseteq \Lambda'$.

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. □

Lemma 2.60 *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. "⇒": 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.

"⇐": 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. □

The set of such matrices is denoted by $\mathrm{Gl}(d, \mathbb{Z})$.

Corollary 2.61 *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 $|\det A| = 1$.* □

Corollary 2.62 *Let Λ be a lattice with basis $b_1, \dots, b_d \operatorname{lin}\Lambda$. Then $c_1, \dots, c_d \in \Lambda$ is another basis of Λ if and only if there is a unimodular transformation $\mathsf{T} :\in \Lambda \to \operatorname{lin}\Lambda$ such that $\mathsf{T}(b_i) = c_i$ for $1 \le i \le d$.* □

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

Definition 2.63 (Determinant of a lattice) *Let $\Lambda' \subseteq \Lambda$ be lattices with $\operatorname{lin}\Lambda = \operatorname{lin}\Lambda'$, and let $\mathcal{B}$ and $\mathcal{B}'$ be bases of Λ and Λ' respectively. Let A be the matrix representation of the identity $\operatorname{lin}\Lambda' \to \operatorname{lin}\Lambda$ 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 2.59 and Corollary 2.62 this definition is independent of the chosen bases.

Exercise 2.33

Exercise 2.34

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

Definition 2.64 (Hermite normal form) *Let $A = (a_{ij}) \in \mathbb{Q}^{d\times m}$ with $m \geq d$ be of full row-rank. The matrix A is in* Hermite normal form *if*

- $a_{ij} = 0$ *for* $j > i$ *and*
- $a_{jj} > a_{ij} \geq 0$ *for* $i > j$ *.*

So a matrix in Hermite normal form is an lower triangular matrix, and the largest entry in each row is on the diagonal.

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

$$\begin{bmatrix} 5 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 3 & 1 & 4 & 0 \end{bmatrix}$$

A matrix in Hermite normal form.

Theorem 2.65 (Hermite normal form) *Let $A \in \mathbb{Q}^{d\times m}$ of full row-rank. Then there is a unimodular matrix $U \in \mathbb{Z}^{m\times m}$ such that AU is in Hermite normal form.*

Proof. Let g be the common denominator of all entries of A. Then gA is an intergral matrix, and if H is in Hermite normal form with a unimodular transformation U such that $gA = HU$, then also $1/gH$ is in Hermite normal form and $A = 1/gHU$. Hence, in the following we can replace A by gA and assume that A is an integral matrix.

Now observe that the following three transformations on the columns of a matrix A can be realized by a multiplication with suitably chosen unimodular matrix T from the right:

(1) Exchanging two columns, and
(2) multiplying a column by -1, and
(3) adding an integral multiple of one column to another column.

These operations are called *elementary transformations* for a matrix. Any succession of such operations is then realized by the product of the corresponding transformation matrices, which is again unimodular. In the following, we will show that we can transform A into its Hermite normal form using only such elementary transformations. The unimodular matrix U in the theorem is then given by the product of the corresponding tranformation matrices.

We show that we can tranform A into its Hermite normal form by induction on the rows of A. So assume that A already has the form

$$A = \begin{bmatrix} B & \mathbf{0} \\ M & C \end{bmatrix} \tag{2.6}$$

for matrices B, C, M where $B \in \mathbb{Z}^{k \times k}$ is in Hermite normal form and $k \geq 0$. Consider the first row $(c_{11}, \ldots, c_{1,m-k})$ of the matrix C. Using elementary column operations we can transform C such that

(1) $c_{11} \geq c_{12} \geq \ldots, c_{1,m-k} \geq 0$ and
(2) $c := c_{11} + c_{12} + \cdots + c_{1,m-k}$ is as small as possible.

Then $c_{11} > 0$ as A has full row rank. Further, if $c_{12} \neq 0$, then we can subtract the second from the first column and reorder the columns if necessary to obtain a smaller total sum c. Hence, $c_{12} = c_{13} = \ldots = c_{1,m-k} = 0$. The column operations on C clearly extend to A without affecting B and M, so we can apply them to A to obtain a matrix

$$A = \begin{bmatrix} B & 0 & \mathbf{0} \\ m & c_{11} & 0 \\ M' & c_1' & C' \end{bmatrix},$$

where m' is a row vector of length k, the first row of the matrix M. By adding or subtracting multiples of the $(k+1)$st column (the one containing c_{11}) to the first k columns of A we can assume that all entries of m are nonnegative and smaller than c_{11}.

In this way we have again reached a matrix of the form (2.6), but this time B has size $(k+1) \times (k+1)$. After d steps A is in Hermite normal form using only elementary operations. □

Remark 2.66 *Using only elementary column operations in the proof was convenient as this directly provides a proof that the transformation matrix turning A into its Hermite normal form H is unimodular.*

However, this is inefficient for cumputations. Here one usually does the following. To transform the first row of C into one where all but the first elements are zero one does the following steps:

(1) swap a column with a non-zero entry in the first position to the front, possibly multiply by -1 to make it positive
(2) for any column c_j with non-zero first entry c_{1j} one computes the greatest common divisor g of c_{11} and c_{1j} and two integers x, y such that $g = xc_{11} + y + c_{1j}$. This can be done with the extended Euclidean algorithm. Now we replace the first column c_1 by $xc_1 + yc_j$ and the column c_j by $1/g(c_{1j}c_1 - c_{11}c_j)$. Note that in the second linear combinations the coeffcients $1/g c_{1j}$ and $1/g c_{11}$ are both integral.

A simple consideration shows that the transformation matrix corresponding to the transformation used in the second step has determinant ± 1 and thus is unimodular.

Using this approach implies that a Herminte normal form of any rational matrix can be computed in polynomial time in the size of the input matrix A.

Theorem 2.67 *The Hermite normal form of a matrix $A \in \mathbb{Q}^{d\times m}$ is unique.* □

Remark 2.68 *We can use the Hermite normal form to efficiently perform various tasks on lattices. For this, Let B and B' be matrices whose columns generate lattices $\Lambda := \Lambda(B)$ and $\Lambda' := \Lambda(B')$.*

(1) The first d colunms of the Hermite normal form of B give a basis of the lattice Λ.
(2) The lattices Λ and Λ' are equal if and only if the Hermite normal forms of B and B' coincide.
(3) lattice$'$ is a sublattice of Λ if and only if the Hermite normal forms of B and the matrix obtained by adding the columns of B' to B coincide.

For the Hermite normal form we have used elementary column transformations, which we can realize by multiplication with a unimodular matrix from the right. Clearly, we can study the same transformations also for the rows of a matrix, and we can realize them by multiplications with a unimodular matrix from the left. This leads to another important normal form of a matrix, which we explain with the next theorem.

Theorem 2.69 (Smith normal form) *Let $A \in \mathbb{Z}^{d\times m}$ be a matrix of full row rank. Then there are unimodular matrices $L \in \mathbb{Z}^{d\times d}$ and $R \in \mathbb{Z}^{m\times m}$ such that $S = (s_{ij})_{1\le i\le d, 1\le j\le m} := LAR$ satisfies*

(1) $s_{ij} = 0$ for $i \neq j$,
(2) $s_{ii} > 0$ for $1 \le i \le d$, and
(3) $s_{i-1,i-1}$ divides s_{ii} for $2 \le i \le d$.

The matrix S is unique, the companion matrices L and R are not.

The last statement about the non-uniqueness of L and R follows from the obsevation that there are unimodular matrices that commute with S. When actually computing smith normal forms with their companions, this fact can be used for an attempt to keep entries in L and R small.

Proof. As in the proof of the Hermite normal form it suffices to show that we can transform A into its Smith normal form using elementary row and column operations. The existence of the companions then follows.

We again use induction. Suppose that after some elementary transformations A has the form

$$A \;=\; \begin{bmatrix} S & \mathbf{0} \\ \mathbf{0} & C \end{bmatrix} \tag{2.7}$$

where S is a diagonal matrix with positive entries $s_{11}, \ldots, s_{kk}$ for $k \geq 0$ on the diagonal such that $s_{j-1,j-1}$ divides s_{jj} for $2 \leq j \leq k$, and s_{kk} devides all entries of C.

Among all transformations of C that we can reach with elementary row and column operations we pick one such that $\min(|c_{ij}| \mid 1 \leq i \leq d, 1 \leq j \leq mand c_{ij} \neq 0)$ is minimal. We can also assume that this minimum is attained by a_{11}. Then clearly c_{11} is the only non-zero element in the first row and column, as otherwise we can obtain a smaller entry by a suitable row of column operation. Further, a similar consideration shows that c_{11} must divide all other entries of C. We have extended our induction form (2.7) from k to $k+1$.

Uniqueness of S follows from the observation that in each step the element c_{11} that we construct is the greatest common divisor of the elements in C. □

You will use the Smith normal form to reprove Theorem 2.53 using bases of the lattices in a representation *w.r.t.* to a basis of the vector space in Exercise 2.35. Exercise 2.35

2.3.3 Metric Geometry

In this section, we will give a short discussion about lattices and metric geometry (mainly following [4]). 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

$$\Lambda^\star \;:=\; \mathrm{Hom}_{\mathbb{Z}}(\Lambda, \mathbb{Z})$$

and the *dual vector space* as

$$(\Lambda \otimes_{\mathbb{Z}} \mathbb{R})^\star \;:=\; \mathrm{Hom}_{\mathbb{R}}(\Lambda \otimes_{\mathbb{Z}} \mathbb{R}, \mathbb{R})\,.$$

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 $\Lambda \subset \mathbb{R}^d$ 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 $(\mathbb{R}^d)^\star$:

$$\mathbb{R}^d \cong (\mathbb{R}^d)^\star, \quad x \to \langle \cdot, x \rangle.$$

In particular, we get under this identification

$$\Lambda^\star \;=\; \{x \in \mathbb{R}^d \,:\, \langle x, y \rangle \in \mathbb{Z} \;\forall\, y \in \Lambda\} \subseteq \mathbb{R}^d\,.$$

Note that while $\Lambda^{\star\star} = \Lambda$, it may happen that $\Lambda^\star \neq \Lambda$. For instance, if $\Lambda = \mathbb{Z}^d/2$, then $\Lambda^\star = 2\mathbb{Z}^d$.

2.3.4 Hilbert Bases

Let $v_1, \ldots, v_n \in \Lambda$. Then $C := \operatorname{cone}(v_1, \ldots, v_n)$ 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 $\lambda_h \in \mathbb{Z}_{\geq 0}$ 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 $\mathcal{H}_1 := \{e_1, e_2, -(e_+e_2)\}$ 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 $\gcd(a_1, \ldots, a_d) = 1$.

Theorem 2.70 *Let $v_1, \ldots, v_n \in \Lambda$, $C := \operatorname{cone}(v_1, \ldots, v_n)$, 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 $y_1, \ldots, y_k \in \mathcal{H}$.

(2) Let $x \in C \cap \Lambda$ be any lattice vector in C. Then there are $\eta_1, \ldots, \eta_k \geq 0$ 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 $h \in \Pi \cap \mathbb{Z}^d = \mathcal{H}$. 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 $b \in \mathbb{R}^d$ such that

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

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

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 $x \notin \mathbb{Z}_{\geq 0} K$. 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

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

By our choice of x we get $x_1, x_2 \in \mathbb{Z}_{\geq 0} K$, so that $x \in \mathbb{Z}_{\geq 0} K$, a contradiction. □

From the above proof it follows that for a simplicial cone all Hilbert basis elements ecept for the generators of the cone are contained in the fundamental parallelepiped of the cone. Computing these points in the parallelepiped can be done by computing the Smith normal form. This, together with the generators of the cone is only a generating set G for the integer points in the cone. So we need to check for all of the (finitely many points) whether it is a sum of two other elements in G and in this case remove it from G.

For non-simplicial cones we can obtain a Hilbert basis in three steps:

(1) Triangulate the cone
(2) Compute a Hilbert basis in each simplicial cone
(3) Combine all Hilbert bases. This is a generating set for the integer points in the original cone. Reduce this set to a Hilbert basis by removing all points from it that are the sum of two other points in the set.

Definition 2.71 (homogeneous) *Let $\Lambda \subset \mathbb{R}^d$ be a lattice and $C \subseteq \mathbb{R}^d$ a finitely generated cone with generators $v_1, \ldots, v_d \in \Lambda$. 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 $1 \leq j \leq d$.*

The height *of an integer point $x \in C$ is*

$$\mathrm{ht}(x) \ := \ c^t x$$

Definition 2.72 (normal cone) *A finitely generated cone C which is homogeneous w.r.t. a functional c is* normal *if all Hilbert basis elements have height* 1.

2.4 Lattice polytopes

Definition 2.73 *A* lattice polytope *is a polytope in $\mathbb{R}^d$ with vertices in a given lattice $\Lambda \subset \mathbb{R}^d$.*

Note that $\dim(P) \leq \mathrm{rank}(\Lambda)$. Usually we will consider full-dimensional lattice polytopes, *i.e.*, $\dim(P) = \mathrm{rank}(\Lambda)$. However, we note that we can always consider P as a full-dimensional lattice polytope with respect to its *ambient lattice* $\mathrm{aff}(P) \cap \Lambda$ of rank $\dim(P)$ in its *ambient affine space* $\mathrm{aff}(P)$. Note that we need to be careful when considering lattices in faces of a polytope *w.r.t.* to the lattice of the polytope, see Exercise 2.36.

Exercise 2.36

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).

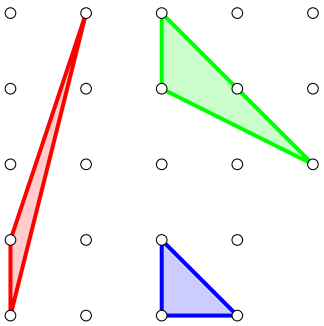


Fig. 2.13: Lattice triangles

2.4.1 Equivalence

Having introduced the objects of our interest, we should next state when two of them are considered isomorphic. Figure 2.13 shows three examples of lattice triangles 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*.

Definition 2.74 *Two lattice polytopes $P \subset \mathbb{R}^d$ and $P' \subset \mathbb{R}^{d'}$ (with respect to lattices $\Lambda \subset \mathbb{R}^d$ and $\Lambda' \subset \mathbb{R}^{d'}$) are* isomorphic *or* unimodularly equivalent*, if there is an affine lattice isomorphism of the ambient lattices $\Lambda \cap \operatorname{aff}(P) \to \Lambda' \cap \operatorname{aff}(P')$ mapping the vertices of P onto the vertices of P'.*

Recall from Definition 2.51 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 $T : \Lambda \to \Lambda'$ is a (linear) lattice isomorphism and $b \in \Lambda'$.

Luckily, by Corollary 2.61, in our usual situation $\Lambda = \mathbb{Z}^d = \Lambda'$ there is an easy criterion to check when a linear map $\mathbb{R}^d \to \mathbb{R}^d$ is a lattice automorphism of $\mathbb{Z}^d$. The matrix corresponding to the map must have integal entries and its determinant is 1 or -1.

Again, as we have seen from the example above, it is very important to realize that in our setting *isomorphisms do not preserve angles or distances*! Let us note an immediate consequence of Corollary 2.61

Corollary 2.75 *Unimodularly equivalent lattice polytopes have the same number of lattice points and the same volume.* □

2.4.2 Examples of Lattice Polytopes and Constructions.

A theory only comes to life through its examples and counterexamples. Luckily, there are many interesting lattice polytopes, reflecting the many mathematical fields where lattice polytopes play a role. Repeatedly, the same polytope comes by several different names, due to the fact that it has been (re-)discovered from different points of departure. In the following we collect only the most important constructions and examples as provisions for the road through this text. More examples are treated in the exercises.

Definition 2.76 $\Delta_d := \operatorname{conv}(0, e_1, \ldots, e_d)$ *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. Exercise 2.37

We discuss ways to construct new lattice polytopes from given ones. We have seen already the Minkowski sum construction introduced in

Definition 2.11. Clearly, if in this construction both summands are lattice polytopes, then so is their sum.

One of the most useful constructions is the product of two (or more) polytopes. Given two lattice polytopes P in $\mathbb{R}^d$ and Q in $\mathbb{R}^e$ we can construct a lattice polytope $P \times Q$, the *product* of P and Q in $\mathbb{R}^{d+e}$ via

$$P \times Q \ := \ \left\{ (p,q) \in \mathbb{R}^{d+e} \ : \ p \in P \text{ and } q \in Q \right\} .$$

The product has vertices (p,q) for vertices p of P and q of Q. Thus $P \times Q$ is a lattice polytope. The *prism* over P is a special case of a product where Q is just an interval. Mostly, one takes $Q = [0,1]$ if nothing else is specified.

Let $P = \text{conv}(v_1, \ldots, v_n)$ be a polytope. P is a *pyramid* with *apex* v_1 if there is an affine hyperplane H such that $v_2, \ldots, v_n \in H$ and $v_1 \notin H$.

Given a polytope P, we can construct a *pyramid over* P by embedding P into $\{0\} \times \mathbb{R}^d \subseteq \mathbb{R} \times \mathbb{R}^d$ and taking the convex hull with any $x \notin \{0\} \times \mathbb{R}^d$. We define

$$\text{Pyr}(P) := \text{conv}(\{0\} \times P, e_0) ,$$

where e_0 is the first standard unit vector in $\mathbb{R} \times \mathbb{R}^d$.

Let $P \subseteq \{\mathbf{0}\} \times \mathbb{R}^d$ be a polytope and $x, y \notin \{0\} \times \mathbb{R}^d$, such that the segment between x and y intersects P in the interior of P. Then

$$\text{BiPyr}(P) := \text{conv}(P, x, y) ,$$

is the *bipyramid* with *apices* x and y. A polytope Q is a *bipyramid* if it can be written as an (affine image) of the bipyramid over a polytope P.

The *join* of two lattice polytopes P and Q of dimensions d and e is

$$P \star Q \ := \ \text{conv}\left(P \times \mathbf{0}_e \times \{0\}, \mathbf{0}_d \times Q \times \{1\}\right) ,$$

where $\mathbf{0}_d$ and$\mathbf{0}_e$ are the zero vectors in dimension d and e. This is clearly again a lattice polytope. Note that a pyramid is a special case of this, where we take Q to be a single point.

Further constructions, *e.g.* Cayley polytopes and Lawrence prisms will be discussed at the relevant places in the next chapters.

Lattice polytopes also play an important role in various branches of mathematics. We give a few examples.

(1) In *enumerative combinatorics* one can study the *order polytope*
(2) *cut polytopes* or *traveling salesperson polytopes* in *combinatorial optimization*
(3) *hypersimplex*
(4) *Birkhoff* polytope and the *permutation polytopes*

2.4.3 Volumes

This section is devoted to a fundamental result on lattice polytopes. In Section 1.2 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*. We have seen that for polygons this implies that there are only finitely many isomorphism types with a fixed number of lattice points. Unfortunately, no such result is true in dimensions three and above and you have constructed examples in Exercise 1.9. 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.

Remark 2.77 *Note that here 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 $\mathbb{Z}^d$.*

Consider the standard simplex Δ_d defined in Definition 2.76. Note that $\operatorname{vol}(\Delta_d) = 1/d!$ The following observation shows that the standard simplex defined in is indeed the *smallest* possible lattice polytope:

Proposition 2.78 *Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice simplex. Then there is an affine lattice homomorphism $\varphi : \mathbb{Z}^d \to \mathbb{Z}^d, x \mapsto Ax + b$ mapping the vertices of Δ_d onto the vertices of P. In this case,*

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

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

$$\operatorname{vol}(P) = |\det(\varphi)|\,\operatorname{vol}(\Delta_d) = \left|\det\left(\begin{pmatrix} v_1 & \cdots & v_d \end{pmatrix}\right)\right| \frac{1}{d!}. \qquad \square$$

Corollary 2.79 *Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope. Then*

$$d!\,\operatorname{vol}(P) \;\in\; \mathbb{Z}_{\geq 1}\,.$$

We have $d!\,\operatorname{vol}(P) = 1$ if and only if P is a unimodular simplex.

Proof. By Theorem 2.35 we can triangulate P 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.

Definition 2.80 *The* normalized volume *of a d-dimensional lattice polytope $P \subset \mathbb{R}^d$ is defined as the positive integer*

$$\operatorname{nvol}(P) \;:=\; d!\,\operatorname{vol}(P)\,.$$

Remark 2.81 *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,* $\operatorname{nvol}(P) \geq 1$ *for* any *lattice polytope.*

Note that, if $P = \operatorname{conv}(0, v_1, \ldots, v_d)$ is a d-dimensional lattice simplex in $\mathbb{R}^d$, then by Proposition 2.78 the normalized volume of P equals the volume of the parallelepiped spanned by $v_1, \ldots, v_d$.

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.

Theorem 2.82 *Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope,* $\operatorname{nvol}(P) = V$*. Then there exists some lattice polytope $Q \subset \mathbb{R}^d$ 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.

Corollary 2.83 *There exist only finitely many isomorphism classes of lattice polytopes of given dimension and volume.* □

We will first prove Theorem 2.82 for simplices. We need the following useful observation to extend this result to arbitrary polytopes. The proof is left as Exercise 2.38. The centroid of a simplex with vertices $v_0, \ldots, v_d$ is $\frac{1}{d+1} \sum_{i=0}^{d} v_i$.

Lemma 2.84 *Let $P \subset \mathbb{R}^d$ 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 $v_0, \ldots, v_d$ are the vertices of S, then

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

Exercise 2.38

Proof (of Theorem 2.82). We can assume that one vertex of P is the origin $\mathbf{0}$. First, let $P = \operatorname{conv}(\mathbf{0}, v_1 \dots, v_d)$ be a simplex. Let $V \in \mathbb{Z}^{d\times d}$ be the matrix whose columns are the coordinate vectors of $v_1, \dots, v_d$. By the Hermite normal form (Theorem 2.65) (where we transpose the left and right side of the equation) there exists $U \in \mathrm{Gl}_d(\mathbb{Z})$ such that $UV = H$ and H is an upper triangular matrix with non-negative integer entries such that in each column the maximal element is on the diagonal.

We denote the columns of the right matrix by $h_1, \dots, h_d$. Therefore, U defines a unimodular transformation mapping P to

$$Q \;:=\; \operatorname{conv}(\mathbf{0}, h_1, \dots, h_d) \subseteq [0, \det\, H]^d\,,$$

where the last inclusion follows, as $\det H \geq h_{ii}$ for all $1 \leq i \leq d$ and $0 \leq h_{ij} \leq \max h_{ii}$. This proves the claim for simplices, as $\operatorname{nvol}(P) = \operatorname{nvol}(Q) = \det H$.

In general, there exists a lattice d-simplex $S \subseteq P$ as in Lemma 2.84. Then the previous part of the proof shows that there exists a unimodular transformation $\varphi : \mathbb{Z}^d \to \mathbb{Z}^d$ such that

$$\varphi(S) \;\subseteq\; [0, \operatorname{nvol}(S)]^d\,.$$

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

$$\begin{aligned} P \;\cong\; \varphi(P) &\subseteq (-d)\varphi(S) + \sum_{i=0}^{d} \varphi(v_i) \\ &\subseteq\; [0, -d \operatorname{nvol}(S)]^d + \sum_{i=0}^{d} \varphi(v_i)\,. \end{aligned}$$

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

2.5 Software

We can du actual computations with polytopes, cones and fans using the software framework `polymake`.

```
polytope> $c=cube(3);
polytope> print $c->VERTICES;
1 0 0 0
1 1 0 0
1 0 1 0
1 0 0 1
1 1 1 0
1 1 0 1
1 0 1 1
1 1 1 1
```

2.6 Problems

included on p

2.1. Prove Carathéodory's Theorem (Theorem 2.4).

included on page 27

2.2. Show that the preimage of the projection of a face F is again a face (but not necessarily the original one).

included on page 27

2.3. If some $x \in \mathbb{R}^d$ is in the relative interior of two faces of a convex set, then the two faces coincide.

included on page 27

2.4. Let $\pi : \mathbb{R}^d \to \mathbb{R}^m$ be a projection that maps a d-dimensional polytope P onto a m-dimensional polytope Q. Then, if x is a point in the interior of Q, $\operatorname{relint}(\pi^{-1}(x) \cap P) \subseteq \operatorname{int}(P)$.

included on page 28

2.5. Show that a d-dimensional polytope has faces in any dimension $0 \leq k \leq d-1$.

included on page 28

2.6. Prove that any $(d-2)$-dimensional face of a d-dimensional polytope is contained in precisely two facets.

included on page 28

2.7. Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with $\mathbf{0} \in \operatorname{int} P$. Prove that dualizing the dual polytope $P^\star$ gives you back the original polytope P.

included on page 29

2.8. Show that simple and simplicial are dual notions.

included on page 31

2.9. Prove Proposition 2.30.

included on page 31

2.10. Prove that the tangent cone of a face of a polytope is precisely the intersection of the half spaces defining F.

included on page 32

2.11. Show that any subdivision $\mathcal{S}$ of a polygon P such that $\mathcal{V}(\mathcal{S}) = \mathcal{V}(P)$ is regular.

included on page 33

2.12. Prove that the subdivision in Figure 2.9 is not regular.

included on page 34

2.13. Show that a discrete additive subgroup of $\mathbb{R}^d$ is closed.

included on page 34

2.14. Let Λ be a discrete closed subset of $\mathbb{R}^d$ (for instance, a discrete additive subgroup by Exercise 2.13) and B a bounded subset of $\mathbb{R}^d$. Then $\Lambda \cap B$ is a finite set. Give an example that shows that this is not correct for general discrete subsets.

2.15. Show that the definition of a lattice in Definition 2.37 does not depend on the norm chosen to define the balls.

2.16. Show that in Definition 2.37 we can choose the same ε for all $x \in \Lambda$.

2.17. Prove that the following subsets of $\mathbb{R}^d$ are lattices.
(1) B_d
(2) Recall the definition of D_d from (2.5). Let us define $\mathrm{D}_d^{1/2} := \mathrm{D}_d + (\frac{1}{2}\mathbf{1} + \mathrm{D}_d)$ for even d. Show that this is a lattice. For $d = 8$ this is the root system E_8.
(3) E_7
(4) E_6
These are the so called *root systems*.

included on page 36

2.18. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice wit 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 $(x + \Lambda) \cap (y + \Lambda) = \varnothing$ for $x, y \in \Lambda$, $x \neq y$.

included on page 38

2.19. Show that any full-dimensional cone contains a lattice basis.
Hint: Use induction over the dimension.

included on page 38

2.20. Let $b_1, \ldots, b_d$ be linearly independent lattice points in a lattice Λ of rank d. Show that the closed fundamental parallelepiped spanned by $b_1, \ldots, b_d$ contains a lattice basis of Λ.

included on page 38

2.21. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and $v_1, \ldots, v_d \in \Lambda$ be such that $\operatorname{vol} \Pi(v_1, \ldots, v_d) = \det \Lambda$. Then $v_1, \ldots, v_d$ is a basis of Λ.

included on page 39

2.22. Let Λ' be a sublattice of $\Lambda \subseteq \mathbb{R}^d$ with rank d. Let Π be the fundamental parallelepiped of a lattice basis of Λ.
Show that $v \mapsto v + \Lambda'$ is a bijektion from $\Pi \cap \Lambda$ to Λ / Λ' ist.

included on page 39

2.23. Show that $\mathbb{Z}^2 / < k_1 e_1, k_2 e_2 >_{\mathbb{Z}} \cong \mathbb{Z}/k_1\mathbb{Z} \oplus \mathbb{Z}/k_2\mathbb{Z}$ for $k_1, k_2 \in \mathbb{Z}$

included on page 39

2.24. Let Λ be a lattice of rank d in $\mathbb{R}^d$ and let L be a linear subspace in $\mathbb{R}^d$ of dimension n. Show that, if $L \cap \Lambda$ is a lattice of rank n, then any lattice basis of $L \cap \Lambda'$ can be extended to a lattice basis of Λ.

included on p

2.25. Let Λ be a lattice and $v \in \Lambda$ prtimitive. Show that v is part of some lattice basis.

included on p

2.26. Let Λ be a lattice of rank d in $\mathbb{R}^d$ and $\mathcal{B} := \{b_1, \ldots, b_d\} \subset \Lambda$ linearly independent.
Show that $\mathcal{B}$ is a lattice basis of Λ if and only if $\Pi(\mathcal{B})$ as volume $\det \Lambda$.

included on page 39

2.27. The following map is a (canonical) isomorphism

$$\psi : \mathbb{R}^d \to ((\mathbb{R}^d)^*)^*,\ x \longmapsto (u \mapsto u(x))\,.$$

included on page 39

2.28. The map ψ ψ from Exercise 2.27 induces a natural isomorphism between Λ and $(\Lambda^*)^*$.

included on page 39

2.29. Let Λ be a lattice of rank d in $\mathbb{R}^d$, and $T : \mathbb{R}^d \to \mathbb{R}^d$ a linear map with $T(\Lambda) \subseteq \Lambda$.
Show that for $T^* : (\mathbb{R}^d)^* \to (\mathbb{R}^d)^*, \quad \varphi \mapsto (v \mapsto \varphi(T(v)))$ we have that $T^*(\Lambda^*) \subset \Lambda^*$.

included on page 39

2.30. let $b_1, \ldots, b_d$ be a basis of $\mathbb{R}^d$. For $x = \sum_{i=1}^d \lambda_i b_i \in \mathbb{R}^d$ we define $b_i^*(x) = \lambda_i$. Show that $b_1^*, \ldots, b_d^*$ is a basis of $(\mathbb{R}^d)^*$.

included on page 39

2.31. Let $b_1, \ldots, b_d$ be a lattice basis of the lattice Λ in $\mathbb{R}^d$. Then $b_1^*, \ldots, b_d^*$ is a lattice basis of the lattice Λ^* in $(\mathbb{R}^d)^*$.

included on page 39

2.32. Prove Lemma 2.56.

included on page 42

2.33. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice, $v_1, \ldots, v_k \in \Lambda$, $L := \operatorname{lin}(v_1, \ldots, v_k)$ and $L^\perp$ its orthogonal complement with orthogonal projection $\pi : \mathbb{R}^d \to L^\perp$.
(1) Show that $\Gamma := \pi(\Lambda)$ is a lattice in $L^\perp$.
(2) Show that $\Gamma^\star \subseteq \Lambda^\star$.

included on page 42

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

$$\Pi(v_1, \ldots, v_d) \;=\; \left\{ \sum \lambda_i b_i \mid \lambda_i \in [0,1) \right\}.$$

Show that

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

2.35. Reprove Theorem 2.53 using the Smith normal form (Theorem 2.69).

2.36. Construct a Λ-polytope P and a face F where

$$\operatorname{aff} F \cap \Lambda \;\neq\; \operatorname{aff} F \cap \langle P \cap \Lambda \rangle \;\neq\; \operatorname{aff} F \cap \langle F \cap \Lambda \rangle .$$

included on page 49

2.37. Show that Δ_d has volume $1/d!$.

Hint: think of Δ_d as iterated pyramids or subdivide $[0,1]^d$ into $d!$ simplices.

included on page 52

2.38. Let $P \subseteq \mathbb{R}^d$ be a d-dimensional lattice polytope (or any convex body) Show that there is a simplex $S \subseteq P$ with vertices $v_0, \ldots, v_d$ such that

$$P \;\subseteq\; (-d)(S-x) \;+\; x \;=\; (-d)S \;+\; (d+1)x \tag{2.8}$$

and

$$P \subseteq\; (d+2)(S-x) \;-\; x \;=\; (d+2)S \;-\; (d+1)x \tag{2.9}$$

where

$$x \;:=\; \frac{1}{d+1}\sum_{i=0}^{d} v_i$$

is the centroid of S.

Hint: Choose $S := \operatorname{conv}(v_0, \ldots, v_d) \subseteq P$ with maximal volume in P.
For any $0 \le i \le d$ let H_i be the facet hyperplane of the facet of S not containing v_i, $r_i := \mathrm{d}(v_i, H_i)$ and $R_i := \{x : \mathrm{d}(x, H_i) \le r_i\}$.
Show that $P \subseteq R_i$ for $0 \le i \le d$.
Express $\bigcap_{i=0}^{d} R_i$, $(-d)(S-x)+x$, and $(d+2)(S-x)-vx$ in barycentric coordinates with respect to $v_0, \ldots, v_d$ and compare.

included on page 9

2.39. Sei K eine konvexe Menge in $\mathbb{R}^d$, und $a, b \in \mathbb{Z}_{\ge 0}$. Zeige $(a+b)K = aK + bK := \{ax + by : x, y \in K\}$. (Gilt das auch für $a, b < 0$?)

included on page 9

2.40. Recall the isolation theorem : Given an open convex set S in $\mathbb{R}^d$. Then any point outside of S can be strictly separated from S. Finde explizite Beispiele in Dimension 2, dass
(1) dies die Voraussetzung konvex braucht
(2) dies die Voraussetzung offen braucht

(3) eine abgeschlossene konvexe Menge kann einen Extrempunkt haben, der keine Seite (Ecke) ist
(4) eine kompakte Menge K eine Seite F haben kann, die eine Seite G hat, die aber keine Seite von K ist

included on p

2.41. Wie kann man die affine Hülle mithilfe von 'Affin-Kombinationen' beschreiben? kleinster ist!

included on page 9

2.42. (Härter) Sei $S \subset \mathbb{R}^d$, $x \in \mathbb{R}^d$. Zeige: x ist ein Extrempunkt von $\operatorname{conv}(S)$ g.d.w. $x \in S$ und $x \notin \operatorname{conv}(S \backslash \{x\})$.

included on page 9

2.43. Check that Weyl-Minkowski for cones implies that for polytopes

included on page 9

2.44. Man erinnere sich, wieso die Determinante einer linearen Abbildung unabhängig von der Basiswahl ist. Nun beweise für ein Gitter $\Lambda \subset \mathbb{R}^d$, dass wenn T eine lineare Abbildung von $\mathbb{R}^d$ nach $\mathbb{R}^d$ ist, so dass die Einschränkung $T_\Lambda : \Lambda \to \Lambda$ wohldefiniert ist und surjektiv, dann ist T_Λ bijektiv. (Tipp: wieso ist T bijektiv?) Zeigen Sie allgemeiner(?), dass ein Homomorphismus von $\Lambda \to \Lambda$ surjektiv ist g.d.w. bijektiv.

included on page 9

2.45. Dualizing non-polyhedral cones.

included on page 9

2.46. Existence of a Hilbert basis

included on page 9

2.47. Man mache sich an einem Beispiel plausibel (oder beweise für $i = 1$), dass für gegebenes $i \in \{1, \ldots, n\}$ und für ganzzahlige $n \times n$-Matrizen der ggT aller Determinanten von $i \times i$-Untermatrizen bei Multiplikation mit unimodularen Matrizen invariant bleibt. Wieso impliziert dies die Eindeutigkeit der Smith-Normalform?

included on page 9

2.48. Man berechne die Smith-Normalform für

$$\begin{pmatrix} 3 & 0 \\ 0 & 14 \end{pmatrix}$$

und für eine 3×3-Matrix Ihrer Wahl.

included on page 9

2.49. Sei P ein d-dim. Gitterpolytop in $\mathbb{R}^d$ mit $0 \in \operatorname{int}(P)$ und F eine Facette von P. Zeige dass es eine lineare unimodulare Transformation gibt, die F auf eine Teilmenge von $\mathbb{R}^{d-1} \times \{m\}$ für $m \in \mathbb{Z}_{\geq 1}$ abbildet. qDie Zahl m ist der ganzzahlige Abstand des Ursprunges von F). Hinweis: Betrachten Sie η_F und bilden Sie es auf e_d^* ab.

2.50. Ist ein Skalarprodukt $\langle \cdot, \cdot \rangle$ auf $\mathbb{R}^d$ gegeben, so ist

$$\varphi : \mathbb{R}^d \to (\mathbb{R}^d)^*,\ y \mapsto (x \mapsto \langle y, x \rangle)$$

ein Isomorphismus.

included on page 9

2.51. Ein Gitter-Isomorphismus $\mathbb{Z}^n \to \mathbb{Z}^n$ wurde definiert als eine $\mathbb{Z}$-lineare Abbildung, die bijektiv ist. Man mache sich klar, dass hier eine $\mathbb{Z}$-lineare Abbildung nichts anderes als ein Gruppenhomomorphismus ist (wenn man von Gruppen und Homomorphismen schon gehört hat). Prüfe, dass die inverse Abbildung eines Gitterisomorphismus auch wieder ein Gitterisomorphismus ist. Kennen Sie Beispiele z.B. aus der Analysis wo 'bijektiv' und 'Isomorphismus' nicht das gleiche sind? (Idee: stetige Funktionen).

included on page 9

2.52. Man mache sich klar:
Jeder Gitter-Isomorphismus $\mathbb{Z}^n \to \mathbb{Z}^n$ definiert auch einen Vektorraum-Isomorphismus $\mathbb{R}^n \to \mathbb{R}^n$ (Hinweis: Betrachte die Standardbasis). Jeder Gitter-Isomorphismus ist durch eine $\mathrm{Gl}_n(\mathbb{Z})$-Matrix gegeben. Dies ergibt eine Bijektion zwischen Gitterisomorphismen und $\mathrm{Gl}_n(\mathbb{Z})$-Matrizen.

included on page 9

2.53. Zeige, dass für $v_1, \ldots, v_d \in \mathbb{R}^d$ das Volumen des aufgespannten Parallelepipeds gleich $d!$ mal dem Volumen der konvexen Hülle von $0, v_1, \ldots, v_d$ ist.

included on page 9

2.54. Zeige, dass unter einer affin-linearen Abbildung die konvexe Hülle des Bildes einer Menge gleich dem Bild der konvexen Hülle ist.

included on page 9

2.55. Hmm, kann man eigentlich einen Isomorphiebegriff für rationale Polytope (also solche, deren Ecken alle rationalen Koordinaten besitzen) formulieren?

included on page 9

2.56. Finde das normalisierte Volumen der konvexen Hülle von $(2, 0, 4)$, $(1, 1, 0)$, $(0, 2, -2)$.

included on page 9

2.57. Ist der Endlichkeitssatz für Gittersimplizes scharf? (Offen: was für Gitterpolytope?)

Ehrhart Theory 3

Contents

In this chapter we will be concerned with 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 $P \subseteq \mathbb{R}^d$, the *Ehrhart counting function*,

$$\mathsf{ehr}_P(k) \;:=\; |k \cdot P \cap \mathbb{Z}^d|\,,$$

is the evaluation of a polynomial $\mathsf{ehr}_P(t)$ of degree d in $t = k$. This polynomial $\mathsf{ehr}_P(t)$ is called the *Ehrhart polynomial* of P, and it is at the heart of the theory of lattice polytopes.

3.1 Motivation

Pick's Theorem and Reciprocity

Monomials of degree d in $\mathbb{R}[x_1, \ldots, x_d]$

Semi-Magic Squares A magic square is an n by n grid filled with n^2 positive integers, such that the sum of each row, each column, and the two main diagonals is the same for all. This number is the *magic constant*. Sometimes it is additionally required that the entries in each row, column and diagonal are pairwise distinct and the total set of entries is $\{1, \ldots, n^2\}$. See Table 3.1 for a famous example that already appeared in the painting *Melancholia I* by Albrecht Dürer in 1514.

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Table 3.1: Dürers magic square of 1514.

The number of possible $n \times n$ magic squares with magic constant b is given by the set of positive integer solutions to

$$\sum_{i=0}^{n-1} x_{ij} \;=\; \sum_{i=0}^{n-1} x_{ji} \;=\; \sum_{i=0}^{n-1} x_{ii} \;=\; \sum_{i=0}^{n-1} x_{i,n-i} \;=\; b\,.$$

for $0 \leq j \leq n-1$.

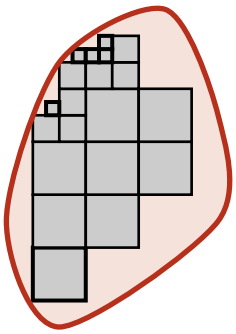


Fig. 3.1: Approximating a convex body by smaller and smaller cubes

Volumes The most important natural invariant of a convex body is its volume. Computing the volume of a convex body is in general a complicated problem. Counting lattice points in multiples of a polytope is directly related to it. Let $P \subset \mathbb{R}^d$ be a convex body. As illustrated in Figure 3.1, we can approximate the volume by counting the volume of little cubes centered at the more and more refined lattice $\mathbb{Z}^d/k$ (for $k \to \infty$).

$$\begin{aligned}\mathrm{vol}(P) \;=\; \int_P \mathsf{dx} \;&=\; \lim_{k\to\infty} \frac{1}{k^d} |P \cap (\mathbb{Z}^d/k)| \;=\; \lim_{k\to\infty} \frac{1}{k^d} |kP \cap \mathbb{Z}^d| \\ &=\; \lim_{k\to\infty} \frac{1}{k^d} \mathsf{ehr}_P(k)\end{aligned} \tag{3.1}$$

We see that knowing infinitely many values of the Ehrhart counting function allows to determine the volume. However, if we would know

that $\mathsf{ehr}_P(k)$ is actually a polynomial function, then by Equation (3.1) it must have degree d and leading coefficient $\mathrm{vol}(P)$. In particular, the Ehrhart polynomial would be determined by knowing $d+1$ many values of it. It follows that if the Ehrhart counting function of P is polynomial with constant term 1 (as we will show later for lattice polytopes P), then $\mathrm{vol}(P)$ can be explicitly computed from $|kP \cap \mathbb{Z}^d|$ for $k = 1, \ldots, d$. This looks already very much like a generalization of Pick's formula (which we have seen in Pick's Formula (Theorem 1.8))! In Exercise 3.1, the reader is invited to work this out explicitly in dimension three. Exercise 3.1

Exploiting the important reciprocity principle which we will also learn about later in this chapter, one can even show that (and this is just one possibility of such a generalized Pick's formula), the volume of a d-dimensional lattice polytope can be determined from knowing the number of lattice points in kP for $k = 1, \ldots, \lceil d/2 \rceil$ together with the number of interior lattice points of kP for $k = 1, \ldots, \lfloor d/2 \rfloor$. This gives a nice formula for the volume of a three-dimensional lattice polytope (see Exercise 3.2) that should satisfy the curiosity of the reader for a Pick's formula in dimension three and convey the usefuleness of Ehrhart's theorem. Exercise 3.2

Of course, there are many more arguments why Ehrhart polynomials are important:

- they allow to read off important properties of the polytope,
- their coefficients form a basis for the space of ...,
- they have algebro-geometric analogues,
- ...

3.1.1 Examples of Ehrhart polynomials

In this short section, we compute for some simple examples the counting function $\mathsf{ehr}_P(k)$ of a polytope directly. We will observe that it is indeed given by a polynomial, and that evaluating at negative integers gives the number of interior points.

Before we start, we want to give a formal definition of the counting function. For this, let $S \subseteq \mathbb{R}^d$, and let $k \in \mathbb{Z}_{>0}$. The *k-th-dilation of a set* of S is the set

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

We introduce the following counting function.

Definition 3.1 *The* Ehrhart counting function *of a bounded subset $S \subseteq \mathbb{R}^d$ is the function*

$$\begin{aligned} \mathsf{ehr}_S(k) \;:\; \mathbb{Z}_{\geq 1} &\longrightarrow \mathbb{Z}_{\geq 1} \\ k &\longmapsto \left| kS \cap \mathbb{Z}^d \right| . \end{aligned}$$

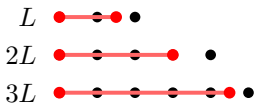


Fig. 3.2

With this definition we can look at our first examples. Let $L := [a,b] \subset \mathbb{R}$, $a,b \in \mathbb{R}$ be an interval on the real line. Here, counting is easy, L contains $\lfloor b \rfloor - \lceil a \rceil + 1$ integers. The k-th dilate of P is $[ka, kb]$. By the same argument it contains $\lfloor kb \rfloor - \lceil ka \rceil + 1$ integral points, so

$$\mathrm{ehr}_L(k) \;=\; \lfloor kb \rfloor - \lceil ka \rceil + 1\,.$$

Figure 3.2 shows the interval $I = [0, \frac{3}{2}]$ and its second and third dilation.

If the boundary points a and b are integral and $a \le b$, 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

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

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 some examples of polytopes in general dimension $d \ge 0$. Let us first consider the *standard simplex*

$$\Delta_d \;:=\; \mathrm{conv}(\mathbf{0}, e_1, \ldots, e_d)$$

introduced in Definition 2.76. See Figure 3.3 for the lattice points in a multiple of this ismplex.

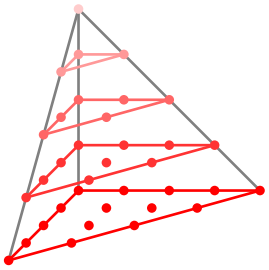


Fig. 3.3: Lattice points in a standard simplex.

Proposition 3.2 *Let Δ_d be the d-dimensional standard simplex. Then*

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

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

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 ith coordinate equals the number of dots between the ith bar and the $(i+1)$st bar for $1 \le i \le d-1$ (we don't write down the number of dots after the last bar, it is determined by the rest):

$$\cdot\,\cdot \mid \cdot\,\cdot\,\cdot \mid\mid \cdot \qquad \longleftrightarrow \qquad x \;=\; (2,3,0)$$

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

Exercise 3.3

Another simple, but very important example is the unit cube defined in Example 2.7(1). 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

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

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

3.2 Generating Functions for Lattice Points

The examples in the previous sections show that we really want to investigate lattice points $S := P \cap \mathbb{Z}^d$ in polytopes or polyhedra $P \subseteq \mathbb{R}^d$, *i.e. count* them (if the nuber is finite), *enumerate* them, explore *structure* on this set S, or explain their *interactions* with polyhedral geometry, algebra and other field.

All of this requires us to first find a way to distinguish lattices points in a polyhedron from all others, *i.e.* a way to encode them, preferably in an *efficient* and *explicit* way, that we can easily write down in a *short* and *concise* form. It should be simple from our notation to decide whether a point is in our list or not.

We have already seen two more indirect ways already above, directly from the interior and exterior description of a polytope. A lattice point x is in our set S if it is either a convex combination of the vertices of P or satisfies all defining inequlities of P. This description is fine for a single particular lattice point. But it does not tell us much about the whole set of points, nor about the structure of the set.

For this, we need to find a way to make our description of the set S more explicit. In a first, rather naïve approach, we could now be tempted to explicitely list all lattice points in our polytope (this clearly only works well for bounded objects). To make a simple example, look at the polytope $P_3 := [0, 3]$. This is the simple segment shown in Figure 3.4. The naïve approach gives us the list:

Fig. 3.4: The polytope P_3.

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

This works well in this small example, but consider the structurally similar example $P_{10002} := [0, 10002]$. Here, our plain list

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

easily exceeds a line, and also the length of this book. To get a compact encoding of the points we need a better idea.

Here is one that might look really strange at first, but will prove to be very powerful. We can replace each point $k \in P_3$ with its monomial t^k. With this we define a polynomial that contains precisely the monomial corresponding to points in our polytope:

$$1 + t + t^2 + t^3 \ = \sum_{i=0}^{3} t^i\,,$$

The option to write our polynomial as a sum already shows a quite compact way to encode the lattice points. Observe, that the representation is not really more complicated for P_{10002}. However, it is pretty obvious

that this particular compact notation as a sum is only possible in very special cases, so we need to look further.

If you look at the polynomial you may realize that there is another option to write this more condensed than using a sum: We can also write this as the geometric series

$$\mathsf{G}_{P_3}(t) \;:=\; \frac{1-t^4}{1-t}\,.$$

whose expansion is again our polynomial. Again, doing the same for P_{10002} does not really make this notation more complicated:

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

We will see that this idea of using a geometric series to specify the lattice points in a polyhedron is both sufficiently flexible to work for all polyhedra, and efficient enough that we can use it to really study the structure of the set of lattice points.

Her comes another surprising and powerful property of our last observation. If we try to do write down the lattice points of the unbounded polyhedron $P_\infty := [0,\infty)$, then our first two approaches obviously become infeasible. However, the third works and turns out to be even shorter and more appealing[1]! As a geometric series we can consisely describe all lattice points in P_∞ via the monomials in

$$\mathsf{G}_{[0,\infty)}(t) \;:=\; \frac{1}{1-t}\,.$$

[1] If the reader feels slightly wary about what happens at $t=1$, be assured that in our approach here we will not deal with any analytic convergence issues and will not evaluate at certain values.

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.

It will soon become apparent it is indeed quite useful and natural to encode lattice points not only in polytopes, but more generally in any bounded or unbounded subset of $\mathbb{R}^d$, as in the last example of a ray in $\mathbb{R}^1$. 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 now want to formalize this idea, and directly generalize it to arbitrary dimensions. Let $\Bbbk$ be some ground field (you can just think of $\Bbbk = \mathbb{C}$, if you like). We assign the monomial

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

in d variables to a lattice point $a = (a_1, \ldots, a_d) \in \mathbb{Z}^d$. In the above example all lattice points were non-negative and thus lead to the "usual kind" of monomials. In general, the coordinates of a are allowed to be

negative, so this is a *Laurent polynomial* living in the *Laurent polyonmial ring*

$$\mathsf{L} \;=\; \Bbbk[t_1^{\pm 1}, \ldots, t_d^{\pm 1}] \; .$$

Moreover, note that the sum of monomials for the cone $x \geq 0$ is infinite. Since we do not care about convergence, we will actually consider our sums not as Laurant polynomials, but as series in a subset of the L-module

$$\widehat{\mathsf{L}} \;:=\; \Bbbk t_1^{\pm 1}, \ldots, t_d^{\pm 1}$$

of *formal Laurent series*. We give an example before we write down the proper definition.

Example 3.3 *Let P be the polygon*

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

(see Figure 3.5). Recall that the convex hull of a matrix is defined to be the convex hull of the column vectors of the matrix. We list the lattice points as monomials in the Laurent polynomial

$$\begin{array}{ccccc} & & t_1^2 t_2^2 & & \\ & + t_2 + t_1 t_2 & + t_1^2 t_2 & & \\ & + t_1 & + t_1^2 & + t_1^3 & \\ & & + t_1^2 / t_2 & & \end{array} \; .$$

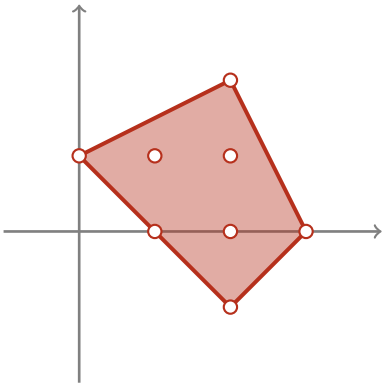


Fig. 3.5: The polygon of Example 3.3.

Definition 3.4 (integer point *series*) *For $S \subset \mathbb{R}^d$ the* integer point series $\widehat{\mathsf{G}}_S$ *is the formal Laurent series*

$$\widehat{\mathsf{G}}_S(t) \;:=\; \sum_{a \in S \cap \Lambda} t^a \;\in\; \widehat{\mathsf{L}} \; .$$

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,

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

Remark 3.5 (Warning) *When dealing with formal power series and rational series, one has to be very careful in order not to make a mistake. Therefore, we would like to give an example here (just for one variable) that justifies this caution: Consider the following expression of formal Laurent series*

$$\begin{aligned} \widehat{\mathsf{G}}_{\mathbb{R}}(t)\,(1-t) \;&=\; (\cdots + t^{-2} + t^{-1} + 1 + t + t^2 + \cdots)(1-t) \\ &=\; (\cdots + t^{-2} + t^{-1} + 1 + t + t^2 + \cdots) \\ &\qquad -\; (\cdots + t^{-1} + 1 + t + t^2 + t^3 \cdots) \\ &=\; 0 \end{aligned}$$

Clearly, we deduce

$$\widehat{\mathsf{G}}_{\mathbb{R}}(t) \;=\; \cdots + t^{-2} + t^{-1} + 1 + t + t^2 + \cdots \;=\; \frac{0}{1-t} \;=\; 0 \qquad (3.2)$$

However, this is wrong! The left side of the last equation is definitely not zero as a Laurent series. So, where is our mistake? In case the reader hasn't already found it, we will explain this apparent riddle in Remark 3.10.

Actually, not all Laurent series appear as a generating series for lattice points in polyhedra. The ones we will encounter have a nice additional structure that we will work out with the next definitions and theorems.

Definition 3.6 (*summable* Laurent series) *A Laurent series $\widehat{\mathsf{G}} \in \widehat{\mathsf{L}}$ is* summable *if there is a Laurent polynomial $g \in \mathsf{L}$ such that the series $g\widehat{\mathsf{G}}$ is a Laurent polynomial.*

Clearly all Laurent polynomials are summable. On the other hand, the series

$$1 + t^2 + t^3 + t^5 + t^7 + t^{11} + t^{13} + t^{17} + \ldots \;=\; 1 + \sum_{k \text{ prime}} t^k$$

cannot be summable. We will denote the set of all summable Laurent series by L^{sum}. We leave the proof of the following proposition to the reader as Exercise 3.4.

Exercise 3.4

Proposition 3.7 *L^{sum} is a L-submodule of $\widehat{\mathsf{L}}$.* □

Example 3.8 *Before we continue we want to work out some simple, but quite important examples of summable series coming from polyhedra.*

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

$$\widehat{\mathsf{G}}_{P_\infty}(t) \;=\; \sum_{a \in \mathbb{Z}_{\geq 0}} t^a = 1 + t + t^2 + t^3 + \cdots .$$

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

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

$$\widehat{\mathsf{G}}_C(t,s) \;=\; \sum_{a,b \in \mathbb{Z}_{\geq 0}} t^a s^b \;=\; \left(\sum_a t^a\right)\left(\sum_b s^b\right)$$

$$= \; 1 + t + s + t^2 + s^2 + ts + t^3 + \cdots .$$

Similar to the previous case we can use the polynomial

$$g(t,s) \;:=\; (1-t)(1-s)$$

to obtain

$$g(t,s)\cdot \widehat{\mathsf{G}}_C\,(t,s) \;=\; (1-t)\cdot\left(\sum_{a\in\mathbb{Z}_{\geq 0}} t^a\right)\cdot(1-s)\cdot\left(\sum_{b\in\mathbb{Z}_{\geq 0}} s^b\right) \;=\; 1.$$

Hence, $\widehat{\mathsf{G}}_C\,(t,s)$ is a summable series.

(3) Finally, let $V := \{e_1,\ldots,e_d\}$ and $C = \mathrm{cone}(V)$. In the same way, we see

$$\prod_{i=1}^{d}(1-t^{e_i})\cdot\sum_{z\in\mathbb{Z}^d_{\geq 0}} t^z \;=\; \prod_{i=1}^{d}(1-t^{e_i})\cdot\sum_{(n_1,\ldots,n_d)\in\mathbb{Z}^d_{\geq 0}} (t^{e_1})^{n_1}\cdots(t^{e_d})^{n_d} = 1 \tag{3.3}$$

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

Proposition 3.9 *There is a natural homomorphism from summable series to* rational functions

$$\Phi : \mathsf{L}^{\mathrm{sum}} \;\longrightarrow\; \mathsf{R} := \Bbbk(t_1,\ldots,t_d)\,,$$

mapping $\widehat{\mathsf{G}}$ to f/g if $g\widehat{\mathsf{G}} = f$ in $\widehat{\mathsf{L}}$. We will abbreviate this also by writing

$$\widehat{\mathsf{G}} \overset{\Phi}{\mapsto} \frac{f}{g}$$

The proof of this proposition is left as Exercise 3.5. Exercise 3.5

Remark 3.10 (Resolving the warning of Remark 3.5) *We can now explain where the mistake was. The equation (3.2) should be replaced by the following correct expression:*

$$\begin{aligned}\Phi(\widehat{\mathsf{G}}_{\mathbb{R}}\,(t)) \;&=\; \Phi(\cdots+t^{-2}+t^{-1}+1+t+t^2+\cdots)\\ &=\; \frac{0}{1-t} \;=\; 0.\end{aligned}$$

In other words, not the Laurent series is zero but only its associated rational function! While it is often very convenient to use the equality sign '=' between a summable Laurent series and a rational function (instead of using a cumbersome and non-standard notation such as Φ), one cannot stress enough that one must be aware that such an equality only holds on the level of rational functions and not on the level of Laurent series. We hope to make this point clear by using the $\overset{\Phi}{\longmapsto}$ symbol instead in these situations.

In particular, we see from the previous example that Φ is not an injective map. However, it clearly is for Laurent *polynomials* (check!). In other words, L is a submodule of $\mathsf{L}^{\mathrm{sum}}$, and $\Phi|_{\mathsf{L}}$ is the identity map. A more general criterion on injectivity is proven in Exercise 3.6. Exercise 3.6

Definition 3.11 (integer point *generating function*) *Suppose $S \subseteq \mathbb{R}^d$ is a set so that $\widehat{\mathsf{G}}_S(t)$ is summable. The* integer point generating function *of S is*

$$\mathsf{G}_S(t) \;:=\; \Phi(\widehat{\mathsf{G}}_S(t))\,.$$

If $S \subseteq \mathbb{R}^d$ is bounded, then we are allowed to identify (see also Exercise 3.6)

$$\mathsf{G}_S(t) \;=\; \sum_{a \in S \cap \mathbb{Z}^d} t^a\,.$$

In the one-dimensional example $P_\infty = [0,\infty)$ above we have already computed the image of the generating series in R, it is $\mathsf{G}_{P_\infty}(t) = \frac{1}{1-t}$.

We can now generalize this observation to rational simplicial cones (which will be generalized to half-open simplicial cones later). Let D be a simplicial rational cone in $\mathbb{R}^d$ with primitive ray generators $V := \{a_1, \ldots, a_d\}$. We recall the *fundamental parallelepiped* of V from Definition 2.42

$$\Pi(V) \;:=\; \left\{ \sum_{v \in V} \mu_v v \;:\; \mu_v \in [0,1) \text{ for } v \in V \right\}$$

We know from Corollary 2.44 that the fundamental parallelepipeds tile the space without overlap (strictly, there we talked about lattice bases, however, the same argument works for the generating set V).

Proposition 3.12 *In this notation, $\widehat{\mathsf{G}}_D(t)$ is summable with*

$$\mathsf{G}_D(t) \;=\; \frac{\sum_{y \in \Pi(D) \cap \mathbb{Z}^d} t^y}{\prod_{i=1}^d (1 - t^{a_i})}$$

Proof. Let $\mathbb{Z}_{\geq 0}V$ stand for the set of $\mathbb{Z}_{\geq 0}$-linear combinations of V. By replacing the Laurent monomial t^{e_i} by t^{a_i} in (3.3), we get

$$\prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{z \in \mathbb{Z}_{\geq 0}V} t^z \;=\; \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{(n_1,\ldots,n_d) \in \mathbb{Z}^d_{\geq 0}} (t^{a_1})^{n_1} \cdots (t^{a_d})^{n_d} \;=\; 1.$$

By Corollary 2.44 we get

$$\begin{aligned}
\prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{x \in D \cap \mathbb{Z}^d} t^x \;&=\; \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{y \in \Pi(D) \cap \mathbb{Z}^d} \sum_{z \in \mathbb{Z}_{\geq 0}V} t^{y+z} \\
&=\; \prod_{i=1}^d (1 - t^{a_i}) \cdot \sum_{z \in \mathbb{Z}_{\geq 0}V} t^z \cdot \sum_{y \in \Pi(D) \cap \mathbb{Z}^d} t^y \\
&=\; \sum_{y \in \Pi(D) \cap \mathbb{Z}^d} t^y\,.
\end{aligned}$$

□

Our integer point generating series contain a monomial for every lattice point in a set. If we have the series for two sets S, S', then we can obtain the series for the union $S \cup S'$ by adding the two series and subtracting all lattice points that we encoded in both series, *i.e.* the generating series for the lattice points in the intersection $S \cap S'$. This principle clearly extends to the union of any finite number of sets. We can compute the generating series from the generating series of the sets and all partial intersections if we keep track of the multiplicities a partial intersection appears in the total sum. This is called the *principle of inclusion-exclusion*. You will study this in more detail in Exercise 3.9. Triangulating a rational polyhedral cone into rational simplicial cones (see Section 2.2)) and using inclusion-exclusion (see also Figure 3.6) yields the following general result.

Corollary 3.13 *The integer point generating series of a rational polyhedral cone is summable.*

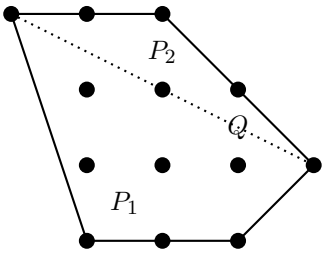


Fig. 3.6: Let Q be the dotted chord of the polygon and P_1, P_2 the two polygons obtained by cutting P along Q. Then $|P \cap \mathbb{Z}^2| = |P_1 \cap \mathbb{Z}^2| + |P_2 \cap \mathbb{Z}^2| - |Q \cap \mathbb{Z}^2|$.

3.3 Ehrhart's theorem

After these preparations, let us prove Ehrhart's theorem.

Theorem 3.14 (Ehrhart's Theorem) *The Ehrhart counting function given by $k \mapsto \mathrm{ehr}_P(k)$ for $k \in \mathbb{Z}_{\geq 1}$ extends to a polynomial function $t \mapsto \mathrm{ehr}_P(t)$ of degree d and leading coefficient $\mathrm{vol}(P)$.*

Definition 3.15 (Ehrhart *polynomial*) *For a polytope P the polynomial $\mathrm{ehr}_P(t)$ as in the previous theorem is the* Ehrhart polynomial *of P.*

We have already seen in § 2.1.2 that it is convenient to homogenize a polytope and work with the cone over P instead of P. Recall that we have defined $C(P)$ in (2.2) via

$$C(P) \;:=\; \mathrm{cone}\,(\{1\} \times P) \;\subseteq\; \mathbb{R}^{d+1}\,,$$

We usually write a vector $x \in \mathbb{R}^{d+1}$ with indices starting from 0 and use x_0 for the special coordinate. See Figure 3.7 for the cone over a triangle.

In our setting the especially convenient property of this representation of our polytope is the fact that we can recover all dilates of P from $C(P)$. More precisely, for any $k \geq 0$ we get 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 $\{k\} \times \mathbb{Z}^d$. Hence,

$$\widehat{\mathsf{G}}_{C(P)}\,(t, 1, \ldots, 1) \;=\; \sum_{k \geq 0} \left| kP \cap \mathbb{Z}^d \right| t^k \;=\; 1 + \sum_{k \geq 1} \mathrm{ehr}_P(t)\, t^k.$$

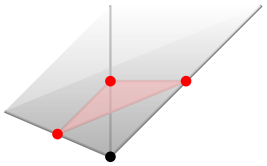


Fig. 3.7

As substituting variables clearly keeps summability, by Corollary 3.13 the following definitions make sense.

Definition 3.16 *Let P be a lattice d-polytope. The* Ehrhart series *of P is the summable formal Laurent series*

$$\widehat{\mathrm{Ehr}}_P(t) \;:=\; 1 + \sum_{k\geq 1} \mathrm{ehr}_P(t)\, t^k \;\in\; \Bbbk t$$

in one variable t. The corresponding rational function will be denoted

$$\mathrm{Ehr}_P(t) \;:=\; \Phi(\widehat{\mathrm{Ehr}}_P(t)) \;\in\; \Bbbk(t)\,.$$

To proceed we consider some well-known results on generating functions.

Lemma 3.17 *For $j \in \mathbb{Z}_{\geq 0}$,*

$$\sum_{\mathbb{Z}_{\geq 0}} \binom{k+d-j}{d} z^k \;\overset{\Phi}{\longmapsto}\; \frac{z^j}{(1-z)^{d+1}}\,.$$

Exercise 3.7

The proof will be given in Exercise 3.7.

Proposition 3.18 *Let $f, g : \mathbb{R} \to \mathbb{R}$ be such that*

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

Then $f(t)$ is a polynomial of degree at most d if and only if $g(z) = \sum_{k\in\mathbb{Z}_{\geq 0}} g_k z^k$ is a polynomial of degree at most d. In this case:

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

and the leading coefficient of f is $\frac{g(1)}{d!}$. In particular, f has degree d if and only if $g(1) \neq 0$.

Exercise 3.8

Proof. We define the polynomials $f_j(t) := \binom{t+d-j}{d}$ for $0 \leq j \leq d$. The set $\{f_o, \ldots, f_d\}$ is a basis of $\mathbb{R}[t]_{\leq d}$ (Exercise 3.8).

Let f be a polynomial of degree at most d. Then there are $g_0, \ldots, g_d$ 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 $\frac{1}{d!}\sum g_j$. We compute

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

For the converse direction, injectivity of Φ on polynomials implies $f(t) = \sum_{j=0}^{d} g_j \binom{t+d-j}{d}$. Now, we use again the basis property. □

Now, let us compute the Ehrhart generating function for lattice simplices.

Proposition 3.19 *Let S be a d-simplex. Then*

$$\mathrm{Ehr}_S(t) \;=\; \frac{h^\star(t)}{(1-t)^{d+1}}$$

where $h^\star$ is a polynomial of degree $\le d$. Further, for $h^\star(t) = \sum_{k=0}^{d} h_k^\star t^k$, we have

$$h_k^\star \;=\; \#(\Pi(C(S)) \cap \mathbb{Z}^{d+1} \cap \{x \mid x_0 = k\}) \in \mathbb{Z}_{\ge 0}.$$

In particular, $h_0^\star = 1$ and $h^\star(1) \neq 0$.

Proof. Let $\{a_0, a_1, \ldots, a_d\}$ be the vertex set of $\{1\} \times S$, with $a_i = (1, v_i)$ for $i = 0, \ldots, d$. Applying the substitution $(t_0, t_1, \ldots, t_d)$ by $(t_0, 1, \ldots, 1)$ to Proposition 3.12 we obtain that

$$\mathrm{Ehr}_S(t) \;=\; \frac{h^\star(t_0)}{(1-t_0)^{d+1}}$$

for the polynomial $h^\star(t_0) = \sum_{(y_0,y) \in \Pi(C(S)) \cap \mathbb{Z}^{d+1}} t_0^{y_0}$.

Let $(y_0, y) = \sum_{i=0}^{d} \lambda_i (1, v_i) \in \Pi(C(S)) \cap \mathbb{Z}^{d+1}$, so $0 \le \lambda_i < 1$ for $i = 0, 1, \ldots, d$. In particular, $y_0 < d+1$, so $y_0 \le d$. Moreover, $y_0 \ge 0$ with equality if and only if also $y = (0, 0, \ldots, 0)$. □

We have now collected all necessary tools and definitions to prove Ehrhart's Theorem (Theorem 3.14).

Proof (of Ehrhart's Theorem (Theorem 3.14)). Combining Proposition 3.19 with Proposition 3.18 we get that the Ehrhart counting function of an n-dimensional lattice simplex in $\mathbb{R}^d$ uniquely extends to a polynomial function of degree at most n.

For a general polytope P we triangulate it into maximal-dimensional simplices F_i and consider the triangulation of $C(P)$ into the associated simplicial cones $C(F_i)$. Then we apply inclusion-exclusion (e.g. Exercise 3.9). Finally, we use (3.1). □

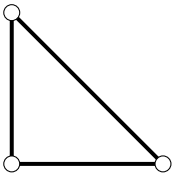


Fig. 3.8: The boundary complex of a triangle

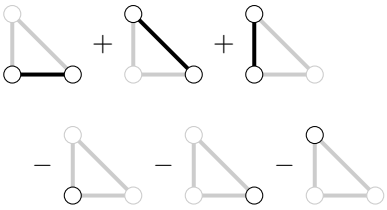


Fig. 3.9: Inclusion-Exculsion on the boundary complex

Exercise 3.9

Remark 3.20 *At this point it is intuitive, but wrong, to conclude*

$$\mathrm{ehr}_P(0) \;=\; \left|0P \cap \mathbb{Z}^d\right| \;=\; 1\,.$$

As we will see later in Corollary 3.35, $\mathrm{ehr}_P(0) = 1$ does hold if P is a polytope. But the interpretation as $\left|0P \cap \mathbb{Z}^d\right|$ is wrong as the following example shows.

We can count lattice points in dilations of complexes of lattice polytopes. The entire chain of arguments given carries over to this setting. We obtain a counting function which is the evaluation of a polynomial. Consider, for example, $\mathcal{C}$ to be the boundary of a standard triangle, see Figure 3.8. Then our counting polynomial turns out to be $\mathrm{ehr}_{\mathcal{C}}(k) = 3k$ with constant coefficient zero! See Figure 3.9. We will come back to this example in Remark 3.36.

Exercise 3.10

Exercise 3.11

Exercise 3.12

Exercise 3.13

Exercise 3.14

Exercise 3.15

Exercise 3.16

3.4 Stanley's theorem

3.4.1 Half-Open Decompositions of Cones

The goal of this chapter is to deduce more information about the Ehrhart polyonomial. For instance, as we have seen in Remark 3.20, we haven't even determined what its constant term is! And while we know that the numerator of the Ehrhart series of a d-dimensional lattice simplex is a polynomial of degree at most d whose coefficients are all nonnegative integers, we weren't able to conclude these strong statements for arbitrary polytopes from our naive inclusion-exclusion proof of Ehrhart's theorem. In fact, this is the content of Stanley's celebrated theorem, and in order to prove it we will need a more refined way of decomposing our polytopes into simplices. The goal is to have no overlap in order to avoid any overcounting (and thus subtraction). This is called *half-open decomposition* [9, 31]. There are various ways how to do this. We will use a generic reference point as an arbiter to decide which points belong to which cells. As above, the right setting to do this is to consider cones instead of polytopes.

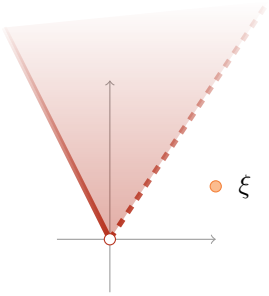


Fig. 3.10: Making a cone half open. The right face and the origin are not part of the half open cone.

Definition 3.21 (half-open decomposition) *Given a vector $\xi \in \mathbb{R}^d$, we define the* half-open cone C^ξ *with respect to $\xi \in \mathbb{R}^d$*

$$C^\xi := \{y \in C \,:\, y + \varepsilon\xi \in C \text{ for all } \varepsilon > 0 \text{ small enough}\} .$$

We say $\xi \in \mathbb{R}^d$ is generic *with respect to C (respectively, a triangulation $\mathcal{T}$ of C) if ξ is not in the linear hull of a $(d-1)$-dimensional face of C (respectively, any simplicial $(d-1)$-cone in $\mathcal{T}$).*

Exercise 3.17

C^ξ can also be described as precisely the set of elements in C that are not visible from ξ (Exercise 3.17). See Figure 3.10 for an example. Let us note some properties:

- If ξ is generic with respect to C, then

$$C^\xi = \{y \in C \,:\, y + \varepsilon\xi \in \operatorname{int} C \text{ for all } \varepsilon > 0 \text{ small enough}\} ,$$

- If $\xi \in C$, then $C^{\xi} = C$, and if ξ is additionally generic, then

$$C^{-\xi} \;=\; \operatorname{int} C\,.$$

- If $\xi \in C$ is generic with respect to a triangulation $\mathcal{T}$ of C, then it is also generic with respect to C. In this case, $\xi \in \operatorname{int} D \subset \operatorname{int} C$ for a unique $D \in \mathcal{T}[d]$.

Our first goal is to show that *making cones half-open* is compatible with decompositions.

Proposition 3.22 *Let $\mathcal{T}$ be a triangulation of the d-cone C, and let $\xi \in \mathbb{R}^d$ be generic with respect to $\mathcal{T}$. Then we have the following disjoint union:*

$$C^{\xi} \;=\; \bigsqcup_{D \in \mathcal{T}[d]} D^{\xi}.$$

where $\mathcal{T}[d]$ is the set of d-dimensional faces of the triangulation (see Definition 2.22).

In particular, if $\xi \in C$ is generic with respect to $\mathcal{T}$, then

$$C \;=\; \bigsqcup_{D \in \mathcal{T}[d]} D^{\xi} \qquad \text{and} \qquad \operatorname{int} C \;=\; \bigsqcup_{D \in \mathcal{T}[d]} D^{-\xi}.$$

A half-open decomposition in this way is illustrated in Figure 3.11, where this shows a slice through C containing ξ.

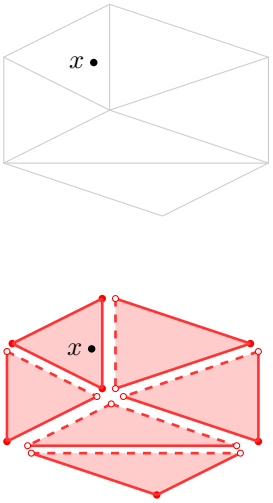


Fig. 3.11: A triangulation and its half open decomposition.

Proof. Let $y \in D^{\xi}$. Then for any $\varepsilon > 0$ small enough $y + \varepsilon\xi \in \operatorname{int}(D) \subset \operatorname{int}(C)$, so $y \in C^{\xi}$. Conversely, let $y \in C^{\xi}$, so $y + \varepsilon\xi \in \operatorname{int}(C)$ for any $\varepsilon > 0$ small enough. This implies that there exists a unique $D \in \mathcal{T}[d]$ so that $y + \varepsilon\xi \in \operatorname{int} D$ for small enough $\varepsilon > 0$. The uniqueness argument implies disjointness of the union on the right hand side. □

We remark that there is also a beautiful generalization of the previous result using indicator functions described in the book of Hemmecke et al. [18].

Let us now focus on simplicial d-cones $D \subset \mathbb{R}^d$.

Definition 3.23 *Let D be a simplicial d-cone in $\mathbb{R}^d$ and $V = \{v_1, \ldots, v_d\} \subset \mathbb{R}^d$ the primitive ray generators. Let us note that $\xi \in \mathbb{R}^d$ is generic with respect to D if and only if all coefficients λ_v in the unique representation $\xi = \sum \lambda_v v$ are non-zero. We define*

$$I_+(\xi) \;:=\; \{v \in V \;:\; \lambda_v > 0\} \quad \text{and} \quad I_-(\xi) \;:=\; \{v \in V \;:\; \lambda_v < 0\}\,.$$

Using this notation, let us note the following alternative description of a half-open simplicial cone (Exercise 3.18).

Exercise 3.18

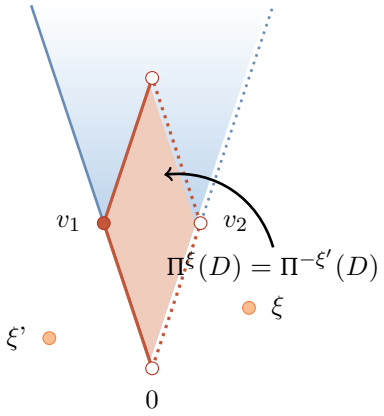


Fig. 3.12: Half open cone and fundamental parallelepiped for ξ and $-\xi'$. The dashed lines and the vertices with withe points are not part of the cone or fundamental parallelepiped.

Lemma 3.24 *Let $\xi \in \mathbb{R}^d$ be generic with respect to a simplicial d-cone D with primitive ray generators V. Then*

$$D^{\xi} = \left\{ \sum_{v \in V} \mu_v v \ : \ \begin{array}{l} \mu_v \geq 0 \text{ for } v \in I_+(\xi) \text{ and} \\ \mu_v > 0 \text{ for } v \in I_-(\xi) \end{array} \right\}.$$

We have seen in Corollary 2.44 how to translate $\mathbb{R}^d$ with translates of parallelepipeds. In the following, we will use this idea for the half-open cones D^{ξ}.

Definition 3.25 *Let D be a simplicial d-cone with primitive ray generators V. In case $\xi \in \mathbb{R}^d$ is generic, we define the* half-open parallelepiped *$\Pi^{\xi}(D)$ with respect to ξ as*

$$\Pi^{\xi}(D) := \left\{ \sum_{v \in V} \mu_v v \ : \ \begin{array}{l} \mu_v \in [0,1) \text{ for } v \in I_+(\xi) \text{ and} \\ \mu_v \in (0,1] \text{ for } v \in I_-(\xi) \end{array} \right\}$$

Note that $\Pi^{\xi}(D) \subset D^{\xi}$. See Figure 3.12 for an illustration. For x strictly in the interior of D we recover the usual half-open fundamental parallelepiped of D with generating set V.

The following result generalizes Corollary 2.44 and is left as Exercise 3.19.

Exercise 3.19

Lemma 3.26 *Let $V = \{v_1, \ldots, v_d\} \subset \mathbb{R}^d$ be linearly independent, and suppose $\xi \in \mathbb{R}^d$ is generic with respect to the simplicial cone $D := \operatorname{cone} V$. 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 $z \in \Pi^{\xi}(D)$.

We can further decompose each of the half-open simplicial cones into half-open boxes. Recall that $\mathbb{Z}_{\geq 0}V$ stands for the set of $\mathbb{Z}_{\geq 0}$-linear combinations of V.

Proposition 3.27 *Let V be the set of primitive ray generators of a simplicial d-cone $D \subset \mathbb{R}^d$, and let $\xi \in \mathbb{R}^d$ be generic with respect to D. Then we have the following disjoint union:*

$$D^{\xi} = \bigsqcup_{w \in \mathbb{Z}_{\geq 0}V} w + \Pi^{\xi}(D)$$

Proof. The fact that the translates by Λ-vectors are pairwise disjoint follows from the uniqueness in Lemma 3.26. From the existence part we see that $\mathbb{R}^d$ is covered by all Λ-translates of $\Pi^{\xi}(D)$. It remains to observe that for $w \in \Lambda$

$$D^{\xi} \cap \left(w + \Pi^{\xi}(D) \right) = \begin{cases} w + \Pi^{\xi}(D) & \text{for } w \in \mathbb{Z}_{\geq 0}V \\ \emptyset & \text{else,} \end{cases}$$

We leave the verification of this identity to the reader (Exercise 3.20). □

Exercise 3.20

Exercise 3.21

Exercise 3.22

3.4.2 The integer point generating function of half-open cones

Let us compute the integer point generating series and generating function for half-open cones.

Corollary 3.28 *Let $V = \{v_1, \dots, v_d\} \subset \mathbb{Z}^d$ be a linearly independent set of primitive vectors, let $D = \operatorname{cone} V$, and let $\xi \in \mathbb{R}^d$ be generic with respect to V. Then the integer point generating function of the half-open cone D^ξ is summable, and*

$$\mathsf{G}_{D^\xi}(t) \;=\; \frac{\mathsf{G}_{\Pi^\xi(D)}(t)}{(1-t^{v_1})(1-t^{v_2})\cdots(1-t^{v_d})}\,. \tag{3.4}$$

Using Proposition 3.27 the proof follows precisely along the lines of the proof of Proposition 3.12 (just replace Corollary 2.44 by Lemma 3.26). Together with Proposition 3.22 we get the following nice formula.

Corollary 3.29 *Let C be a rational cone in $\mathbb{R}^d$, let $\mathcal{T}$ be a triangulation of C into rational simplicial cones, and let $\xi \in C$ be generic. Then*

$$\widehat{\mathsf{G}}_C(t) \;=\; \sum_{S\in\mathcal{T}[d]} \widehat{\mathsf{G}}_{S^\xi}(t)\,, \;\text{ and }\; \widehat{\mathsf{G}}_{\operatorname{int} C}(t) \;=\; \sum_{S\in\mathcal{T}[d]} \widehat{\mathsf{G}}_{S^{-\xi}}(t)\,. \tag{3.5}$$

In particular, both series are summable, and (3.5) also holds on the level of rational functions.

Proof. Equation (3.5) is a translation of Proposition 3.22 into generating functions. By Corollary 3.28, all the summands are summable Laurent series. □

3.4.3 Stanley's theorem and the h^*-polynomial of a lattice polytope

Let us apply the previous results to cones over lattice polytopes.

Proposition 3.30 *Let $P \subset \mathbb{R}^d$ 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 $\xi \in C(P)$ be generic. Then $\widehat{\mathrm{Ehr}}_P(t)$ is summable with sum*

$$\mathrm{Ehr}_P(t) = \mathsf{G}_{C(P)}(t,\mathbf{1}) = \frac{\sum_{S\in\mathcal{T}[d+1]} \mathsf{G}_{\Pi^\xi(C(S))}(t,\mathbf{1})}{(1-t)^{d+1}}\,. \tag{3.6}$$

Exercise 3.23

Now, we are nearly done. It remains to show the following lemma, which we leave to the reader as Exercise 3.24.

Lemma 3.31 *Let $S \subset \mathbb{R}^d$ be a d-dimensional lattice simplex, and let $\xi \in \mathbb{R}^{d+1}$ be generic. We define*

$$h^\star_{i,C(S),\xi} \;:=\; \Big|\{y \in \Pi^\xi(C(S)) \cap \mathbb{Z}^{d+1} \;:\; y_0 = i\}\Big|$$

Then

(1) $\xi \in \operatorname{int} C(S)$ *if and only if* $h^\star_{0,C(S),\xi} = 1$. *Otherwise,* $h^\star_{0,C(S),\xi} = 0$.
(2) $-\xi \in \operatorname{int} C(S)$ *if and only if* $h^\star_{d+1,C(S),\xi} = 1$. *Otherwise,* $h^\star_{d+1,C(S),\xi} = 0$.

In particular, $\sum_{i=0}^{d+1} h^\star_{i,C(S),\xi} \geq 1$.

Exercise 3.24

Here is the main result of this chapter.

Theorem 3.32 (Stanley's Non-Negativity Theorem) *Let P be a d-dimensional lattice polytope. Then*

$$\operatorname{Ehr}_P(t) = \frac{h^\star_0 + h^\star_1 t + h^\star_2 t^2 + \cdots + h^\star_d t^d}{(1-t)^{d+1}},$$

$h^\star_1, \ldots, h^\star_d \geq 0$ *and* $h^\star_0 = 1$. *In particular,*

$$\operatorname{ehr}_P(t) = \binom{t+d}{d} + h^\star_1 \binom{t+d-1}{d} + \cdots + h^\star_{d-1}\binom{t+1}{d} + h^\star_d \binom{t}{d}, \tag{3.7}$$

Proof. We simply apply Proposition 3.30. In this notation

$$h^\star_0 + h^\star_1 t + h^\star_2 t^2 + \cdots + h^\star_d t^d \;=\; \sum_{S \in \mathcal{T}[d+1]} \mathsf{G}_{\Pi^\xi(C(S))}(t, \mathbf{1})$$

From Lemma 3.31 and $\xi \in \operatorname{int}(C(P))$ (as ξ is generic), we conclude that $h^\star_0 = 1$ and $h^\star_{d+1} = 0$. The last statement follows now from Proposition 3.18. □

Definition 3.33 ($h^\star$-polynomial) *The polynomial $h^\star$ that appears in the numerator of the rational generating function of the Ehrhart series of P is the* $h^\star$-polynomial *of P.*

Example 3.34 *Why do we consider the h^*-polynomial and don't stick to the original description? For this, let us consider the Reeve simplex from (1.1) for $m = 13$, i.e.*

$$R \;:=\; \operatorname{conv}(\mathbf{0}, e_1, e_2, e_1 + e_2 + 13e_3).$$

Then the Ehrhart polynomial is $1 - 1/6t + t^2 + 13/6t^3$, however, it's h^*-polynomial is $1 + 12t$. This shows why working with the h^*-polynomial is so much more convenient: the values are integers and they are nonnegative. As the proof shows, the reason is that they have a nice counting interpretation as the number of lattice points in half-open parallelepipeds.

Corollary 3.35 *Let P be a d-dimensional lattice polytope for $d \geq 0$. Then the following holds:*

(1) The constant term of the Ehrhart polynomial is 1 if P is non-empty.
(2) $h^\star(1) = \sum_{i=0}^{d} h^\star_i = d!\operatorname{vol}(P) = \operatorname{nvol}_{\mathbb{Z}^d}(P)$.

(3) $h_1^\star = \mathrm{ehr}_P(1) - d - 1 = |P \cap \mathbb{Z}^d| - d - 1$.

Proof. (1) This follows from Equation (3.7) by plugging in $t = 0$.
(2) This follows from Proposition 3.18 (or directly from Equation (3.7)).
(3) This follows from plugging in $t = 1$ into Equation (3.7). □

Remark 3.36 *We already raised the issue of the constant coefficient in Remark 3.20. Coming back to the boundary $\mathcal{C}$ of the standard triangle, there are two different half-open decompositions.*

The one on the left yields an $h^\star$-polynomial $1 + t + t^2$ while the one on the right yields $3t$. Which one is "correct"? Looking at the cone over $\mathcal{C}$, we see that the decomposition on the left contains the origin (once), while the one on the right does not. This explains the difference:

$$\frac{1+t+t^2}{(1-t)^2} \;=\; \frac{3t}{(1-t)^2} + 1\,.$$

We also see that there is exactly one choice for the multiplicity of the origin (in this case zero) so that the $h^\star$-polynomial has degree ≤ 1 which we need if we want the counting function to agree with the evaluation of a polynomial. We will identify this choice with the Euler characteristic in Remark 3.46 below.

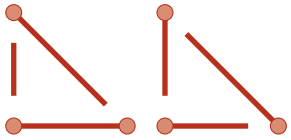


Fig. 3.13: Two half open decompositions of the boundary of a triangle.

Exercise 3.25

Finally, let us note the following theorem proved by Stanley in [53]. A completely different proof appears in (Beck, Sottile [9]). The reader can try to give a proof using the methods developed above in Exercise 3.26.

Theorem 3.37 (Stanley's Monotonicity Theorem) *Let P and Q be two lattice polytopes such that $P \subseteq Q$, $d = \dim Q$ and let $h_P^\star$ and $h_Q^\star$ be their $h^\star$-polynomials. Then $h_{P,i}^\star \leq h_{Q,i}^\star$ for all $0 \leq i \leq d$.*

Exercise 3.26

Proof. easy if $\dim P = \dim Q$, else, choose $\xi' \in \operatorname{relint} Q$ and wiggle to generic $\xi \in \operatorname{relint} P$. then half-open decomposition from C^ξ induces on Q the same half-open decomposition as ξ'. proof missing

Corollary 3.38 *For two lattice polytopes P and Q with $Q \subseteq P$ we have* $\deg Q \leq \deg P$. *In particular, any face of P has degree at most* $\deg P$. □

3.4.4 Where does the h^*-notation come from?

Example 3.39 *$h^\star$ of Δ_d. do half-open simplex as well Δ_d with k facets removed has $\binom{d+1-k}{j+1-k}$ many j-faces.*

The origin for the funky notation $h^\star$ is its close connection to the h-vector from enumerative combinatorics. Suppose $\mathcal{C}$ is a simplicial

complex with f_0 vertices, f_1 edges, and so forth. Then the combinatorial h-vector of $\mathcal{C}$ is defined by the implicit equation

$$f_j = \sum_{k=0}^{d} h_k \binom{d+1-k}{j+1-k} \tag{3.8}$$

This is, in fact, an invertible linear transformation between f-vector and h-vector. Its relation to the h^*-vector is given by the following result [11]:

Theorem 3.40 (Betke and McMullen 1985) *Let P be a lattice polytope with a triangulation $\mathcal{T}$. Let $h^\star$ be the $h^\star$-vector of P and h the h-vector of the triangulation. Then $h_k \leq h_k^\star$ for $0 \leq k \leq d$ with equality if and only if the triangulation is unimodular.*

Proof. The number of simplices with k facets removed in a half-open decomposition satisfies the h-vector equation. Such a simplex has a box point at height k, so it contributes one to $h_k^\star$. It contributes more if the simplex was not unimodular. □

3.5 Reciprocity

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

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

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

$$\mathsf{ehr}_L(-k) = (-k)(b-a) + 1 = -\left((-k)(b-a) - 1\right) = -\mathsf{ehr}_{\operatorname{int} L}(-k)\ .$$

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. As we only want to count the lattice points in the interior of the k-th dilate of the simplex, we can first consider all lattice points and then 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

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

Translating this by $\mathbf{1} \in \mathbb{R}^d$ gives the simplex defined by the inequalities

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

and this simplex clearly contains the same number of lattice points. We have computed this number in Proposition 3.2, so

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

We see that also the number of interior lattice 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

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

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

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

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

3.5.1 Stanley reciprocity for cones

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

Lemma 3.41 *Let $D \subset \mathbb{R}^d$ be a simplicial cone with primitive generators $V = \{v_1, \ldots, v_d\}$, and let $\xi \in \mathbb{R}^d$ be generic.*

Then the map

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

is a bijection.

Proof. Let $y \in \Pi^{\xi}(V)$, 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

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

which proves the claim. □

It follows from Corollary 3.29 (pick $-\xi \in \operatorname{int} C$) that $\widehat{\mathsf{G}}_{\operatorname{int} C}(t)$ is also a summable Laurent series.

Theorem 3.42 (Stanley's Reciprocity Theorem) *Let C be a d-dimensional polyhedral cone with rational generators. Then*

$$\mathsf{G}_C(t) = (-1)^d\, \mathsf{G}_{\operatorname{int} C}\left(\frac{1}{t}\right).$$

Proof. Let $\mathcal{T}$ by a triangulation of C and $\xi \in C$ 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 3.41 implies

$$\mathsf{G}_{\Pi^{\xi}(S)}(t) = \sum_{a \in \Pi^{\xi}(S) \cap \mathbb{Z}^d} t^a = \sum_{a \in \Pi^{-\xi}(S) \cap \mathbb{Z}^d} t^{s(S)-a} = t^{s(S)}\, \mathsf{G}_{\Pi^{-\xi}(S)}\left(\frac{1}{t}\right).$$

By Corollary 3.29 and Corollary 3.28 we can just sum up this equation over all maximal cones to obtain the desired result:

$$\begin{aligned} \mathsf{G}_C(t) &= \sum_{S \in \mathcal{T}[d]} \mathsf{G}_{S^{\xi}}(t) = \sum_{S \in \mathcal{T}[d]} \frac{\mathsf{G}_{\Pi^{\xi}(S)}(t)}{\prod_{v \in V(S)} (1 - t^v)} \\ &= \sum_{S \in \mathcal{T}[d]} \frac{t^{s(S)}\, \mathsf{G}_{\Pi^{-\xi}(S)}\left(\frac{1}{t}\right)}{\prod_{v \in V(S)} (1 - t^v)} \\ &= (-1)^d \sum_{S \in \mathcal{T}[d]} \frac{\mathsf{G}_{\Pi^{-\xi}(S)}\left(\frac{1}{t}\right)}{\prod_{v \in V(S)} (1 - \frac{1}{t^v})} \\ &= (-1)^d \sum_{S \in \mathcal{T}[d]} \mathsf{G}_{S^{-\xi}}\left(\frac{1}{t}\right) = (-1)^d\, \mathsf{G}_{\operatorname{int} C}\left(\frac{1}{t}\right). \end{aligned}$$ □

It is important to note that Stanley's theorem is clearly *wrong* on the level of Laurent series!

3.5.2 Ehrhart-Macdonald reciprocity for lattice polytopes

Finally, we can formalize our observation from the beginning of this section.

Theorem 3.43 (Ehrhart-Macdonald Reciprocity) *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional lattice polytope with Ehrhart polynomial $\mathrm{ehr}_P(t)$, and let $k \in \mathbb{Z}_{>0}$. Then*

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

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

Lemma 3.44 *Let f be a polynomial. Then*

$$\sum_{k\in\mathbb{Z}} f(k)t^k \overset{\Phi}{\longmapsto} 0.$$

Proof. It suffices to prove this for the basis $f_m := \binom{t+m}{m}$, $m \in \mathbb{Z}_{\geq 0}$, of $\mathbb{R}[t]$. So pick some m. Then

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

We compute the other sum:

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

□

Using this we can finally prove our reciprocity theorem.

Proof (Ehrhart-Macdonald Reciprocity (Theorem 3.43)). We make two computations:

$$\Phi\left(\sum_{k\geq 1} |\operatorname{int} kP \cap \mathbb{Z}^d|\, t^k\right) \;=\; \mathsf{G}_{\operatorname{int} C(P)}\,(t,1,\ldots,1)\,,$$

and, using Lemma 3.44 for the second equation,

$$\begin{aligned}\Phi\left((-1)^d \sum_{k\geq 1} \operatorname{ehr}_P(-k)\, t^k\right) \;&=\; \Phi\left((-1)^d \sum_{k\leq -1} \operatorname{ehr}_P(k)\, \frac{1}{t^k}\right)\\ &=\; \Phi\left((-1)^{d+1} \sum_{k\geq 0} \operatorname{ehr}_P(k)\, \frac{1}{t^k}\right)\\ &=\; (-1)^{d+1} \operatorname{Ehr}_P\left(\frac{1}{t}\right)\\ &=\; (-1)^{d+1} \mathsf{G}_{C(P)}\left(\frac{1}{t},1,\ldots,1\right)\end{aligned}$$

Theorem 3.42 and Exercise 3.6 imply

$$\sum_{k\geq 1} |\operatorname{int} kP \cap \mathbb{Z}^d|\, t^k \;=\; (-1)^d \sum_{k\geq 1} \operatorname{ehr}_P(-k)\, t^k\,.$$

Comparing coefficients of these two Laurent series gives the desired result. □

As an immediate application we can compute the Euler characteristic.

Proposition 3.45 (Euler-Characteristic) *Let $\mathcal{S}$ be a subdivision of the rational polytope $P \subset \mathbb{R}^d$ into rational polytopes. Then*

$$\sum_{\emptyset \neq F \in \mathcal{S}} (-1)^{\dim F} \;=\; 1\,.$$

The restriction to rational objects is an artefact of our method and is not necessary for the validity of the assertion.

Proof. Scaling P and $\mathcal{S}$ by a positive integer, we can assume that $\mathcal{S}$ contains only integral polytopes. Using the disjoint decomposition of P into the relative interiors of faces of $\mathcal{S}$ we see that for all $k \in \mathbb{Z}_{\geq 1}$

$$|kP \cap \mathbb{Z}^d| = \sum_{F \in \mathcal{S}} |\operatorname{relint} kF \cap \mathbb{Z}^d|\,.$$

Thus, by Ehrhart-Macdonald Reciprocity (Theorem 3.43), we have an equality

$$\operatorname{ehr}_P(t) = \sum_{F \in \mathcal{S}} (-1)^{\dim F} \operatorname{ehr}_F(-t)$$

of polynomials. Evaluating at $t = 0$ and applying Corollary 3.35(1) yields the desired identity. □

Remark 3.46 *The same argument shows that the constant coefficient of the counting polynomial of a complex of lattice polytopes equals the Euler-characteristic of the complex:* $\mathrm{ehr}_{\mathcal{C}}(0) = \chi(\mathcal{C})$. *This resolves the riddle raised in Remarks 3.20 and 3.36.*

3.6 Properties of the h^*-polynomial

As an immediate application of the results about counting lattice points that we have obtained so far we prove some facts about the relation between the geometry or combinatorics of lattice polytopes and their $h^\star$-vector. We will obtain more such results in the following chapters.

3.6.1 Degree and codegree of lattice polytopes

Let us give some more applications regarding the $h^\star$-polynomial.

Definition 3.47 (Degree and Codegree) *The* degree *of P is defined as*

$$\deg(P) := \max(k \in \mathbb{Z}_{\geq 0} \ : \ h_k^\star \neq 0).$$

The codegree *of P is defined as*

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

Ehrhart's theorem implies $0 \leq \deg(P) \leq d$, so $1 \leq \operatorname{codeg}(P) \leq d+1$. 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.

Corollary 3.48 *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 3.49 and the Ehrhart-Macdonald Reciprocity (Theorem 3.43). □

Exercise 3.27

Lemma 3.49 *Let p be a polynomial of degree d with rational generating function*

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

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

The proof is left as Exercise 3.28. Applied to our situation this has the following immediate consequence. Exercise 3.28

Corollary 3.50 *Let P be a lattice polytope. The highest non-zero coefficient $h^\star_{\deg(P)}$ of $h^\star$ equals the number of lattice points in* $\operatorname{int}((\operatorname{codeg} P)P)$. □

Finally, using reciprocity it is possible to compute the second highest coefficient of the Ehrhart polynomial. Exercise 3.29

Proposition 3.51 *Let P be a lattice polytope with Ehrhart polynomial $\operatorname{ehr}_P(t) = c_0 + c_1 t + c_2 t^2 + \cdots + c_d t^d$. Then c_{d-1} equals half of the normalized surface area of the boundary of P.*

You will prove this result in Exercise 3.29.

The following proposition is immediate from the fact that the sum of the coefficients of the $h^\star$-polynomial is the lattice volume and that the linear coefficient counts the number of lattice points minus $(d+1)$.

Proposition 3.52 *A d-dimensional lattice polytope P has lattice volume $\operatorname{nvol}_{\mathbb{Z}^d}(P) = |P \cap \mathbb{Z}^d| - d$ if and only if $\deg(P) \leq 1$.*

In particular, P has lattice $\operatorname{nvol}_{\mathbb{Z}^d}(P) = 1$ if and only if its degree $\deg(P)$ is 0. In this case P is the standard simplex. □

Proposition 3.53 *Let P be a lattice polytope of degree $\deg P \leq k$. Then $\operatorname{int} F \cap \mathbb{Z}^d = \varnothing$ for all faces F of P of dimension at least $k+1$.*

Proof. Assume there is a face F of P of dimension $k+1$ that contains a relative interior lattice point v. Then there are $k+2$ vertices $u_1, \ldots, u_{k+2}$ of F such that

$$v = \sum_{i=1}^{k+2} \lambda_i u_i \quad \sum_{i=1}^{k+1} \lambda_i = 1 \quad \text{and} \quad \lambda_i > 0 \quad \text{for} \quad 1 \leq i \leq k+2\,.$$

Further, we can find $d-1-k$ vertices $u_{k+3}, \ldots, u_{d+1}$ of P such that $u_1, \ldots, u_{d+1}$ is affinely independent. Consider

$$v' := \sum_{i=1}^{k+2} \frac{1}{d-k} \lambda_i u_i = \sum_{i=k+3}^{d+1} \frac{1}{d-k} u_i\,.$$

This is a point in int P. Now $(d-k)v'$ is integral, so $(d-k)$ int $P \cap \mathbb{Z}^d \neq \varnothing$. Thus, codeg $P \leq (d-k)$, or deg $P \geq k+1$.

In particular, this implies that for deg $P = 0$ only the vertices are lattice points, and for deg $P = 1$ the only lattice points that are not vertices are on the edges of P.

Let $X = \{x_1, \ldots\ x_k\} \subseteq P \cap \Lambda$ be a set of k lattice points that is not entirely contained in a proper face of P. Then $x := x_1 + \cdots + x_k$ is an interior lattice point of kP. This proves the next propisition.

Proposition 3.54 *Let P be a d-dimensional lattice polytope of degree at most s. Then any subset $W \subseteq P \cap \Lambda$ of at most $d-s$ lattice points is contained in a proper face of P.* □

We have viewed these propositions so far by first fixing the dimension. We could swap this view and fix the degree. Then the proposition for example tells us that in a polytope of dimension $d \geq s+2$ any two lattice points must be in a common face.

Let P be a d-dimensional lattice polytope in $\mathbb{R}^d$. We define the *lattice pyramid* over P as

$$\operatorname{Pyr}(P) \;:=\; \operatorname{conv}(P \times \{0\}, e_{d+1}) \subseteq \mathbb{R}^{d+1},$$

where $e_1, \ldots, e_{d+1}$ is the standard basis of $\mathbb{R}^{d+1}$. See Figure 3.14 for an example. In Exercise 3.30 you will show the following proposition.

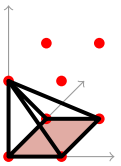


Fig. 3.14: A lattice pyramid over a unit square

Exercise 3.30

Exercise 3.31

Proposition 3.55 *For a lattice polytope P the lattice pyramid $\operatorname{Pyr}(P)$ of P has the same $h^\star$-polynomial as P.* □

Definition 3.56 (Lawrence Prism) *A* Lawrence prism *with heights*

$$h_1, \ldots, h_d \;\geq\; 0 \qquad \text{and} \qquad h_1 + \cdots + h_d \;\geq\; 2$$

is the polytope

$$\operatorname{Law}(h_1, \ldots, h_d) \;:=\; \operatorname{conv}\begin{pmatrix} \mathbf{0}, e_1, \ldots, e_{d-1}, \\ e_1 + h_1 e_d, \ldots, e_{d-1} + h_{d-1} e_d, h_d e_d \end{pmatrix}.$$

Let $\Delta_2^2 := 2\,\Delta_2$. This is sometimes called the *exceptional triangle*. We have the following proposition.

Proposition 3.57 *Let P be a k-fold lattice pyramid over a lawrence prism or the exceptional triangle for some $k \geq 0$. Then P has degree 1.*

Proof. The $h^\star$-polyonmial of the exceptional triangle is $1+3t$, which proves this part of the proposition. Further, lattice pyramids do not change the $h^\star$-polynomial, so we only have to check the proposition for lawrence prisms.

For a lawrence prism $L := \operatorname{Law}(h_1, \ldots, h_d)$ we have a natural lattice projection $\pi : L \to \Delta_{d-1}$. Hence, if kL has an interior lattice point, then so has $k\,\Delta_{d-1}$. Hence $k \geq d$, and $\deg L \leq 1$.

As by assumption $h_1 + \cdots + h_{d-1} \geq 2$ for L we can find d lattice points not contained in a common face of L, so dL contains an interior lattice point. Hence, $\deg L = 1$. □

Definition 3.58 *A lattice polytope P is* empty *if the vertices are the only lattice points in P.*

Proposition 3.59 *Let P be a lattice polytope of degree at most 1 such that no lattice point is strictly between two other lattice points. Then P is empty.*

Proof. By Corollary 3.38 any face of P has degree at most 1. Hence, no lattice point can be in the interior of a k-dimensional face for $k \geq 2$. □

Exercise 3.32

Proposition 3.60 *Let P be a lattice polytope of degree $\deg P = 1$ such that $\mathcal{V}(P) = P \cap \mathbb{Z}^d$. Then P is a simplex or there are $u_1, u_2, u_3, u_4 \in \mathcal{V}(P)$ such that*

$$u_1 + u_2 \;=\; u_3 + u_4\,.$$

Proof.

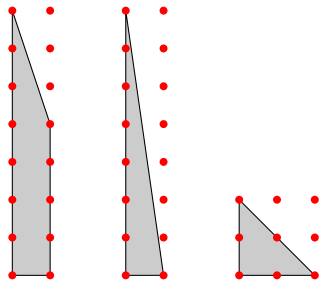


Fig. 3.15

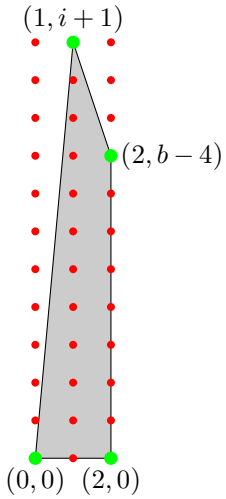


Fig. 3.16: Lattice polygons realizing $4 \leq b \leq 2i + 6$

3.6.2 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 Chapter 1 by proving Scott's inequlity (Theorem 1.10). Now, we just have to exploit the properties of the $h^\star$-polynomial.

Proposition 3.61 *A polynomial $h_2^\star t^2 + h_1^\star t + 1$ for $h_1^\star, h_2^\star \in \mathbb{Z}_{\geq 0}$ is the $h^\star$-polynomial of a lattice polygon if and only if*

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

See Exercise 3.34 for concrete examples.

Proof. Let us first show that these conditions are necessary. Note that $h_2^\star$ is the number of interior lattice points i, while $h_1^\star = b + i - 3$, where b is the number of boundary lattice points. Moreover, $\mathrm{vol}(P) = \mathrm{nvol}_{\mathbb{Z}^d}(P)/2 = (1 + h_1^\star + h_2^\star)/2$. Hence, Scott's theorem tells us that, if $i \geq 1$ and $P \ncong 3\Delta_2$, then $h_1^\star \leq 3h_2^\star + 3$. Finally, if $i \geq 1$, then $h_2^\star = i \leq h_1^\star = b + i - 3$, 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 3.15. In fact, it is not difficult to show that these In fact, as Exercise 3.33 shows these are *precisely* the lattice polygons without interior lattice points.

Let $i \geq 1$. The condition $h_2^\star \leq h_1^\star \leq 3h_2^\star + 3$ 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 3.16. □

All possible pairs $(h_1^\star, h_2^\star)$ are depicted in Figure 3.17. Let us now deduce all Ehrhart polynomials $c_2t^2 + c_1t + 1$ of lattice polygons. By Pick's Theorem 1.8 c_2 equals the area of P, and by Proposition 3.51, 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.

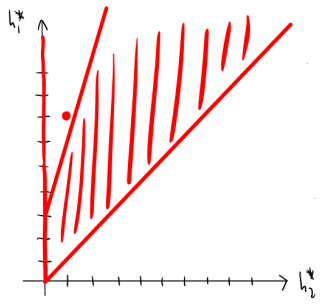


Fig. 3.17: $(h_2^\star, h_1^\star)$ of lattice polygons

Corollary 3.62 *A polynomial $c_2t^2 + c_1t + 1$ with $c_1, c_2 \in {}^1/_2\mathbb{Z}$ and $c_1 \geq {}^3/_2$ 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.

Exercise 3.34

3.6.3 Polytopes with Small Degree

3.7 Brion's theorem

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. Recall the tangent cone of F in P from Definition 2.29:

$$\mathsf{T}_F P := \{v \in \mathbb{R}^d \ : \ \exists\, w \in F,\ \varepsilon > 0 :\ w + \varepsilon(v - w) \in P\}\,.$$

The tangent cone is the common intersection of all supporting half-spaces at F. We have seen in Proposition 2.30 that the shifted cone $\mathsf{T}_F P - x$ for some $x \in F$ is dual to the normal cone of F.

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

Theorem 3.63 (Brianchon-Gram Theorem) *Let P be a rational d-polytope. Then*

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

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

The Brianchon-Gram identity is valid more generally on the level of indicator functions. In order to prove it, we need to study the complex of visible faces. We say that a face F of a polytope P is *visible* from a point $v \notin P$ if for some (equivalently every) $w \in \operatorname{relint} F$ the segment $\operatorname{conv}(v, w)$ intersects P only in w.

Lemma 3.64 *F is visible from v if and only if $v \notin \mathsf{T}_F P$.*

Proof. If $v \notin \mathsf{T}_F P$, there is a separating linear functional a:

$$\langle a, v \rangle \; > \; \max\langle a, \mathsf{T}_F P \rangle \geq \max\langle a, P \rangle .$$

But then, this strict inequality is true for every point of the form $(1-\lambda)v + \lambda w$ for $\lambda \in [0,1)$. So none of them can belong to P. That is, F is visible from v.

If, conversely, $v \in \mathsf{T}_F P$, we know that there are $w' \in F$ and an $\varepsilon > 0$ so that $v' := w' + \varepsilon(v - w') \in P$. Further, taking a smaller ε if necessary, we can assume that $w'' := w + \varepsilon(w - w') \in F$, because $w \in \operatorname{relint} F$. But then the point

$$\varepsilon^2 v + (1-\varepsilon^2)w \;=\; (1-\varepsilon)w'' + \varepsilon v'$$

belongs to both $\operatorname{conv}(v, w)$ and to P, and F is not visible from v. □

Corollary 3.65 *If P is a rational polytope and $v \notin P$ a rational point, then the set* $\operatorname{visible}_P(v)$ *of faces of P visible from v is a polyhedral complex, and as such is isomorphic to a rational subdivision of a rational polytope.*

Proof. From the definition of visibility we see that $G \preceq F \in \operatorname{visible}_P(v)$ implies $G \in \operatorname{visible}_P(v)$. So $\operatorname{visible}_P(v)$ is a subcomplex of the boundary of P.

Let H be a rational hyperplane separating v from P, and consider the rational polytope $Q := H \cap \operatorname{conv}(P \cup \{v\})$. Then

$$\big\{H \cap \operatorname{conv}(F \cup \{v\}) \;:\; F \in \operatorname{visible}_P(v)\big\}$$

is a subdivision of Q which is combinatorially isomorphic to $\operatorname{visible}_P(v)$. □

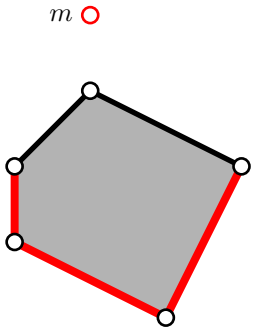


Fig. 3.18: $m \notin P$. The complex S is drawn in red.

Proof (of the Brianchon-Gram Theorem (Theorem 3.63)). 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. We have to distinguish the two cases $m \in P$ and $m \notin P$.

(1) $m \in P$: Then $m \in \mathsf{T}_F P$ for every non-empty face F of P. Hence, the coefficient of t^m on the right hand side is

$$\sum_{\emptyset \neq F \preceq P} (-1)^{\dim F} = 1 ,$$

using Euler's relation.

(2) $m \notin P$: See Figure 3.18. By Lemma 3.64, the coefficient of t^m on the right hand side is

$$\sum_{\emptyset \neq F \preceq P} (-1)^{\dim F} - \sum_{\emptyset \neq F \in \text{visible}_P(m)} (-1)^{\dim F} = 1 - 1 = 0\,,$$

using the fact that the Euler-characteristic of $\text{visible}_P(m)$ is 1 by Corollary 3.65 and Remark 3.46.

□

Now recall the map $\Phi : \widehat{\mathsf{L}} \longrightarrow \mathsf{R}$ that we introduced in Section 3.2. 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

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

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^-. The series are

$$\begin{aligned}
\widehat{\mathsf{G}}_{C^+}(t) &= \sum_{k \geq 0} t^k \\
\widehat{\mathsf{G}}_{C^-}(t) &= \sum_{k \leq 3} t^k = t^3 \sum_{k \leq 0} t^k = t^3 \sum_{k \geq 0} t^{-k}\,,
\end{aligned}$$

so we obtain the functions

$$\begin{aligned}
\mathsf{G}_{C^+}(t) &= \Phi(\widehat{\mathsf{G}}_{C^+}(t)) = \frac{1}{1-t} \\
\mathsf{G}_{C^-}(t) &= \Phi(\widehat{\mathsf{G}}_{C^-}(t)) = t^3 \frac{1}{1-\frac{1}{t}} = \frac{-t^4}{1-t}
\end{aligned}$$

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

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

We observe that

$$\mathsf{G}_P(t) = \mathsf{G}_{C^+}(t) + \mathsf{G}_{C^-}(t)\,.$$

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

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

This can only hold if $\Phi(\widehat{\mathsf{G}}_{\mathbb{R}}(t)) = 0$, 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.

Proposition 3.66 *Let $C \subseteq \mathbb{R}^d$ be a polyhedral cone with integer point series $\widehat{\mathsf{G}}_C(t)$. If* $\operatorname{lineal} C \neq \{0\}$ *then* $\Phi(\widehat{\mathsf{G}}_C) = 0$.

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

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

Applying the map Φ gives

$$t^v \Phi(\widehat{\mathsf{G}}_C(t)) = \Phi(\widehat{\mathsf{G}}_C(t)) \qquad \Longleftrightarrow \qquad (1-t^v)\Phi(\widehat{\mathsf{G}}_C(t)) = 0\,.$$

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

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

Theorem 3.67 (Brion's Theorem) *Let P be a rational d-polytope. Then*

$$\mathsf{G}_P(t) = \sum_{v \text{ vertex of } P} \mathsf{G}_{\mathsf{T}_v P}(t) \ .$$

Proof. Apply the map Φ to both sides of the Brianchon-Gram Identity of Brianchon-Gram Theorem (Theorem 3.63). The only non-pointed tangent cones are those originating from a vertex of P, so by Proposition 3.66 only the contributions of the vertices are non-zero on the right hand side. □

Exercise 3.35

Exercise 3.36

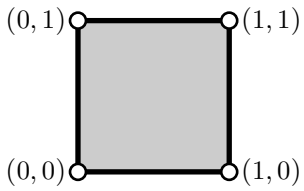


Fig. 3.19

Example 3.68 *Let P be the $= 0/1$-square in $\mathbb{R}^2$. See Figure 3.19. Then*

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

So $\mathsf{G}_P(1,1) = 1+1+1+1 = 4$.

The theorem provides us with a general method to explicitly compute the function $\mathsf{G}_P(t)$. We have seen in Corollary 3.28 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.

3.8 Problems

3.1. Determine a formula for the volume of a 3-dimensional lattice polytope using the number of lattice points in the k-multiple for $k = 1, 2$ and 3.

included on page 63

included on page 63

3.2. Determine a formular for the volume of a 3-dimensional lattice polytope using $|P \cap \mathbb{Z}^3|$, $|\operatorname{int}(P) \cap \mathbb{Z}^3|$, $|2P \cap \mathbb{Z}^3|$.
The reader is also invited to find many more such formulas by using different values of the Ehrhart polynomial.

included on page 64

3.3. Show

$$\sum_{k=0}^{\infty} \binom{k+d}{d} x^k = \frac{1}{(1-x)^{d+1}}.$$

(Why is the equality sign justified here?)

included on page 68

3.4. The goal of this exercise is to give a proof of Proposition 3.7.

(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 $g, h \in L^{\mathsf{sum}}$ 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 $\Phi(f + g) = \Phi(f) + \Phi(g)$.

included on page 69

3.5. Prove that there is a natural homomorphism from summable series to rational functions

$$\Phi : \widehat{\mathsf{L}} \longrightarrow \mathsf{R} := \Bbbk(x_1, \ldots, x_d),$$

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

included on page 69

3.6. Let S, S' be subsets of the a (possibly translated) pointed cone in $\mathbb{R}^d$. Then $\mathsf{G}_S(t) = \mathsf{G}_{S'}(t)$ implies $\widehat{\mathsf{G}}_S(t) = \widehat{\mathsf{G}}_{S'}(t)$.

included on page 72

3.7. Prove Lemma 3.17.
Hint: do $j = 0$ first

included on page 72

3.8. Zeige dass $\binom{t+d-j}{d}$ mit $j = 0, \ldots, d$ eine Basis des Vektorraums der Polynome vom Grad $\leq d$ ist.

included on page 73

3.9. Let subsets $S_1, \ldots, S_m$ of $\mathbb{R}^d$ be given. Then

$$\widehat{\mathsf{G}}_{\bigcup_{i\in[m]} S_i}(t) = \sum_{\emptyset \neq I \subseteq [m]} (-1)^{|I|+1} \widehat{\mathsf{G}}_{\bigcap_{i\in I} S_i}(t).$$

Remark: This is just the usual inclusion-exclusion formula for sets.

included on p

3.10. Determine the Ehrhart polynomial of the reeve tetrahedron defined in (1.1) for $m \in \mathbb{Z}_{\geq 1}$.
What do you observe for $m = 20$?

included on page 74

3.11. Let P be a lattice polytope with Ehrhart polynomial $\mathsf{ehr}_P(t)$. Compute the Ehrhart polynomial of the bipyramid over P.

included on page 74

3.12. Compute the Ehrhart polynomial of the cross polytope.

included on page 74

3.13. Let P be a d-dimensional lattice polytope with Ehrhart polynomial $\sum_{k=0}^{d} c_k t^k$. Show that

$$c_{d-1} = \frac{1}{2}\operatorname{vol}(\partial P).$$

Here, $\operatorname{vol}(\partial P)$ denotes the surface area of P, namely,

$$\operatorname{vol}(\partial P) := \sum_{F \in \mathsf{F}(P)} \operatorname{vol}(F),$$

where $\mathsf{F}(P)$ is the set of facets of P and $\operatorname{vol}(F)$ denotes the (non-normalized) volume with respect to the lattice $\operatorname{aff}(F) \cap \mathbb{Z}^d$. For instance, note that $\operatorname{vol}(\operatorname{conv}((1,0),(0,1)))$ equals 1 and not $\sqrt{2}$. Hence,

$$\operatorname{vol}(\partial \operatorname{conv}((1,0),(0,1),(-1,0),(0,-1))) = 4\,.$$

included on page 74

3.14. 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

$$|\mathbb{Z}^k \cap \operatorname{relint}(t\Delta)| = \binom{t-1}{k}\,.$$

(2) Suppose P admits a unimodular triangulation $\mathcal{T}$ with $f_0(\mathcal{T})$ vertices, $f_1(\mathcal{T})$ edges, $\ldots$, $f_d(\mathcal{T})$ d-simplices. Show that

$$\mathsf{ehr}_P(t) = \sum_{k=0}^{d} f_k(\mathcal{T}) \binom{t-1}{k}\,.$$

(3) Conclude that any two unimodular triangulations have the same f-vector $(f_0, \ldots, f_d)$.

included on page 74

3.15. Prove that the coefficients of the Ehrhart polynomial of a d-dimensional lattice polytope are in $\mathbb{Z}/d!$.

3.16. For integers p,q with $\gcd(p,q) = 1$ define the tetrahedron

$$\Delta_{pq} = \operatorname{conv} \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & p \\ 0 & 0 & 0 & q \end{bmatrix} .$$

(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 $h^\star$-polynomial of Δ_{pq}.
(3) For which parameters are Δ_{pq} and $\Delta_{p'q'}$ unimodularly equivalent?

included on page 74

3.17. Let $\xi \in \mathbb{R}^d$ and C a d-cone. Then

$$C^\xi \;=\; \{y \in C \;:\; y_\varepsilon \in C \text{ for all } \varepsilon > 0 \text{ small enough}\},$$

where $y_\varepsilon := (1-\varepsilon)y + \varepsilon\xi$.

included on page 75

3.18. Prove Lemma 3.24.

included on page 76

3.19. Prove Lemma 3.26.

included on page 76

3.20. Check carefully and rigorously the last identity in the proof of Proposition 3.27.

included on page 76

3.21. Show directly that $C \backslash C[x)$ is a union of faces of C.

included on page 76

3.22. Let $\mathcal{T}$ be a triangulation of a full-dimensional cone C. Show that there is always a generic element $\xi \in \operatorname{int}(C)$.

included on page 77

3.23. Consider the polygon with vertices $(0,0),(1,0),(0,2),(2,4)$. Compute, using a half-open decomposition $\mathsf{G}_{C(P)}(t_1,t_2,t_3)$.

included on page 78

3.24. Prove Lemma 3.31.

included on page 79

3.25. 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 $w : \mathcal{V}(Q) \to \mathbb{R}$, leading to linear functions l_σ on simplices σ of the triangulation. Now, choose generic values of w on $\mathcal{V}(P) \backslash \mathcal{V}(Q)$ such that $w(v) > l_\sigma(v)$ for all σ in the triangulation of Q and vertices $v \in \mathcal{V}(P) \backslash \mathcal{V}(Q)$.

included on p

3.26. Let Q, P be lattice polytopes with $Q \subseteq P$. Show Stanley's Monotonicity Theorem (Theorem 3.37)

$$h_Q^* \leq h_P^* \text{ coefficientwise.}$$

Hint: Choose a triangulation as in Exercise 3.25.

.

included on page 85

3.27. Give a direct geometric proof using Carathéodory's Theorem (Theorem 2.4) that $\operatorname{codeg}(P) \leq d+1$ for a d-dimensional lattice polytope.

included on page 86

3.28. Prove Lemma 3.49.

included on page 86

3.29. Prove Proposition 3.51.

included on page 87

3.30. Show that $h^\star_{\mathrm{Pyr}(P)} = h^\star_P$ for a lattice polytope P.

included on page 87

3.31. Let $m \in \mathbb{Z}_{\geq 1}$. Use Exercise 3.30 to show that

$$f_m(k) \;:=\; \sum_{j=1}^{k} j^m$$

is a polynomial in k. What is its degree and leading coefficient?

included on page 88

3.32. 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 :-)

included on page 89

3.33. 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 $\operatorname{conv}((0,0),(a,0),(0,1),(0,b))$ for some $a, b \geq 0$.

included on page 89

3.34. Are
(1) $1 + 8t + t^2$
(2) $1 + 9t + t^2$
(3) $1 + 2t + 2t^2$
(4) $1 + t + 2t^2$

h^*-polynomials of a lattice polygon?

3.35. Compute the Ehrhart generating function of $P = [0,1]^2$ using the Brion's Theorem (Theorem 3.67).

3.36. Apply Brion's identity to

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

and verify that both rational functions coincide (you may want to use a computer for this).

Geometry of Numbers 4

Contents

Geometry of numbers deals with the relation between two objects: convex bodies on the one hand, and lattices one 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 Corollary 4.3, 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

Minkowski's two theorems are the basis of this whole branch of discrete mathematics. Both essentially tell us something about generators of the lattice and prove that we can find such generators with a bounded Euclidean length. The theorems, of which we will only prove the first, are however not constructive. We will remedy this in Chapter 6. Throughout, $\Lambda \subset \mathbb{R}^d$ is a lattice of rank d (the reader may think of $\mathbb{Z}^d$).

A set $K \subseteq \mathbb{R}^d$ is *centrally symmetric* if $x \in K$ implies $-x \in K$.

Definition 4.1 *A subset $K \subseteq \mathbb{R}^n$ is a* convex body *if K is bounded and convex. The set of convex bodies in $\mathbb{R}^d$ is deneted by $\mathcal{C}$. The subset of* centrally symmetric *convex bodies is $\mathcal{C}_0$.*

Note that the definition of the term *convex body* varies in the literature. The following theorem establishes a fundamental correspondence between lattice points in a centrally symmetric convex body and its volume.

Theorem 4.2 (van Der Corput, 1935) *Let $K \subset \mathbb{R}^d$ be a centrally symmetric convex set. Then*

$$\operatorname{vol}(K) \leq 2^d \left|K \cap \Lambda\right| \det \Lambda\,.$$

If K is compact, then the inequality is strict.

Minkowski's First Theorem, that he proved almost forty years earlier, is now a direct corollary of this. This result is the fundamental theorem in this area and it is considered to be the starting point of the theory.

Corollary 4.3 (Minkowski's First Theorem, 1898) *Let $K \subseteq \mathbb{R}^d$ be convex and centrally-symmetric with $\operatorname{vol} K > 2^d \det \Lambda$.*

Then there exists $a \neq 0$ in $K \cap \Lambda$. If K is also compact, then it suffices to assume $\operatorname{vol} K \geq 2^d \det \Lambda$. □

Exercise 4.1

Exercise 4.2

For the proof of these results we need the following lemma, which uses a beautiful pidgeonhole-style argument to prove that the intersection of a sufficiently large set with some affine translate of the lattice is large.

Lemma 4.4 (Generalized Blichfeldt's Theorem, 1914) *Let $\mathcal{S} \subseteq \mathbb{R}^d$ be a (Lebesgue measurable) set with $\operatorname{vol}(\mathcal{S}) > m \det(\Lambda)$ for a positive integer m. Then there exist $m+1$ pairwise distinct points $p_1, \ldots, p_{m+1} \in \mathcal{S}$ such that $p_i - p_j \in \Lambda$ for all i, j.*

Proof. By considering a sufficiently large subset, we may assume that $\mathcal{S}$ is bounded. Choose a closed fundamental parallelepiped (see Definition 2.42) $\overline{\Pi} := \overline{\Pi}(\Lambda)$ of Λ. Note that $\det\Lambda = \operatorname{vol}\overline{\Pi}$. For any $x \in \Lambda$ let

$$\mathcal{S}_x := \{y \in \overline{\Pi} \mid x + y \in \mathcal{S}\} = \overline{\Pi} \cap (\mathcal{S} - x)$$

Note that $\mathcal{S}_x \neq \emptyset$ if and only if $x \in (\mathcal{S} - \overline{\Pi}) \cap \Lambda$. As $\mathcal{S} - \overline{\Pi}$ is bounded, Exercise 2.14 implies that there are only finitely many $x \in \Lambda$ with $\mathcal{S}_x \neq \emptyset$. This implies that the function

$$f \;:=\; \sum_{x\in\Lambda} \mathrm{id}_x\,,$$

where id_x is the indicator function on $\mathcal{S}_x$ (i.e., it evaluates to 1 on $\mathcal{S}_x$ and 0 elsewhere), is well-defined. Using that fundamental parallelepiped tile the space (Corollary 2.44) we compute

$$\begin{aligned}\int_{\overline{\Pi}} f\,dx \;&=\; \sum_{x\in\Lambda}\int_{\overline{\Pi}} \mathrm{id}_x\;dx \;=\; \sum_{x\in\Lambda}\operatorname{vol}(\mathcal{S}_x)\\ &=\; \sum_{x\in\Lambda}\operatorname{vol}(\overline{\Pi}\cap(\mathcal{S}-x)) \;=\; \sum_{x\in\Lambda}\operatorname{vol}(\mathcal{S}\cap(x+\overline{\Pi})) = \operatorname{vol}(\mathcal{S})\\ &>\; m\det\Lambda \;=\; \int_{\overline{\Pi}} m\,dx\end{aligned}$$

Hence there is $y \in \overline{\Pi}$ with $f(y) > m$. Since f only evaluates to integers, we get $f(y) \geq m+1$. In particular, there exist $x_1, \ldots, x_{m+1} \in \Lambda$ such that $y \in \mathcal{S}_{x_1} \cap \cdots \cap \mathcal{S}_{x_{m+1}}$. Therefore, defining $p_i := y + x_i \in \mathcal{S}$ for $i = 1, \ldots, m+1$ yields $m+1$ points which have the desired properties. □

Now, we can easily prove van der Corput's Theorem (Theorem 4.2).

Proof (of van der Corput's Theorem (Theorem 4.2)). We will give an indirect proof. Let us assume that

$$\operatorname{vol}(K) \;>\; m2^d\det(\Lambda)$$

for a positive integer m. Our goal is to show that there exist m distinct pairs of *non-zero* lattice points $\pm x_1, \ldots, \pm x_m$ in K. Together with the origin this will give $2m+1$ lattice points in K.

Let $\boldsymbol{T} := \frac{1}{2}K$. Then $\operatorname{vol}\boldsymbol{T} = \frac{\operatorname{vol}K}{2^d} > m\det\Lambda$. Hence, by Generalized Blichfeldt's theorem (Lemma 4.4), there are $m+1$ distinct points $p_1, \ldots, p_{m+1} \in \boldsymbol{T}$ such that $p_i - p_j \in \Lambda$ for all i, j. Choose $x_i := p_i - p_{m+1}$ for $i = 1, \ldots, m$ as the desired lattice points. Note that $x_i = p_i + (-p_{m+1}) \in \boldsymbol{T} + \boldsymbol{T} = K$.

Let K be compact and $\operatorname{vol}K = 2^d\det\Lambda$. Since K is compact, for each $x \in 2K\backslash K$ there exists $0 < \epsilon_x < 1$ such that $x \notin (1+\epsilon_x)K$.

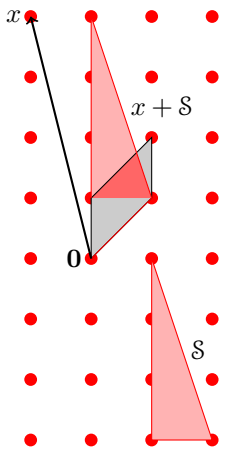
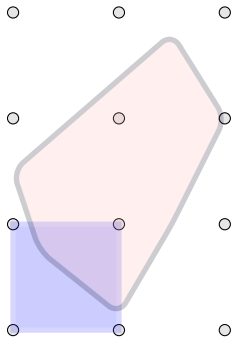
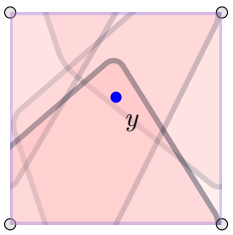


Fig. 4.1



(a) The set $\mathcal{S}$ and the fundamental parallelepiped $\overline{\Pi}$



(b) And the shifted intersections with the fundamental parallelepiped

Fig. 4.2: Illustrating the proof of Generalized Blichfeldt's theorem (Lemma 4.4)

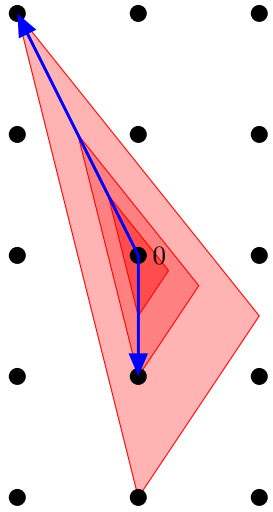


Fig. 4.3: A triangle in the plane together with two scaled copies with scaling factors λ_1 and λ_2.

Boundedness of $2K$ implies that $2K$ has only finitely many lattice points. Let ϵ be the minimum over ϵ_x for all $x \in (2K \setminus K) \cap \Lambda$. This choice ensures that $(1+\epsilon)K$ and K have the same set of lattice points (note that $\alpha K \subseteq \alpha' K$ for $0 < \alpha < \alpha'$ as K is centrally-symmetric and convex). Since $\mathrm{vol}((1+\epsilon)K) > 2^d \det \Lambda$, the result follows. □

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 6.4 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. [24, 49, 50]. Although we cannot easily compute a shortest vector of a lattice, Minkowski's Theorem at least allows us to estimate the length of such a vector.

Proposition 4.5 *Let $\Lambda \subset \mathbb{R}^d$ be a lattice. Then there is a vector $v \in \Lambda \setminus \{\mathbf{0}\}$ such that*

$$\|v\| \leq \sqrt{d} (\det \Lambda)^{1/d} .$$

Proof. Let $\mathrm{V_d}$ be the volume of the d-dimensional unit ball $\mathcal{B}_\mathrm{d}$ and choose

$$\alpha \;:=\; 2 \left(\frac{\det \Lambda}{\mathrm{V_d}} \right)^{1/d} . \tag{4.1}$$

Then

$$\mathrm{vol}(\alpha\, \mathcal{B}_\mathrm{d}) \;=\; \alpha^d \mathrm{V_d} \;\geq\; 2^d \det \Lambda .$$

By Minkowski's First Theorem (Corollary 4.3) there is a non-zero lattice point v in $\alpha\, \mathcal{B}_\mathrm{d}$, hence, of length at most α. We need to estimate the size of α.

The volume of the unit ball is

$$\mathrm{V_d} \;:=\; \frac{\pi^{\lfloor d/2 \rfloor} 2^{\lceil d/2 \rceil}}{\prod_{0 \leq i < d/2} (d-2i)} \;\approx\; \left(\frac{2\pi e}{d} \right)^{d/2} \;\geq\; \left(\frac{4}{d} \right)^{d/2} ,$$

where the first approximation follows from Stirling's formula $d! \approx \sqrt{2\pi d} \frac{d}{e}^d$ adn the second from $2\pi e \geq 4$. Inserting this into (4.1) proves the result. □

Exercise 4.3

Definition 4.6 (Successive Minima) *Let $K \in \mathcal{C}_0$. For $1 \leq k \leq d$ we define the k-th* successive minimum of K *to be the number*

$$\lambda_k \;:=\; \lambda_k(K) \;:=\; \inf_{\lambda > 0} \{ \dim \mathrm{lin}(\lambda K \cap \Lambda) \;\geq\; k \}.$$

For $K = \mathcal{B}_\mathrm{d}$ we call $\lambda_k := \lambda_k(\mathcal{B}_\mathrm{d})$ the k-th successive minimum of the lattice Λ. *See also Figure 4.3.*

Then

$$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_d \,.$$

Note that $\lambda_1 > 0$ as Λ is discrete. The following corollary is equivalent to Minkowski's First Theorem (Corollary 4.3).

Corollary 4.7 *Let $K \in \mathcal{C}_0$. Then $\lambda_1^d \operatorname{vol} K \;\leq\; 2^d \det \Lambda$.*

Note that a compact centrally symmetric convex body defines a norm $\|.\|_K$ on $\mathbb{R}^d$ via

$$\|x\|_K \;:=\; \max_{\mu} \left(\mu x \in K \right) ,$$

and any norm is of this form.

Proposition 4.8 *Let $K \in \mathcal{C}_0$ be compact and $\Lambda \subseteq \mathbb{R}^d$ be a lattice with successive minima $\lambda_1, \ldots, \lambda_d$ with respect to K. Then there is a (vector space) basis $v_1, \ldots, v_d \in \Lambda$ such that $\|v_i\|_K = \lambda_i$ for $1 \leq i \leq d$.*

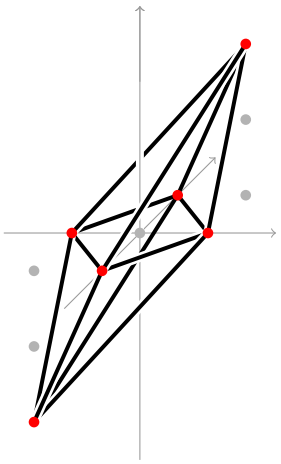
Proof. Pick some index $1 \leq j \leq d$. By definition of λ_j there is a sequence $(w_i)_{i \geq 1} \subseteq \Lambda$ of lattice vectors such that $\lim_{i\to\infty} \|w_i\| = \lambda_j$. For sufficiently large i we have $w_i \in 2K$. K is compact, so we can find a convergent sub-sequence w_{i_k}, converging to some vector w. We need to prove that $w \in \Lambda$. By definition, $\lim_{k\to\infty} \|w - w_{i_k}\|_K = 0$, so for sufficiently large k

$$\|w - w_{i_k}\|_K \;<\; \lambda_1/2 \,.$$

The triangle inequality then implies for sufficiently large k, l

$$\|w_{i_k} - w_{i_l}\|_K \;\leq\; \|w - w_{i_k}\|_K + \|w - w_{i_l}\|_K < \lambda_1 \,.$$

But $w_{i_l} - w_{i_l}$ is a lattice vector, so $w_{i_k} = w_{i_l}$ for sufficiently large k, l. Hence, $w_{i_k} = w$ for sufficiently large k, and w is a lattice vector. □



Remark 4.9 *The vectors found in the previous proposition need not be a basis of the lattice Λ. For an example, the lattice polytope*

$$P \;:=\; \operatorname{conv}\left(\pm e_1, \pm e_2, \pm(e_1 + e_2 + 2e_3)\right)$$

in the lattice $\mathbb{Z}^3$ is centrally symmetric and its lattice points are the vertices and the origin. Hence, the successive minima are $\lambda_1 = \lambda_2 = \lambda_3 = 1$, but no subset of the vertices is a lattice basis of $\mathbb{Z}^3$.

The following result is a cornerstone of the theory of successive minima. We will not prove this much stronger theorem here. A proof of the upper bound can be found in [26].

Theorem 4.10 (Minkowski's Second Theorem, 1896) *Let $K \in \mathcal{C}_0$. Then*

$$\frac{1}{d!} \cdot 2^d \det \Lambda \leq \lambda_1 \cdots \lambda_d \operatorname{vol} K \leq 2^d \det \Lambda.$$

Theorem 4.11 (Minkowski, 1910) *Let $K \subset \mathbb{R}^d$ be a centrally symmetric convex set with $\operatorname{int}(K) \cap \Lambda = \{0\}$. Then $|K \cap \Lambda| \leq 3^d$.*

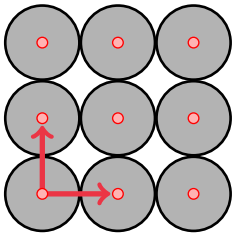
Proof. We may choose $\Lambda = \mathbb{Z}^d$. Assume the statement fails. We consider the map $\varphi : \mathbb{Z}^d \to (\mathbb{Z}/3\mathbb{Z})^d$ given by assigning each coordinate its congruence class modulo 3. This is a homomorphism (so $\varphi(x \pm y) = \varphi(x) \pm \varphi(y)$). Note that $(\mathbb{Z}/3\mathbb{Z})^d$ 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

$$p := \frac{x - y}{3} \in \Lambda.$$

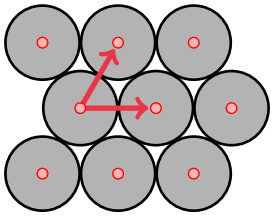
Since K is centrally symmetric,

$$\mathbf{0} \neq p = \frac{x}{3} + \frac{-y}{3} \in \frac{2}{3}K.$$

This contradicts the assumption in the theorem. □



(a) Packing of the square lattice



(b) Packing of the hexagonal lattice

Fig. 4.4: The packing radius for different lattices

Recently, it was shown that up to unimodular transformations the standard cube $[-1, 1]^d$ is the only centrally-symmetric lattice polytope with $\operatorname{int}(K) \cap \Lambda = \{0\}$ and $|K \cap \Lambda| = 3^d$ [20].

Theorem 4.12 (Betke, Henk, Wills, 1993 [10]) *Let $K \in \mathcal{C}_0$. Then*

$$|K \cap \mathbb{Z}^n| \leq \left\lfloor \frac{2}{\lambda_1} + 1 \right\rfloor^d$$

Proof. proof missing

Conjecture 4.13 (Betke, Henk, Wills, 1993 [10]) *Let $K \in \mathcal{C}_0$. Then*

$$|K \cap \mathbb{Z}^n| \leq \prod_{i=1}^{d} \left\lfloor \frac{2}{\lambda_i} + 1 \right\rfloor.$$

4.2 Coverings and Packings

For $r > 0$ and $z \in \mathbb{R}^d$ let

$$\mathcal{B}_r(z) := \{x \in \mathbb{R}^d \mid \|x - z\| < r\}$$

be the *open ball* of radius r around z. In this section we consider the configuration of all translates of such a ball to all lattice points. We want

to determine for which radii these translates are pairwise disjoint or cover the whole space, and relations between these two. We start with the first and introduce the *packing radius* of a lattice, which is the largers redius of a ball such that any two translates to a lattice point either coincide or are disjoint.

Definition 4.14 (packing radius) *Let Λ be a lattice in $\mathbb{R}^d$. The* packing radius *is*

$$\varrho(\Lambda) \;:=\; \sup_{r>0} \left(\mathcal{B}_r(x) \cap \mathcal{B}_r(y) \;=\; \varnothing \text{ for all } x, y \in \Lambda\right) ,$$

i.e. the largest $r > 0$ such that the open balls of radius r around any two distinct lattice points do not intersect.

Exercise 4.4

See Figure 4.4 for some examples. You will prove the folloing lemma in Exercise 4.4.

Proposition 4.15 *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice and v a shortest non-zero lattice vector in Λ. Then $\varrho(\Lambda) \;=\; \frac{1}{2}\|v\|$.* □

Exercise 4.5

Recall that the dual of a lattice Λ is defined to be the set of all linear functionals that map lattice points to integers. This is itself a lattice $\Lambda^\star$ in $\left(\mathbb{R}^d\right)^\star$.

Proposition 4.16 *Let Λ be a lattice in $\mathbb{R}^d$ with dual lattice $\Lambda^\star$. Then*

$$\varrho(\Lambda) \cdot \varrho(\Lambda^\star) \;\leq\; {}^d\!/_4 \,.$$

Proof. By Proposition 4.15 the packing radius is half the length of a shortest non-zero lattice vector, and by Proposition 4.5 we can bound this length with

$$\varrho(\Lambda) \;\leq\; \frac{1}{2}\sqrt{d}(\det \Lambda)^{1/d} \qquad \varrho(\Lambda^\star) \;\leq\; \frac{1}{2}\sqrt{d}(\det \Lambda^\star)^{1/d}$$

both for Λ and its dual. The proposition now follows as $\det \Lambda \cdot \det \Lambda^\star \;=\; 1$. □

Exercise 4.6

Now we switch the view and want to find out how large we need to make the radius of our balls so that the translates cover the wohle space. This is captured with the next definition.

Definition 4.17 (Covering Radius) *Let Λ be a lattice in $\mathbb{R}^d$. The* covering radius *is*

$$\mu(\Lambda) \;:=\; \max_{x \in \mathbb{R}^d} \mathrm{d}(x, \Lambda) \,,$$

i.e. the largest possible distance between any point in $\mathbb{R}^d$ and its nearest lattice point.

See Figure 4.5 for an example. The reader should convince her- or himself that the covering radius is indeed well-defined and finite. In particular, the maximum is attained for some point $x \in \mathbb{R}^d$ (by a standard compactness argument).

Lemma 4.18 *Let Λ be a lattice with successive minima $\lambda_1, \ldots, \lambda_d$ and linearly independent vectors $v_1, \ldots, v_d$ such that $\lambda_i = \|v_i\|$ for $1 \leq i \leq d$. Then*

$$\mu(\Lambda) \;\geq\; \frac{1}{2}\|v_i\| \qquad\qquad \text{for } 1 \leq i \leq d\,.$$

Proof. Let $u = 1/2 v_d$. Assume there is $w \in \Lambda$ such that $\mathrm{d}(u, w) < 1/2\|v_d\|$. Then

$$\|w\| \;\leq\; \|u\| \;+\; \mathrm{d}(u, w) \;<\; \|v_d\|\,,$$

so u cannot be linearly independent of $v_1, \ldots, v_{d-1}$ by the choice of v_d. Hence, w is in the span of $v_1, \ldots, v_{d-1}$. But then $2w - v_d$ is linearly independent, and

$$\|2w - v_d\| \;=\; \|2(w-u)\| \;<\; \|v_d\|$$

again contradicting the choice of v_d. Hence, $\mathrm{d}(u, \Lambda) = \mathrm{d}(u, \mathbf{0}) = \frac{1}{2}\|v_d\|$. This implies that

$$\mu(\Lambda) \;\geq\; \frac{1}{2}\|v_d\| \;\geq\; \frac{1}{2}\|v_i\|$$

for $1 \leq i \leq d$, where the latter follows from $\|v_d\| \geq \|v_i\|$ for all i. □

Proposition 4.19 *Let Λ be a lattice in $\mathbb{R}^d$ with dual lattice $\Lambda^\star$. Then*

$$4\,\mu(\Lambda) \cdot \varrho(\Lambda^\star) \;\geq\; 1$$

Proof. Let Λ be a lattice with successive minima $\lambda_1, \ldots, \lambda_d$ and linearly independent vectors $v_1, \ldots, v_d \in \Lambda$ such that $\lambda_i = \|v_d\|$ for $1 \leq i \leq d$. Let u be a shortest non-zero lattice vector in $\Lambda^\star$. Proposition 4.15 and Lemma 4.18 imply for any $1 \leq i \leq d$

$$4\,\mu(\Lambda) \cdot \varrho(\Lambda^\star) \;=\; 2\,\mu(\Lambda) \cdot \|u\| \;\geq\; \|v_i\| \cdot \|u\|\,. \tag{4.2}$$

The vectors $v_1, \ldots, v_d$ are a basis, so for at least one i we have $|v_i(u)| \geq 1$. Hence, for that i

$$\|v_i\| \cdot \|u\| \;\geq\; 1\,,$$

which, together with (4.2) implies the claim.

The following theorem is the key ingredient for the flatness theorem that we will prove in Section 4.3.

Theorem 4.20 *Let Λ be a lattice in $\mathbb{R}^d$ with dual lattice $\Lambda^\star$. Then*

$$4\,\mu(\Lambda)\cdot\varrho(\Lambda^\star) \;\leq\; d^{3/2}\,.$$

Our proof of this theorem is based on an argument by Schnorr, Lagarias, and Lenstra [36].

Proof. We use induction over d. For $d = 1$ we have, for some $\lambda > 0$,

$$\Lambda \;=\; \lambda\mathbb{Z}^d \qquad\qquad \text{and} \qquad\qquad \Lambda^\star \;=\; \lambda^{-1}\mathbb{Z}^d\,.$$

Thus, $\mu(\Lambda) = \lambda/2$ and $\varrho(\Lambda^\star) = \lambda^{-1}/2$, so that $4\,\mu(\Lambda)\,\varrho(\Lambda^\star) = 1$.

Now let $d > 1$. We choose a shortest non-zero lattice vector $v \in \Lambda$. Then $\|v\| = 2\,\varrho(\Lambda)$. Let L be the orthogonal complement of v with projection $\pi : \mathbb{R}^d \to L$ and $\Gamma := \pi(\Lambda)$. Then Γ is a lattice in L and $\Gamma^\star \subseteq \Lambda^\star$ by Exercise 2.33. Hence

$$\varrho(\Gamma^\star) \;\geq \varrho(\Lambda^\star)\,. \tag{4.3}$$

We now want to bound $\mu(\Lambda)$. For this, let $x \in \mathbb{R}^d$, $y = \pi(x)$ and u a closest point to y in Γ. Then

$$\|u - y\| \;\leq\; \mu(\Gamma)\,.$$

Consider the line $\pi^{-1}(u)$. Any two neighboring lattice points of Λ on this line have distance $\|v\|$. Hence, we can pick a point $w \in \Lambda \cap \pi^{-1}(u)$ such that

$$\mathrm{d}(x, w + (y - u)) \;\leq\; \frac{1}{2}\|v\|\,.$$

Using the right angled triangle $x, w, w + (y - u)$ we compute

$$\|x - w\|^2 \;\leq\; \|x - (w + (y - u))\|^2 + \|y - u\|^2\,.$$

Now x was chosen arbitrary, so we can assume it is a point with maximum distance to the lattice and we can estimate (note that w need not be a lattice point closest to x)

$$\mu(\Lambda)^2 \;\leq\; \|x - w\|^2 \;\leq\; \mu(\Gamma)^2 + \frac{1}{4}\|v\|^2 \;=\; \mu(\Gamma)^2 + \varrho(\Lambda)^2\,.$$

Hence, we obtain

$$\begin{aligned}
\mu(\Lambda)^2 \cdot \varrho(\Lambda^\star)^2 \;&\leq\; \mu(\Gamma)^2 \cdot \varrho(\Lambda^\star)^2 + \varrho(\Lambda)^2 \cdot \varrho(\Lambda^\star)^2 \\
&\leq \mu(\Gamma)^2 \cdot \varrho(\Gamma^\star)^2 + \varrho(\Lambda)^2 \cdot \varrho(\Lambda^\star)^2 \\
&\leq\; (d-1)^3 + \frac{1}{16}d^2 \\
&\leq\; d^3\,,
\end{aligned}$$

where the second inequality follows from (4.3), the third from Proposition 4.16 and the fourth by induction. This proves the theorem. □

4.3 Flatness Theorem

Playing around with two-dimensional convex sets the reader may get the impression that a convex body without interior lattice points cannot be arbitrarily wide. Indeed this is a fundamental fact in the geometry of numbers. The following considerations are based on an argument given in [5].

Definition 4.21 (width) *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with dual lattice $\Lambda^\star$. Let $K \subset \mathbb{R}^d$ be a full-dimensional convex body. The* width *of K with respect to a non-zero lattice vector $a \in \Lambda^\star$ is defined as*

$$\operatorname{width}(K; a) := \max_{x \in K} a(x) - \min_{x \in K} a(x).$$

We define the width *of K with respect to Λ as*

$$\operatorname{width}_\Lambda(K) := \inf(\operatorname{width}(K; a) \,:\, a \in \Lambda^\star \setminus \{0\}).$$

You will show in Exercise 4.8 that for full-dimensional convex bodies the infimum is actually a minimum, and in Exercise 4.9 that the width of convex bodies with dimension less than the ambient dimension is actually 0. Recall that an *ellipsoid* is the image of a ball (in some norm) under an affine linear map. See Definition A.2 for a full definition and the whole Appendix A for properties. Our approach to bound the lattice width of empty convex bodies will proceed in three steps. We first prove it for balls, then extend to ellipsoids and finally use Theorem A.5 to approximate an arbitrary convex body with ellipsoids from the interior and the exterior. The following lemma does the first two steps.

Exercise 4.8

Exercise 4.9

Lemma 4.22 *Let Λ be a lattice, $v \in \Lambda^\star$ a shortest non-zero lattice vector and E an ellipsoid such that $E \cap \Lambda = \varnothing$. Then $\operatorname{width}_v(E) \le d^{3/2}$.*

Proof. We prove this first for the case that E is a ball. In this case we know by Proposition 4.15 that $\|v\| = 2\,\varrho(\Lambda^\star)$. Let r be the radius of the ball. Then $r \le \mu(\Lambda)$. Now

$$\operatorname{width}_v(E) \;=\; r\|v\| \;=\; 2\,\varrho(\Lambda^\star)\,\mu(\Lambda)\,,$$

and the latter is at most $d^{3/2}$ by Theorem 4.20.

For the extension to ellipsoids we use that the bound $d^{3/2}$ obtained is independent of the lattice. Further, any ellipsoid is a linear image of a ball and the image of a lattice Λ for a non-singular linear map T is a lattice.

More precisely, let $x \mapsto Tx + t$ be the affine map such that $T(E) = \mathcal{B}$ is a ball, and let $\Lambda' := T(\Lambda)$. Then Λ' is a lattice in $\mathbb{R}^d$ and $\mathcal{B} \cap \Lambda' = \varnothing$. Hence, for a shortest non-zero vector $v' \in \Lambda'$, its preimage $c := T^{-1}v$ and a shortest non-zero vector $vw \in \Lambda$ we have

$$\operatorname{width}_w(E) \;\le\; \operatorname{width}_{v'}(E) \;=\; \operatorname{width}_v(\mathcal{B}) \;\le\; d^{3/2}\,. \qquad \square$$

We can extend our bound for the width of a convex body from balls and ellipsoids to general convex bodies with empty interior, albeit only with a weaker right hand side. The key observation for this is Theorem A.5, which tells us the we can estimate any convex body from the interior and exterior with a suitably chosen ellipsoid.

Theorem 4.23 *Let $K \subset \mathbb{R}^d$ be a convex body with $K \cap \Lambda = \emptyset$. Then*

$$\operatorname{width}_\Lambda(K) \;\leq\; d^{\frac{5}{2}}\,.$$

Proof. Let E be a maximum volume ellipsoid in K with center z. Then also $E \cap \Lambda = \varnothing$. Let v be a shortest non-zero lattice vector in Λ such that $\operatorname{width}(E; v) \leq d^{3/2}$ by the previous Lemma 4.22.

Clearly, the width of K is translation invariant, so we can assume that z is the origin. By Theorem A.5 we deduce $K \subseteq dE$, and thus

$$\operatorname{width}_v(K) \;\leq\; d \operatorname{width}_v(E) \leq d \cdot d^{3/2} \;=\; d^{5/2}\,. \qquad \square$$

Remark 4.24 *In fact, the bound of the previous theorem can be strengthened to be of order $d^{3/2}$, so that*

$$\operatorname{width}_\Lambda(K) \;\leq\; \mathcal{O}\left(d^{\frac{3}{2}}\right)\,.$$

Note that the upper bound only depends on the dimension and not on the given lattice. It is unknown and an active subject of current research, whether the sharp bound is actually of the form $\mathcal{O}(d)$.

4.4 Finiteness of lattice polytopes with few interior lattice points

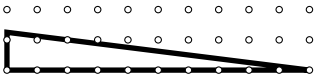


Fig. 4.6: An arbitrarily big rational triangle with one interior lattice point

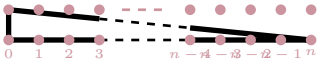


Fig. 4.7: An arbitrarily big triangle without interior lattice points

If a lattice polytope does not have interior lattice points, its volume can be arbitrarily large. However, if the polytope is centrally symmetric, Minkowski's First Theorem (Corollary 4.3) shows that its volume is bounded, if it contains only one interior lattice point. The same statement is wrong without central symmetry. The examples in Figure 4.6 have one non-lattice vertex. The reader will not be able to construct such examples of arbitrary large volume and only one interior lattice point using *lattice* polytopes. The reason for this is one of the arguably most important finiteness result about lattice polytopes. We prove here a qualitative version, following and extending an idea of Borisov & Borisov [14] (see also [13, Theorem 4.1]).

Theorem 4.25 *Given positive integers d, i, there is a bound $V(d, i)$ so that every lattice d-polytope with exactly i interior lattice points has volume less than $V(d, i)$.*

For dimension $d = 2$, Scott's theorem Theorem 1.10 makes this result precise. In general, this is still subject of current research. From Corollary 2.83 we derive a powerful finiteness theorem.

Corollary 4.26 *Given positive integers d, i, there are, up to lattice equivalence, only finitely many lattice d-polytopes with exactly i interior lattice points.*

4.4.1 Finiteness of barycentric coordinates of lattice simplices

For the proof of Theorem 4.25 we need to investigate the barycentric coordinates of interior lattice points in simplices, if the number of interior lattice points is bounded. The trick is to consider a quite general setup.

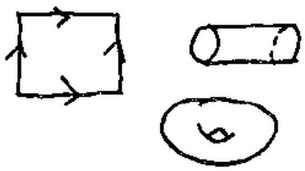


Fig. 4.8: The torus T^d

Let $T^d := \mathbb{R}^d/\mathbb{Z}^d$. Any element in T^d has a unique representative in the half-open standard square $[0,1)^d$, see Figure 4.8. We denote the quotient map $\mathbb{R}^d \to T^d$ by $x \mapsto [x]$. We consider the *open simplex*

$$\mathring{\Delta}_d \;:=\; \{x \in \mathbb{R}^d \;:\; x_i > 0 \text{ for all } i = 1,\ldots,d \text{ and } \sum_{i=1}^{d} x_i < 1\} \;\subset\; \mathbb{R}^d$$

and its (bijective) image in T^d

$$\Delta_d \;:=\; \{[x] \in T^d \;:\; x \in \mathring{\Delta}_d\} \;\subset T^d.$$

For $y \in T^d$, let us define the generated subgroup $\langle y\rangle = \{ky \;:\; k \in \mathbb{Z}\} \subset T^d$. For the considerations in the next paragraph the following is the crucial definition:

$$\mathscr{M}_i^d \;:=\; \{y \in \Delta_d \;:\; |\langle y\rangle \cap \Delta_d| \le i\} \subset T^d$$

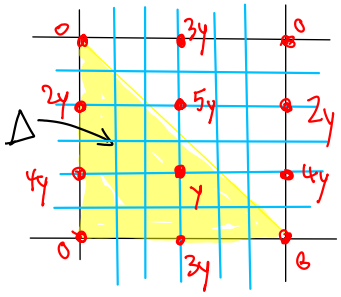


Fig. 4.9: An element $y \in \mathscr{M}_1^2$ and $\langle y\rangle$

Example 4.27 *Let $d = 2$, $y := [(1/2, 1/3)] \in \Delta_2$. Then*

$$\langle y\rangle \;=\; \{[(0,0)],[(1/2,1/3)],[(0,2/3)],[(1/2,0)],[(0,1/3)],[(1/2,2/3)]\}.$$

See Figure 4.9 for an illustation. Hence, $\langle y\rangle \cap \Delta_d = \{[(1/2,1/3)]\}$, thus, $y \in \mathscr{M}_1^2$.

The main result of this section will be the following proposition.

Proposition 4.28 *$\mathscr{M}_i^d$ is finite.*

Note that so far there is no lattice involved! This is all just about subgroups of the torus of finite order. In order to relate this to our lattice polytope problem, let us recall the notion of *barycentric coordinates*. If a d-dimensional simplex S has vertices $v_0,\ldots,v_d$, then any point x in S can be uniquely written as $x = \beta_0 v_0 + \cdots + \beta_d v_d$ with $\beta_0 + \cdots + \beta_d = 1$ and $\beta_0,\ldots,\beta_d > 0$. Here, x is in the interior of S if and only if $\beta_0,\ldots,\beta_d > 0$. Now, the relation to our problem about lattice polytopes is given by the following observation.

Corollary 4.29 *Let $S \subset \mathbb{R}^d$ be a d-dimensional lattice simplex with $i := |\operatorname{int}(S) \cap \Lambda| \geq 1$. For vertices $v_0, \ldots, v_d$ of S, we define the bijective map*

$$\beta \ : \ \operatorname{int}(S) \to \Delta_d, \quad \sum_{j=0}^{d} \beta_i v_j \mapsto [(\beta_1, \ldots, \beta_d)] \, .$$

Then

$$\beta(\operatorname{int}(S) \cap \Lambda) \subseteq \mathscr{M}_i^d \, .$$

So the set of barycentric coordinates an interior lattice point of such a simplex can have is finite.

Proof. The map β is called barycentric coordinates. It is linear and thus yields a homomorphism $\mathbb{R}^d \to T^d$. As k times a lattice point $w \in \operatorname{int}(S) \cap \Lambda$ is a lattice point we have $\langle \beta(w) \rangle \cap \Delta_d$ is contained in $\beta(\operatorname{int}(S) \cap \Lambda)$.

We may assume that after a lattice translation $v_0 = \{\mathbf{0}\}$. Let $x = \sum_{i=1}^d \beta_i v_i \in \operatorname{int}(S) \cap \Lambda$, and $y := \beta(x) = [(\beta_1, \ldots, \beta_d)] \in \Delta_d$. If for $k \in \mathbb{Z}_{\geq 0}$, $ky \in \Delta_d$, then there exists $x' = \sum_{i=1}^d \beta_i' v_i \in \operatorname{int}(S)$ with $\beta(x') = [(\beta_1', \ldots, \beta_d')] = ky = [(k\beta_1, \ldots, k\beta_d)]$. This implies that $\beta_i' - k\beta_i \in \mathbb{Z}$ for $i = 1, \ldots, d$, thus

$$x' = \left(\sum_{i=1}^{d} (\beta_i' - k\beta_i) v_i \right) + k \left(\sum_{i=1}^{d} \beta_i v_i \right) \in \Lambda.$$

Hence, the number of elements in $\langle y \rangle \cap \Delta_d$ is at most the number of elements in $\operatorname{int}(S) \cap \Lambda$ which is i. This proves $y \in \mathscr{M}_i^d$. □

In other words, there are only *finitely* many barycentric coordinates possible for interior lattice points in a lattice simplex which contains a certain, non-zero number of interior lattice points overall.

Let us give some preparations for the proof of Proposition 4.28. We need a natural translation-invariant distance function on T:

$$\mathrm{d}(y, y') \ := \ \min\{\|x - x'\| \ : \ y = [x], y' = [x'] \text{ for } x, x' \in \mathbb{R}^d\} \, .$$

Look at Figure 4.10 to get a better intuition for this definition. Note that there are two kinds of elements of the group T^d: the rational points have finite order, and the irrational points have infinite order.

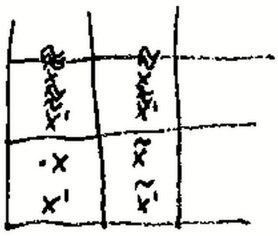


Fig. 4.10: Illustrating the definition of our metric

Lemma 4.30 *For $x \in \{0\}^r \times \mathbb{R}^{d-r}$ (with $0 \leq r \leq d$) and $\varepsilon > 0$ there is a positive integer k and $z \in \{0\}^r \times \mathbb{R}^{d-r}$ with $[z] = [kx]$ and $||z|| < \varepsilon$.*

Proof. If x is rational, then there exists a positive integer k such that $[kx] = \mathbf{0}$, so define $z = \mathbf{0} \in \mathbb{R}^d$. If x is irrational, then $\langle [x] \rangle$ is infinite.

As T^d is compact, there must be an accumulation point. Hence, there are natural numbers $k' > k''$ so that

$$\mathrm{d}((k'-k'')[x],[\mathbf{0}]) = \mathrm{d}(k'[x],k''[x]) \;<\; \varepsilon\,.$$

Choose $k := k' - k''$. As $kx \in \{0\}^r \times \mathbb{R}^{d-r}$, the definition of the metric $\mathrm{d}([kx],[\mathbf{0}])$ implies the existence of $z \in \{0\}^r \times \mathbb{R}^{d-r}$, as desired. (Note that we do not claim that $z \in [0,1]^d$, see Figure 4.11.) □

Fig. 4.11: z doesn't have to be in $[0,1]^d$

Proof (Proposition 4.28). As Δ^d is in bijection with ${}^\circ\Delta_d{}^d$, every element in $\mathscr{M}_i^d \subset \Delta^d$ corresponds to an element in $\mathscr{M}_i^d \subset {}^\circ\Delta_d{}^d$. Let us define the (compact) closure of ${}^\circ\Delta_d{}^d$ in $\mathbb{R}^d$:

$$\overline{\Delta^d} \;:=\; \{x \in \mathbb{R}^d \;:\; x_i \geq 0 \text{ for all } i = 1,\ldots,d \text{ and } \sum_{i=1}^d x_i \leq 1\} \;\subset\; \mathbb{R}^d$$

We assume that $\mathscr{M}_i^d$ (thus, $\hat{\mathscr{M}}_i^d$) is not finite. Then there exists an accumulation point $x^* \in \overline{\Delta^d}$ of $\hat{\mathscr{M}}_i^d$. Changing the coordinate system on T^d if necessary, we may assume that $x_1^* = \ldots = x_r^* = 0$, and $x_{r+1}^*,\ldots,x_d^*, 1 - \sum_{j=1}^d x_j^* > 0$. In particular,

$$x^* \in \{0\}^r \times \mathbb{R}_{>0}^{d-r}.$$

We can assume this by permuting just the coordinates, since $\mathscr{M}_i^d$ can be characterized in a symmetric way, see Exercise 4.10.

Exercise 4.10

Let us choose $\varepsilon > 0$ so that $\mathcal{B}_\varepsilon(x^*) \cap (\mathbb{R}_{>0}^r \times \mathbb{R}^{d-r}) \subset {}^\circ\Delta_d{}^d$, see Figure 4.12.

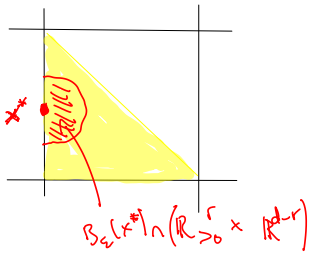


Fig. 4.12: $\mathcal{B}_\varepsilon(x^*) \cap (\mathbb{R}_{>0}^r \times \mathbb{R}^{d-r}) \;\subset\; {}^\circ\Delta_d{}^d$

Now, Lemma 4.30 implies the existence of a positive integer k and and $z^* \in \{\mathbf{0}\}^r \times \mathbb{R}^{d-r}$ so that $[kx^*] = [z^*]$ and $\|z^*\| < \varepsilon/2i$. With x^* being an accumulation point of $\hat{\mathscr{M}}_i^d$, there is an $x \in \hat{\mathscr{M}}_i^d$ such that

$$||x - x^*|| < \varepsilon/(2(ik+1)) \text{ and } x \neq x^* - z^*/k.$$

Note that we have $x - x^* \in \mathbb{R}_{>0}^d \times \mathbb{R}^{d-r}$. We define for $j = 0,1,\ldots,i$

$$w_j := x^* + jz^* + (jk+1)(x - x^*) \in \mathbb{R}^d.$$

Let us show that

$$[w_j] \in \langle [x] \rangle \cap \Delta^d \text{ for } j = 0\ldots,i,$$

where all these $(i+1)$ elements are pairwise different. This would show $[x] \notin \mathscr{M}_i^d$, which is a contradiction.

First, we observe that

- $w_j \in \mathbb{R}_{>0}^r \times \mathbb{R}^{d-r}$.
- $||w_j - x^*|| < j\frac{\varepsilon}{2i} + (jk+1)\frac{\varepsilon}{2(ik+1)} \leq \varepsilon$.

Hence, the definition of ε implies that $w_j \in {}^{\circ}\Delta_d{}^d$. Next, let us use $[kx^*] = [z^*]$ to deduce

$$[w_j] = j[z^*] + (jk+1)[x] - jk[x^*] = [(jk+1)x] \in \langle [x] \rangle.$$

Finally, let us note

$$w_j = x + j(z^* + k(x - x^*)).$$

As $z^* + k(x - x^*) \neq \mathbf{0}$ by the choice of x, we see that $w_0, \ldots, w_i$ are pairwise different. This finishes the proof. □

4.4.2 Coefficient of asymmetry

Now that we have braved the technical core in the proof of Theorem 4.25, the machinery will give us a volume bound $V(d,i)$ in terms of a parameter $\varepsilon(d,i)$ that we introduce below. It will depend only on the dimension and the number of interior lattice points.

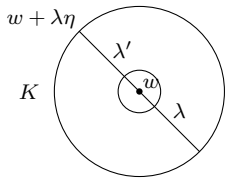
The smallest barycentric coordinate of a point inside a simplex is a measure for how far in the interior of the simplex the point sits. To measure the same thing for points in more general polytopes (or convex bodies), we use the convex-geometric notion of coefficient of asymmetry.

Definition 4.31 *Let $K \subset \mathbb{R}^d$ be a d-dimensional convex body, $w \in \operatorname{int} K$, then*

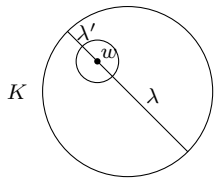
$$\operatorname{ca}(K;w) := \sup_{\eta \in \mathbb{R}^d \setminus \{\mathbf{0}\}} \frac{\max\{\lambda > 0 \ : \ w + \lambda\eta \in K\}}{\max\{\lambda > 0 \ : \ w - \lambda\eta \in K\}}$$

is the coefficient of asymmetry.

We have $\operatorname{ca}(K;w) \geq 1$. Note that $\operatorname{ca}(K;w) = 1$ if and only if K is centrally symmetric with respect to w. So, the closer $\operatorname{ca}(K;w)$ is to 1 the more w lies in the 'center' of K (the converse may not be true). See Figure 4.13 for two examples. We now extend Proposition 4.28 from simplices to polytopes.



(a) An example with $\operatorname{ca}(K;w) = 1$



(b) An example with $\operatorname{ca}(K;w) \gg 1$

Fig. 4.13: Coefficient of Asymmetry

Definition 4.32 (Minimal barycentric coordinates) *For positive integers d and i, the minimal barycentric coordinate of any interior lattice point in any lattice d-simplex with precisely i interior lattice points will be denoted by* $\operatorname{sbc}(d,i)$. *This definition yields a well-defined* positive *number* $\operatorname{sbc}(d,i)$ *because of Corollary 4.29, a consequence of the main result of the previous section.*

You will prove some simple properties in Exercise 4.11. Here is a simple fact that you will prove in Exercise 4.12.

Exercise 4.11

Lemma 4.33 *For $d \geq 1$ and $i \geq 1$ we have* $\operatorname{sbc}(d+1,i) \leq \operatorname{sbc}(d,i)/2$.

□

Exercise 4.12

Proposition 4.34 *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional lattice polytope with $i > 0$ interior lattice points, and let $w \in \operatorname{int} P \cap \mathbb{Z}^d$. Then*

$$\operatorname{ca}(P; w) \leq \max\left(\frac{1}{\operatorname{sbc}(d, i')} - 1 \ : \ 1 \leq i' \leq i\right) .$$

The proof uses two auxiliary results. You will prove the following lemma in Exercise 4.13.

Lemma 4.35 *Let $P \in \mathbb{R}^d$ be a polytope, and let $w \in \operatorname{int} P$. Then the coefficient of asymmetry is attained at a vertex. That is, there is a vertex v of P so that*

$$\operatorname{ca}(P; w) = \frac{1}{\max\{\lambda > 0 \ : \ w - \lambda(v - w) \in P\}} . \tag{4.4}$$

□

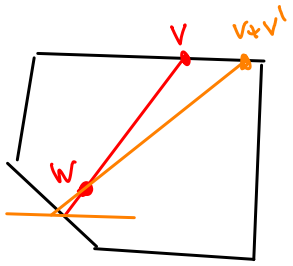


Fig. 4.14: The coefficient of asymmetry is attained at a vertex

The following corollary justifies the claim that the coefficient of asymmetry of a point in a polytope is a qualitative generalization of the smallest barycentric coordinate of a point in a simplex.

Exercise 4.13

Corollary 4.36 *Let $S = \operatorname{conv}(v_0, \ldots, v_d) \subset \mathbb{R}^d$ be a d-simplex, and let $0 < \beta_0 \leq \ldots \leq \beta_d$ with $\sum_{j=0}^d \beta_j = 1$. Set $w := \sum_{j=0}^d \beta_j v_j$. Then*

$$\operatorname{ca}(S; w) = \frac{1}{\beta_0} - 1.$$

Exercise 4.14

You will give a proof of this in Exercise 4.14.

Exercise 4.15

Proof (of Proposition 4.34). Let v be a vertex of P as in (4.4). Let $c := \operatorname{ca}(P; w)$, and denote the opposite point by $v' := w - \frac{1}{c}(v - w)$. There is a face F of P which contains v' in its relative interior. In a lattice triangulation of F there must be a lattice simplex S' which contains v' in its relative interior. Hence, the lattice simplex $S := \operatorname{conv}(v, S')$ of dimension $1 \leq d' \leq d$ contains w in its relative interior, and the segment $\operatorname{conv}(v, v')$ certifies $\operatorname{ca}(S; w) \geq c$. Furthermore, every relative interior point of S is an interior point of P, so S contains j interior lattice points for $1 \leq j \leq i$. The statement follows now from the previous corollary. □

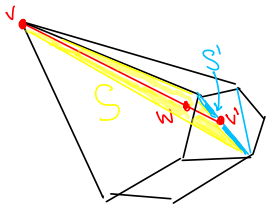


Fig. 4.15: $\operatorname{ca}(P; w) \leq \operatorname{ca}(S; w)$ for some simplex S

Exercise 4.16

4.4.3 Bounding the volume

We are finally in the position to finish the proof of Theorem 4.25. For this we need the following observation. You will prove this in Exercise 4.17.

Lemma 4.37 *Let K be a d-dimensional convex body with $\mathbf{0} \in \operatorname{int} K$. Set $c := \operatorname{ca}(K; \mathbf{0})$. Then $-\frac{1}{c}K \subseteq K$.*

Exercise 4.17

Proposition 4.38 *Let $K \subset \mathbb{R}^d$ be a d-dimensional convex body. If $w \in \operatorname{int} K \cap \mathbb{Z}^d$, then*

$$\operatorname{vol}(K) \leq 2^{d-1} \operatorname{ca}(K;w)^d (|\operatorname{int} K \cap \mathbb{Z}^d| + 1) .$$

Proof. We set $i := |\operatorname{int} K \cap \mathbb{Z}^d|$ and $c := \operatorname{ca}(K;w)$. We may assume that $w = \mathbf{0}$. Consider $Q := \operatorname{conv}(-\frac{1}{c}K \cup \frac{1}{c}K)$. We have $Q = -Q$, and $\frac{1}{c}K \subseteq Q \subseteq K$ by the previous lemma. Hence, $|\operatorname{int} Q \cap \mathbb{Z}^d| \leq i$ so that by van der Corput's Theorem (Theorem 4.2) $\operatorname{vol} Q \leq (i+1)2^{d-1}$. This yields $\operatorname{vol}(K) \leq c^d \operatorname{vol}(Q)$ from which the statement follows. □

The bound is tight, as you will show in Exercise 4.18. This implies Theorem 4.25 with

Exercise 4.18

$$V(d,i) \;=\; (i+1)2^{d-1} \left(\frac{1}{\operatorname{sbc}(d,i)} - 1 \right)^d .$$

Let us finish by presenting without proof the currently best and most general result. The following theorem is a combination of results obtained by Hensley [27], Lagarias and Ziegler [37] and Pikhurko [45].

Theorem 4.39 (Hensley; Lagarias & Ziegler; Pikhurko) *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional lattice polytope such that $I_l(P) \neq \emptyset$. Then*

$$\operatorname{vol}(P) \leq (8dl)^d (8l+7)^{d \cdot 2^{2d+1}} |\operatorname{int} P \cap l\mathbb{Z}^d|$$

4.5 Lower Bounds

We can make the bound $V(d,i)$ of the previous theorem more precise. Similar to the volume we can also look at the total number of lattice points of a lattice polytope when the number of interior lattice points is fixed. For this, let $L(d,i)$ be the maximal number of lattice points of a d-dimensional lattice polytope with exeactly i interior lattice points.

For integers $m_1, \ldots, m_d$ we consider the following simplex

$$S^d_{(m_1,\ldots,m_d)} \;:=\; \left\{ x \in \mathbb{R}^d \mid x_i \geq 0 \,,\; \sum \frac{x_i}{m_i} \leq 1 \right\} .$$

This is a lattice simplex with vertices $\mathbf{1}$ and $m_i e_i$ for the unit basis vectors e_i. Hence, it is a lattice simplex. See Figure 4.16 for an example.

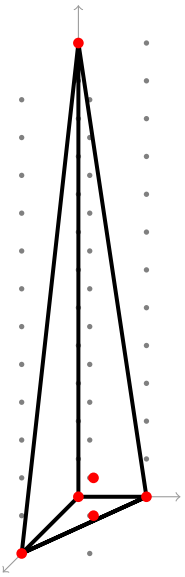


Fig. 4.16: $S^d_{(2,3,12)}$

We compute its volume and number of lattice points for a particular choice of the parameters m_i. We define a sequence $(a_j)_j \geq 1$ via

$$a_1 \;:=\; 2 \qquad \text{and} \qquad a_j \;:=\; \prod_{l=1}^{j-1} a_l + 1 \quad \text{for } j \;\geq\; 2$$

and for fixed $d \geq 3$ and $i \geq 1$ we set

$$k_j \;:=\; a_j \quad \text{for } 1 \le j \le d-1 \qquad \text{and} \qquad k_d \;:=\; (i+1)(a_d - 1)\,.$$

The sequence of the a_i is the Sylvester sequence. It satisfies the following properties, which you will prove in Exercise 4.19.

Lemma 4.40 *(1) For $d \ge 1$ we have* $1 - \sum_{i=j}^{d} \frac{1}{a_j} \;=\; \left(\prod_{j=1}^{d} a_j\right)^{-1}$

(2) for $d \ge 4$ we have $\prod_{i=1}^{d} a_i \;\ge\; 2^{2^{d-a}}$ for a constant $a \approx 0.5856\ldots$.

We define the Sylvester simplices by

$$S_i^d \;:=\; S^d_{(k_1,\ldots,k_d)}\,.$$

Exercise 4.19

It follows from Lemma 4.40(1) that for $i = 1$

$$\sum_{j=1}^{d} \frac{1}{k_j} \;\le\; 1 \qquad\qquad \frac{1}{k_d} + \sum_{j=1}^{d} \frac{1}{k_j} \;=\; 1$$

so that $(1,1,\ldots,1)^t$ is in the interior of S_1^d, while $(1,1,\ldots,2)^t$ is not. As the k_i are strictly increasing we conclude that S_1^d has exactly one interior lattice point. Similarly we can show that $(1,1,\ldots,s)^t$ for $1 \le s \le i$ are the only interior lattice points of S_i^d.

The volume of S_i^d is

$$\operatorname{vol}(S_i^d) \;=\; \frac{1}{d!}\prod_{j=1}^{d} k_j \;=\; \frac{i+1}{d!}(a_d - 1)^2\,. \tag{4.5}$$

We estimate the number of lattice points. For this, let R be the ridge of S_i^d defined by $x_1 = x_2 = 0$.

Exercise 4.20
Exercise 4.21
Exercise 4.22

It follows from Exercise 4.20 that $L(S+t) \le L(S)$ with equality if $t \in \mathbb{Z}^d$. By Exercise 4.21 know that

$$\begin{aligned}\operatorname{vol}(R) \;&=\; \int_{C_{d-2}} |(R+t) \cap \mathbb{Z}^{d-2}|\, dt \\ &=\; \int_{C_{d-2}} L(R+t)\, dt \;\le\; L(R) \;\le\; L(S_i^d)\,.\end{aligned}$$

Thus

$$L(S_i^d \;\ge\; \operatorname{vol}(R) \;\ge\; \frac{d(d-1)}{2\cdot 3}\operatorname{vol}(S_i^d) \tag{4.6}$$

Theorem 4.41 (Perles, Zaks, Wills [61]) *Let $i \ge 1$. We have*

$$\begin{aligned} V(3,i) \;&\ge\; 6(i+1) \qquad L(3,i) \;\ge\; 16i + 23 \\ V(4,1) \;&\ge\; 147 \qquad\quad L(4,1) \;\ge\; 680 \end{aligned} \tag{4.7}$$

and for $d \ge 4$

$$V(d,i) \;\ge\; \frac{i+1}{d!}2^{2^{d-a}} \qquad L(d,i) \;\ge\; \frac{i+1}{6(d-2)!}2^{2^{d-a}} \tag{4.8}$$

where $a \approx 0.5856\ldots$.

Proof. For the special cases in dimensions 3 and 4 in (4.7) see Exercise 4.23.

We know that the volume of S_i^d is

$$\operatorname{vol}(S_i^d) \;=\; \frac{i+1}{d!}(a_d - 1)^2$$

by (4.5). Using Lemma 4.40(2) we estimate

$$a_d - 1 \;\geq\; 2^{2^{d-1-a}}$$

from which the lower bound on the voume follows. The bound for the lattice points now follows from this and (4.6). □

Exercise 4.23

4.6 Empty lattice simplices

Every lattice polytope has a triangulation which uses all the lattice points. Its simplices have the property that the only lattice points they contain are their vertices.

Definition 4.42 (empty) *A lattice polytope P is* empty *if the vertices of P are the only lattice points in P.*

Empty simplices in this sense can be regarded as the fundamental building blocks of lattice polytope theory. Because of its number theoretic nature, the study of these objects is in general very hard. In this section, we will present what we know (in low dimension) and what we do not yet know (in higher dimensions).

Let us start with the simplest cases $d = 1$ and $d = 2$. There is (up to equivalence) only one empty segment, $[0, 1]$. By Pick's Formula (Theorem 1.8), an empty triangle must be unimodular as well. The only other empty polygon is the unit square $[0, 1]^2$ up to unimodular equivalence (Exercise 4.24). The situation is significantly more subtle in dimension ≥ 3. The *Reeve simplices* $\mathsf{R}_d(m)$ that we have seen in (1.1) are examples of empty lattice simplices in any dimension ≥ 3 of arbitrary large normalized volume m.

Exercise 4.24

Surprisingly, in dimension 3 an astonishing and completely not obvious result still holds.

Theorem 4.43 (Howe (in Scarf 1985)) *If $P \subset \mathbb{R}^3$ is an empty lattice polytope in the lattice $\mathbb{Z}^3$, then* $\operatorname{width}_{\mathbb{Z}^3}(P) = 1$.

Here $\operatorname{width}_{\mathbb{Z}^3}(P)$ is the lattice width defined in Definition 4.21. We will only prove the theorem for the crucial case of an empty tetrahedron. Here the previous result takes the following form.

Theorem 4.44 (White 1964) *If $T \subset \mathbb{R}^3$ is an empty lattice tetrahedron, then T is equivalent to*

$$T_{pq} := \operatorname{conv} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & p \\ 0 & 0 & 0 & q \end{pmatrix} .$$

Note that the first coordinate is always 0 or 1 on the vertices of T_{pq}, hence, the lattice width is one. By now, there are several proofs known (White 1964 [60], Morrison & Stevens 1984 [40], Howe (in Scarf 1985) [47], Sebö 1999 [52])[2]Before we prove these two theorems we need the following useful observation by Scarf which is true in arbitrary dimensions, not just in dimension three. For this, let us define the following function. For $a \in \mathbb{Z}^d$ with $D := \sum_{j=1}^d a_j - 1 > 0$ define

[2] The history of these proofs is interesting

$$f\colon \{1, \dots, D-1\} \to \mathbb{Z}, \quad h \mapsto \sum_{j=1}^{d} \left\lceil \frac{a_j h}{D} \right\rceil .$$

Lemma 4.45 (Scarf's criterion) *For $a \in \mathbb{Z}^d$ the d-dimensional simplex $T = \operatorname{conv}(e_1, \dots, e_d, a)$ is empty if and only if $f(h) > h+1$ for $h = 1, \dots, D-1$.*

If $d = 3$, this is equivalent to $f(h) = h+2$ for $h = 1, \dots, D-1$ and $\gcd(a_j, D) = 1$ for $j = 1, \dots, d$.

Proof. First, observe that $f(h) \geq \sum_{j=1}^d \frac{a_j h}{D} = \frac{D+1}{D} h > h$, and thus $f(h) \geq h+1$ for all h.

Next, we have the following inequality description of $T \setminus \{e_1, \dots, e_d, a\}$ (Exercise 4.25).

$$\left\{ x \in \mathbb{R}^d \; : \; \begin{array}{c} 0 \;\leq\; \sum_{j=1}^d x_j - 1 \;<\; D \;\text{ and} \\ \frac{a_i}{D} - 1 \;<\; -x_i + \frac{a_i}{D} \sum_{j=1}^d x_j \;\leq\; \frac{a_i}{D} \text{ for } i = 1, \dots, d \end{array} \right\}$$

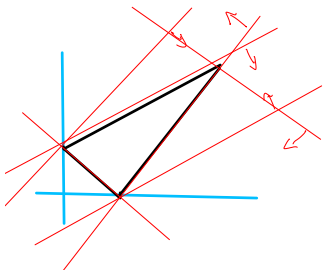


Fig. 4.17: Inequality description of $T \setminus \{e_1, e_2, a\}$

Let us show that T is not empty if and only if there is an $h \in \{1, \dots, D-1\}$ with $f(h) = h+1$.

If there is an $x \in \mathbb{Z}^d \cap T \setminus \{e_1, \dots, e_d, a\}$, set $h := \sum_{j=1}^d x_j - 1$. The above inequality description yields $0 \leq h < D$. This implies $h \in \{1, \dots, D-1\}$, as for $h = 0$, x would be a non-vertex lattice point in $\operatorname{conv} e_1, \dots, e_d$ which is not possible. Moreover, the conditions for $i = 1, \dots, d$ are equivalent to $\frac{a_i h}{D} \leq x_i < \frac{a_i h}{D} + 1$ so that necessarily $x_i = \lceil \frac{a_i h}{D} \rceil$, and we obtain $f(h) = \sum_{j=1}^d x_j = h+1$.

If, on the other hand, there is an $h \in \{1, \dots, D-1\}$ with $f(h) = h+1$, set $x_i = \lceil \frac{a_i h}{D} \rceil$ for $i = 1, \dots, d$. This defines $x \in \mathbb{Z}^d$ that satisfies all above inequalities, hence, T is not empty.

Finally, if $d = 3$, we consider $f(h) + f(D-h) = \sum_{j=1}^d \lceil a_j \frac{h}{D} \rceil + \lceil a_j \frac{D-h}{D} \rceil$. Using

$$\left\lceil a_i \frac{h}{D} \right\rceil + \left\lceil a_i \frac{D-h}{D} \right\rceil = \begin{cases} a_j & \text{if } D \text{ divides } a_j h \\ a_j + 1 & \text{if } D \text{ does not divide } a_j h \end{cases}$$

we obtain $f(h) + f(D-h) \leq \sum_{j=1}^{d}(a_j+1) = D+1+d = D+4$. If T is empty, our previous considerations show that $f(h) + f(D-h) \geq h+2 \ + \ D-h+2 = D+4$ so that $f(h) = h+2$ for all $h = 1, \ldots, D-1$, and D never divides $a_j h$ for $j = 1, \ldots, d$. This also immediately implies $\gcd(a_j, D) = 1$, since otherwise $D/\gcd(a_j, D) \in \{1, \ldots, D-1\}$, thus, D wouldn't divide $a_j D/\gcd(a_j, D) = \operatorname{lcm}(a_j, D)$, a contradiction. □

Exercise 4.25

Let us note that if $D = 1$, then the simplex T in Scarf's criterion is automatically empty and of width one (the sum of all coordinates equals 1 for $e_1, \ldots, e_d$, and 2 for a).

Proof (of the Theorem of White (Theorem 4.44)). Our proof is based on an argument by Scarf, and proceeds in two steps.

(1) We show first that if T is empty, then T is, for some $a_1, a_2, a_3 \geq 0$, equivalent to

$$\operatorname{conv}\begin{pmatrix} 1 & 0 & 0 & a_1 \\ 0 & 1 & 0 & a_2 \\ 0 & 0 & 0 & a_3 \end{pmatrix}$$

(2) Then we use Scarf's criterion (Lemma 4.45) together with the lower bound $a_1, a_2, a_3 \geq 2$ to obtain a contradiction.

Step 1 (Standard form): We can assume that

$$T = \operatorname{conv}\begin{pmatrix} 0 & v_{11} & v_{12} & v_{13} \\ 0 & 0 & v_{22} & v_{23} \\ 0 & 0 & 0 & v_{33} \end{pmatrix}$$

is in Hermite normal form, i.e.

$$v_{11} > 0, \qquad v_{22} > v_{12} \geq 0, \qquad v_{33} > v_{13}, v_{23} \geq 0$$

(cf. Definition 2.64, note that here we look at the transposed form). The triangle spanned by the first three vertices is empty and hence unimodular by Pick's Formula (Theorem 1.8). This implies $v_{11} = v_{22} = 1$, $v_{12} = 0$. Now,

$$T \cong T + \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \operatorname{conv}\begin{pmatrix} 0 & 1 & 0 & v_{13} \\ 0 & 0 & 1 & v_{23} \\ 1 & 1 & 1 & v_{33}+1 \end{pmatrix} \cong \operatorname{conv}\begin{pmatrix} 0 & 1 & 0 & a_1 \\ 0 & 0 & 1 & a_2 \\ 1 & 0 & 0 & a_3 \end{pmatrix}$$

with $a_1 := v_{13} \geq 0$, $a_2 := v_{23} \geq 0$, and $a_3 := v_{33} - v_{13} - v_{23} + 1$. (For the last equivalence we have subtracted the first two coordinates from

the third.) We abbreviate $D := a_1 + a_2 + a_3 - 1 = v_{33} > 0$. If a_3 were negative, then let us consider the following affine combination

$$\begin{pmatrix}1\\1\\0\end{pmatrix} = \frac{D-a_1}{D}\begin{pmatrix}1\\0\\0\end{pmatrix} + \frac{D-a_2}{D}\begin{pmatrix}0\\1\\0\end{pmatrix} + \frac{-a_3}{D}\begin{pmatrix}0\\0\\1\end{pmatrix} + \frac{1}{D}\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}.$$

Here, $D - a_1 = v_{33} - v_{13} > 0$, $D - a_2 = v_{33} - v_{23} > 0$, so this would be a proper convex combination. Therefore, $(1,1,0)^t \in \operatorname{int} T$, a contradiction to T being empty.

Step 2: Recall the function f used in Scarf's criterion: For $a \in \mathbb{Z}^d$ with $D := \sum_{j=1}^d a_j - 1 > 0$ we have defined $f\colon \{1,\dots,D-1\} \to \mathbb{Z}$ via $h \mapsto \sum_{j=1}^d \left\lceil \frac{a_j h}{D} \right\rceil$.

Let $d = 3$ and

$$D \;=\; a_1 + a_2 + a_3 - 1 \geq 1\,.$$

Assume $a_1, a_2, a_3 \geq 2$ and $f(h) = h + 2$ for all h. Make a $D-1$ by 3 table of the numbers ha_i reduced mod D for $h = 1,\dots,D-1$ as exemplified in Table 4.1. Later we will sometimes use the notation $[k]_D$ for the remainder in $\{0,\dots,D-1\}$ of an integer k modulo D. Note that the Dth-row consists simply of zeroes. We will refer to a row for $h \in \{2,\dots,D-1\}$ (mod D) as a *proper* row.

h	$2h$	$3h$	$7h$
1	2	3	7
2	4	6	$\underline{3}$
3	6	9	10
4	8	$\underline{1}$	$\underline{6}$
5	10	4	$\underline{2}$
6	$\underline{1}$	7	9
7	3	10	$\underline{5}$
8	5	$\underline{2}$	$\underline{1}$
9	7	5	8
10	9	8	$\underline{4}$

Table 4.1: Table for $a = (2,3,7)^t$ mod $D = 11$

The a_i are coprime to D, so the three columns will be permutations of the set $\{1,\dots,D-1\}$, (compare Exercise 4.26). Also, we can add the ith and the jth row of the table and reduce it mod D to obtain the $(i+j)$th (mod D) row. Roughly speaking, in each ith column we add a_i on the entry above until this number exceeds D in which case we reduce this entry, see Table 4.1.

Exercise 4.26

In each column we underline the entries where the reduction takes place (a 'jump'). These can be characterized by any of the following equivalent conditions for an entry in a *proper* row: (Exercise 4.27):

- the entry is smaller than the entry directly above
- the entry (in the ith column) is (necessarily strictly) smaller than a_i
- the entry (in the ith column and hth row) satisfies

$$\left\lceil \frac{a_i h}{D} \right\rceil \;=\; \left\lceil \frac{a_i(h-1)}{D} \right\rceil + 1\,.$$

Exercise 4.27

The last condition allows us to make the following crucial observation: As for $h = 2,\dots,D-1$

$$f(h) \;=\; \sum_{i=1}^{3} \left\lceil \frac{a_i h}{D} \right\rceil \;=\; h + 2\,,$$

we have $f(h) = f(h-1)+1$. Hence, in each proper row precisely one entry gives a contribution $\lceil \frac{a_i h}{D} \rceil$ to this sum which is one larger than in the row above. In other words, *each proper row has precisely one underlined entry.* We see that $a = (2,3,7)^t$ yields a simplex which is not empty as there is no underlined entry in row 3 of Table 4.1.

We will use these restrictions in order to get a contradiction. For this, we consider the special entries $D-1$. Let us recall that $1 < a_1, a_2, a_3 < D-1$.

(1) Assume there is a (necessarily proper) row h with two entries $D-1$. In this case, the row $D-h$ has two entries 1. Therefore, we have a (necessarily proper) row with two (underlined) entries 1, a contradiction.

(2) Assume there is a (necessarily proper) row with entries $D-1$ and 1 (say, in the first and second column). Multiplying by a_2 yields another row with entries $D-a_2$ and a_2. Hence, we're in the very first row with entries a_1, a_2, a_3, so $D-a_2 = a_1$, a contradiction (recall $a_3 > 1$).

(3) Next, assume there is a two by two configuration

$$\begin{matrix} {\scriptstyle D-1} & {\scriptstyle \underline{\alpha}} \\ \underline{\beta} & {\scriptstyle D-1} \end{matrix}$$

By symmetry, let these be in the first and second column. Summing these two rows yields again a row with entries $\beta - 1 < \beta < a_1$ and $\alpha - 1 < \alpha < a_2$. Hence, as this cannot be the 1-st row, and there is no proper row with two underlined entries, we see that this must be the D-th row, so $\beta - 1 = 0$, thus $\beta = 1$. Therefore, the first of above two rows has an entry $D-1$ and 1. This gives a contradiction to the previous point.

(4) This leads to the last case, where we are left with dealing with a sub-table of proper rows of the form

$$\begin{array}{c|ccc} h_1 & D-1 & \underline{\alpha} & \beta \\ h_2 & \gamma & D-1 & \underline{\delta} \\ h_3 & \underline{\varepsilon} & \zeta & D-1 \end{array} \tag{4.9}$$

We note that $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta > 1$. Consider

$$h_1 + h_2 \mid \gamma - 1 \quad \underline{\alpha - 1} \quad [\beta + \delta]_D \,,$$

As this is not the 1-st row ($\alpha - 1 < a_2$) or D-th row ($\alpha - 1 \neq 0$), $[\beta+\delta]_D$ cannot be underlined, so $[\beta+\delta]_D > a_3$. In particular, $[\beta+\delta-1]_D \geq a_3$. In fact, as $a_3 < \beta$ and $\delta < a_3$ we see $[\beta+\delta-1]_D > a_3$. By symmetry, this implies that

$$h_1 + h_2 + h_3 \mid [\varepsilon + \gamma - 1]_D \quad [\alpha + \zeta - 1]_D \quad [\beta + \delta - 1]_D \,,$$

is neither the first row, nor the D-th row, and it also does not have an underlined entry which is a contradiction.

□

Exercise 4.28

Exercise 4.29

The reader may wonder whether the previous result also holds in higher dimension. Unfortunately, it fails already in dimension 4, as we will show now. For this, let us define a lattice simplex $S(a,b,c,d) \subset \mathbb{R}^4$ as the convex hull of the columns of the following matrix:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & a \\ 0 & 1 & 0 & 0 & b \\ 0 & 0 & 1 & 0 & c \\ 0 & 0 & 0 & 1 & d \end{pmatrix}$$

It was shown in [25] that for integers $D \geq 9$ and coprime to 6 the 4-simplex $S(2,2,3,D-6)$ is empty, of normalized volume D and has width 2. Hence, there exist infinitely many non-isomorphic empty lattice 4-simplices with width > 1.

On the other hand, it is known that there are only finitely many empty lattice 4-simplices with width > 2, as shown by Barile, Bernardi, Borisov, and Kantor [2]. Up to now, the maximal possible width known is 4, realized by $S(6,14,17,65)$.

4.7 Lattice polytopes without interior lattice points

Focusing again on lattice polytopes, let us make the following definition.

Definition 4.46 *A lattice polytope P is called* hollow *if it does not contain any interior lattice points.*

From the viewpoint of geometry of numbers, hollow lattice polytopes are a somewhat more natural class to consider than empty simplices. In this section, we will prove a structural result on hollow lattice polytopes that will imply the flatness theorem for this class of convex sets.

Let us first look at low dimensions. In dimension one, there is only one hollow lattice segment, $[0,1]$. In dimension two, there are two kinds of hollow lattice polygons. They are depicted in Figure 4.18, see also Exercise 3.33. Observe that one way to construct hollow lattice d-polytopes is to take a hollow polytope $Q \subset \mathbb{R}^{d-1}$ and choose any subpolytope of the infinite prism $Q \times \mathbb{R}$. Observe as well that having width one is equivalent to allowing an integral projection onto the hollow polytope $[0,1]$.

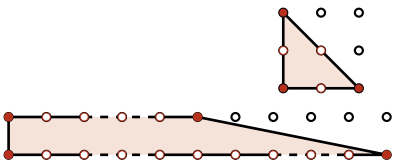


Fig. 4.18: "All" hollow lattice polygons

Exercise 4.30

More generally, the reader should convince oneself that the following observation holds:

If a lattice polytope has a lattice projection onto a hollow lattice polytope (of smaller dimension, not a point), then it was hollow to begin with.

The following theorem states that this is the only way to get hollow polytopes – up to finitely many exceptions.

Theorem 4.47 *There are only finitely many (equivalence classes of) hollow lattice d-polytopes which do not allow an integral projection onto a hollow lattice $(d-1)$-polytope.*

The proof is based on an argument by Averkov et al. It proceeds with the following four steps, which we will explain in detail below:

(1) If P is hollow and contains a "long" segment, then P projects onto a hollow polytope.
(2) If P has "many" lattice points, then P contains a long segment.
(3) If P is hollow and does not project, then there are lattice polytopes $P \subseteq P' \subset P''$ so that P' is hollow, P'' is not hollow, but $\operatorname{int} P'' \cap \mathbb{Z}^d \subset P'$.
(4) $\operatorname{nvol}_{\mathbb{Z}^d} P \leq \operatorname{nvol}_{\mathbb{Z}^d} P'' \leq V(d, |P' \cap \mathbb{Z}^d|)$ which is bounded, since by (2) and (3) the number of lattice points of P' as a non-projectable polytope is bounded.

Step 1: For the first step we need the following lemma.

Lemma 4.48 *Let $Q \subset \mathbb{R}^d$ be a lattice polytope with interior lattice points, and let $\bar{v} \in \partial Q \cap \mathbb{Z}^d$. Then there is a lattice simplex $S \subseteq Q$ with $\bar{v} \in \mathcal{V}(S)$ and $|\operatorname{relint} S \cap \mathbb{Z}^d| = 1$.*

The cross polytope shows that we cannot assume that S is full-dimensional (see Figure 4.19).

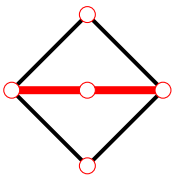


Fig. 4.19: The simplex in Lemma 4.48 may be low-dimensional

Proof. Consider

$$\mathscr{F} := \{R \subseteq Q \text{ lattice polytope} : \bar{v} \in R, R \text{ not hollow}\}.$$

Then $\mathscr{F}$ is a finite non-empty family of lattice polytopes. Hence, there is an inclusion-minimal element $R \in \mathscr{F}$. We claim that R satisfies the assertion of the lemma. As $R \in \mathscr{F}$, there is a relative interior lattice point w.

First, let us prove that R must be a simplex. The line through $\bar{v}$ and w intersects P in a segment $\operatorname{conv}(\bar{v}, \underline{v})$. Let F be the face of Q which contains $\underline{v}$ in its relative interior. Because $w \in \operatorname{relint}(\operatorname{conv}(\bar{v}, F))$ and R is minimal, we must have $R = \operatorname{conv}(\bar{v}, F)$. Also, if F was not a simplex, the carrier of $\underline{v}$ in a triangulation of F would be a proper subpolytope $F' \subset F$ containing $\underline{v}$ in its relative interior – again, contradicting minimality of R.

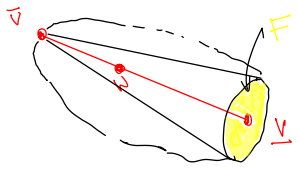


Fig. 4.20: R is a pyramid with apex $\bar{v}$

Next, let us show that $\operatorname{relint}(R) \cap \mathbb{Z}^d = \{w\}$. We can assume that among all lattice points in $\operatorname{relint}(R)$ w has minimal barycentric $\bar{v}$-coordinate. Denote the vertices of F by $v_1, \ldots, v_r$, and set

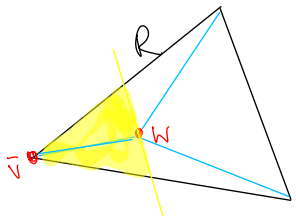


Fig. 4.21: Triangulation of R and the region of all points having larger barycentric $\bar{v}$-coordinate than w

$F_i := \mathcal{V}(F) \setminus \{i\}$ for $i = 1, \dots, r$. The simplices $S_0 := \operatorname{conv}(w, F)$, $S_i := \operatorname{conv}(\bar{v}, w, F_i)$ $(i = 1, \dots, r)$ together with all their faces triangulate R.

A face of this triangulation meets $\operatorname{relint}(R)$ if and only if it contains w. If such a face also contains $\bar{v}$, it cannot contain relative interior lattice points because R was minimal. If it does not contain $\bar{v}$, it is a face of S_0, and all points in S_0 have smaller barycentric $\bar{v}$-coordinate than w. □

With this tool at hand, we can establish the first step.

Lemma 4.49 *Let $P \subset \mathbb{R}^d$ be hollow, $u \in \mathbb{Z}^d$ primitive and $v \in P \cap \mathbb{Z}^d$ so that $v + Nu \in P$ for some $N > \operatorname{sbc}(d-1, 1)^{-1}$.*

Consider the projection $\pi \colon \mathbb{R}^d \to \mathbb{R}^d/\mathbb{R}u$. Then $Q := \pi(P)$ is hollow with respect to $\pi(\mathbb{Z}^d) = \mathbb{Z}^d/\mathbb{Z}u$.

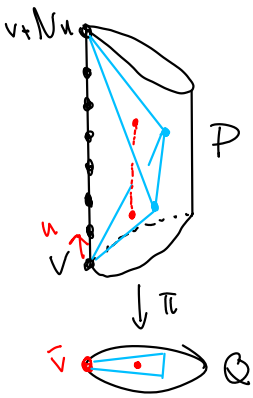


Fig. 4.22: A long edge and a one-point-simplex

Proof. If Q had interior lattice points, according to Lemma 4.48, there would be a simplex $S \subseteq Q$ so that $\bar{v} := \pi(v) \in \mathcal{V}(S)$, and $\operatorname{relint}(S) \cap \mathbb{Z}^d/\mathbb{Z}u = \{w\}$.

If α is the barycentric $\bar{v}$-coordinate of w in S, then the length of the segment $\pi^{-1}(w) \cap P$ is at least $\alpha N \geq \operatorname{sbc}(\dim S, 1)N \geq \operatorname{sbc}(d-1, 1)N > 1$. Therefore, this segment must contain an interior lattice point of P in contradiction to P being hollow. □

Step 2:

Lemma 4.50 *Let $P \subset \mathbb{R}^d$ be a lattice polytope. If $|P \cap \mathbb{Z}^d| > N^d$, then P contains a segment of length N.*

Proof. compare "Rabinowitzs Lemma" [arXiv:1103.0103 Zhong §2]

There must be two different points $v, v' \in P \cap \mathbb{Z}^d$ whose coordinates agree mod N. Then $u := \frac{1}{N}(v - v') \in \mathbb{Z}^d$ and $v, v' = v + Nu \in P$. □

Step 3:

Lemma 4.51 *Suppose the hollow polytope P does not allow a hollow projection. Then there are lattice polytopes $P \subseteq P' \subset P''$ so that P' is hollow, P'' is not hollow, but $\operatorname{int} P'' \cap \mathbb{Z}^d \subset P'$.*

Proof. If there is no $v_1 \in \mathbb{Z}^d \setminus P$ so that $P_1 := \operatorname{conv}(P, v_1)$ is hollow, set $P' := P$. Otherwise, construct recursively hollow polytopes $P_{i+1} := \operatorname{conv}(P_i, v_{i+1})$ until no such extension is possible. The process has to terminate because superpolytopes of non-projectable polytopes are non-projectable and the total number of lattice points is bounded by Lemmas 4.49 and 4.50. Let P' be that last, non-extendable hollow polytope in the sequence.

Now choose $v^1 \in \mathbb{Z}^d \setminus P'$ and set $P^1 := \operatorname{conv}(v^1, P')$. Because P' is non-extendable, P^1 is not hollow. If there is no $v^2 \in \operatorname{int} P^1 \cap$

$\mathbb{Z}^d \setminus P'$, choose $P'' := P^1$. Otherwise, construct recursively $P^{i+1} := \operatorname{conv}(v^{i+1}, P')$ with $v^{i+1} \in \operatorname{int} P^i \cap \mathbb{Z}^d \setminus P'$. The process has to terminate because there are only finitely many lattice points in $P^1 \setminus P'$. The last polytope P'' in this series will be a strict superpolytope of P' and as such not hollow. But, being the last in the series, we have $\operatorname{int} P'' \cap \mathbb{Z}^d \subset P'$. □

Step 4: Let $P \subseteq P' \subset P''$ be as in Lemma 4.51. Then P'' is not hollow and $|\operatorname{int} P'' \cap \mathbb{Z}^d| \leq |P' \cap \mathbb{Z}^d| \leq \operatorname{sbc}(d-1,1)^{-d}$. This holds again, since otherwise by Lemma 4.50 and Lemma 4.49, P' and thus P were projectable.

Now the Theorem 4.25 from the previous section kicks in: $\operatorname{nvol}_{\mathbb{Z}^d} P \leq \operatorname{nvol}_{\mathbb{Z}^d} P'' \leq V(d, \operatorname{sbc}(d-1,1)^{-d})$ is bounded. Then the number of possible equivalence classes for P is finite by Corollary 2.83.

This finially proves Theorem 4.47.

We say a hollow lattice polytope P is *inclusion-maximal* if it is not strictly contained in a hollow lattice polytope.

Corollary 4.52 *There exist only finitely many inclusion-maximal hollow lattice d-polytopes (up to unimodular equivalence). Moreover, any hollow lattice d-polytope that does not admit a hollow projection is contained in an inclusion-maximal hollow lattice d-polytope.*

Proof. If a lattice polytope admits a lattice projection onto a hollow lattice polytope of smaller dimension (not a point), then it is clearly contained in a larger lattice polytope that also projects onto the same lattice polytope, hence, is also hollow. Therefore, inclusion-maximal hollow lattice polytopes do not admit hollow projections, hence, they are only finitely many of these by Theorem 4.47.

Iif a hollow lattice polytope P is not contained in any inclusion-maximal hollow lattice polytope, then there exists an infinite chain of hollow lattice polytopes containing P. In particular, Theorem 4.47 there is a hollow lattice polytope $P' \supset P$ that admits a hollow projection, hence, P does. □

We can now easily deduce the flatness theorem for hollow lattice polytopes. For this we simply note that under lattice projection the width cannot decrease (Exercise 4.31). Exercise 4.31

Corollary 4.53 *The maximal width of a hollow lattice d-polytope equals the maximal width of the finitely many (up to unimodular equivalence) inclusion-maximal lattice d'-polytopes with $d' = 1, \ldots, d$. Moreover, there are only finitely many hollow lattice d-polytopes whose width is strictly larger than the maximal width of hollow lattice $(d-1)$-polytopes.*

4.8 Problems

Exercise 4.32

included on page 100

4.1. Let $K \subseteq \mathbb{R}^d$ be a centrally symmetric convex body with $\operatorname{int}(K) \cap \mathbb{Z}^d = \{0\}$ and $\operatorname{nvol}_{\mathbb{Z}^d}(K) = 2^d$. Show that K is a polytope and each facet of K contains at least one lattice point in its relative interior.

Hint: For any lattice point x choose a half space H_x containing both x and K. Let $S_x := H_x \cap -H_x$. Now consider the intersection of all S_x and prove that this satisfies the assumptions of Minkowski's First Theorem (Corollary 4.3).

included on page 100

4.2. Let $K \subseteq \mathbb{R}^d$ be a centrally symmetric polytope with $\operatorname{int}(K) \cap \mathbb{Z}^d = \{0\}$. Show that K has at most $2(2^d - 1)$ containing a lattice point in their relative interior.

Hint: Choose lattice points in the interior of facets. Consider their coordinates module 3 (*i.e.*, their image under $\mathbb{Z}^d \to (\mathbb{Z}/3\mathbb{Z})^d$). Look at the difference of two points having the same image and use the pidgen-hole principle.

included on page 102

4.3. Prove that the unit ball in dimension d has volume

$$\mathrm{V_d} := \frac{\pi^{\lfloor d/2 \rfloor} 2^{\lceil d/2 \rceil}}{\prod_{0 \le 2i \le d}(d - 2i)}.$$

included on page 105

4.4. Show that the packing radius is finite and equals half of the length of a shortest non-zero lattice vector.

included on page 105

4.5. Let Λ be a lattice in $\mathbb{R}^d$. Show that there is a non-zero $x \in \Lambda$ such that

$$\|x\|_\infty \;\le\; (\det \Lambda)^{1/d}],.$$

included on page 105

4.6. Let $\Lambda_0 \subseteq \Lambda \subseteq \mathbb{R}^d$ be lattices. Show that

$$\varrho(\Lambda) \;\le\; \varrho(\Lambda_0) \;\le\; \left|\Lambda/\Lambda_0\right| \varrho(\Lambda).$$

included on page 106

4.7. Prove

(1) $\mu(\mathbb{Z}^d) = \sqrt{d}/2$
(2) $\mu(D_3) = 1$
(3) $\mu(D_n) = \sqrt{n}/2$ for $n \ge 4$
(4) $\mu(E_8) = 1$

included on page 108

4.8. Show that in the definition of lattice width we can replace the infimum with a minimum for a full-dimensional convex body K. Thus, the width is strictly positive.

4.9. Show that the lattice width of a low dimensional convex body is 0.

4.10. Let $x \in {}^{\circ}\Delta_d{}^d$ as in § 4.4.1. Define $x_0 := 1 - \sum_{i=1}^d x_i$. Prove that $[x] \in \mathscr{M}_i^d$ if and only if

$$\left\{ k \in \mathbb{Z}_{\geq 1} \ : \ \sum_{i=0}^{d} \{kx_i\} = 1 \text{ and } \{kx_i\} > 0 \, \forall \, i = 0, \ldots, d \right\}$$

has at most i elements. Here $\{\cdot\}$ denotes the fractional part in $[0, 1)$.

included on page 113

4.11. (1) Compute $\mathrm{sbc}(2, i)$
(2) $\mathrm{sbc}(d+1, i) \leq 1/2 \, \mathrm{sbc}(d, i)$,
(3) $\mathrm{sbc}(d, i) \leq 1/i 2^{-2^{d-2}}$ using Kahn-Wills-Zaks simplices

For a solution see page 221

included on page 114

4.12. Prove that $\mathrm{sbc}(d+1, i) \leq \mathrm{sbc}(d, i)/2$ for $d, i \geq 1$.
Hint: Let S be a d-simplex with vertices $v_0, \ldots, v_d$ and interior lattice point $x = \sum \lambda_i v_i$ realizing $\mathrm{sbc}(d, i)$ such that $\lambda_d = \mathrm{sbc}(d, i)$. Consider the $(d+1)$-simplex with vertices $(v_i, 0)$ for $0 \leq i \leq d-1$ and $(v_d, \pm 1)$.

included on page 114

***4.13. Prove Lemma 4.35.

For a solution see page 221

included on page 114

4.14. Prove Corollary 4.36.

included on page 114

4.15. Show that the coefficient of asymmetry of an interior point of a d-simplex equals at least d, with equality only for the centroid.

included on page 114

4.16. Let K, K' d-dimensional convex bodies satisfying

$$K' \ \subseteq \ K \ \subseteq \ \mu K' + v$$

for some $\mu > 0, v \in \mathbb{R}^d$.
Show that we have for all $w \in \mathrm{int}\,(K')$

$$\mathrm{ca}(K; w) \ \leq \ \mu \, \mathrm{ca}(K'; w) + \mu - 1 \, .$$

included on page 114

4.17. Prove Lemma 4.37.

included on page 115

4.18. Prove the the bound in Proposition 4.38 is tight.

included on p

4.19. Let $(a_i)_i \geq 1$ be the Sylvester sequence given by

$$a_1 := 2 \qquad \text{and} \qquad a_i := \prod_{j=1}^{i-1} a_j + 1 \quad \text{for } i \geq 2\,.$$

Prove that

(1) for $d \geq 1$ we have $1 - \sum_{i=j}^{d} \frac{1}{a_j} = \left(\prod_{j=1}^{d} a_j\right)^{-1}$

(2) for $d \geq 4$ we have $\prod_{i=1}^{d} a_i \geq 2^{2^{d-a}}$ for a constant $a \approx 0.5856\ldots$.

included on page 116

4.20. Let S_i^d be the Sylvester simplex, l its number of lattice points and $x \in \mathbb{R}$. Show that, if the translate S_i^d has l lattices points then $x \in \mathbb{Z}^d$.

Hint: Show that if one of the facets parallel to a coordinate hyperplane does not contain a lattice point then you can translate the simplex so that it does, while the number of lattice points does not decrease.

included on page 116

4.21. Let P be a lattice polytope and C_d the unit cube. Show that

$$\operatorname{vol}(P) = \int_{C_d} |(P+t) \cap \mathbb{Z}^n|\, dt\,.$$

included on page 116

4.22. recursively we define

$$t_1 := 2, \qquad t_n := 1 + \prod_{j=1}^{n-1} t_j \qquad \text{for} \qquad n \geq 2\,.$$

Show that

(1) $t_n = t_{n-1}^2 - t_{n-1} + 1$ for $n \geq 2$.

(2) $\sum_{j=1}^{n-1} \frac{1}{t_j} = 1 - \frac{1}{t_n - 1}$ for $n \geq 2$.

(3) $2^{2^{n-1}} \geq t_n \geq 2^{2^{n-2}}$.

4.22. let $d, i \in \mathbb{Z}_{\geq 1}$. Define the d-dimensional lattice simplex $S_{d,i}$ mit vertices $v_0, \ldots, v_d$:

$$v_0 := 0, \quad v_j := t_j e_j \quad \text{for} \quad j = 1, \ldots, d-1, \quad v_d := (i+1)(t_d - 1)e_d\,.$$

Show that

$$\operatorname{int}(S_{d,i}) \cap \mathbb{Z}^d = \{(1, 1, \ldots, 1, j) : j = 1, \ldots, i\}\,.$$

and compute the volue (which is conjectured to be the largest possible for dimensions $d \geq 4$).

Hint: Consider barycentric coordinates $(\alpha_0, \ldots, \alpha_d)$ and show by induction $\alpha_j = \frac{1}{t_j}$ for $j = 1, \ldots, d-1$.

4.23. Prove the low dimensional cases in Theorem 4.41.

4.24. Show that Δ_2 and $[0,1]^2$ are up to unimodular equivalence the only empty lattice polygons.

included on page 119

4.25. Verify the inequality description in the proof of Scarf's criterion (Lemma 4.45).

included on page 120

4.26. Show that multiplying with a element coprime to D in $\mathbb{Z}$ induces a group automorphism of $\mathbb{Z}/D\mathbb{Z}$.

included on page 120

4.27. Check the equivalent descriptions of a jump in the second part of the proof of Theorem of White (Theorem 4.44).

included on page 122

4.28. Show, using the table in the proof of the Theorem of White (Theorem 4.44) that T is not empty for $(a_1, a_2, a_3) = (3, 4, 5)$.

included on page 122

4.29. Use the proof of the Theorem of White (Theorem 4.44) to show the following: Let P be an empty lattice tetrahedron with one vertex in the origin. Then the subgroup (or sublattice) of $\mathbb{Z}^3$ that is spanned by the vertices of P is a cyclic quotiont group.

included on page 122

4.30. Find a d-dimensional lattice simplex in $\mathbb{R}^d$ without interior points and lattice width larger than d.

included on page 125

4.31. Prove that projection cannot decrease the width of a convex body.

included on page 126

4.32. Show that $\sum_{i=0}^{d} k^2 = \binom{d+2}{3} + \binom{d+1}{3}$

Hint: You should try to do this via Ehrhart Theory. Consider a $(d-1)$-fold pyramid over a square.

Minkowski meets Ehrhart

5

Contents

5.1 Lattice Polytopes of given h^*-Polynomial

5.1.1 Introduction

With regard to the fundamental results in Ehrhart theory we have seen in Chapter 3 that the Ehrhart polynomial can be more compactly encoded in terms of the $h^\star$-polynomial. In this section, we will give a qualitative answer to the following natural question: how many lattice polytopes have the same $h^\star$-polynomial? In other words, how much information is contained in this polynomial, and to which extent does it determine the polytope? We start with some general observations. Let P be a d-dimensional lattice polytope.

Fig. 5.1: Two lattice polytopes with the same $h^\star$-polynomial $1 + 3t$

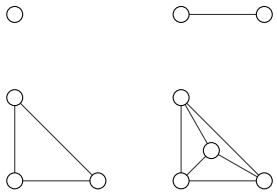


Fig. 5.2: Unimodular simplices in dimensions $0, 1, 2$ and 3

(1) The sum over the coefficients of its $h^\star$-polynomial equals the (normalized) volume of P. Since, by Theorem 3.32, all the coefficients are non-negative integers, the question about the number of lattice polytopes with the same $h^\star$-polynomial is essentially equivalent to the problem of finding all lattice polytopes with given normalized volume and degree (of the $h^\star$-polynomial).
(2) The simplest $h^\star$-polynomial consists only of the constant coefficient 1. In this case, P has normalized volume 1, so it is a unimodular simplex (of arbitrary dimension).
(3) More generally, lattice pyramids with base P have the same $h^\star$-polynomial as P, see Exercise 3.30. Therefore, it makes sense to consider lattice polytopes 'modulo' lattice pyramid constructions. For instance, one may think of unimodular simplices as (successive) lattice pyramids over a point, see Figure 5.2. In this respect, the degree $\deg(P)$ seems to be a more natural invariant to consider than the dimension of a lattice polytope.
(4) It is also insightful to recall that not only the volume but any coefficient of the $h^\star$-polynomial behaves monotonically with respect to inclusions: $Q \subseteq P \implies h_i^\star(Q) \leq h_i^\star(P)$ for any i. In particular, $\deg(Q) \leq \deg(P)$.

Here is the main result of this section. Let us define the function

$$f(c, s) \;:=\; c(2s+1) + 4s - 2\,.$$

Theorem 5.1 (Pyramid theorem) *Let P be a d-dimensional lattice polytope of degree $s := \deg(P)$. If*

$$d \;>\; f(|\mathcal{V}(P)| - d - 1, s)$$

then P is a (possibly successive) lattice pyramid over a lattice polytope of dimension $\leq f(|\mathcal{V}(P)| - d - 1, s)$.

The proof will be given in the next two subsections. From this result we get the desired finiteness result. We note an important consequence of this theorem.

Corollary 5.2 *There are (up to lattice pyramid constructions) only finitely many lattice polytopes of given $h^\star$-polynomial.*

Proof. Note that $h_1^\star(P) = |P \cap \mathbb{Z}^d| - (d+1) \geq |\mathcal{V}(P)| - d - 1$ for any d-dimensional lattice polytope. Let s be the degree of the given polynomial and c its linear coefficient. Therefore, by the pyramid theorem it suffices to prove the theorem for lattice polytopes up to dimension $f(c, s)$. However, in fixed dimension there is only a finite number of lattice polytopes of given normalized volume by Corollary 2.83. □

5.1.2 The pyramid theorem for lattice simplices

We will first consider the situation where P is a d-dimensional lattice simplex of degree $s := \deg(P)$ embedded in $\mathbb{R}^{d+1}$ as $P \times 1$. In this case $|\mathcal{V}(P)| - d - 1 = 0$, so it remains to show that P is a lattice pyramid, if $d \geq 4s - 1$. Let $v_1, \ldots, v_d$ be the vertices of P. Let m be a point in the half-open fundamental parallelepiped $\Pi(P)$ given as $m = \sum_{i=0}^{d} \lambda_i v_i$. Then we define the *support* of m as

$$\operatorname{supp} m := \{i \ : \ \lambda_i \neq 0\}$$

and the height of m as

$$\operatorname{ht}(m) := \sum_{i=0}^{d} \lambda_i .$$

Note that $\operatorname{ht}(m)$ is a non-negative integer.

We will need a criterion how to check whether a lattice simplex is a lattice pyramid. For this, let us define the *support* of the simplex as

$$\operatorname{supp} P \ := \bigcup_{m \in \Pi \cap \mathbb{Z}^{d+1}} \operatorname{supp} m \, .$$

The proof of the following observation is left as Exercise 5.1. Exercise 5.1

Lemma 5.3 *P is a lattice pyramid with apex v_i for some $i \in \{0, \ldots, d+1\}$ if and only if $i \notin \operatorname{supp} P$.* □

In other words, if the support of P is a proper subset of $\{0, \ldots, d+1\}$, then P is a (successive) lattice pyramid over the convex hull $\operatorname{conv}(v_i \ : \ i \in \operatorname{supp} P)$ of those vertices that are contained in the support. Hence, to prove the theorem for simplices we have to show that for any lattice simplex of degree s its support is bounded by $4s - 1$, *i.e.*

$$|\operatorname{supp} P| \ \leq \ 4s - 1 \, .$$

Let us first bound the support of one lattice point in $\Pi(P)$.

Lemma 5.4 *Let $m \in \Pi(P) \cap \mathbb{Z}^{d+1}$. Then*

$$\operatorname{supp} m \ \leq \ 2s \, .$$

Proof. We define

$$m^\star \ := \sum_{i \in \operatorname{supp} m} (1 - \lambda_i) v_i \ = \left(\sum_{i \in \operatorname{supp} m} v_i \right) - m \, .$$

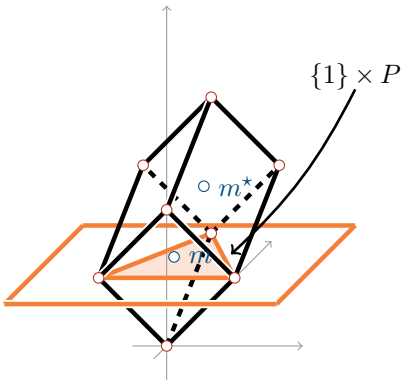


Fig. 5.3: The central symmetry $m \leftrightarrow m^\star$ about the 'green' center of $\Pi(P)$

Then $m^\star \in \Pi(P) \cap \mathbb{Z}^{d+1}$. We observe

$$|\operatorname{supp} m| \;=\; \operatorname{ht}\left(\sum_{i\in\operatorname{supp} m} v_i\right) = \operatorname{ht}(m+m^\star) \;=\; \operatorname{ht}(m)+\operatorname{ht}(m)\;.$$

By Proposition 3.19, $h_i^\star(P) = |\{\operatorname{ht}(x) \,:\, x \in \Pi \cap \mathbb{Z}^{d+1}\}|$, in particular, $\operatorname{ht}(m), \operatorname{ht}(m^\star) \le s$. □

Here is another proof, which uses the notion of the codegree (see Definition 3.47 and Corollary 3.48).

Proof (Alternative proof). Let $P' := \operatorname{conv}(v_i \,:\, i \in \operatorname{supp} m)$. By the monotonicity theorem, $\deg(P') \le s$. Now, $m \in \operatorname{int}(\operatorname{ht}(m)P') \cap \mathbb{Z}^{d+1}$, hence, $\operatorname{codeg}(P') \le \operatorname{ht}(m) \le s$, again by Proposition 3.19. Therefore, $|\operatorname{supp} P'| = \dim(P')+1 = \operatorname{codeg}(P')+\deg(P') \le 2s$. □

Let us choose $m^0 \in \Pi(P) \cap \mathbb{Z}^{d+1}$ whose support $I_0 := \operatorname{supp} m^0$ has the maximal possible number of elements (at most $2s$). Now, we consecutively define a 'greedy' sequence $\{m\}_{k=0,\dots,r}$ of lattice points in $\Pi(P)$ such that the size of each set

$$I_k := \left(\operatorname{supp} m^k\right) \setminus \bigcup_{j<k} \operatorname{supp} m^j$$

is maximal. Note that the support of P is completely covered by these disjoint sets I_k's.

Lemma 5.5 *For $k = 1, \dots, r$, we have*

$$|I_k| \;\le\; |I_{k-1}|/2\,.$$

In particular,

$$|I_k| \;\le\; |I_0|/2^k\,.$$

Proof. The following arguments are illustrated in Figure 5.4. Let us define

$$a \;:=\; |I_{k-1}\setminus \operatorname{supp} m^k|\,,\quad b \;:=\; |I_{k-1}\cap \operatorname{supp} m^k|\,,\quad \text{and}\quad c \;:=\; |I_k|\,.$$

Note that $|I_{k-1}| = a+b$. By the greedy choice of m^{k-1}, we necessarily have $b+c \le |I_{k-1}|$, so

$$c \;\le\; a. \tag{5.1}$$

Let us write

$$m^k \;=\; \sum_{i=0}^{d} \lambda_i^k v_i \,.$$

Recall that any real number $x \in \mathbb{R}$ can be written as $x = k + \{x\}$ for $k \in \mathbb{Z}$ and $\{x\} \in [0,1)$. In this notation, we define

$$u \;:=\; \left\{ m^k + m^{k-1} \right\} \;:=\; \sum_{i=0}^{d} \left\{ \lambda_i^k + \lambda_i^{k-1} \right\} v_i \,.$$

Note that $u \in \Pi(P) \cap \mathbb{Z}^{d+1}$. Since,

$$\left(\operatorname{supp} m^{k-1} \cup \operatorname{supp} m^k \right) \setminus \left(\operatorname{supp} m^{k-1} \cap \operatorname{supp} m^k \right) \;\subseteq\; \operatorname{supp} u \,,$$

the 'greediness' of m^{k-1} again implies that $a + c \le a + b$, so $c \le b$. Together with (5.1) this implies

$$|I_k| \;=\; c \le \frac{a+b}{2} \;=\; |I_{k-1}|/2 \,. \qquad \square$$

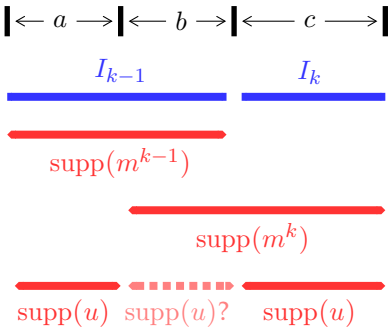


Fig. 5.4: A schematic view on $I_{k-1} \cup I_k$

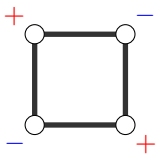
For our lattice simplex P we can now compute

$$\begin{aligned} |\operatorname{supp} P| \;&=\; \sum_{k=0}^{r} |I_k| \;\le\; \left(\sum_{k=0}^{r} \frac{1}{2^r} \right) |I_0| \\ &<\; \left(\sum_{k=0}^{\infty} \frac{1}{2^r} \right) |I_0| \;=\; 2 \cdot |I_0| \,. \end{aligned}$$

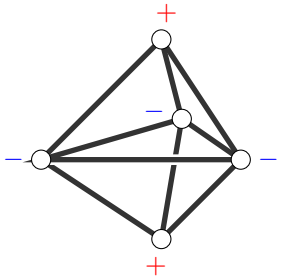
So Lemma 5.4 shows the desired statement

$$|\operatorname{supp} P| \;<\; 4s \,.$$

This finished the proof of Theorem 5.1 in the case of lattice simplices.



(a) Circuit in a square



(b) Circuit in a triangle bipyramid

Fig. 5.5: A two-dimensional and a three-dimensional circuit

5.1.3 Proof of the pyramid theorem

In order to deal with general lattice polytopes, we need the important notion of circuits.

Definition 5.6 *A* circuit $A \subset \mathbb{R}^d$ *is a minimal affinely dependent subset, i.e., A itself is affinely dependent, while any proper subset is affinely independent.*

Here are some facts about circuits A (Exercise 5.2):

- The dimension of the convex hull of a circuit A equals $|A| - 2$.
- There is an (up to scalar multiplication) unique affine relation

$$\sum_{v \in A} \lambda_v \, v \;=\; 0 \qquad\qquad \sum_{v \in A} \lambda_v \;=\; 1 \,,$$

  where $\lambda_v \neq 0$ for any $v \in A$.

Exercise 5.2

- The previous relation yields a partition of A into two non-empty subsets A_+, A_- depending on the signs of the corresponding λ_v. Note that the convex hull of the elements in A_+ (respectively, in A_-) is not contained in the boundary of $\operatorname{conv}(A)$.

Here is the crucial observation:

Lemma 5.7 *Let C be the convex hull of a circuit A. Then*

$$|A| \;\leq\; 2\deg(C) + 2\,.$$

Proof. As observed above, the sum of the lattice points in A_+ is a lattice point in the interior of $|A_+|C$. Therefore,

$$\begin{aligned} |A_+| \;&\geq\; \operatorname{codeg}(C) \\ &=\; \dim(C) + 1 - \deg(C) \\ &=\; (|A_+| + |A_-| - 2) + 1 - \deg(C)\,. \end{aligned}$$

This implies $|A_-| \leq \deg(C) + 1$. The same bound also holds for $|A_+|$. □

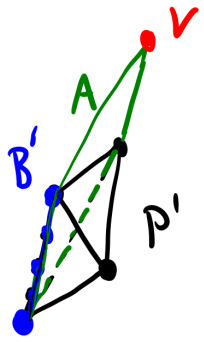


Fig. 5.6: The induction step

We are now in the position to finish the proof.

Proof (Proof of Theorem 5.1 in the general case). Let $c := |\mathcal{V}(P) - d - 1|$. We prove the statement by induction on c. The case $c = 0$ was dealt with in the previous section. So, we may assume $c > 0$, and $d > f(c,s) = c(2s+1) + 4s - 1$. Since P is not a simplex, there exists a vertex v such that $P' := \operatorname{conv}(\mathcal{V}(P)\backslash\{v\})$ is d-dimensional (see Exercise 5.3). Note that $|\mathcal{V}(P')| - \dim(P') - 1 < c$ by construction, and $\deg(P') \leq s$ by the monotonicity theorem. Hence, the induction hypothesis yields that P' is a (possibly successive) lattice pyramid over a lattice polytope B' of dimension

$$\begin{aligned} \dim B' \;&\leq\; f(|\mathcal{V}(P')| - d - 1, \deg(P')) \\ &\leq\; (c-1)(2s+1) + 4s - 1\,. \end{aligned}$$

Since $v \in \operatorname{aff}(P')$, there exists a circuit A among $v \cup \mathcal{V}(P')$ which contains v, see also Figure 5.6. By the monotonicity theorem and Lemma 5.7, $|A| \leq 2s + 2$. We define B as the convex hull of the vertices of B' and the elements in A. Since $v \in \operatorname{aff}(A\backslash v)$, we compute

$$\begin{aligned} \dim(B) \;&\leq\; \dim(B') + |A| - 1 \\ &\leq\; (c-1)(2s+1) + 4s - 1 + 2s + 1 \;=\; f(c,s)\,. \end{aligned}$$

Since $v \in B$, P is a lattice pyramid over B, as desired. □

Exercise 5.3

5.2 Lattice polytopes of small degree

In the last section of this chapter we explain a construction of high-dimensional lattice polytopes of small degree. We will state a general result that shows that any lattice polytope of small degree is given this way. As an application in Ehrhart theory, we prove a finiteness result generalizing the finiteness of lattice polytopes with a given non-zero number of interior lattice points.

5.2.1 Cayley-Polytopes

For this, we will need the notion of a *Cayley polytope*.

Definition 5.8 *Given lattice polytopes $P_0, \dots, P_t$ in $\mathbb{R}^k$, the* Cayley sum *is defined as*

$$P_0 * \cdots * P_t \;:=\; \operatorname{conv}((P_0 \times 0) \cup (P_1 \times e_1) \cdots \cup (P_t \times e_t)) \subset \mathbb{R}^k \times \mathbb{R}^t\,,$$

where $e_1, \dots, e_t$ denotes the standard lattice basis of $\mathbb{R}^t$.

We say $P \subseteq \mathbb{R}^d$ is a Cayley polytope of length $t+1$ *if there exists an affine lattice basis of $\mathbb{Z}^d \cong \mathbb{Z}^k \times \mathbb{Z}^t$ identifying P with the Cayley sum $P_0 * \cdots * P_t$ for some lattice polytopes $P_0, \dots, P_t$ in $\mathbb{R}^k$. Let us note that*

$$\dim(P_0 * \cdots * P_t) \;=\; \dim \operatorname{aff}(P_0, \dots, P_t) + t - 1\,.$$

There is a convenient and useful characterization of Cayley polytopes.

Lemma 5.9 ([7, Proposition 2.3]) *Let us define $u \in (\mathbb{Z}^{d+1})^*$ such that $\langle u, \{1\} \times P \rangle = 1$. Let C be the cone over $\{1\} \times P$. Then the following statements are equivalent:*

(1) P is a Cayley polytope $P_0 * \cdots * P_t$ of length $t+1$
(2) There is a lattice projection P onto a unimodular t-simplex
(3) There are nonzero $x_0, \dots, x_t \in C^\star \cap (\mathbb{Z}^{d+1})^*$ such that

$$x_0 + \cdots + x_t = u$$

Proof. (1) $\Rightarrow$ (2): The definition of a Cayley polytope implies the existence of a surjective lattice homomorphism $\mathbb{Z}^d \to Z^t$, mapping the vertices of P onto $\{0, e_1, \dots, e_t\}$.

(2) $\Rightarrow$ (1): This follows also directly from the definition.

(1) $\Rightarrow$ (3): In Definition 5.8, let $b_1, \dots, b_d, e_1, \dots, e_t$ be the standard basis of $\mathbb{Z}^d$, and $b_1^*, \dots, b_d^*, e_1^*, \dots, e_t^*$ its dual lattice basis. As

$u = (1, 0, \ldots, 0)$, setting $x_i := (0, e_i^*)$ for $i = 1, \ldots, t$ and $x_0 := (1, -e_1^* - \cdots - e_t^*)$ satisfies the desired conditions.

(3) $\Rightarrow$ (2): Let us define

$$\begin{aligned} \varphi : \mathbb{Z}^d &\to \mathbb{Z}^{t+1} \\ m &\mapsto (\langle x_0, m \rangle, \ldots, \langle x_t, m \rangle) \end{aligned}$$

Let $v \in \mathcal{V}(P)$. Then

$$\sum_{i=0}^{t} \langle x_i, v \rangle = \langle w^\vee, v \rangle \;=\; 1\,.$$

Since, $\langle x_i, v \rangle \geq 0$ for $i = 0, \ldots, t$ we see that $\varphi(v) \in \{e_0, \ldots, e_t\}$, where $e_0, \ldots, e_t$ denotes the standard basis of $\mathbb{Z}^{t+1}$. Assume there exists $i \in \{0, \ldots, t\}$ which is not an image of a vertex of P. In this case, we would get $\langle x_i, v \rangle = 0$ for all $v \in \mathcal{V}(P)$, thus, $x_i = 0$, a contradiction. Hence, P projects onto $S := \operatorname{conv}(e_1, \ldots, e_{t+1})$, a unimodular t-simplex (up to unimodular equivalence). □

Since the t-th multiple of a unimodular t-simplex contains no interior lattice points, we conclude from (2) that

$$\operatorname{codeg}(P_0 * \cdots * P_t) \;\geq\; t + 1\,.$$

The following result (which we state without proof) shows that any lattice polytope in high dimensions of small degree decomposes into small-dimensional lattice polytopes.

Theorem 5.10 *Any lattice polytope of degree s is a Cayley polytope of length $\geq d + 1 - (s^2 + 19s - 4)/2$ (equivalently, P is a Cayley polytope of lattice polytopes in dimension $\leq (s^2 + 19s - 4)/2$).*

It is conjectured that $(s^2 + 19s - 4)/2$ can be replaced by a linear function in s. Here is an application in Ehrhart theory.

Theorem 5.11 *There exist only finitely many h^*-polynomials of lattice polytopes of degree s and with given leading coefficient h_s^*.*

This result follows immediately from the following statement combined with Theorem 5.10. Here, let $V(q, k)$ be given as in Theorem 4.25.

Proposition 5.12 *If P is a d-dimensional lattice polytope of degree s that is a Cayley polytope of length $c + 1 \geq d + 1 - N$, then*

$$\operatorname{nvol}_{\mathbb{Z}^d}(P) \leq N!\, N^N\, V(N, h_s^*)^N\,.$$

Proof. We denote by S the unimodular simplex $\Delta_c = \operatorname{conv}(e_0, \ldots, e_c)$, where $e_0 = 0$. Let $d = c + q$ and $\pi : \mathbb{Z}^d = \mathbb{Z}^{c+q} \to \mathbb{Z}^c$ be the projection onto the first c coordinates. For $i = 0, \ldots, c$ we set $P_i \subset \mathbb{R}^q$ such that $e_i \times P_i = \pi^{-1}(e_i) \cap P$.

Set $r = d + 1 - s$, so rP contains exactly $k := h_s^*$ interior lattice points. The interior lattice points in rP are exactly the interior lattice points in $\pi^{-1}(\lambda) \cap rP$, for interior lattice points $\lambda \in rS$. Say $\lambda = (\lambda_1, \ldots, \lambda_c)$ is an interior lattice point of rS such that $\pi^{-1}(\lambda)$ contains an interior lattice point of P. Then $\lambda_1, \ldots, \lambda_c$ and $\lambda_0 = r - \lambda_1 - \cdots - \lambda_c$ are positive integers.

Now, any 'fiber' of π can be identified with a Minkowski sum of $P_0, \ldots, P_c$:

$$\pi^{-1}(\lambda) \cap P \;=\; \lambda \times (\lambda_0 P_0 + \cdots + \lambda_c P_c)\,.$$

Let ω_{ij} be the width of P_j with respect to the i-th coordinate on $\mathbb{R}^q$, the difference between the maximum and the minimum of the i-th coordinates of points in P_j. By Theorem 2.82 there is a choice of coordinates on $\mathbb{R}^q$ such that $\lambda_0 P_0 + \cdots + \lambda_c P_c$ is contained in the standard cube $[0, C]^q$ with the side length C being equal to q times the normalized volume of $\lambda_0 P_0 + \cdots + \lambda_c P_c$. Now, we may choose by Theorem 4.25

$$C \;=\; q\,V(q, k).$$

Since widths are additive and each λ_j is a positive integer, it follows that $\omega_{i0} + \cdots + \omega_{ic} \le C$, for $1 \le i \le q$.

Now P projects onto S, so we can express the normalized volume of P as an integral

$$\operatorname{nvol}_{\mathbb{Z}^d}(P) \;=\; d! \cdot \int_S \operatorname{vol}\left(\pi^{-1}(\lambda) \cap P\right) d\lambda,$$

where vol is the ordinary euclidean volume. The volume of $\pi^{-1}(\lambda) \cap P$ is bounded by the product of its coordinate widths, which is $\prod_{i=1}^{c}(\lambda_0\omega_{i0} + \cdots + \lambda_c\omega_{ic})$. Expanding the product and substituting into the integral above gives

$$\operatorname{nvol}_{\mathbb{Z}^d}(P) \;\le d! \cdot \sum_{j_1,\ldots,j_q} \left(\omega_{1j_1} \cdots \omega_{qj_q} \int_S \lambda_{j_1} \cdots \lambda_{j_q}\, d\lambda\right), \tag{5.2}$$

where the sum is over $(j_1, \ldots, j_q) \in \{0, \ldots, c\}^q$. Now it follows from Hölder's inequality that the integral over S of the monomial $\lambda_{j_1} \cdots \lambda_{j_q}$ is bounded above by the integral of λ_1^q, and a straightforward induction shows that

$$\int_S \lambda_1^q\, d\lambda \;=\; q!/d!.$$

Substituting into (5.2) then gives

$$\mathrm{nvol}_{\mathbb{Z}^d}(P) \;\leq\; q! \cdot \sum_{j_1,\ldots,j_q} (\omega_{1j_1} \cdots \omega_{qj_q}).$$

The sum on the right hand side may be written as $\prod_{i=1}^{q}(\omega_{i0} + \cdots + \omega_{ic})$, which is bounded above by C^q since, for each i, $\omega_{i0} + \cdots + \omega_{ic}$ is less than or equal to C. We conclude that $\mathrm{nvol}_{\mathbb{Z}^d}(P)$ is bounded above by $q! \cdot C^q$. Now the theorem follows, since $q = d - c \leq d - (d - N) = N$. □

TODO: degree one als Bild rein (ohne Beweis)

5.2.2 Small Degree

5.2.3 Normal Form

In many applications, the question arises whether two lattice polytopes P and Q are isomorphic. Of course, isomorphism here means the existence of a unimodular transformation $x \mapsto Ax + b$ for $A \in \mathrm{Gl}_d(\mathbb{Z})$ and $b \in \mathbb{Z}^d$. A brute force way would be to go through all of the finitely many combinatorial isomorphisms between P and Q and check whether the corresponding affine transformations are unimodular. However, given a large list of lattice polytopes this procedure is not feasible. This was the problem faced by Maximilian Kreuzer and Harald Skarke in their large-scale classification of all reflexive polytopes up to dimension four [32, 33] (see § 7.5.2). In this section we present their solution as implemented in the software package PALP [34][1]

Kreuzer and Skarke showed that it is possible to associate to any lattice polytope $P \subset \mathbb{R}^d$ a *normal form*

$$\mathsf{N}(P) \;=\; (w_1 \;\cdots\; w_l) \in \mathrm{Mat}\,\mathbb{Z}d \times l(\mathbb{Z})$$

where l is the number of vertices of P such that $P \cong \mathrm{conv}(w_1, \ldots, w_l)$ and the following property holds:

$$P \cong Q \iff \mathsf{N}(P) \;=\; \mathsf{N}(Q).$$

Hence, any total ordering on the set of integral matrices induces a total ordering on all unimodular equivalence classes of d-dimensional lattice polytopes.

We will describe the various ingredients in this construction step by step. They will also play an important role in the classification algorithm of reflexive polytopes which is described in § 7.5.2.

[1] We remark that there are several choices of such an implementation, and we do not claim that ours is precisely the one used in PALP.

5.2.3.1 Lattice distance

Let us recall the notion of *lattice distance* of a vertex v of a full-dimensional polytope $P \subset \mathbb{R}^d$ from a facet F of P. The hyperplane H spanned by F is given as

$$H = \{x \in \mathbb{R}^d \ : \ \langle \eta_F, x \rangle = b\}$$

for $\eta_F \in (\mathbb{Z}^\star)^d$ a primitive inner normal and $b \in \mathbb{Q}$. Then the *lattice distance* $d(v, F)$ of v from F is defined as $\langle \eta_F, v \rangle - b$. Note that $d(v, F) \geq 0$ with equality if and only if $v \in F$. The lattice distance is illustrated in the following figure:

Here is an equivalent way of viewing these numbers. Define the cone $C(P) := \text{cone}(P \times 1) \subset \mathbb{R}^{d+1}$ over P. Then the rays of the dual cone $C(P)^\star$ are in one-to-one correspondence to facets F of P. Moreover, the ray corresponding to a facet F is generated by a primitive lattice point $u_F \in (\mathbb{Z}^\star)^{d+1})$ such that $u_F = (\eta_F, -b_F)$. Hence, the lattice distance $d(v, F)$ equals $\langle u_F, (v, 1) \rangle$.

Lemma 5.13 *If $P \cong Q$ via an affine unimodular transformation φ, then the lattice distance of a vertex v from a facet F of P equals the lattice distance of the vertex $\varphi(v)$ from the facet $\varphi(F)$ of Q.*

Proof. The statement seems obvious, however, it doesn't hurt to give a detailed proof. Note that $CP \cong CQ$ via a linear unimodular transformation ψ (see Exercise 5.4) such that $\psi((v, 1)) = (\varphi(v), 1)$. Moreover, $C^\star Q \cong C^\star P$ via $\psi^\star$, thus, $u_{\varphi(F)} = (\psi^\star)^{-1}(u_F)$. Hence, $d(\varphi(v), \varphi(F)) = \langle u_{\varphi(F)}, (\varphi(v), 1) \rangle = \langle (\psi^\star)^{-1}(u_F), \psi((v, 1)) \rangle = \langle u_F, (v, 1) \rangle = d(v, F)$. □ □

Exercise 5.4

5.2.3.2 The vertex-pairing matrix

Throughout, we fix a total ordering on the set of integral matrices. We will use the lexicographic ordering, i.e., for a $m \times n$-matrix $\{a_{i,j}\}$ we proceed in this order

$$a_{1,1}, a_{1,2}, \ldots, a_{1,n}, a_{2,1}, a_{2,2}, \ldots, a_{m,n}$$

Let P have the vertex set $\mathcal{V}(P) = \{v_1, \ldots, v_l\}$ (with $|\mathcal{V}(P)| = l$) and the set of facets $\mathcal{F}(P) = \{F_1, \ldots, F_k\}$ with ($|\mathcal{F}(P)| = k$). Then the matrix of vertex-facet lattice distances

$$\{d(v_i, F_j)\}_{i=1,\ldots,l;\ j=1,\ldots,k}$$

is not unique. It depends on the choosen ordering of the vertices and facets of P (corresponding to permuting the rows and columns of the

previous matrix). In order to make it unique, we use our total ordering and define *the vertex-pairing matrix* $\mathrm{VPM}(P)$ of P as the (unique) largest matrix among the set of $l \times k$-matrices obtained in this way.

Note that $\mathrm{VPM}(P)$ encodes the vertex-facet-incidences of P and hence its complete combinatorial structure.

Lemma 5.13 implies

$$P \cong Q \quad \Longrightarrow \quad \mathrm{VPM}(P) = \mathrm{VPM}(Q)\,.$$

It is important to observe that the converse does not hold. The two non-isomorphic lattice polygons in Figure 5.7 have the same vertex-pairing-matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

Fig. 5.7: Two lattice polygons with the same vertex-pairing-matrix

5.2.3.3 The group $\mathrm{Ord}(P)$

We can find an ordering of the set of vertices and facets of P such that

$$\mathrm{VPM}(P) = \{d(v_i, F_j\}_{i=1,\ldots,l;\ j=1,\ldots,k}$$

Of course, there may be several choices how to do so. Let us make this precise. We define $\mathrm{Ord}(P)$ as the set of bijections $\sigma : \{1,\ldots,l\} \to \mathcal{V}(P)$ such that there exists some bijection $\pi : \{1,\ldots,k\} \to \mathcal{F}(P)$ with

$$\mathrm{VPM}(P) = \{d(\sigma(i), \pi(j))\}_{i=1,\ldots,l;\ j=1,\ldots,k}$$

By construction, $\mathrm{Ord}(P)$ only depends on $\mathrm{VPM}(P)$. It is an exercise for the reader to check that

- For each $\sigma \in \mathrm{Ord}(P)$ there is only one such choice for π.
- Identifying $\mathcal{V}(P)$ with $\{1,\ldots,l\}$ realizes $\mathrm{Ord}(P)$ as a subgroup of the full symmetric group on $\{1,\ldots,l\}$.
- Ord is invariant under umimodular equivalence.

In Figure 5.7, $\mathrm{Ord}(P)$ is the full symmetric group with 6 elements. However, $\mathrm{Ord}(P)$ may often be much smaller, see in Figure 5.8.

Fig. 5.8: Lattice triangles with $\mathrm{Ord}(P)$ of size 1, respectively, 2

5.2.3.4 Linear and affine normal forms

For $\sigma \in \mathrm{Ord}(P)$ we define the $d \times l$-matrix

$$A_\sigma := \begin{pmatrix} v_{\sigma(1)} & \cdots & v_{\sigma(l)} \end{pmatrix}.$$

We will need the Hermite normal form theorem for integral matrices in its full generality. For the proof we refer to Exercise ??? .

Theorem 5.14 (General Hermite normal form) *Given a matrix $A \in \mathrm{Mat}_{d\times l}(\mathbb{Z})$ whose column space has full dimension d, there exists a unique unimodular matrix $U \in \mathrm{Gl}_d(\mathbb{Z})$ such that $H := UA$ is in* Hermite normal form*, i.e., there exists an $r \in \{1,\ldots,l\}$ and a strictly increasing function $f\colon \{1,\ldots,d\} \to \{1,\ldots,r\}$ such that for $i = 1,\ldots,d$*

(1) $H_{i,j} = 0$ for $j < f(i)$ and $j > r$
(2) $H_{i,f(i)} > H_{i',f(i)} \geq 0$ for $1 \leq i' < i$

For $\sigma \in \mathrm{Ord}(P)$ let us denote by H_σ the unique matrix UA_σ. Then we define the *linear normal form* $\mathsf{LNF}(P)$ of P as the smallest matrix (with respect to the total ordering) among all H_σ for $\sigma \in \mathrm{Ord}(P)$. By construction, the linear normal form has the property that P and P' are mapped onto each other by a lattice-preserving linear automorphism if and only if $\mathsf{LNF}(P) = \mathsf{LNF}(P')$.

Example 5.15 *Let us consider the triangle P on the left of Figure 5.8. Here,*

$$\mathrm{VPM}(P) = \begin{pmatrix} 6 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

$|\mathrm{Ord}(P)| = 1$*, and for $\sigma \in \mathrm{Ord}(P)$ we have*

$$A_\sigma = \begin{pmatrix} -1 & 2 & -1 \\ -1 & -1 & 1 \end{pmatrix}$$

Therefore,

$$H_\sigma = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 3 & -2 \end{pmatrix}$$

is the linear normal form of P.

Example 5.16 *Let us consider the triangle P on the right of Figure 5.8. Here,*

$$\mathrm{VPM}(P) = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$\mathrm{Ord}(P) = \{\sigma_1, \sigma_2\}$*, and we have*

$$A_{\sigma_1} = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 2 & 2 \end{pmatrix}$$

and

$$A_{\sigma_1} = \begin{pmatrix} 0 & 0 & 1 \\ 2 & -1 & 2 \end{pmatrix}$$

Therefore,

$$H_{\sigma_1} = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$H_{\sigma_2} = \begin{pmatrix} 2 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Hence, H_{σ_1} equals the linear normal form of P.

In order to get the desired affine normal form we apply (5.14) to the $d \times l$-matrix

$$A' := \begin{pmatrix} 0 & v_1 - v_0 & \cdots & v_l - v_0 \end{pmatrix}.$$

This yields a unique matrix $U \in \mathrm{Gl}_d(\mathbb{Z})$ such that UA' is in Hermite normal form. Let us denote for $\sigma \in \mathrm{Ord}(P)$ by H'_σ the unique matrix $U(A_\sigma)'$. Then we define the (affine) *normal form* $\mathsf{N}(P)$ of P as the smallest matrix among all $d \times l$-matrices H'_σ for $\sigma \in \mathrm{Ord}(P)$. By construction, the affine normal form has the desired property that P and P' are mapped onto each other by a lattice-preserving affine automorphism if and only if $\mathsf{N}(P) = \mathsf{N}(P')$.

Example 5.17 *Let us continue with Example 5.15. For the unique $\sigma \in \mathrm{Ord}(P)$ we have*

$$(A_\sigma)' = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

This is already in Hermite normal form, hence

$$H'_\sigma = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

is the affine normal form of P.

Example 5.18 *Let us continue with Example 5.16. Here,* $\mathrm{Ord}(P) = \{\sigma_1, \sigma_2\}$*, and we have*

$$(A_{\sigma_1})' = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 3 & 3 \end{pmatrix}$$

and

$$(A_{\sigma_1})' = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -3 & 0 \end{pmatrix}$$

Therefore,

$$H'_{\sigma_1} = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and

$$H'_{\sigma_2} = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Hence, $H'_{\sigma_1} = H'_{\sigma_2}$ *equals the affine normal form of* P*.*

The reader may wonder whether we really needed $\mathrm{Ord}(P)$ in order to define these normal forms. Indeed, it would have been possible to take the group of all permutations of $\mathcal{V}(P)$. However, in general $\mathrm{Ord}(P)$ is much smaller and therefore computationally more feasible. Moreover, these concepts will be useful when dealing with reflexive polytopes, see Section ???.

5.2.3.5 The algorithm of Kasprzyk and Grinis

See [23]

5.3 Problems

Exercise 5.5

5.1. Prove Lemma 5.3.

included on page 133

5.2. Prove all the basic facts on circuits needed in § 5.1.3.

included on page 135

included on page 136

5.3. 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.

included on page 141

5.4. pb:affine-to-cone

included on page 145

5.5. A dummy exercise.

Short Rational Generating Functions

6

Contents

In Section 4.1 we have shown that any lattice has a non-zero vector of length at most $\sqrt{d}\det\Lambda$. However, the proof was not constructive and we have left open the question how one can actually compute such a vector in polynomial time. We will solve this problem in Section 6.3. This algorithm hinges on the fact that we need to compute a *reduced basis* efficiently. We will give an algorithm for one special reduced basis, the *δ-reduced basis* using the LLL-method in Section 6.4. This will finally give the complete algorithm for counting lattice points. Using this basis algorithm we can also solve the problem of computing a rational generating function for

a cone in polynomial time in fixed dimension, left open in Section 3.3. In Section 6.5 we discuss some improvements of the algorithm. Finally, we will show that we can solve an integer program in polynomial time in fixed dimension.

6.1 Hermite and Smith Normal Forms

Smith normal forms using Kannan and Bachem [29]. See also Gerald Jäger, *A new algorithm for computing the Smith normal form and its implementation on parallel machines*

6.2 Computing Short Rational Generating Functions

In Chapter 3 we have seen that we can express the lattice points in a cone as a rational function. The proof somehow also gives a method to compute such a function by enumerating the lattice points in the fundamental parellelipiped and deriving the appropriate numerator from this. Yet, as we will see below, this is in general not a task that can be done in polynomial time in the size of the input and the dimension. In this section we will develop a different approach using *signed decompositions* of a cone to compute the multivariate rational generating function $\mathsf{G}_P(t)$ of a simplicial cone in polynomial time, at least for fixed dimension. This extends to all cones by using a triangulation without new vertices. We looked at this for polytopes in Theorem 2.35. The same construction works for cones. Note that this construction of a triangulation is polynomial in the size of the input.

The $h^\star$-polynomial, and thus the Ehrhart polynomial can be obtained from the generating function of the cone over the polytope by specializing the rational function at $x = (t, \mathbf{1})$. Similarly, we may count lattice points in a polytope via the generating functions of the vertex cones specialized at $x = \mathbf{1}$, using Brion's Theorem (Theorem 3.67). However, these values are (removable) poles of the generating functions. We will discuss a possible approach to evaluate the functions efficiently in § 6.2.1.

The initial idea for the algorithm presented in this section is due to Barvinok [3] and Barvinok and Pommersheim [6]. For fixed dimension d the algorithm is polynomial in the input size. Practical implementations can be found in the software package `LattE` and its successors `LattE macchiato` and `LattE integrale` [S1, S2] or in `barvinok` [S3, 59]. See Section 6.8 for some examples of computations of short generating functions.

Yet, the algorithm needs Minkowski's First Theorem (Corollary 4.3) to find a short vector in the lattice as a (frequent) intermediate step.

We have already dicussed that its proof as presented in Chapter 4 is not constructive. We solve this in Section 6.3. This in turn relies on a method to obtain a lattice basis that approximates an orthogonal vector space basis, which is the topic of Section 6.4, where we discuss the LLL-algorithm of Arjen Lensta, Hendrik Lensta, and László Lovász. Efficient implentations also use the half open decompositions introduced in § 3.4.1 to get rid of lower dimensional cones in the decomposition or a decomposition of the dual cone to turn lower dimensional cones into cones with lineality. We discuss these improvements in Section 6.5.

In the case of a polytope P, the generating function of the lattice points is actually a *polynomial* (the sum of all monomials for all lattice points in P). Observe however, that we usually cannot write this down in polynomial time in the size of the input, just because there may be more than polynomially many lattice points compared to the number of vertices. Thus, we should not try to expand a rational function to get rid of the poles.

We aim for a polynomial method (in fixed dimension) to compute integer point generating functions of simplicial cones. We theoretically know how to write down the function, the formula is just given by Corollary 3.28. But from an algorithmic point of view this may not be efficient, as its numerator may need too many monomials, compared to the size of the input. An example, which already works in dimension 2, is the following. Consider the cone $C := \operatorname{conv}(e_1, e_1 + ke_2)$ for some $k \in \mathbb{Z}_>$. We need k monomials in the numerator or k cones in a unimodular triangulation, which is not polynomial in the input, which are just the two generators of the cone. See also Figure 6.1

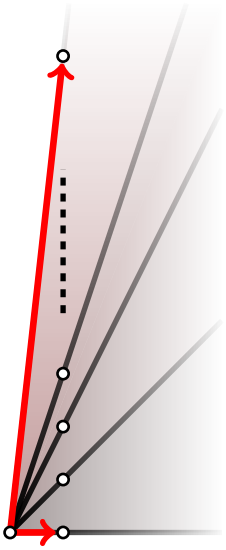


Fig. 6.1: The cone spanned by e_1 and $e_1 + ke_k$ needs k unimodular cones in its decomposition

Hence, if we want a polynomial time algorithm we need a better way to subdivide. The key idea for this is to use *signed* decompositions, which are decompositions where we may take new rays outside of the original cone and use addition and subtraction of rational generating functions to obtain the desired rational generating function of the original cone. It was the achievement of Barvinok [3] to show that with this method you can get away with a polynomial number of (even unimodular) cones.

To make this precise, let C be a d-dimensional cone spanned by primitive rays $v_1, \ldots, v_d$. We define the *index* of the cone C to be

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

The cone C is unimodular if and only if $\operatorname{Index}(C) = 1$. In a triangulation $\mathcal{T}$ of our cone C we will record the index of each cone in $\mathcal{T}$ (note that, for the generating series we also need to take lower dimensional cones

into account to account for overcounting in intersections via inclusion-exclusion). This collection of indices is both a measure of how far we are still from a unimodular triangulation and it gives an indicator whether we are already done or which cones we need to subdivide further.

Oberserve that the index of a face F of a cone C is bounded by the index of C, *i.e.* $\operatorname{Index}(F) \leq \operatorname{Index}(C)$, so we actually only need to track indices of maximal cones and subdivide those if the index is still larger than one. This is, of course, only useful if we can provide a method that subdivides a cone into cones of smaller index. Here the idea of signed decompositions is needed to make this efficiently.

The basic tool in the construction is Minkowski's First Theorem (Corollary 4.3), which tells us that for any compact, convex, and centrally symmetric $K \subseteq \mathbb{R}^d$ with $\operatorname{vol} K \geq 2^d$ there exists $a \neq 0$ in $K \cap \mathbb{Z}^d$.

We use this theorem in the following way. If, for a cone C, the index $\operatorname{Index}(C)$ is still larger than 1, then

$$K \;:=\; \left\{ \frac{1}{\sqrt[d]{\operatorname{Index} C}} \sum \lambda_1 v_i \;:\; -1 \leq \lambda_i \leq 1 \right\}$$

is a compact, convex, and centrally symmetric body with volume

$$\operatorname{vol}(K) \;=\; 2^d \,.$$

Hence, we can conclude that there is $w \in K \cap \mathbb{Z}^d$ different from $\mathbf{0}$. We can write w as a linear combination of the cone generators and, as w is contained in K, we obtain a bound on the size of the coefficients, that is, we know that

$$w \;=\; \lambda_1 v_1 \;+\; \lambda_2 v_2 \;+\; \cdots \;+\; \lambda_d v_d \quad \text{for} \quad 0 \leq |\lambda_i| \;\leq\; (\operatorname{Index}(C))^{-1/d} \,. \tag{6.1}$$

As already observed before, the proof of Minkowski's First Theorem (Corollary 4.3) is not constructive, and it is generally difficult to compute such a point w. See Section 6.3 for an approach.

Consider the vector w obtained in (6.1). By replacing w with $-w$ if necessary we can assume that $w, v_1, \ldots, v_d$ lie in a common half-space. Additionally we may clearly assume that w is primitive. By construction, $|\lambda_i| \leq (\operatorname{Index} C)^{-\frac{1}{d}}$. We define new cones

$$C_j \;:=\; \operatorname{cone}(v_1, \ldots, v_{j-1}, w, v_{j+1}, \ldots, v_d) \qquad \text{for} \qquad 1 \leq j \leq d$$

by replacing v_j by w. We compute the index of these new cones to be

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

and the right hand side is strictly less than $\operatorname{Index} C$ if $\operatorname{Index} C \geq 2$. As the index is an integral number we see that the index actually drops by at least one.

We define a corresponding sign function to make a signed subdivision of C with the cones C_j. For $1 \leq j \leq d$ let

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

Using our decomposition and the corresponding sign function we may write the integer point generating series as the signed sum

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

In our 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 in our triangulation successively until there is no cone of index greater than one left.

Let us compute how many iterations we need in this procedure. After n decomposition steps, a cone D in the decomposition has index at most

$$\operatorname{Index} D \;\leq\; (\operatorname{Index} C)^{\left(\frac{d-1}{d}\right)^n}$$

and we need to check for which n this number drops below 2 (recall that the index is integral, so it must be 1). We take the binary logarithm twice to solve this expression for n:

$$\begin{aligned}
\lg_2\left(\lg_2\left((\operatorname{Index} C)^{\left(\frac{d-1}{d}\right)^n}\right)\right) &= \lg_2\left(\left(\frac{d-1}{d}\right)^n \lg_2(\operatorname{Index} C)\right) \\
&= n\lg_2\left(\frac{d-1}{d}\right) + \lg_2\lg_2(\operatorname{Index} C) \\
&= -n\lg_2\left(\frac{d}{d-1}\right) + \lg_2\lg_2(\operatorname{Index} C)\,.
\end{aligned} \tag{6.2}$$

Algorithm 6.1: Barvinok's Algorithm: Original Version

Input: A polyhedron $P = \{x \mid Ax \leq b\}$ with vertices $v_1, \ldots, v_k$.
Output: The integer point generating function for P as

$$\mathsf{G}_P(t) = \sum_{i \in I} \varepsilon_i \frac{t^{a_i}}{(1-t^{v_{i1}}) \cdots (1-t^{v_{ik_i}})}$$

for $\varepsilon_i \in \{-1, 1\}$, $a_i, v_i j \in \mathbb{Z}^d$.

```
for i ← 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 ← 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;
    end for
    sum up the contributions using the inclusion-exclusion principle;
end for
sum up the contributions using the inclusion-exclusion principle;
```

Hence, if

$$n \;>\; \frac{\lg_2 \lg_2(\operatorname{Index} C)}{\lg_2\left(\frac{d}{d-1}\right)} \;= \mathcal{O}(d \lg_2 \lg_2 \operatorname{Index} C)\,,$$

then the right hand side of (6.2) is negative, so that

$$\operatorname{Index} D \;\leq\; \left\lfloor (\operatorname{Index} C)^{\left(\frac{d-1}{d}\right)^n} \right\rfloor \;\leq (\operatorname{Index} C)^{\left(\frac{d-1}{d}\right)^n} \;<\; 2\,,$$

i.e.

$$\operatorname{Index} D \;=\; 1\,.$$

So the number of iterations until we reach unimodular cones is indeed polynomial. However, we also need to check that the number of cones we produce is polynomial. In n steps we produce at most

$$\begin{aligned}(d2^d)^n \;&=\; 2^{nd \lg_2 d} \leq 2^{Md^2 \lg_2 d \lg_2 \lg_2 \operatorname{Index} C} \\ &=\; (\lg_2 \operatorname{Index} C)^{Md^2 \lg_2 d} \\ &=\; (\lg_2 \operatorname{Index} C)^{\mathcal{O}(d^2 \lg_2 d)}.\end{aligned}$$

cones. Hence, we conclude that with this approach indeed, in fixed dimension, the number of cones is bounded by a polynomial in $\lg_2 \operatorname{Index} C$. This is in the order of the input size of our cone in binary encoding. We summarize the algorithm in Algorithm 6.1 and the following theorem.

Theorem 6.1 *Let $d \in \mathbb{Z}_{>0}$ be fixed. Then there is a polynomial time algorithm that computes the integer point generating function $\mathsf{G}_P(t)$ in the form*

$$\mathsf{G}_P(t) := \sum_{i \in I} \varepsilon_i \frac{t^{a_i}}{(1-t^{v_{i1}}) \cdots (1-t^{v_{is_i}})} ,$$

where $\varepsilon_i \in \{-1,1\}$, $a \in \mathbb{Z}^d$, $v_{ij} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$ *for all* i,j *and* $s_i \leq d$, *for any* d*-dimensional polyhedron* P *given in its exterior description.* □

Note that, in this theorem, the index set I runs over all cones, including lower dimensional ones, in the subdivision.

6.2.1 Polynommial Time Evaluation

We can use Theorem 6.1 to compute $h^\star$-polynomials or Ehrhart polynomials by computing the generating function of the cone over the polytope. Similarly, using Brion's Theorem (Theorem 3.67), we can count lattice points in P and multiples of P (and thus also comput the Ehrhart polynomial via interpolation) by computing the rational generating functions of all vertex cones. However, this usually requires us to evaluate the generating function at $x = (t, \mathbf{1})$ or $x = \mathbf{1}$. Although we now from the theory that these are regular points of the rational functions, they are poles in the representation we obtain. We use tools from analysis to evaluate them (Note again, that expansion into a Taylor series, though theoretically a method to remove the pole, is not an option if we want evaluate this in polynomial time.).

One possible approach is to define a curve $\gamma(s)$ for a real parameter $s \geq 0$ such that $\gamma(0)$ is $(t, \mathbf{1})$ or $\mathbf{1}$ (depending on whether we look at the cone over P or at a vertex cone of P) and the only pole of our generating function on that curve occours for $s = 0$. Then we take the limit $s \to 0$. We need the following lemma.

Lemma 6.2 *Let* $v_1, \ldots, v_k \in \mathbb{R}^d$. *Then there is* $m \in \mathbb{R}^d$ *such that* $\langle\, m, v_j \,\rangle \neq 0$ *for* $1 \leq j \leq k$.

Proof. We use the moment curve

$$m(\lambda) \;:=\; \left(1, \lambda, \lambda^2, \ldots, \lambda^{d-1}\right) .$$

The map

$$\lambda \longmapsto \prod_{j=1}^{d} \langle\, m(\lambda), v_j \,\rangle$$

is a nonzero polynomial of degree $(d-1)k$. Hence, it has at most $(d-1)k$ zeros and we can try a polynomial number of values to find a λ such that $m(\lambda)$ gives the claim. □

Using this lemma we can find $m = (m_1, \ldots, m_d) \in \mathbb{R}^d$ such that, in the notation of Theorem 6.1,

$$\langle m, a_i \rangle \neq 0 \qquad \langle m, v_{ij} \rangle \neq 0 \qquad \text{for } i \in I \text{ and } 1 \leq j \leq s_i \,.$$

Now consider (we look at evaluation at $\mathbf{1}$, the case for $(t, \mathbf{1})$ is similar)

$$x(r) \;:=\; (e^{rm_1}, \ldots, e^{rm_d}) \,.$$

We get the desired evaluation as

$$\lim_{r \to 0} \mathsf{G}_P\left(x(r)\right) \,.$$

Let

$$\alpha_i \;:=\; \langle m, a_i \rangle \qquad\qquad \nu_{ij} \;:=\; \langle m, v_{ij} \rangle \,.$$

Then

$$\mathsf{G}_P\left(x(r)\right) \;=\; \sum_{i \in I} \varepsilon_i \frac{e^{\alpha_i r}}{\prod_{j=1}^{s_i}(1 - e^{u_{ij} r})} \,,$$

and the summands are all rational functions in one variable r which are defined for all $r > 0$. We want to compute the constant term of the Laurent expansion of all summands at $r = 0$. Now consider a single such fraction. We can transform it to obtain

$$\frac{e^{\alpha_i r}}{\prod_{j=1}^{s_i}(1 - e^{u_{ij} r})} \;=\; \frac{1}{r^{s_i}} e^{\alpha_i r} \prod_{j=1}^{s_i} \frac{r}{1 - e^{u_{ij} r}} \,. \tag{6.3}$$

Now each factor

$$\frac{r}{1 - e^{u_{ij} r}}$$

is defined for all r and we can compute the Laurent expansion up to degree $s_i + 1$:

$$\frac{r}{(1 - e^{u_{ij} r})} \;=\; T_{ij}(r) \;+\; R_{ij}(r^{s_i+1}) \,,$$

and similarly we get

$$e^{\alpha_i r} \;=\; S_i(r) \;+\; R'_{ij}(r^{k+1}) \,.$$

We compute the product up to degree $s_i + 1$:

$$P_i(r) \;:=\; S_i(r) \prod_{j=1}^{s_i} T_{ij}(r) \;+\; R''_i(r^{s_i+1}) \,.$$

Let c_i be the coefficient of r^{s_i} (note that (6.3) has an additional factor of $\frac{1}{r^{s_i}}$, so for this product c_i is the constant coefficient). We sum them up with the given signes to obtain

$$c \;:=\; \sum_{i \in I} \varepsilon_i c_i \,.$$

This is the desired limit and thus the evaluation at $\mathbf{1}$.

Remark 6.3 *Using the* Todd-polynomials $\mathrm{td}_m(\xi_1, \ldots, \xi_d)$ *defined by*

$$\prod_{i=1}^{k} \frac{x\xi_i}{1 - e^{-x\xi_i}} \;=\; \sum_{m=0}^{\infty} \mathrm{td}_m(\xi_1, \ldots, \xi_d) x^m$$

one may obtain a closed formula for the evaluation of $\mathsf{G}_C(\mathbf{1})$*, see e.g. [18, Thm. 7.2.1]. However, this requires us to evaluate the Todd polynomials.*

6.2.2 Integer Linear Programming via Evaluation

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

6.3 The Shortest Vector Problem

In this section we consider Minkowski's problem of finding a non-zero vector of shortest length in a lattice.

(SVP). Let Λ be a lattice with lattice basis $v_1, v_2, \ldots, v_d$. The *Shortest Vector Problem (SVP)* asks to find, in polynomial time in the dimension and the input size of the lattice basis, a non-zero vector $u \in \Lambda \setminus \{\mathbf{0}\}$ of shortest possible length.

This is a quite famous and important optimization problem. Observe that a shortest non-zero lattice vector has length $\lambda_1(\Lambda)$, the first successive minimum introduced in Definition 4.6.

An important relaxation of the shortest vector problem is the *approximate shortest Vector problem (SVP)*$_\gamma$ that asks, for a given bound $\gamma = \gamma(d) \geq 1$ to find a non-zero lattice vector u of length

$$\|u\| \;\leq\; \gamma\lambda_1 \,.$$

In fact, our algorithm for (SVP) is based on a solution for the approximate problem by constructing a *reduced basis*. We show that the coefficients of a shortest vector in such a basis are bounded by a constant depending on the dimension only. Hence, we can solve the shortest vector problem by enumerating over all possible coefficients (in fixed dimension).

In this section we explore the difficulties in the computation of a short basis vector, introduce *reduced bases* and show how such bases bound the size of coefficients for a shortest vector. This proves that, in fixed dimension and given a reduced basis, we can solve (SVP) in polynomial time.

In the following Section 6.4 we introduce a special type of reduced bases, the *δ-reduced bases* of Arjen Lenstra, Hendrik Lenstra and László Lovász from 1982 together with a polynomial time algorithm for their computation, again in fixed dimension.

Let us first discuss why the computation of a short vector, or a basis with short vectors is more involved for lattice bases than for vector space bases. We know from Proposition 4.5 that there is a vector of length at most $\sqrt{d}\det\Lambda$, but the proof did not give a method to actually construct such a vector, not even by enumeration. However, the problem would be easy to solve if vectors in the lattice basis actually were pairwise othogonal. In this case, the shortest of the lattice basis vectors is in fact a non-zero lattice vector of shortest length.

If we disregard the lattice structure for a moment, any vector space basis can be transformed into an orthogonal one using Gram-Schmidt orthogonalization. This algorithm runs in polynomial time depending on the dimension. However, it clearly does not respect the lattice structure. The example of the hexagonal lattice shown in Figure 6.2 shows in fact that, in general, there even does not exist a basis with pairwise orthogonal vectors, and we have also already seen bases with vectors of necessarily different lengths.

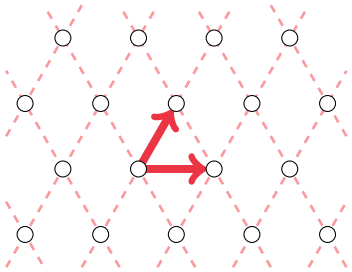


Fig. 6.2: The hexagonal lattice

For an approximate solution of the shortest vector problem we want to discuss how close we can get to an orthogonal basis for lattice vectors (while being able to compute the basis in polynomial time).

Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with a basis $v_1, v_2, \ldots, v_d \in \mathbb{R}^d$. The order of the basis vectors is important for the following considerations. We consider the increasing chain of subspaces

$$V_0 := \{\mathbf{0}\} \qquad V_k := \operatorname{lin}(v_1, \ldots, v_k) \qquad \text{for } 1 \le k \le d\,.$$

together with the induced lattices $\Lambda_k := \Lambda \cap V_k$ on these spaces. For $0 \le k \le d$ let $\pi_k : \mathbb{R}^d \to V_k$ be the orthogonal projection onto the subspace V_k and define a new set of vectors via

$$\begin{aligned} w_k &:= v_k - \pi_{k-1}(v_k) \\ &= v_k - \sum_{j=1}^{k-1} \lambda_{jk} w_j \qquad \text{with} \quad \lambda_{jk} := \frac{\langle\, v_k, w_j \,\rangle}{\|w_j\|^2}\,. \end{aligned}$$

Fig. 6.3: Orthogonal projection of a lattice generator

See also Figure 6.3. This is the Gram-Schmidt-orthogonalization of the lattice basis $v_1, \ldots, v_d$. So in particular we have

$$\langle\, w_i, w_j \,\rangle = 0 \quad \text{for } 1 \le i < j \le d \quad \text{and} \quad \mathrm{d}(v_k, V_{k-1}) = \|w_k\|\,.$$

Fig. 6.4: Distance of v_k from the subspace V_k is given by the norm of w_k.

See also Figure 6.4.

Example 6.4 *Let* $v_1 := \begin{pmatrix} 2 \\ 1 \end{pmatrix}, v_2 := \begin{pmatrix} 1 \\ 2 \end{pmatrix}$. *This is a basis of* $\mathbb{R}^2$ *with Gram-Schmidt-orthogonalization*

$$w_1 \;=\; v_1 \qquad \text{and} \qquad w_2 \;=\; \begin{pmatrix} -3/5 \\ 6/5 \end{pmatrix} \;=\; -4/5 v_1 + v_2\,,$$

see Figure 6.5.

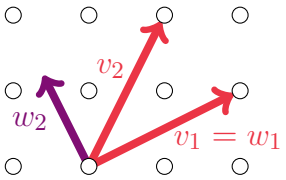


Fig. 6.5: The lattice basis of Example 6.4

We can write the original lattice basis in terms of the Gram-Schmidt basis as

$$v_k = w_k + \sum_{j=1}^{k-1} \lambda_{jk} w_j \quad \text{for } 1 \le k \le d\,. \tag{6.4}$$

The vectors $w_1, \ldots, w_d$ are pairwise orthogonal, so

$$\det \Lambda = \prod_{j=1}^{d} \|w_j\|\,. \qquad \text{and} \qquad \det \Lambda_k = \prod_{j=1}^{k} \|w_j\|\,.$$

The Gram-Schmidt vectors give a lower bound for the length of a shortest vector of the lattice.

Proposition 6.5 *Let* Λ *be a* d*-dimensional lattice with basis* $v_1, v_2, \ldots, v_d$ *and Gram-Schmidt-orthogonalization* $w_1, w_2, \ldots, w_d$*. Then*

$$\|u\| \;\ge\; \min(\|w_1\|, \ldots, \|w_d\|)$$

for all $u \in \Lambda \setminus \{0\}$.

Proof. We can write u as a linear combination

$$u \;=\; \sum_{j=1}^{d} \eta_j w_j\,.$$

Let k be the highest index such that $\eta_k \neq 0$. We can rewrite

$$u \;=\; \eta_k w_k + \sum_{j=1}^{k-1} \mu_j w_j$$

for some coefficients μ_j, $1 \le j \le k-1$. By othogonality, $|\eta_k| \ge 1$, so that

$$\|u\| \;\ge\; |\eta_k| \|w_k\| \;\ge\; \|w_k\|\,. \qquad \square$$

Definition 6.6 (orthogonality defect) *The* orthogonality defect of *the lattice basis* $v_1, v_2, \ldots, v_d$ *is*

$$M_\Lambda \;:=\; \frac{1}{\det \Lambda} \prod_{j=1}^{d} \|v_j\|\,.$$

Observe that the basis vectors $v_1, v_2, \ldots, v_d$ are pairwise orthogonal if and only if $M_\Lambda = 1$. In all other cases M_Λ is strictly larger than 1.

With this notion we have a measure how close a basis is to orthogonality.

Definition 6.7 *A lattice basis is* reduced *if its orthogonality defect is bounded by a constant M_d depending on the dimension only.*

This definition leaves open whether there actually exists such a constant M_d and how large we should choose it so that there is a reduced basis. We anwser this in the next Section 6.4 with an algorithm to compute a reduced basis and an explicit value for M_d.

The usefulness of notion is demonstrated by the following proposition, which shows that we can compute a shortest non-zero lattice vector from a reduced lattice basis in polynomial time.

Theorem 6.8 *Let Λ be a lattice with reduced basis $v_1, \ldots, v_d$ and let $u \in \Lambda \backslash \{0\}$ be a shortest non-zero lattice vector. Then*

$$u \;=\; \sum_{j=1}^{d} \lambda_j v_j \qquad \text{with} \qquad |\lambda_j| \;\leq\; \sqrt{d}M \quad \text{for } 1 \leq j \leq d.$$

Proof. Let v_1 be the shortest vector among $v_1, \ldots, v_d$, and let $V = (v_1, \ldots, v_d)$. Then $u = V\lambda$ for $\lambda = (\lambda_1, \ldots, \lambda_d)$. Hence, $\lambda = V^{-1}u$.

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

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

So

$$|\lambda_j| \leq \sum |u_i| \frac{M}{\|v_1\|} \;\leq\; \sqrt{d}\|u\| \frac{M}{\|v_1\|} \;\leq\; \sqrt{d}M\,,$$

where the last inequality uses $\|u\| \leq \|v_1\|$. □

Hence, we can solve the shortest vector problem in polynomial time by enumerating all $N := (2\sqrt{d}M)^d$ choices for the coefficients of the shortest vector, once we can find a reduced basis in polynomial time.

Theorem 6.9 *In fixed dimension d we can find $w \in \Pi_0 \cap \mathbb{Z}^d$, $w \neq 0$ in time polynomial in $\log^3 \max(\|v_i\|)$.* □

6.4 Short Lattice Bases

We have seen in the previous section that reduced bases allow the computation of a shortest vector, and thus count lattice points in a polytope, in

polynomial time. Yet, so far we don't even know that such bases exist for our lattice Λ. We address this question in the following by introducing a very special type of reduced basis together with a polynomial time algorithm first described by Arjen Lenstra, Hendrik Lenstra and László Lovász in 1982 [38]. The algorithm is known as as the LLL-algorithm in honour of the three authors.

Definition 6.10 (δ-LLL-reduced basis) *Let Λ be a lattice with lattice basis $v_1, \ldots, v_d$ and Gram-Schmidt orthogonalization $w_1, \ldots, w_d$. Let λ_{jk} be the coefficients of the representation of the v_j's in the Gram-Schmidt basis as in (6.4).*

The basis $v_1, \ldots, v_d$ is δ-reduced *for some $1/4 < \delta < 1$ if*

(1) $|\lambda_{jk}| \leq 1/2$ for all $1 \leq j < k \leq d$ and
(2) for all $1 \leq k \leq d-1$

$$\delta \, \mathrm{d}(v_k, V_{k-1})^2 \leq \mathrm{d}(v_{k+1}, V_{k-1})^2 \tag{6.5}$$

We mostly consider this definition for the particular choice $\delta = 3/4$.

We say that a coefficient λ_{jk} is *weakly reduced* if it satisfies condition (1) of the definition. A lattice basis is *weakly reduced* if all coefficients are weakly reduced.

Geometrically a basis is δ-reduced if the vector v_{k+1} is not much closer to the subspace spanned by the first $k-1$ basis vectors than the vector v_k, see Figure 6.6. Observe that we could equally write this condition with the Gram-Schmidt-vectors $w_1, w_2, \ldots, w_d$ as

$$\delta \|w_k\|^2 \;\leq\; \|w_{k+1} + \lambda_{k,k+1} w_k\|^2$$

for all $1 \leq k \leq d-1$.

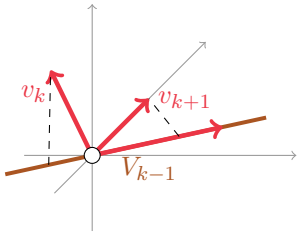


Fig. 6.6: The second condition for LLL

Example 6.11 *Here is an example of a $3/4$-reduced basis and one that is not. Consider the three vectors*

$$v_1 := \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \qquad v_2 := \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \qquad v_3 := \begin{bmatrix} 1 \\ -1 \\ 3 \end{bmatrix}$$

Their Gram-Schmidt-orthogonalization is

$$w_1 := \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \qquad w_2 := \begin{bmatrix} -2/5 \\ 4/5 \\ 1 \end{bmatrix} = v_2 - \frac{2}{5} w_1$$

$$w_3 := \begin{bmatrix} 1 \\ -2 \\ 2 \end{bmatrix} = v_3 - \frac{1}{5} w_1 - w_2$$

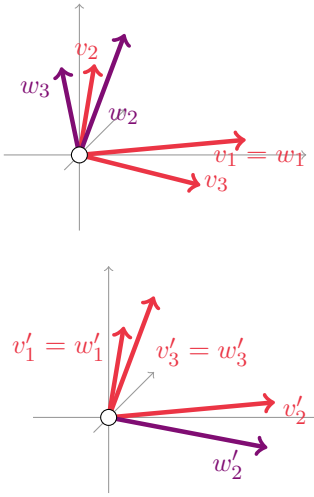


Fig. 6.7: A lattice basis that is not $3/4$-reduced and one for the same lattice that is reduced.

Then λ_{13} *violates condition (1) of the definition, and* v_1 *and* v_2 *violate condition (2), as* $\mathrm{d}(v_1, V_0)^2 = 5$ *and* $\mathrm{d}(v_1, V_0)^2 = 9/5$ *but* $3/4 \cdot 5 > 9/5$.

However, the basis

$$v_1' := \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \qquad v_2' := \begin{bmatrix} 2 \\ 1 \\ 0 \end{bmatrix} \qquad v_3' := \begin{bmatrix} 1 \\ -2 \\ 2 \end{bmatrix},$$

that spans the same lattice, is LLL-reduced. It has Gram-Schmidt-orthogonalization

$$w_1' := \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \quad w_2' := \begin{bmatrix} 2 \\ 1/2 \\ -1/2 \end{bmatrix} = v_2' - \frac{1}{2} w_1' \quad w_3' := \begin{bmatrix} 1 \\ -2 \\ 2 \end{bmatrix} = v_3'.$$

For an orthogonal basis $w_1, \ldots, w_d$ of $\mathbb{R}^d$ we can find a permutation such that the distances $\mathrm{d}(w_k, V_{k-1})$ strictly increase for $2 \leq k \leq d$. The condition for a δ-reduced basis is a relaxation of this. We only require that, if a basis vector is shorter than a previous one, it is shorter by at most a factor of δ. The following considerations will show that this relaxation is sufficient to compute such a basis in polynomial time (in the dimension and the input size), and it will lead to a universal bound as required in the approximate shortest vector problem. Hence, we can use this together with Theorem 6.8 to actually compute the shortest vector.

It is important to note that the notion of reduced bases and the algorithm we are going to present has many more important applications apart from the computation of a shortest vector. We will see some of them in the following sections. For more applications see for example [42]. Here is the main theorem of this section.

Theorem 6.12 (Lenstra, Lenstra, Lovász, 1982) $\Lambda \subset \mathbb{R}^d$ *a lattice. Then we can find a basis* $v_1, \ldots, v_d$ *of* Λ *in polynomial time such that*

$$\|v_1\|, \ldots, \|v_d\| \leq M \det \Lambda$$

We need some preparations for the proof of this theorem. Consider the representation of our given basis in (6.4). Assume that for some pair of indices $i < k$ the absolute value of the coefficient λ_{ik} is larger than $1/2$. Then there is a unique $\mu_{ik} \in \mathbb{R}$ and $a_{ik} \in \mathbb{Z}$ such that

$$|\mu_{ik}| \leq 1/2 \qquad \lambda_{ik} = a_{ik} + \mu_{ik}.$$

We set

$$v_k' := v_k - a_{ik} v_i \qquad \text{and} \qquad v_j' := v_j \quad \text{for } j \neq k..$$

This leaves the subspaces V_j invariant and $v_1', \ldots, v_j'$ is still a basis of the lattice Λ_j for $1 \leq j \leq d$. The new basis has the same Gram-Schmidt

orthogonalization $w_1, \ldots, w_n$. We want to compute the coefficients λ'_{jk} for the new basis in the representation (6.4).

We consider a fixed k between 1 and d. Clearly, the adjustment of v_k at most affects the coefficients λ_{jk} for this k and $1 \leq j \leq k-1$, so $\lambda'_{jl} = \lambda_{jl}$ for $l \neq k$ and $j < l$. We compute the new coefficients for v'_k. For this, we can write $v'_k = v_k - a_{ik} v_i$ as

$$v'_k \;=\; w_k + \sum_{j=1}^{k-1} \lambda_{jk} w_j - a_{ik} v_i \,.$$

The vector v_i is in the subspace V_i, so it has a representation

$$v_i \;=\; \sum_{j=1}^{i} \eta_j w_j \,,$$

So we can write

$$v'_k \;=\; w_k + \sum_{j=1}^{i} (\lambda_{jk} - a_{ik}\eta_j) w_j + \sum_{j=i+1}^{k-1} \lambda_{jk} w_j \,,$$

Now $v_i - w_i \in V_{i-1}$, so $\eta_i = 1$ and thus

$$|\lambda_{ik} - \eta_i a_{ik}| \;=\; |\lambda_{ik} - a_{ik}| \;=\; |\mu_{ik}| \;\leq\; 1/2 \,.$$

So the coefficient $\lambda'_{ik} := \lambda_{ik} - \eta_i$ is weakly reduced, and the new coefficients for v'_k are

$$\begin{aligned} \lambda'_{jk} &:= \lambda_{jk} - a_{ik}\eta_j && \text{for} j \leq i \\ \lambda'_{jk} &:= \lambda_{jk} && \text{for} j > i \end{aligned}$$

We want to use this to make all coefficients weakly reduced, that is, to make the lattice basis weakly reduced. However, we have to be careful, as making λ'_{ik} weakly reduced also affects λ_{jk} for $j < i$. So, for fixed k we apply this procedure to all λ_{ik} with i in *decreasing* order. Doing this for all $1 \leq k \leq d$ gives us a weakly reduced basis. This procedure is formalized in Algorithm 6.2.

There are $\binom{d}{2}$ coefficients, and reducing λ_{ik} with the above procedure we have to touch at most $i \leq d$ other coefficients, so this process terminates after at most $\mathcal{O}(d^3)$ steps. We summarize this in the following proposition.

Proposition 6.13 *Any lattice Λ has a weakly reduced basis. More precisely, we can transform any basis into a weakly reduced one in $\mathcal{O}(d^3)$ steps using Algorithm 6.2.* □

Algorithm 6.2: Weakly Reduced Basis

Input: Λ lattice in $\mathbb{R}^d$ of rank d with lattice basis $v_1, \ldots, v_d$.
Output: weakly reduced lattice basis $v'_1, \ldots, v'_d$
Compute the Gram-Schmidt orthogonalization $w_1, \ldots, w_d$;
Compute coefficients λ_{jk}, $1 \leq j < k \leq d$ such that
$v_k = w_k + \sum_{j=1}^{k-1} \lambda_{jk} w_j$;
for *k from 2 to d* **do**
  for *j from* $k-1$ *to* 1 **do**
    Determine $\mu_{jk} \in \mathbb{R}$, $a_{jk} \in \mathbb{Z}$ such that $\lambda_{jk} = \mu_{jk} + a_{jk}$ and $|\mu_{jk}| \leq 1/2$,;
    $v_k \leftarrow v_k - a_{jk} v_j$;
  end for
end for
return $v_1, \ldots, v_d$;

How can we transform a weakly reduced basis into a reduced one? We will show that repeatedly applying the following two steps lead to a successful algorithm.

(1) If a weakly reduced basis has a pair of vectors v_j, v_{j+1} violating condition (6.5), then we exchange v_j and v_{j+1}.
(2) The new basis will usually not be weakly reduced anymore. We fix this by applying Algorithm 6.2 again.

We repeat these two steps until we reach a reduced basis. This is formalized in Algorithm 6.3.

Algorithm 6.3: LLL

Input: A lattice basis $v_1, \ldots, v_d$.
Output: A reduced lattice basis $v'_1, \ldots, v'_d$
Make $v_1, \ldots, v_d$ weakly reduced (Algorithm 6.2);
while *V not δ-reduced* **do**
  Find a pair v_j, v_{j+1} that violates (6.5) and exchange the two vectors;
  Make $v_1, \ldots, v_d$ weakly reduced (Algorithm 6.2);
end while
return $v_1, \ldots, v_d$;

We clearly obtain a δ-reduced basis if this procedure terminates. We introduce a new numerical invariant of a lattice basis. The *potential* of a lattice basis $v_1, \ldots, v_d$ is defined as

$$D(v_1, \ldots, v_d) \;:=\; \prod_{j=1}^{d} \det \Lambda_j \,. \tag{6.6}$$

We can express $D(v_1, \ldots, v_d)$ also in the Gram-Schmidt orthogonalization.

$$D(v_1, \ldots, v_d) \;=\; \prod_{k=1}^{d} \prod_{j=1}^{k} \|w_j\| \,.$$

Note that $D(v_1, \ldots, v_d)$ depends on the order of the basis vectors. It puts more weight on those vectors coming first in the basis. Hence, it will change if we exchange two of the basis vectors.

Let us determine the change in D after one iteration of Algorithm 6.3. We have observed above that making a basis weakly reduced does not change the subspaces V_i and the lattices Λ_i, hence, it also does not change D. Assume that v_j and v_{j+1} for $1 \leq j \leq d-1$ violate the condition of Definition 6.10(1). Let $v'_1, \ldots, v'_d$ be the basis obtained by exchanging v_j and v_{j+1}, i.e.

$$v'_{j+1} := v_j \qquad v'_j := v_{j+1} \qquad v'_i := v_i \qquad \text{for } i \neq j, j+1 \,.$$

Let V'_i, Λ'_i be the new subspaces and lattices, $1 \leq i \leq d$. Then

$$V'_i = V_i \qquad\qquad \Lambda'_i = \Lambda_i \qquad\qquad \text{for } i \neq j \,,$$

while

$$V'_j := \operatorname{lin}(v'_1, \ldots, v'_{j-1}, v'_j) = \operatorname{lin}(v_1, \ldots, v_{j-1}, v_{j+1}) \,.$$

The new Gram-Schmidt vectors are

$$\begin{aligned}
w'_i \;&:=\; w_i \quad \text{for } i \neq j, j+1 \\
w'_j \;&:=\; v_{j+1} - \sum_{i=1}^{j-1} \lambda_{i,j+1} w_i \;=\; v_{j+1} - \pi_{j-1}(v_{j+1}) \\
w'_{j+1} \;&:=\; v_j - \sum_{i=1}^{j-1} \lambda_{ij} w_i - \frac{\langle\, v_j, w'_j \,\rangle}{\|w'_j\|^2} w'_j \\
&=\; v_j - \pi_{j-1}(v_j) - \frac{\langle\, v_j, w'_j \,\rangle}{\|w'_j\|^2} w'_j
\end{aligned}$$

By our assumption on v_j and v_{j+1} we have

$$\delta \cdot \mathrm{d}(v_k, V_{k-1})^2 \;>\; \mathrm{d}(v_{k+1}, V_{k-1})^2$$

Consequently, the vectors w_j and w'_j satisfy

$$\delta \cdot \|w'_j\|^2 \;>\; \|w_j\|^2 \;=\; \beta \cdot \|w'_j\|^2$$

for some $\beta < \delta < 1$. Hence, $1/\beta \|w'_{j+1}\|^2 = \|w_{j+1}\|^2$ as for all other i we have $w'_i = w_i$ and

$$\det \Lambda = \prod_{i=1}^{d} \|w_i\| = \prod_{i=1}^{d} \|w'_i\|$$

is invariant. This implies that

$$\det \Lambda'_j \;<\; \sqrt{\delta} \det \Lambda_j \qquad \text{and} \qquad \det \Lambda'_i \;=\; \det \Lambda_i \quad \text{for } i \neq j\,,$$

so also

$$D(v'_1, \ldots, v'_d) \;=\; \sqrt{\delta} D(v_1, \ldots, v_d) \;<\; D(v_1, \ldots, v_d)\,. \tag{6.7}$$

Hence, in each iteration, $D(v_1, \ldots, v_d)$ drops be at least a factor of $\sqrt{\delta} < 1$, so Algorithm 6.3 runs in polynomial time if $D(v_1, \ldots, v_d)$ has a polynomial lower bound in terms of the dimension. We provide such a bound with the following lemma.

Lemma 6.14 *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with lattice basis $v_1, \ldots, v_d$ and first successive minimum $\lambda_1 := \min_{u \in \Lambda \setminus \{\mathbf{0}\}}(\|u\|)$ introduced in Definition 4.6. Then*

$$D(v_1, \ldots, v_d) \;\geq\; \lambda_1^{d(d+1)/2} \prod_{j=1}^{d} j^{-j/2}\,.$$

Proof. Clearly $\lambda_1 \leq \min_{u \in \Lambda_j \setminus \{\mathbf{0}\}}(\|u\|)$ for all $1 \leq j \leq d$. Let v be the shortest non-zero vector in Λ. Then a shortest vector in Λ_j has length at least $\|v\|$. Thus, from Proposition 4.5 we conclude

$$\det \Lambda_j \;\geq\; \frac{\|v\|^j}{\sqrt{j}^i} \;\geq\; \frac{\lambda_1^j}{\sqrt{j}^j} \qquad \text{for all } 1 \leq j \leq d\,.$$

Multiplying this inequality for all $1 \leq j \leq d$ gives the lemma. □

Let us return to the orthogonality defect M defined in Definition 6.6 before we determine the precise running time of the LLL algorithm. We have seen in Theorem 6.8 that a polynomial upper bound for the orthogonality defect of a lattice basis allows us to solve the shortest vector problem (SVP) in polynomial time. We show now that M of a δ-reduced basis $v_1, \ldots, v_d$ is bounded by $M_d := 2^{\frac{1}{2}\binom{d}{2}}$ for $\delta = 3/4$. Hence, we can use this M in definition Definition 6.7 and are guaranteed that bases satisfying the definition actually do exist.

Proposition 6.15 *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with reduced basis $v_1, \ldots, v_d$. Let $w_1, \ldots, w_d$ be its Gram-Schmidt orthogonalization. Then*

$$\|w_j\|^2 \;\leq\; \|v_j\|^2 \;\leq\; \|w_j\|^2 + \frac{1}{4}\sum_{i=1}^{j-1} \|w_i\|^2 \qquad \textit{for } 1 \leq j \leq d$$

$$\|w_j\|^2 \;\geq\; (\delta - \frac{1}{4})\|w_{j-1}\|^2 \qquad \textit{for } 2 \leq j \leq d\,.$$

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

$$\begin{aligned} \mathrm{d}(v_j, V_{j-1})^2 &= \|w_j\| \\ \mathrm{d}(v_{j+1}, V_{j-1})^2 &= \|w_{j+1}\|^2 + \lambda_{j+1,j}^2 \|w_j\|^2 \;\leq\; \|w_{j+1}\|^2 + \frac{1}{4}\|w_j\|^2 \,. \end{aligned}$$

By assumption

$$\mathrm{d}(v_{j+1}, V_{j-1})^2 \;\geq\; \delta \cdot \mathrm{d}(v_j, V_{j-1})^2$$

so

$$\|w_{j+1}\|^2 + \frac{1}{4}\|w_j\| \;\geq\; \delta \cdot \|w_j\|^2$$

The second inequality follows. □

We define $\alpha := \frac{1}{\delta - \frac{1}{4}}$.

Proposition 6.16 *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with δ-reduced basis $v_1, \ldots, v_d$. Then*

(1) $\|v_1\| \leq \alpha^{\frac{d-1}{2}} \lambda_1$
(2) $\|v_1\| \leq \alpha^{\frac{d-1}{4}} (\det \Lambda)^{\frac{1}{d}}$

Proof. Let $e_1, \ldots, w_d$ be the Gram-Schmidt orthogonalization of $v_1, \ldots, v_d$. By Proposition 6.15 $\|w_{j+1}\|^2 \geq (\delta - \frac{1}{4})\|w_j\|^2$, so $\|w_j\|^2 \leq \alpha \|w_{j+1}\|^2$. By induction we obtain

$$\|w_j\|^2 \;\leq\; \alpha \|w_k\|^2 \qquad \text{for } 1 \leq j < k \leq d \,. \tag{6.8}$$

Hence, we obtain for all $1 \leq j \leq d$

$$\|v_1\|^2 \;=\; \|w_1\|^2 \;\leq \alpha^{j-1} \|w_j\|^2 \;\leq\; \alpha^{d-1} \|w_j\|^2 \,, \tag{6.9}$$

so

$$\|v_1\|^2 \;\leq\; \alpha^{d-1} \min_j \|w_j\|^2$$

and by Proposition 6.5

$$\|v_1\| \;\leq\; \alpha^{\frac{d-1}{2}}\lambda - 1\,.$$

This proves the first item. Taking the product of (6.9) for all j gives

$$\|v_1\|^{2d} \;\leq\; \prod_{i=1}^{d} \alpha^{i-1}\|w_i\|^2 \;=\; \alpha^{\frac{d(d-1)}{2}}\|w_1\|^2\cdots\|w_d\|^2 \;=\; \alpha^{\frac{d(d-1)}{2}}\,(\det\Lambda)^2\,.$$

□

For the following estimate we spacialize to the case $\delta = \frac{3}{4}$, so $\alpha = 2$.

Corollary 6.17 *Let $\Lambda \subset \mathbb{R}^d$ be a lattice with 3/4-reduced basis $v_1, \ldots, v_d$. 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

$$\begin{aligned}\prod_{j=1}^{d}\|v_j\| \;&\leq\; \prod_{j=1}^{d} 2^{j-1}\|w_j\|^2 \\ &=\; 2^{\frac{1}{2}\binom{d}{2}}\prod j = 1^d\|w_j\| \;\leq\; 2^{\frac{1}{2}\binom{d}{2}}\det\Lambda\,.\end{aligned}$$

□

Corollary 6.18 *The orthogonality defect M of a 3/4-reduced basis is at most $2^{\frac{1}{2}\binom{d}{2}}$.* □

Proposition 6.19 *Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice with a reduced basis $v_1, \ldots, v_d$. Let $\lambda_1 := \min_{a\in\Lambda-\{\mathbf{0}\}}\|a\|$ 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*

$$|\eta_i| \;\leq\; 2^{\frac{d-1}{2}}\left(\frac{3}{2}\right)^{d-i}\alpha \;\leq\; 3^d\alpha \qquad \text{for } 1 \leq i \leq d\,.$$

Proof. proof missing □

Now let us return to the problem of determining the runtime of the LLL algorithm. For simplicity we assume in the following that the initial lattice basis satisfies $v_j \in \mathbb{Z}^d$. In this case we have

$$D := D(v_1, \ldots, v_d) \;\geq\; 1\,. \tag{6.10}$$

By (6.7), the value of D drops by at least a factor of $\sqrt{\delta}$ each time we swap a pair of basis vectors that violate condition Definition 6.10(1), so we need at most $k = \lceil \frac{1}{\log 1/\sqrt{\delta}} \log D \rceil$ swaps.

Now $\|w_j\| \leq \|v_j\|$ for $1 \leq j \leq d$, so we can bound the initial value of D by

$$D \;\leq\; \left(\max_j \|v_j\| \right)^{d(d+1)/2} ,$$

and we can bound the number of iterations by

$$k \;=\; \left\lceil \frac{1}{\log 1/\sqrt{\delta}} \frac{d(d+1)}{2} \log \left(\max_j \|v_j\| \right) \right\rceil . \tag{6.11}$$

The input size of the LLL algorithm is bounded from below by

$$I \;:=\; \langle v_1, \ldots, v_d \rangle \;\leq\; \max \left(d, \max_j \|v_j\| \right) ,$$

so the right hand side of (6.11) is polynomial in I for $\delta < 1$. More precisely, we habe that the number of swaps we have to perform in the worst case satisfies

$$k \;=\; \mathcal{O}\left(d^2 (\log d + s) \right)$$

where s is the largest binary encoding length of an entry of a vector in the lattice basis. After each swap we have to restore the property that our lattice basis is weakly reduced. By Proposition 6.13 this takes at most $\mathcal{O}(d^3)$ steps, so overall, the lattice beasis reduction needs at most $\mathcal{O}\left(d^5 (\log d + s) \right)$ steps.

To show that LLL actually runs in polynomial time we also have to show that all numbers computed in intermediate steps of the algorithm have a binary encoding size bounded by a polynomial in I.

Remark 6.20 *The additional assumption that all lattice basis vectors all have integral entries can be removed. We just scale the initial basis with the common denominator of all entries of the basis vectors.*

Remark 6.21 *In the form we have discussed the LLL algorithm needs at most $\mathcal{O}\left(d^5 (\log d + s) \right)$ steps on numbers of size $\mathcal{O}(d + s)$. This corresponds to the original form of the algorithm given by Arjen Lenstra, Hendrik Lenstra and László Lovász [38]. There habe been found several improvements that run significantly faster, for example*

(1) Claus-P. Schorr has improved the bound to $\mathcal{O}(d^4 (\log d + s))$ [48]
(2) Arne Storjohann has shown that we can compute a reduced basis in time $\mathcal{O}(n^3 (\log d + s))$ on integers of the same size [56].

6.4.1 Applications of LLL

(1) factoring polynomials [38]
(2) knapsack [35]
(3) quadratic equations
(4) ...

6.5 Variations of Barvinok's Algorithm

In the previous section we gave a description of the basic version of Barvinok's algorithm. Since its publication in 1994 there have been found various improvements. We will shortly discuss some of them.

A fundamental problem that influences the running time of the algorithm are the lower dimensional cones that we have to consider for the inclusion-exclusion step. In § 3.4.1 we have seen a way to avoid lower dimensional faces by looking at a *half-open decomposition* of our cone into simplicial cones. Using such a decomposition significantly reduces the number of cones we have to consider. Namely, only d instead of $d2^d$ new cones in each step of the decomposition. This half open decomposition works nicely also with the signed decompositions we have used in Barvinok's algorithm. You can work out the details in Exercise 6.1.

Exercise 6.1

A slightly different idea is the following. We have seen that the rational generating function of cones with nontrivial lineality space are 0. We can exploit this to remove the contribution of lower dimensional cones by first dualizing and subdividing on the dual side. Then intersections on the dual side give unions on the primal side, and those vanish in the rational generating function, as thez contain a line.

Let us make this precise. If $C \subseteq \mathbb{R}^d$ is a polyhedral cone, then let $\mathcal{S} := \{D_i \ : \ i \in I\}$ be the maximal cones of a subdivision of the dual cone $C^\vee$ *i.e.*

$$C^\vee \ = \ \bigcup_{i \in I} D_i$$

Then

$$C \ = \ \bigcap_{i \in I} D_i^\vee$$

and on the level of generating series

$$\widehat{\mathsf{G}}_C\,(x) \ = \ \widehat{\mathsf{G}}_{\bigcap_{i\in I} D_i^\vee}\,(x)$$

We can rewrite the right hand side to

$$\widehat{\mathsf{G}}_{\bigcap_{i\in I} D_i^\vee}\,(x) \ = \ \sum \widehat{\mathsf{G}}_{D_i^\vee}\,(x) \ + \ \sum_{J \subseteq I} \delta_J \widehat{\mathsf{G}}_{\bigcup_{j\in J} D_j^\vee}\,(x)$$

Algorithm 6.4: Barvinok's Algorithm: Polarized Version

Input: A polyhedron $P = \{x \mid Ax \leq b\}$ with vertices $v_1, \ldots, v_k$.
Output: The integer point generating function for P as

$$\mathsf{G}_P(t) = \sum_{i \in I} \varepsilon_i \frac{t^{a_i}}{(1 - t^{v_{i1}}) \cdots (1 - t^{v_{ik_i}})}$$

for $\varepsilon_i \in \{-1, 1\}$, $a_i, v_i j \in \mathbb{Z}^d$.

for $i \leftarrow 1$ **to** k **do**
  Compute vertex cone C_i at vertex v_i;
  Dualize the cones to $C_i^\star$;
  Triangulate $C_i^\star$ into k_i simplicial cones $C_{ij}^\star$;
  for $j \leftarrow 1$ **to** k_i **do**
    do a signed decomposition of $C_{ij}^\star$ into unimodular cones $(C_{ij}^k)^\star$.;
    Dualize back to C_{ij}^k;
    compute the unique interior point a_{ij}^k in C_{ij}^k;
  end for
  sum up the contributions using the inclusion-exclusion principle;
end for
sum up the contributions using the inclusion-exclusion principle;

for $\delta_I \in \{0, \pm 1\}$. Observe that any nontrivial union of two dual cones $D_i^\vee$ and $D_j^\vee$ for $i \neq j$ contains a line, as there is a linear hyperplane H spanned by some vector u in primal space (the dual of the dual) that intersects the cones at most in their boundary and has the two cones on different sides. Then $\mathbb{R}u \in D_j^\vee \cup D_j^\vee$. Hence, these serices vanish if we pass to the generating functions via our map Φ, so that

$$\mathsf{G}_C(x) \;=\; \sum_{i \in I} \mathsf{G}_{D_i^\vee}(x) \;,$$

where we have lost all contributions except for the dual maximal cones. The following observation shows that this is a decomposition into cones of index 1. You will prove this in Exercise 6.2.

Lemma 6.22 $\operatorname{Index} C = 1 \Leftrightarrow \operatorname{Index} C^* = 1$

Exercise 6.2

Hence, with this *dualization trick* we obtain a decomposition into unimodular cones where we only have to consider the maximal cones. This is a significant improvement over our original version where we had to keep track of all lower dimensional cones introduced by the inclusion-exclusion principle. We summarize the algorithm in Algorithm 6.4.

6.6 The Closest Vector Problem

6.7 Integer Programming in Fixed Dimension

The integer programming problem is the task to find an integral point in a polyhedron given by inequalities that maximizes a linear functional, *i.e.* find, for $A \in \mathbb{Z}^{m\times d}$, $b \in \mathbb{Z}^m$ and $c \in \mathbb{Z}^d$,

$$\begin{aligned} &\max(\langle\, c, x\,\rangle) \\ &\text{subject to} \quad Ax \;\leq\; b \\ &\qquad\qquad\quad x \;\in\; \mathbb{Z}^d\,. \end{aligned}$$

Different from the linear programming problem, where we drop the requirement that $x \in \mathbb{Z}^d$, this problem is known to be in the class NP, but not known to be in P.

However, for fixed dimension, we can give a polynomial time algorithm for the integer programming problem. This algorithm is due to Hendrik Lenstra. It is based on flatness and its proof via ellipsoids, together with the computation of reduced bases with the LLL-algorithm. As for flatness, the method has three steps. We first consider balls and extend to ellipsoids. Then we use the John ellipsoids to squeeze a polytope P between two ellipsoids and use the method for ellipsoids to find a feasible integer point in P or assert that there is none. Flatness is used to slice a polytope with a polynomial number of integral translates of a lattice hyperplane and descend in dimension if we cannot yet decide whether P has an integral point.

Let us make this precise and start with the construction for balls in the next proposition.

Proposition 6.23 *Let Λ be a lattice with basis $v_1, \ldots, v_d$ and $\mathcal{B}_\mathrm{d} := \mathcal{B}_d(z)$ be the unit ball with center z. Then we can find, in polynomial time,*

(1) either a lattice point $u \in \mathcal{B}_\mathrm{d} \cap \Lambda$, or
(2) a lattice functional $c \in \Lambda^\star$ with $\|c\| \leq 2^{\mathcal{O}(2^d)}$ such that $\mathcal{B}_\mathrm{d} \cap \Lambda$ is covered by at most $\mathcal{O}(2^d)$ hyperplanes of the form

$$\{x \,:\, \langle\, c, x\,\rangle \;=\; \beta\}\,.$$

for some $\beta \in \mathbb{Z}$.

Proof. Assume that $v_1, \ldots, v_d$ is a reduced basis with orthogonality defect bounded by

$$M \;\leq\; \prod_{j=1}^{d} \frac{\|v_i\|}{\|w_i\|} \;\leq\; 2^{\frac{d(d-1)}{2}}\,,$$

where $w_1, \ldots, w_d$ is the associated Gram-Schmidt basis. Reorder the basis such that

$$\|v_1\| \;\leq\; \|v_2\| \;\leq\; \ldots \;\leq\; \|v_d\|\,.$$

This may destroy reducedness of the basis, but does not affect the orthogonality defect. We distinguish two cases

(1) if $\|v_d\| \leq \frac{1}{d}$, then we consider the representation

$$z \;=\; \sum_{i=1}^{d} \lambda_i v_i$$

of the center in our basis. The point

$$u \;=\; \sum_{i=1}^{d} \lfloor \lambda_i \rfloor v_i$$

is a lattice point and

$$\|u - z\| \;\leq\; \sum_{i=1}^{d} \|v_i\| \;\leq\; d\|v_d\| \;\leq\; 1\,.$$

Hence $u \in \mathcal{B}_\mathrm{d} \cap \Lambda$.

(2) Otherwise we have $\|v_d\| > \frac{1}{d}$. Let

$$H \;:=\; \mathrm{lin}(v_1, \ldots, v_{d-1}).$$

Then $H + v_d = H + w_d$, so

$$\Lambda \;\subseteq\; \bigcup_{\beta \in \mathbb{Z}} H + \beta v_d \;=\; \bigcup_{\beta \in \mathbb{Z}} H + \beta w_d\,.$$

Now

$$\frac{normv_d}{\|w_d\|} \;\leq\; M \;\leq\; 2^{\frac{d(d-1)}{2}}\,,$$

so

$$\|w_d\| \;\geq\; 2^{-\frac{d(d-1)}{2}} \|v_d\| \;\geq\; \frac{1}{d} 2^{-\frac{d(d-1)}{2}}\,.$$

Further

$$\max_{\beta \in \mathbb{Z}} \left(H + \beta v_d \cap \mathcal{B}_\mathrm{d} \neq \varnothing\right) \;-\; \max_{\beta \in \mathbb{Z}} \left(H + \beta v_d \cap \mathcal{B}_\mathrm{d} \neq \varnothing\right) \;\leq 2\,.$$

So $H + \beta v_d \cap \Lambda \neq \varnothing$ for at most $2d2^{\frac{d(d-1)}{2}}$ different β's. Let $c := \frac{w_d}{\|w_d\|^2}$. Any $u \in \Lambda$ can be written as $u = \mu w_d + h$ for $h \in H$ and $\mu \in \mathbb{Z}$. This implies

$$\langle\, c, u \,\rangle \;=\; \mu \;\in\; \mathbb{Z}\,.$$

so that $c \in \Lambda^\star$ and $\|c\| \leq \frac{1}{\|w_d\|} \leq 2^{\mathcal{O}(2^d)}$. □

Algorithm 6.5: Computing an enclosing ellipsoid

Input: A polyhedron $P = \{x \mid Ax \leq b\}$ for $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$.
Output: An ellipsoid E and a vector a such that
$a + E \subseteq P \subseteq a + 2dE$
Compute a ball E_0 containing P and translate so that the cetner is in the origin;
if $\frac{1}{2d}E_0 \subseteq P$ **then**
  return E_0;
else
  find $x \in \frac{1}{2d}E_0 \setminus P$;
  find halfspace H^+ containing P but not x via separation algorithm;
  let $E_0' := E_0 \cap H^+$;
  compute smallest ellipsoid E_1 containing E_0';
  find affine transformation T_0 such that $T_0 E_1$ is a ball centered at the origin;
  recursively call this algorithm;
end if

Geometrically, this proposition tells us that either we can find a reduced basis with only short vectors, or there must be a short dual vector.

Corollary 6.24 *The proposition is also true if we replace the ball by an ellipsoid $E = T\,\mathcal{B}_\mathrm{d} + a$ for an invertible linear transformation T.*

Proof. Pull back to a ball with T^{-1} and consider the lattice $T^{-1}\Lambda$. □

By Theorem A.5 we know that for a convex body K there is an ellipsoid E centered at the origin such that

$$a + E \;\subseteq\; K \;\subseteq\; a + dE\,.$$

However, the proof of this theorem given in the appendix was not constructive. Note first, that for us it is sufficient to find an approximation of E where we relax the scaling factor on the right hand side. It suffices to find E such that

$$a + E \;\subseteq\; K \;\subseteq\; a + 2dE\,.$$

For general convex bodies the computation of E is an SDP-Problem. However, in our case the convex body is a polyhedron and the algorithm becomes simpler. It is the same algorithm that is used for the ellipsoid method of linear programming. We sketch an approach below. For a full algorithm with proof the reader sould consult any book on linear programming, *e.g.* [50, Ch. 13]. The algorithm for the ellipsoid is given in Algorithm 6.5. It can be shown that in each recursive call the volume of the ellipsoid drops by a factor of at least $(1 - \frac{1}{d})$. Hence, the algorithm terminates after a polynomial number of steps.

Proposition 6.25 *For a polytope $P \subseteq \mathbb{R}^d$ we can compute in polynomial time an ellipsoid E and a vector a such that*

$$a + E \;\subseteq\; K \;\subseteq\; a + 2dE\,. \qquad \square$$

This proposition allows us to extend Corollary 6.24 to an algorithm that computes an integer point in a polytope or asserts that the polytope contains no integer point.

Theorem 6.26 (Lenstra) *For a polytope P we can decide, for fixed dimension in polynomial time in the input size, whether P contains an integer point.*

Proof (sketch). The algorithm is given in Algorithm 6.6. Its correctness follows from the considerations above. It remains to check the running time. For this, let $T(d)$ denote the number of recursive calls in dimension d. Then the total running time is $T(d)$ times a polynomial in d.

By the previous corollary on ellipsoids we know that

$$T(d) \;\leq\; T(d-1) \cdot \left(d \cdot 2^{\frac{d(d-1)}{2}} + 1 \right),$$

where the first d comes from the flatness theorem and the rest from the bound given for ellipsoids. This implies

$$T(d) \;\leq\; \prod_{k=1}^{d} \left(k \cdot 2^{\frac{k(k-1)}{2}} + 1 \right) \;\leq\; 2^{\mathcal{O}(d^3)}\,. \qquad \square$$

6.8 Software

We give examples for the computation of short generating functions in `LattE` and `polymake`.

6.9 Problems

included on page 168

6.1. Show that we can use a half open decomposition in Barvinok's algorithm.

included on page 169

6.2. Prove Lemma 6.22.

For a solution see page 221

Algorithm 6.6: Integer Feasibility in fixed dimension

Input: A polyhedron $P = \{x \mid Ax \leq b\}$ for $A \in \mathbb{Q}^{m \times n}$ and $b \in \mathbb{Q}^m$.
Output: An integer point in $P \cap \mathbb{Z}^d$, or the assertion that $P \cap \mathbb{Z}^d$ is empty.

Compute an ellipsoid E such that $z + E \subseteq P \subseteq z + 2dE$;
Use the LLL-algorithm to compute a lattice basis $v_1, \ldots, v_d$ with Gram-Schmidt orthogonalization $w_1, \ldots, w_d$ such that the orthogonality defect with respect to the norm $\|.\|_E$ is bounded.;
reorder the basis by increasing norm;
Determine $\lambda_1, \ldots, \lambda_d$ such that $z = \sum_{i=1}^{d} \lambda_i v_i$ and let $u = \sum_{i=1}^{d} \lfloor \lambda_i \rfloor v_i$;
if $u \in P$ **then**
  return u;
end if
Set $c := w_d$;
foreach $\beta \in \{\lfloor \min(\langle c, x \rangle \,:\, x \in P) \rfloor, \ldots, \lceil \max(\langle c, x \rangle \,:\, x \in P) \rceil\}$ **do**
  use the Hermite Normal Form algorithm to compute a lattice basis $V' := \{v'_1, \ldots, v'_{d-1}\} \subseteq \mathbb{Q}^d$ and $d \in \mathbb{Q}^d$ such that $d + \Lambda(V') = \{x \in \mathbb{Z}^d \,:\, \langle c, x \rangle = \beta\}$;
  recursively solve the integer feasibility problem on $\left\{x' \,:\, A(d + \sum x'_j v'_j) \leq b\right\}$;
  if *recursive call produces a lattice point* u **then**
    return u;
  end if
end foreach
return no lattice point found;

Reflexive and Gorenstein polytopes

7

Contents

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 $h^\star$-vector. What else is there to discover?

Here is a plan for this chapter. We start bydefining reflexive polytopes and explore some of their basic features. Next, we present some of their surprising properties in dimensions 2 and 3. In Section 7.2 we explore the combinatorics of reflexive polytopes in the more tractable situation, where all facets are simplices. In Section 7.3 we also consider 'divisors' of reflexive polytopes, called Gorenstein polytopes, and show that this is a natural class of lattice polytopes to work with. 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.

7.1 Reflexive polytopes

Let us recall the definition of a dual polytope of a d-dimensional polytope $P \subset \mathbb{R}^d$ from Theorem 2.16.Let $P \subseteq \mathbb{R}^d$ be a full-dimensional polytope with $\mathbf{0} \in P$. The *dual polytope* or *polar* of P is

$$P^\star := \{\alpha \in (\mathbb{R}^d)^\star \,:\, \alpha(x) \;\geq\; -1 \text{ for all } x \in P\}$$

Exercise 7.1
Exercise 7.2
Exercise 7.3
Exercise 7.4

Check Exercises 7.1 to 7.4 for some examples and properties.

It is well-known that the vertices of $P^\star$ correspond one-to-one to facets of P. More precisely, the vertices are the unique inner facet normals evaluating as -1 on facets. Recall from Chapter 2 that for full-dimensional lattice polytopes there is a canonical choice for the facet normals as a primitive lattice vector in the dual lattice. We will in the following alsways assume that normal vectors are primitive dual lattice vectors. The most important result is the *duality theorem* (which holds more generally for convex bodies containing the 0 in their interior):

$$P^{\star\star} \;=\; P$$

Let $P \subset \mathbb{R}^d$ be a d-dimensional lattice polytope (with respect to $\Lambda = \mathbb{Z}^d$, and $0 \in \operatorname{int} P$.

Definition 7.1 *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*

$$\begin{aligned} \langle\, \eta_F, x \,\rangle \;&=\; -c_F \quad \forall x \in F \\ \langle\, \eta_F, x \,\rangle \;&\geq\; -c_F \quad \forall x \in P \end{aligned}$$

In this case, c_F is called (signed) integral distance *of the origin from the facet F. The origin is in the polytope if $c_F \geq 0$.*

Recall that the *lattice distance* of a lattice point v from a lattice hyperplane H is given by

$$|\langle u, x \rangle - \langle u, v \rangle| \tag{7.1}$$

if the hyperplane H has primitive normal u and x is any point in H.

Definition 7.2 *A polytope P is called* reflexive, *if there exists $w \in \operatorname{int} P \cap \Lambda$ such that all facets have lattice distance 1 from w.*

Equivalently, for any facet $F \in \mathcal{F}(P)$ there exists a lattice point $u \in \Lambda^\star$ 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.

Proposition 7.3 *Let P be a reflexive polytope with respect to w, then*

$$\operatorname{int} P \cap \Lambda = \{w\}$$

Proof. Let $F \in \mathcal{F}(P)$. By definition, no lattice point lies strictly between the hyperplanes $\operatorname{aff}(F)$ and its parallel hyperplane through w. See Figure 7.1. Therefore, $\operatorname{conv}(w, F) \cap \Lambda = \{w\} \cup (F \cap \Lambda)$. Since $P = \bigcup_{F \in \mathcal{F}(P)} \operatorname{conv}(w, F)$, the statement follows. □

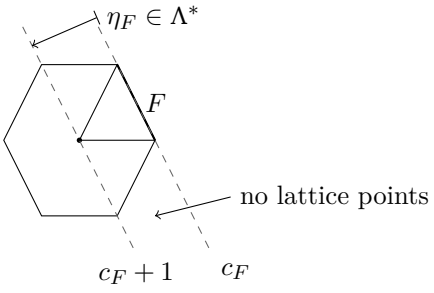


Fig. 7.1: Proof of Proposition 7.3.

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.

As a consequence, here is the promised characterization of reflexive polytopes (Exercise 7.5).

Exercise 7.5

Proposition 7.4 *Let P be a d-dimensional lattice polytope in $\mathbb{R}^d$ with $0 \in \operatorname{int} P$. Then the following are equivalent:*

- *P reflexive,*
- *P^* lattice polytope*
- *P^* reflexive.* □

Fig. 7.2: (Non-)reflexive polygons

This result is illustrated in Proposition 7.1. Coming back to Proposition 7.3, the reader will prove in Exercise 7.6 that any lattice polygon with one interior lattice points is also a reflexive polygon (see Exercise 7.14 for the complete list). However, this is not true in dimension 3 and higher

(Exercise 7.7). Yet, this property suffices to compute Ehrhart polynomials of 3-dimensional lattice polytopes (Exercise 7.8). Exercise 7.6 Exercise 7.7 Exercise 7.8

From Theorem 4.25 and Proposition 7.3 we can immediately deduce the finiteness of these polytopes.

Corollary 7.5 *There exist only finitely many reflexive d-polytopes up to isomorphism.* □

Surprisingly, these finite sets of polytopes together with their faces 'cover' the space of *all* lattice polytopes.

Proposition 7.6 *Any lattice polytope is isomorphic to the face of a reflexive polytope (of higher dimension).*

Proof. Any lattice polytope with no interior lattice points is isomorphic to the face of a lattice polytope with interior lattice points. Therefore, we may assume that $P \subseteq \mathbb{R}^d$ is a d-dimensional lattice polytope with $\mathbf{0} \in \operatorname{int}(P)$.

Let $F_1, \ldots, F_k$ be the facets of P, so in our notation

$$P \;=\; \{x \in \mathbb{R}^d \,:\, \langle \eta_{F_i}, x \rangle \geq c_{F_i} \;\text{ for } i = 1, \ldots, k\}\,,$$

for $c_{F_i} \in \mathbb{Z}_{\leq -1}$. If $c_k \leq -2$, we define P' as the set of $(x, x_{d+1}) \in \mathbb{R}^{d+1}$ satisfying

- $\langle \eta_{F_i}, x \rangle \geq c_{F_i}$ for $i = 1, \ldots, k-1$
- $\langle \eta_{F_k}, x \rangle - x_{d+1} \geq c_{F_k} + 1$
- $x_{d+1} \geq -1$

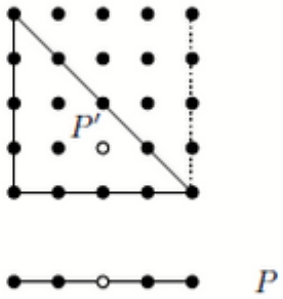


Fig. 7.3: P and P'

Then P' is a lattice polytope with $(\mathbf{0}, 0) \in \operatorname{int}(P')$ that is combinatorially a wedge over P, see Figure 7.3. All the previous inequalities describe facets of P'. In particular, P' has $P \times \{-1\}$ as a facet. Let us define the invariant

$$f(P) \;:=\; \sum_{F \in \mathcal{F}(P)\,:\, c_{F_i} < -1} |c_{F_i}|\,.$$

Then $f(P') < f(P)$. In particular, iterating this construction yields after finitely many steps a lattice polytope P'' such that $f(P'') = 0$, i.e., P'' is reflexive. □

7.1.1 Dimension 2 and the number 12

We turn to a remarkable result about reflexive polygons.

Theorem 7.7 *The numbers of boundary lattice points of a reflexive polygon and its dual add up to* 12.

by a reflex-

At least five different proofs appear in [28, 46]: by exhaustion, by a walk in the space of polygons, using toric varieties, using modular forms, or via relations in $\mathrm{SL}_2(\mathbb{Z})$.

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 a complete unimodular fan.

Lemma 7.8 *Let Σ be a complete unimodular fan in $\mathbb{R}^2$. Every ray $\tau \in \Sigma[1]$ with primitive generator v is contained in precisely two 2-cones $\sigma = \mathrm{cone}(v, w)$ and $\sigma' = \mathrm{cone}(v, w')$ in Σ.*

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, $w + w' = k_2 v$. □

Lemma 7.9 *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 $P^\star$ dual to v_2 has length $2 - a$. (If v_2 is not a vertex, then $a = 2$.)

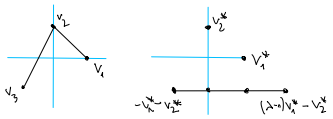


Fig. 7.5: The dual edge has length $2 - a$

Proof. Let $\{v_1^\star, v_2^\star\}$ be the basis dual to the basis $\{v_1, v_2\}$. Then the vertices of $P^\star$ dual to the edges at v_2 containing v_1 and v_3 respectively are $v_1^\star + v_2^\star$ and $(a-1)v_1^\star + v_2^\star$, respectively. □

In light of this lemma, Theorem 7.7 follows from the following theorem.

Theorem 7.10 *Let Σ be a complete unimodular fan in $\mathbb{R}^2$. Then*

$$\sum_{\tau \in \Sigma[1]} (3 - a(\tau)) = 12\,, \tag{7.2}$$

where $a(\tau)$ is the paramter defined in Lemma 7.8.

This is the theorem we will prove by walking in the space of fans.

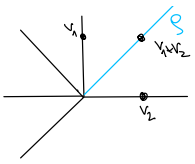


Fig. 7.6: Smooth blow-up of a 2-dimensional fan

Proof (of Theorem 7.7). Let P be a reflexive polygon with vertex set V and boundary points B. Then B is the set of generators of a uniomdular complet fan, and we get

$$12 \;=\; \sum_{u \in B} 3 - a(u) \;=\; \sum_{u \in B} 1 \;+\; \sum_{u \in V} 2 - a(u) \;=\; |\partial P \cap \Lambda| \;+\; |\partial P^\star \cap \Lambda^\star|$$

□

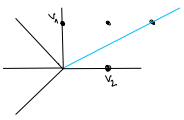


Fig. 7.7: Not a smooth blow-up

Here are the steps in our walk.

Definition 7.11 *Let Σ be a unimodular fan in $\mathbb{R}^2$, and let $\sigma \in \Sigma[2]$ with primitive generators v_1, v_2. Set $\varrho := \operatorname{cone}(v_1 + v_2)$, and*

$$\operatorname{pull}(\Sigma; \varrho) := \Sigma \setminus \{\sigma\} \cup \{\varrho, \operatorname{cone}(\varrho, v_1), \operatorname{cone}(\varrho, v_2)\}\,.$$

We say that the fan $\operatorname{pull}(\Sigma; \varrho)$ is obtained as a smooth blow-up of σ in Σ.

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 7.9, these steps preserve the validity of equation (7.2). You will classify 2-dimensional fans which are minimal with respect to blow ups in Exercise 7.10. You will consider the 3-dimensional setting in Exercise 7.11.

Exercise 7.9

Exercise 7.10

Exercise 7.11

Lemma 7.12 *If the complete unimodular fan Σ in $\mathbb{R}^2$ satisfies (7.2), and Σ' is a smooth blow-up of Σ, then Σ' also satisfies (7.2).*

It remains to show that these steps connect the space of fans.

Theorem 7.13 *Let Σ and Σ' be two complete unimodular fans in $\mathbb{R}^2$. Then there is another complete unimodular fan Σ'' which can be obtained by a sequence of smooth blow-ups from both Σ and Σ'.*

The corresponding statement in general dimension has been conjectured by Oda. This Strong Oda Conjecture is still wide open. This question is stronger than the question of connectivity of the space of complete unimodular fans, where we can have intermediate blow-donws. This weaker statement has been shown in all dimensions. It was the foundation of the celebrated Weak Factorization Theorem.

For the proof of Theorem 7.13 we need three lemmas.

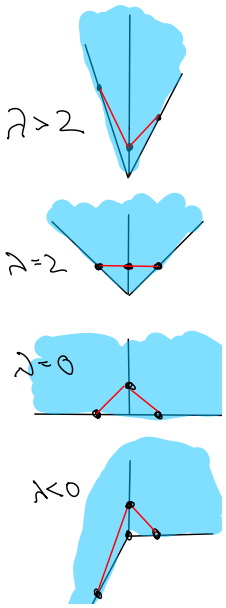


Fig. 7.8: Different λ's

Lemma 7.14 *In the notation of Lemma 7.8 let $P := \operatorname{conv}(\mathbf{0}, v, w, w')$.*

(1) $\mathbf{0}$ is a vertex of $\operatorname{conv}(\mathbf{0}, w, v, w')$ if and only if $a(\tau) \leq 1$, but
(2) v is a vertex of $\operatorname{conv}(\mathbf{0}, w, v, w')$ if and only if $a(\tau) \leq 1$.

Proof. $\mathbf{0}$ is a vertex if and only if $\frac{1}{2}(w + w') = \frac{a}{2}v$ for some $\frac{a}{2} > 0$, so $a \geq 1$.

Similarly, v is a vertex if and only if $\frac{a}{2} < 1$, so $a \leq 1$. □

Using this fact we can prove a crucial step towards connectivity:

Lemma 7.15 *Let Σ be a unimodular fan in $\mathbb{R}^2$ which refines a unimodular fan Σ'. Then Σ can be obtained from Σ' by a sequence of smooth blow-ups.*

Proof. Use induction on $r := |\,\Sigma[1] \setminus \Sigma'\,|$. If $r = 0$, we have $\Sigma = \Sigma'$.

If $r \geq 1$, all ray parameters of rays of Σ that do not belong to Σ' must be ≥ 1 by Lemma 7.14(1). On the other hand, if $\sigma \in \Sigma'[2]$ contains

rays of Σ 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 7.14 and hence must have parameter $= 1$. □

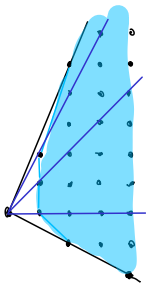


Fig. 7.9: Unimodularly subdividing a 2-cone

Lemma 7.16 *Let $\sigma \subset \mathbb{R}^2$ be a pointed 2-cone. Then there is a unimodular fan Σ with support σ.*

We will prove the corresponding statement in general dimension in Chapter 8.

Proof. Consider the polyhedron $P := \operatorname{conv}(\sigma \cap \mathbb{Z}^2 \setminus \{\mathbf{0}\})$. The bounded segments of P generate cones which form a fan with support σ. For any such segment, the triangle it forms with $\mathbf{0}$ does not contain any other lattice points. Hence, it is unimodular by Pick's theorem. □

Proof (Theorem 7.13). The collection $\overline{\Sigma} := \{\sigma \cap \sigma' \,:\, \sigma \in \Sigma, \sigma' \in \Sigma'\}$ is a complete fan. By Lemma 7.16, there is a complete unimodular fan Σ'' refining $\overline{\Sigma}$. Now, we use the previous lemma. □

Putting it all together, Lemma 7.12 and Theorem 7.13 imply Theorem 7.10.

7.1.2 Dimension 3 and the number 24

In dimension three, there is a possibly even more striking result.

Theorem 7.17 *If P is a 3-dimensional reflexive polytope, then*

$$\sum_{e \text{ edge of } P} \operatorname{length} e \cdot \operatorname{length} e^\star \;=\; 24\,.$$

This result was first proved by Dimitrios Dais as follows. By [8], 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 [17], 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 7.12).

Exercise 7.12

Lemma 7.18 *Let Σ be a complete unimodular fan in $\mathbb{R}^d$. Every $(d-1)$-cone $\tau \in \Sigma[d-1]$ with primitive generators $v_1, \ldots, v_{d-1}$ is contained in precisely two d-cones $\sigma = \operatorname{cone}(\tau, v_d)$ and $\sigma' = \operatorname{cone}(\tau, v'_d)$ in Σ.*

In this situation, there are unique integers $a(\tau, v_i)$ so that

$$v_d + v'_d \;=\; \sum_{i=1}^{d-1} a(\tau, v_i) v_i\,. \qquad \square$$

Next, we construct a complete unimodular fan from a reflexive 3-polytope.

Proposition 7.19 *Let P be a 3-dimensional reflexive polytope, and let $\mathcal{T}$ be a full lattice triangulation of its boundary. Then $\Sigma := \{\operatorname{cone}\sigma \,:\, \sigma \in \mathcal{T}\}$ is a complete unimodular fan.*

Further, if $\operatorname{conv}(v_1, v_2) \in \mathcal{T}[1]$ is contained in an edge e of P, then the dual edge $e^\star$ of $P^\star$ has length $2 - a(\tau, v_1) - a(\tau, v_2)$ where $\tau = \operatorname{cone}(v_1, v_2) \in \Sigma$. (Otherwise $a(\tau, v_1) + a(\tau, v_2) = 2$.)

Proof. For Σ, 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 $\operatorname{conv}(\mathbf{0}, \sigma)$ is unimodular.

In order to compute the length of $e^\star$, consider the two 3-cones $\sigma = \operatorname{cone}(\tau, v_3)$ and $\sigma' = \operatorname{cone}(\tau, v_3')$ of Σ 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 $\{v_1^\star, v_2^\star, v_3^\star\}$ be the basis dual to the basis $\{v_1, v_2, v_3\}$. Then the vertices of $P^\star$ dual to the facets of P containing $\{v_1, v_2, v_3\}$ and $\{v_1, v_2, v_3'\}$ are $v_1^\star + v_2^\star + v_3^\star$ and $v_1^\star + v_2^\star + (a(\tau, v_1) + a(\tau, v_2) - 1)v_3^\star$, respectively. □

Thus, Theorem 7.17 follows from the following fan version.

Theorem 7.20 *Let Σ be a complete unimodular fan in $\mathbb{R}^3$. Then*

$$\sum_{\substack{\tau \in \Sigma[2] \\ \text{with primitive} \\ \text{generators } v_1, v_2}} (2 - a(\tau, v_1) - a(\tau, v_2)) \;=\; 24\,.$$

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.

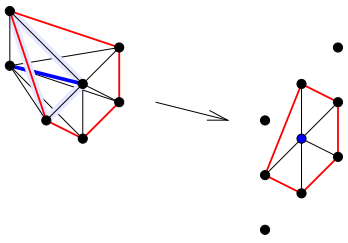


Fig. 7.10: Quotient fan $\Sigma\,/\,\varrho$

Lemma 7.21 *Let Σ be a complete unimodular fan in $\mathbb{R}^3$, and let $\varrho \in \Sigma[1]$ with primitive generator v. Then the projection $\pi\colon \mathbb{R}^3 \to \mathbb{R}^3/\mathbb{R}v$ maps $\operatorname{star}(\varrho; \Sigma)$ to a complete unimodular fan $\Sigma\,/\,\varrho$. If $\tau \in \operatorname{star}(\varrho; \Sigma)$ is a 2-cone with primitive generators v, v', then the corresponding ray $\pi(\tau)$ of $\Sigma\,/\,\varrho$ 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 $\pi(v_1) + \pi(v_2) = a(\tau, v')\pi(v')$. □

Proof (Theorem 7.20). Let us first collect what we need. Our fan Σ gives rise to a triangulation of the 2-sphere with vertex set $\Sigma[1]$, edge set $\Sigma[2]$, and triangle set $\Sigma[3]$. As such, we have $3|\,\Sigma[1]| - |\,\Sigma[2]| = 6$ from Euler's formula and double counting of edge-triangle-incidences. Also, we have $\sum_{v\in\Sigma[1]} \deg v = 2|\,\Sigma[2]|$, where $\deg v$ denotes the number of edges containing the vertex v. Armed with these formulas we compute

$$\begin{aligned}
&\sum_{\substack{\tau\in\Sigma[2]\\ \text{with primitive}\\ \text{generators } v_1,v_2}} (2 - a(\tau,v_1) - a(\tau,v_2)) \\
&\qquad = \sum_{\mathrm{cone}(v)\in\Sigma[1]} \sum_{\substack{\tau\in\Sigma[2]\\ \tau=\mathrm{cone}(v,w)}} (1 - a(\tau,w)) \\
&\qquad = \sum_{\mathrm{cone}(v)\in\Sigma[1]} \sum_{\substack{\tau\in\Sigma[2]\\ \tau=\mathrm{cone}(v,w)}} ((3 - a(\tau,w)) - 2) \\
&\qquad = \sum_{\mathrm{cone}(v)\in\Sigma[1]} 12 - 2\deg v = 12|\,\Sigma[1]| - 4|\,\Sigma[2]| = 24\,.
\end{aligned}$$

Here we have used Theorem 7.10 for the quotient fans $\Sigma\,/\,\varrho$ in the third equality. □

7.2 The combinatorics of simplicial reflexive polytopes

Throughout, let $P \subset \mathbb{R}^d$ be a d-dimensional reflexive polytope with the origin of the lattice $\Lambda = \mathbb{Z}^d$ in its interior.

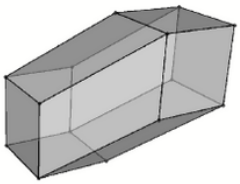


Fig. 7.11: a reflexive 3-polytope

7.2.1 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.

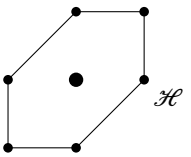


Fig. 7.12: The hexagon

Example 7.22

$d = 2$: $|\mathcal{V}(P)| \leq 6$, *only attained by the reflexive hexagon* $\mathscr{H}$, *see Figure 7.12.*
$d = 3$: $|\mathcal{V}(P)| \leq 14$, *only attained by the polytope in Figure 7.11*
$d = 4$: $|\mathcal{V}(P)| \leq 36$, *only attained by* $\mathscr{H} \times \mathscr{H}$.

Based upon these observations we state the following daring conjecture.

Conjecture 7.23 $|\mathcal{V}(P)| \leq 6^{\frac{d}{2}}$, *equality holds for* d *even and* $P \cong \mathscr{H}^{\frac{d}{2}}$.

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.

7.2.2 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. We will see that free sums of reflexive polytopes are reflexive, but let us first recall the definition. For two polytopes $P_i \subseteq \mathbb{R}^{d_i}$, $d_i \in \mathbb{Z}_{\geq 0}$, with $0 \in \operatorname{int}(P_i)$ $(i = 1, 2)$ the *free sum* is the polytope

$$P_1 \circ P_2 \;:=\; \operatorname{conv}(P_1 \times \{\mathbf{0}\}, \{\mathbf{0}\} \times P_2) \subseteq \mathbb{R}^{d_1+d_2}$$

Example 7.24

(1) Let $P_1 = P_2 = [-1, 1]$ be a segment of length 2 around the origin. Then $P_1 \circ P_2$ is the convex hull of $\pm e_1, \pm e_2$. See Figure 7.13.

(2) For $P_1 = \mathscr{H}$ and $P_2 = [-1, 1]$ the free sum $P_1 \circ P_2$ is $\operatorname{BiPyr}(\mathscr{H})$. See Figure 7.14.

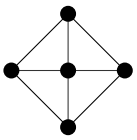


Fig. 7.13: The free sum of $P_1 = P_2 = [-1, 1]$

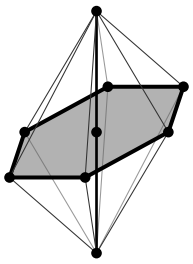


Fig. 7.14: The free sum of a hexagon and a segment.

You will examine the relation between products and sums in Exercise 7.13.

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.

Proposition 7.25 *Let $P_1,\ P_2$ be reflexive. Then*

$$\begin{aligned} \operatorname{ehr}_{P_1 \times P_2}(k) &= \operatorname{ehr}_{P_1}(k) \operatorname{ehr}_{P_2}(k)\ , \\ h^\star_{P_1 \circ P_2}(t) &= h^\star_{P_1}(t) h^\star_{P_2}(t)\,. \end{aligned}$$

Exercise 7.13

While the first result follows directly from the construction, the second one is not obvious. We will leave this as an exercise. We will prove it in the last chapter (Corollary 8.27). Here is our main theorem. Its proof will occupy the remainder of this section.

Theorem 7.26 *Let P be reflexive and simplicial. Then $|\mathcal{V}(P)| \leq 3d$, and equality holds only if d is even and $P \cong \underbrace{\mathscr{H} \circ \ldots \circ \mathscr{H}}_{\frac{d}{2}}$.*

Simplicial reflexive d-polytopes with $3d-1$ vertices are also completely known.

7.2.3 The addition property

Lattice points in reflexive polytopes satisfy a partial addition property. For this let us define a relation.

Definition 7.27 *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:

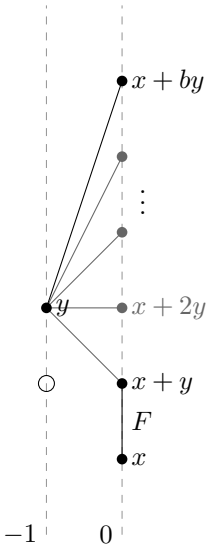
Proposition 7.28 *Let $x, y \in \partial P \cap \Lambda$, $x \neq y$. Then*

(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 $a, b \in \mathbb{Z}_{\geq 1}$ 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) and (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 $b \in \mathbb{Z}_{\geq 1}$ such that $x + by \sim y$. □



You can use this in Exercise 7.14 to construct the complete list of 16 reflexive polygons.

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 7.15).

Corollary 7.29 *The diameter of the vertex-edge graph of a simplicial reflexive polytope is at most three.*

Exercise 7.14

Exercise 7.15

7.2.4 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 $b_1, \ldots, b_d$. Let $F_i \in \mathcal{F}(P)$ such that

$$F_i \cap F \;=\; \operatorname{conv}(b_1, \ldots, b_{i-1}, b_{i+1}, , \ldots, b_d)\,.$$

Then there exists a unique $m_i \in \mathcal{V}(P)$ such that $\mathcal{V}(F_i) = \{b_1, \ldots, m_i, \ldots, b_d\}$ for $i = 1, \ldots, d$.

Note that $b_1, \ldots, b_d$ is in general not a lattice basis. We can still define the dual (vector space) basis $b_1^*, \ldots, b_d^* \in (\mathbb{R}^d)^*$. 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.

Lemma 7.30 *Let vv be a vertex of a simplicial reflexive polytope with $\langle \eta_F, v\rangle = 0$.*

(1) For $1 \le d$

$$v \in F_i \iff v = m_i \iff \langle b_i^*, v\rangle < 0.$$

In particular, there is always such a facet F_i containing v.

(2) If $\langle b_i^*, m_i\rangle = -1$ and $\langle \eta_F, m_i\rangle = 0$ for all $i = 1, \ldots, d$, then $b_1, \ldots, b_d$ is a lattice basis.

Proof. $i \in \{1, \ldots, d\}$.

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 $0 \in \operatorname{int}(P)$. Since $\langle \eta_F, m_i\rangle \ge 0$, 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: $j \ne i$: $\langle \eta_F, b_j\rangle + \alpha_i \langle b_i^*, b_j\rangle = -1$,
$\langle \eta_F, m_i\rangle + \alpha_i \langle b_i^*, m_i\rangle = -1$. Now, we can prove (1) and (2).

(1) $\eta_F = -b_1^* - \ldots - b_d^*$, $\langle \eta_F, v\rangle = 0 \Rightarrow \exists i : \langle b_i^*, v\rangle < 0$. 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: $\alpha_i = 1$ $\forall i = 1, \ldots, d$, hence $b_i^* = \eta_{F_i} - \eta_F \in \Lambda^*$ $\forall i = 1, \ldots, d$. Therefore $x = \sum_{i=1}^d \lambda_i b_i \in \Lambda \Rightarrow \lambda_i = \langle b_i^*, x\rangle \in \mathbb{Z} \Rightarrow b_1, \ldots, b_d$ is a lattice basis. □

Combining this lemma with the addition property for the lattice points in the dual reflexive polytope yields our desired result.

Proposition 7.31 *$v \in \mathcal{V}(P)$, $\langle \eta_F, v\rangle = 0$. If $-F \in \mathcal{F}(P)$, then there are $I, J \subseteq \{1,\ldots,d\}, I \cap J = \emptyset, |I| = |J|$ 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

$$I \;:=\; \{i \in \{1,\ldots,d\} \qquad \text{such that} \langle b_i^*, v\rangle \;<\; 0\} \qquad \neq\; \emptyset\,.$$

Then $i \in I \overset{(1)}{\Longrightarrow} v = m_i$.

$$\begin{aligned}
-F \in \mathcal{F}(P) &\implies F_i \cap F \;=\; \emptyset \\
&\implies \eta_{F_i} \not\sim \eta_{-F} = -\eta_F \\
&\overset{\text{Addition}}{\Longrightarrow} \eta_{F_i} - \eta_F \in \partial P^* \cap \Lambda^* \\
&\implies -1 \le \langle \alpha_i^* b_i^*, \pm b_i^*\rangle = \pm\alpha_i \in \mathbb{Z} \\
&\overset{\alpha_i>0}{\Longrightarrow} \alpha_i = 1 \\
&\implies \langle b_i^*, v\rangle = \langle \eta_{F_i} - \eta_F, v\rangle = \underbrace{\langle \eta_{F_i}, v\rangle}_{=-1} - \underbrace{\langle \eta_F, v\rangle}_{=0} \\
&\implies \langle b_i^*, v\rangle = -1
\end{aligned}$$

Using the same argument for $-F$ shows that $\langle b_j^*, v\rangle > 0 \Longrightarrow \langle b_j^*, v\rangle = 1$. □

7.2.5 Special facets

We can now prove Theorem 7.26. The key idea is the following notion (due to Øbro).

Definition 7.32 (Special Facet) *Let $F \in \mathcal{F}(P)$ such that $\sum_{v\in\mathcal{V}(P)} v \in \mathrm{cone}(F)$. 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 $i \in \{-1, 0, 1, \ldots\}$):

$$H_P(F,i) \;:=\; \{v \in \mathcal{V}(P) : \langle\, \eta_F, v\,\rangle = i\}\ \forall i \in \mathbb{Z}_{\ge -1}$$

Clearly,

$$|H_P(F,0)| \;=\; d\,.$$

Moreover, Lemma 7.30 yields

$$|H_P(F,1)| \;\le\; d.$$

By definition of a special facet we have the following inequality:

$$0 \geq \langle \eta_F, \sum_{v \in \mathcal{V}(P)} v \rangle = \sum_{i \geq -1} i|H_P(F,i)| = -d + \sum_{i \geq 1} i|H_P(F,i)|. \quad (7.3)$$

Hence, we can simply count the vertices:

$$|\mathcal{V}(P)| = \sum_{i \geq -1} |H_P(F,i)| \leq \underbrace{|H_P(F,-1)|}_{=d} + \underbrace{|H_P(F,0)|}_{\leq d} + \underbrace{\sum_{i \geq 1} |H_P(F,i)|}_{\leq d} \leq 3d. \quad (7.4)$$

It remains to consider the equality case ($|\mathcal{V}(P)| = 3d$). In this case, equality in (7.3) 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 (7.3) and show that any vertex of P lies in $H_P(F,i)$ for $i = -1, 0, 1$. Therefore, $-\eta_F \in P^\star$. So, $-P^\star \subseteq P^\star$, and thus $-P^\star = P^\star$. 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 7.30(1) yields

$$H_P(F,0) = \{m_1, \ldots, m_d\},$$

as defined in the previous subsection. Let $k \in \{1, \ldots, k\}$. By Proposition 7.31 there are $I, J \subseteq \{1, \ldots, d\}, I \cap J = \emptyset, |I| = |J|$ such that $m_k = \sum_{j \in J} b_j - \sum_{i \in I} b_i$. Since all $m_1, \ldots, m_d$ are pairwise different, Lemma 7.30(1) yields that $m_k = b_{j_k} - b_k$ for some $j_k \in \{1, \ldots, d\}$, $j_k \neq k$. In other words,

$$\begin{aligned} \sigma : \{1, \ldots, d\} &\to \{1, \ldots, d\} \\ k &\mapsto j_k \end{aligned}$$

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,

$$P = \mathrm{conv}(\pm b_1, \pm(b_1 - b_2), \pm b_2, \ldots, \pm b_d, \pm(b_{d-1} - b_d), \pm b_d).$$

It remains to show that $b_1, \ldots, b_d$ is a lattice basis, since it that case

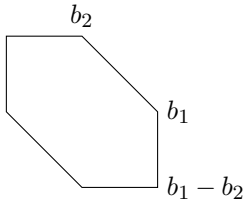


Fig. 7.15: The situation for $d = 2$.

$$P \;\cong\; \underbrace{\mathscr{H} \circ \cdots \circ \mathscr{H}}_{\frac{d}{2}} .$$

See Figure 7.15. We observe that for any $i = 1, \ldots, d$

$$\langle b_i^*, m_i \rangle = \langle b_i^*, b_{j_i} - b_i \rangle = -1$$

$$\langle \eta_F, m_i \rangle = 0$$

Hence, Lemma 7.30(2) finishes the argument. This proves Theorem 7.26.

7.3 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 $\Lambda = \mathbb{Z}^d$ and $\bar{\Lambda} = \mathbb{Z}^{d+1}$. Recall from Chapter 2 that the *cone over* P (or the *homogenization* of P) is

$$C_P \;:=\; \operatorname{cone}(\{1\} \times P) \subseteq \mathbb{R}^{d+1}$$

with dual cone

$$C_P^\star \;:= \{u \in (\mathbb{R}^{d+1})^* \;\; \langle u, x \rangle \geq 0 \; \forall x \in C_P\}$$

The unique *primitive inner normals* of facets $F \in \mathcal{F}(P)$ are $u_F = (-c_F, \eta_F)$, since

$$\langle\, (-c_F, \eta_F), (x, 1) \,\rangle = \langle\, \eta_F, x \,\rangle - c_F \begin{cases} = 0 & x \in F \\ \geq 0 & x \in P \end{cases}$$

By duality of cones we have the correspondence:

$$\begin{aligned} \text{facets of } P \;&\leftrightarrow\; \text{rays of } C_P^\vee \\ F \;&\leftrightarrow\; \operatorname{cone}(u_F) \end{aligned}$$

We are going to denote cones associated to lattice polytopes as Gorenstein cones.

Definition 7.33 *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 $u_C \in \bar{\Lambda}^\star$ 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.

See Exercise 7.16 for some properties. Exercise 7.16

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.

Theorem 7.34 *The following are equivalent for a d-dimensional lattice polytope $P \subseteq \mathbb{R}^d$ of degree s and codegree r:*

(1) rP reflexive
(2) $\forall k \geq r$: $\operatorname{int}(kP) \cap \Lambda = w + (k-r)P \cap \Lambda$ for some $w \in \operatorname{int}(rP) \cap \Lambda$
(3) $C_P^\vee$ Gorenstein cone

In this case: $u_{C_P^\star} = \{r\} \times w$ and r is the unique $k \in \mathbb{Z}_{\geq 1}$ such that kP is reflexive.

Proof. Let $x' = (k, x)$ for $x \in kP$, $u'_F = (-\beta_F, u_F)$ for a facet $F := \{x : \langle u_F, x \rangle \geq \beta_F$ of P, and $\bar{\Lambda} := \mathbb{Z}e_0 \times \Lambda$. The cone C_P over P has facets $F' = \operatorname{cone}(F)$ defined by $\langle u'_F, x' \rangle \geq 0$ for facets F of P.

(1) $\Rightarrow$ (2): We prove both inclusions in (2). The direction "$\supseteq$" is clear.

We prove the other direction. Let w be the unique interior point of rP, so that

$$\langle u'_F, w' \rangle \;=\; 1 \qquad \text{for all facets } F \text{ of } C_P.$$

Let $x \in \operatorname{int}(kP) \cap \Lambda$ for some $k \geq r$. Then

$$\langle u'_F, x' - w' \rangle \;=\; \underbrace{\langle u'_F, x \rangle}_{\geq 1} - \underbrace{\langle u'_F, w' \rangle}_{=1} \;\geq\; 0 \;\forall F \in \mathcal{F}(P)$$

In particular,

$$x' - w' \in (C_P^\star)^\star \;=\; C_P \qquad \text{and} \qquad \langle u'_P, x' - w' \rangle \;=\; k - r$$

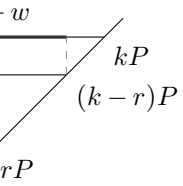
Hence, $x - w \in (k-r)P \cap \Lambda$, as desired.

(2) $\Rightarrow$ (3): We want to show that $\langle u_F, w \rangle = 1$ for all facets F of P. For this let us define $C' := \operatorname{cone}(w, F')$. Choose a lattice basis $b_1, \ldots, b_{d+1}$ such that $b_1, \ldots, b_d \in \operatorname{cone}(F)$ and $b_{d+1} \notin \operatorname{cone}(F)$. By translating b_{d+1} with a multiple of $\sum_{i=1}^d b_d$ we can assume that $b_{d+1} \in C'$.

Therefore, $b_{d+1} \in \operatorname{int} C_P \cap \bar{\Lambda}$. In particular, there exists some $k \geq r$ such that $b_{d+1} \in \operatorname{int}(\{k\} \times kP) \cap \bar{\Lambda}$. By assumption, there exists some $m \in (k-r)P \cap \Lambda$ such that $b_{d+1} = w' + m'$ and

$$\langle b^*_{d+1}, F' \rangle \;=\; 0 \;=\; \langle u_F, F' \rangle$$

for the dual lattice vector to b_{d+1}. As 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.

(3) $\Rightarrow$ (1): Let $w' \in \operatorname{int} C_P \cap \bar{\Lambda}$ such that

$$\langle\, u'_F, w' \,\rangle \;=\; 1 \qquad\qquad \text{for all facets } F \text{ of } P\,.$$

Then there exists $k \geq r$ such that $w' \in \operatorname{int} kP \cap \bar{\Lambda}$. Let $F \in \mathcal{F}(P)$, so,

$$1 \;=\; \langle\, w', u'_F \,\rangle \;=\; -k\beta_F \;+\; \langle\, u_F, w \,\rangle\,.$$

Hence, kP is reflexive (w.r.t. w).

Let us show the additional last statement in the theorem. Assume $k > r$, then

$$\begin{aligned} |\operatorname{int} kP \cap \bar{\Lambda}| \;&\geq\; |w + (k-r)P \cap \bar{\Lambda}| = |(k-r)P \cap \bar{\Lambda}| \\ &\geq\; |P \cap \bar{\Lambda}| > 1 \end{aligned}$$

This is a contradiction. □

See Exercise 7.17 for an example of a non-Gorenstein cone. This motivates our main definition.

Definition 7.35 (Gorenstein polytope) *P is a* Gorenstein polytope *of index r if it satisfies the conditions of Theorem 7.34.*

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 7.3. For instance, reflexive polytopes are precisely Gorenstein polytopes of codegree 1. You will prove a criterion similar to Proposition 7.28 in Exercise 7.19

Example 7.36

(1) See Figure 7.17. $C_P^\vee$ is not a Gorenstein cone, $\Rightarrow P$ is not a Gorenstein polytope. $r = \operatorname{codeg} P = 1$, $\operatorname{int} P \cap \Lambda = 2 > 1$; $h_0^* = 1$, $h_1^* = 2$.

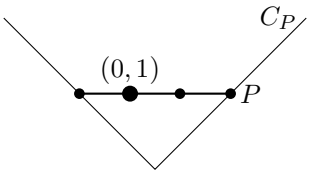
(2) See Figure 7.18. $P = [0,1]^2$ is a Gorenstein polytope of codegree $r = \operatorname{codeg}(P) = 2$. ($2P$ is reflexive, see Figure 7.19).

(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 7.20.*

Corollary 7.37 *For a Gorenstein polytope of index r we have*

$$\operatorname{ehr}_P(-k) \;=\; (-1)^d \operatorname{ehr}_P(k-r) \qquad\qquad \forall k \in \mathbb{Z}$$

Proof. This follows from Theorem 7.34(2). □



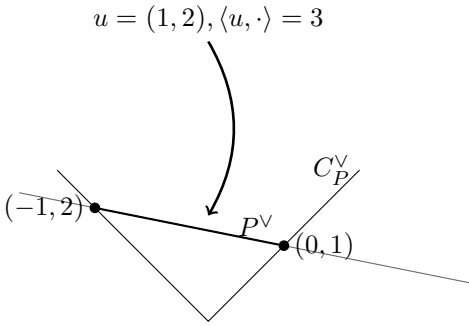


Fig. 7.17: The cone over $P = [-1,2]$ and its Gorenstein dual.

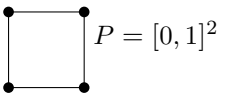


Fig. 7.18: The unit square

Exercise 7.17

Exercise 7.18

Exercise 7.19

Exercise 7.20

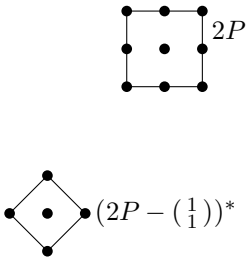


Fig. 7.19: Twice the unit square and its dual.

Theorem 7.38 *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional lattice polytope of degree s and codegree r. Then the following three conditions qgree.*

(1) P is a Gorenstein polytope of index r.
(2) $\widehat{\mathrm{Ehr}}_P(t^{-1}) = (-1)^{d+1} t^r \widehat{\mathrm{Ehr}}_P(t)$
(3) $h^\star_i = h^\star_{s-i} \quad \forall i = 0, \ldots, s$

Proof. For a Gorenstein polytope of index r we have

$$\begin{aligned}\sum_{k\geq 1} |\operatorname{int} kP \cap \bar{\Lambda}| t^k &= \sum_{k\geq 1} (-1)^d \mathrm{ehr}_P(-k)\, t^k = \sum_{k\geq 1} \mathrm{ehr}_P(k-r)\, t^k \\ &= \sum_{k\geq r} \mathrm{ehr}_P(k-r)\, t^k = t^r \sum_{k\geq 0} \mathrm{ehr}_P(k)\, t^k\end{aligned}$$

So by Stanley's Reciprocity Theorem (Theorem 3.42)

$$\widehat{\mathrm{Ehr}}_P\left(\frac{1}{t}\right) = (-1)^{d+1} \widehat{\mathrm{Ehr}}_{\operatorname{int} P}(t) = (-1)^{d+1} t^r \widehat{\mathrm{Ehr}}_P(t)\,. \tag{7.5}$$

This proves the first implication.

On the level of rational functions we get

$$\begin{aligned}\frac{\sum_{i=0}^s h^\star_i t^i}{(1-t)^{d+1}} &= (-1)^{d+1} \frac{1}{t^r} \frac{\sum_{i=0}^s h^\star_i \left(\frac{1}{t}\right)^i}{(1-\frac{1}{t})^{d+1}} = (-1)^{d+1} \frac{1}{t^r} \cdot \frac{1}{t^s} \frac{\sum_{i=0}^s h^\star_i t^{s-i}}{(1-\frac{1}{t})^{d+1}} \\ &= \frac{\sum_{i=0}^s h^\star_i t^{s-i}}{(1-t)^{d+1}} = \frac{\sum_{i=0}^s h^\star_{s-i} t^i}{(1-t)^{d+1}}\,,\end{aligned}$$

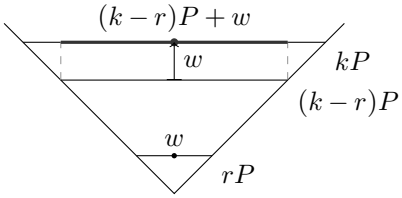


Fig. 7.20

where the first equality follows from (7.5). Comparing the coefficients yields (3). Conversely, if (3) holds, then

$$(-1)^{d+1} \widehat{\mathrm{Ehr}}_P\left(\frac{1}{t}\right) = t^r \widehat{\mathrm{Ehr}}_P(t)\,,$$

and by reciprocity

$$(-1)^{d+1} \widehat{\mathrm{Ehr}}_P\left(\frac{1}{t}\right) = \widehat{\mathrm{Ehr}}_{\operatorname{int} P}(t) = (-1)^d \sum_{k\geq 1} \mathrm{ehr}_P(-k)\, t^k\,,$$

while

$$t^r \widehat{\mathrm{Ehr}}_P(t) = \sum_{k\geq 0} \mathrm{ehr}_P(k)\, t^{k+r} = \sum_{k\geq r} \mathrm{ehr}_P(k-r)\, t^k\,.$$

Again comparing coefficients gives $\mathrm{ehr}_P(-k) = (-1)^d \mathrm{ehr}_P(k-r)$ for $k \geq r$ and $\mathrm{ehr}_P(-k) = 0$ for $1 \leq k \leq r$. Hence

$$\mathrm{ehr}_P(-k) = (-1)^d \mathrm{ehr}_P(k-r) \qquad \text{for } k \geq 1\,. \qquad \square$$

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.

Proposition 7.39 *Let P be a Gorenstein polytope (as in Theorem 7.34). Then*

$$\begin{aligned} P^\vee &:= \{x \in C_P^\star \,:\, \langle u_{C_P^\star}, x\rangle = 1\} \\ &= \operatorname{conv}((-c_F, \eta_F) : F \in \mathcal{F}(P)) \end{aligned}$$

is also a Gorenstein polytope of the same dimension, degree and codegree as P, called the dual Gorenstein polytope.

Proof. $u_{C_P^\star} = w$, hence, $\langle u_{C_P^\star}, u_P \rangle = r$. Let $G \in \mathcal{F}(P^\star)$. Then $\langle u_G, G \rangle = 0$ and $\langle u_G, u_{C_P} \rangle = 1$. Therefore, $rP^\star$ is reflexive. □

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 7.36(2) with $r = 2$, $P^\vee$ is just isomorphic to P. See also Exercise 7.21. Exercise 7.21

Let us consider the case of a reflexive polytope P, say, $0 \in \operatorname{int}(P)$. Then we recover the duality of reflexive polytopes:

$$\begin{aligned} P^\vee &= \{x \in (\mathbb{R}^{d+1})^* : \langle x, (y,1)\rangle \geq \ \forall y \in P,\ \langle x, (0,1)\rangle = 1\} \\ &= \{(x,1) : \langle x, y\rangle \geq -1 \ \forall y \in P\} \\ &= P^\star \times 1. \end{aligned}$$

This gives another proof of Proposition 7.4.

7.4 Finiteness of Gorenstein polytopes of given degree

In this section we are going to prove the following result in Ehrhart theory:

Theorem 7.40 *There exist only finitely many symmetric h^*-polynomials of lattice polytopes of degree s.*

Equivalently, the normalized volume of any Gorenstein polytope of degree s is bounded by a number depending only on s.

We remark that Theorem 7.40 follows from Theorem 5.11, since for Gorenstein polytopes the leading coefficient $h_s^* = h_0^* = 1$ is fixed!

Then, why do we prove Theorem 7.40? The answer is that we can give a complete, self-contained and insightful proof for Gorenstein polytopes without having to rely on Theorem 5.10 whose proof is out of reach of this book. Corollary 5.2 lets us deduce an interesting consequence:

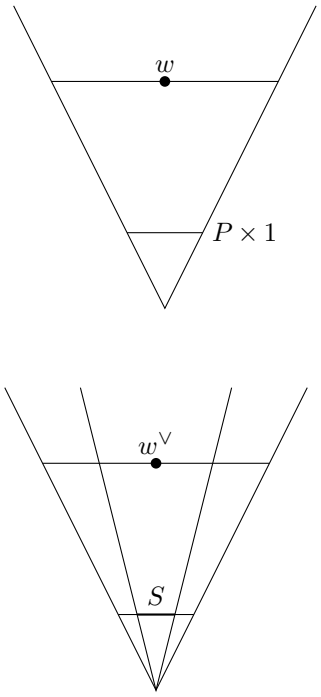


Fig. 7.21: P and $P^\vee$.

Corollary 7.41 *There exist only finitely many Gorenstein polytopes of degree s up to isomorphism and lattice pyramid constructions.*

For $s = 1$ and $s = 2$ these finite lists are completely known.

The proof of Theorem 7.40 proceeds in the same way as that of Theorem 5.11. We use Proposition 5.12 to reduce the problem to the existence of Cayley decompositions of Gorenstein polytopes with large dimension and small degree. Next, instead of invoking Theorem 5.10, we can prove this claim directly.

Proposition 7.42 *If P is a Gorenstein d-polytope of degree $s \geq 1$ and $d \geq 2s$, then P is a Cayley polytope of lattice polytopes in dimension $\leq 2s - 1$.*

Proof. See Figure 7.21. Let us identify P and $P \times 1$. We denote by $w^\vee = u_{C_P}$ and by $w = u_{C_P^\star}$. Then we can choose a lattice d-simplex $S \subseteq P^\vee$ such that $w^\vee \in \operatorname{cone}(S)$. We can find

$$x_1, \ldots, x_k \in \mathcal{V}(S) \qquad \text{such that } w^\vee = \left(\sum_{i=1}^{k} x_i\right) + x_{k+1}\,,$$

where $x_{k+1} \in \Pi(S)$. Let us recall $d + 1 - s = r = \langle w, w^\vee \rangle$. We consider two cases: If $x_{k+1} = 0$, then $d + 1 - s = k$, so $k = d + 1 - s \geq d + 2 - 2s$. If $x_{k+1} \neq 0$, then we get $d + 1 - s = k + \langle w, x_{k+1} \rangle \leq k + \deg(S) \leq k + \deg(P^\vee) = k + s$ by Proposition 3.19, Theorem 3.37, Proposition 7.39. Therefore, in this case, $k + 1 \geq d + 2 - 2s$. In any case, Lemma 5.9 implies that $P^\vee$ is a Cayley polytope of length $\geq d + 2 - 2s$.

The proof of Theorem 7.40 follows now from applying Proposition 5.12 with $N = 2s - 1$.

7.5 Classification of reflexive polytopes

7.5.1 Smooth reflexive polytopes

Øbro [43]

7.5.2 All reflexive polytopes

Kreuzer and Skarke [33]

7.6 Problems

included on page 176

7.1. Show that for $\emptyset \neq A \subset \mathbb{R}^d$ (equipped with some scalar product) we always have $((A^\circ)^\circ)^\circ = A$.

7.2. Let P be a d-dimensional lattice polytope containing $\mathbf{0}$ in its interior. Show that $\mathcal{V}(P^*) \subset \mathbb{Q}^d$.

included on page 176

7.3. Let $T : \mathbb{R}^d \to \mathbb{R}^d$ be a linear map that sends a d-dimensional polytop P containing $\mathbf{0}$ in its interoir to Q (*i.e.* $Q = T(P)$). What is the relation between Q^* and P^*?

included on page 176

7.4. Show that $S_{d,\mathbf{1}} := \operatorname{conv}(e_1, \ldots, e_d, -\mathbf{1})$ is reflexive.

included on page 177

7.5. Prove Proposition 7.4.

included on page 178

7.6. Show that a lattice polygon is reflexive if and only if it contains precisely one interior lattice point.

included on page 178

7.7. 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?

included on page 178

7.8. Compute h^*-polynomial and Ehrhart polynomial of a 3-dimensional reflexive polytope having b many lattice points.

included on page 180

7.9. Prove Lemma 7.12.

included on page 180

7.10. Classify unimodular fans in $\mathbb{R}^2$ which are minimal with respect to blow-ups.

included on page 180

7.11. Define smooth blow-ups for three-dimensional unimodular fans (or higher-dimensional); and show the invariance of the equality in Theorem 7.20 under smooth blow-ups.

included on page 181

7.12. Prove Lemma 7.18.

included on page 184

7.13. Let P, Q be any polytopes (not necessarily with vertices in the lattice) that contain $\mathbf{0}$ in the interior.
Show that the dual of the product is the free sum of the duals.

included on page 185

7.14. The complete list of unimodular equivalence classes of reflexive polygons is in Figure 7.22.

(1) Pick your favorite and compute its dual polytope. To which representative in the list is it unimodularly equivalent?

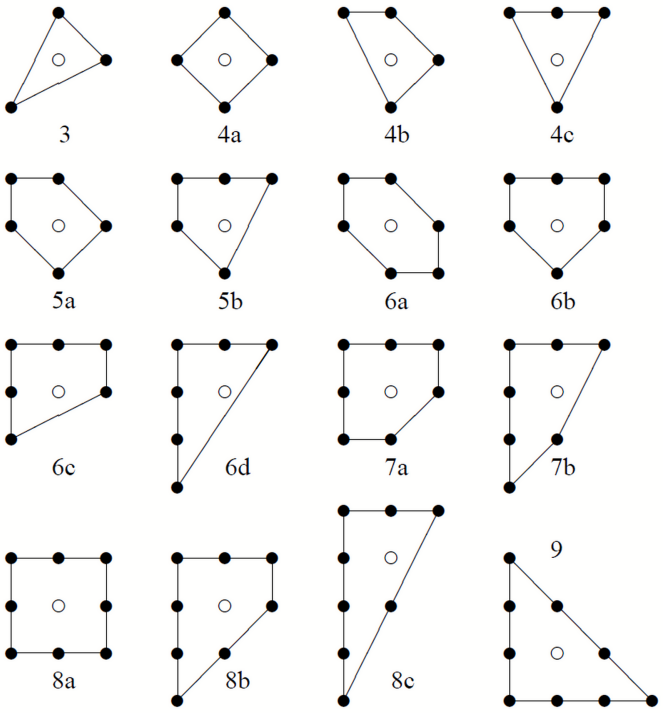


Fig. 7.22: The 16 reflexive polygons.

(2) Use Proposition 7.28 to prove that this list is complete.

included on p

7.15. Prove Corollary 7.29, *i.e.* show that any pair of vertices of a simplicial reflexive polytope can be connected by at most three edges.

included on p

7.16. Let C be a $(d+1)$-dimensional polyhedral cone. Show that $C \cong C_P$ if and only if there is a lattice point w in the dual lattice with $\langle w, x \rangle = -1$ for all primitive generators of C.
Further, in this case w is primitive and in the interior of C^*.

included on page 191

7.17. Show explicitely that for $P = \mathrm{conv}(0, 3)$ the dual cone C_P^* is not Gorenstein.

included on page 191

7.18. Let $\Lambda \subset \mathbb{R}^d$ be a lattice of rank d. We may choose (why ?) $v_1, \ldots, v_d \in \Lambda$ recursively such that v_{i+1} has the minimal non-zero distance from the subspace $\langle v_1, \ldots, v_i \rangle$. Show that $v_1, \ldots, v_d$

is a lattice basis of Λ. In particular, any primitive vector of Λ can be completed to a lattice basis.

included on page 191

7.19. Show that any pair of vertices of a Gorenstein polytope of index $r > 1$ either is in a common face or is an antipodal pair (with respect to the point w, where w is the unique interior point of rP).

included on page 191

7.20. 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 ?

included on page 193

7.21. Find the dual Gorenstein polytope for the Gorenstein polytope $P = [0, 1]^2$ and show that it is isomorphic to P.

Unimodular Triangulations

8

Contents

- unimodular cover
- integer Carathéodory + BGHMW
- IDP
- vectors u, v, w; covectors a, b, c; scalars α, β, γ

- `\psubdiv` $\mathcal{S}$
- `\regsubdiv{\vw}{V}` $\mathcal{S}_w(V)$
- `\reglift{\vw}{V}` $\mathrm{lift}(w)$
- `\regfunction{\vw}{V}` Ψ_w
- `\pull{\psubdiv}{\vv}` $\mathrm{pull}(\mathcal{S}; v)$

It 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. (Yet, there is no theorem to date that would pin down what the previous statement actually means.)

We will define regular triangulations, and prove our first theorem for cones in Section 8.2. Then, we define the particularly nice class of compressed polytopes in Section 8.3, and give a few examples of important triangulations. Section 8.4 can be regarded as a capstone section of these notes. We use unimodular triangulations to prove unimodality of the $h^\star$ coefficients of Gorenstein polytopes with regular unimodular triangulation, tying together ideas from Chapters 3 and 7 with this one. Finally, in Section 8.5, 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.

8.1 Regular Triangulations

Regular subdivisions form a well-behaved class of subdivisions of a given point configuration. Regular subdivisions are partially ordered by refinement (see Definition 8.2). Hence, they form a poset. This poset is isomorphic to the face lattice of the so called secondary polytope. This was proved by Gel′fand, Kapranov, and Zelevinsky [22], see also [19]. The proof is beyond the scope of these notes. The maximal elements in the poset are the regular triangulations, which in particular proves that every point configuration has a triangulation (see Proposition 8.7 in the next section).

In this and the following section we will work with point configurations. We may think of $\mathscr{A} = P \cap \mathbb{Z}^d$, but the results with workmore generally for any point set and produce a subdivision of its convex hull. Though we will use this only at one place, the whole theory easlily carries over to vector configurations and subdivisions of fans.

There is a close connection to linear and integer programming as well as to Gröbner bases of toric ideals. We will not cover this here, but the interested reader can find this in [19] or [57].

Definition 8.1 (regular subdivision) *A subdivision $\mathcal{S}$ of the point configuration $\mathscr{A}$ is* regular *if there is a weight vector $\omega \in \mathbb{R}^{\mathscr{A}}$ such that $\mathcal{S}$ is the projection of the lower hull of the polyhedron*

$$\operatorname{lift}(\omega) \;:=\; \operatorname{conv}(v \times [\omega_v, \infty) \;:\; v \in \mathscr{A})$$

in $\mathbb{R}^{d+1}$. *We write* $\mathcal{S}_\omega(\mathscr{A})$ *or* $\mathcal{S}_\omega(P)$ *for the regular subdivision induced by* ω.

A subdivision is a triangulation if all cells are simplices.

Here, the lower hull is the polyhedral complex of those facets whose normal has negative first coordinate. The faces of $\mathcal{S}_\omega(\mathscr{A})$ are the domains of linearity of the function $\Psi_\omega \colon P \to \mathbb{R}$ given by

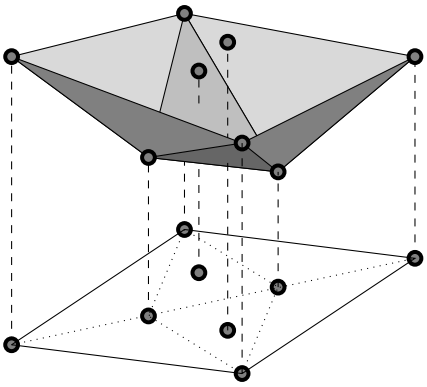
$$v \;\mapsto\; \min\bigl\{h \;:\; (v,h) \in \operatorname{lift}(\omega)\bigr\}\,.$$

Less formally, a regular subdivision can be thought of as a subdivision that can be realized as a "convex folding" of the polytope (Figure 8.1 on the left). All three triangulations in Figure 8.2 are regular while the triangulation on the right in Figure 8.1 is not.

Fig. 8.1: A regular triangulation via folding

Definition 8.2 *Refinement of a subdivision.*

Fig. 8.2: Regular triangulations



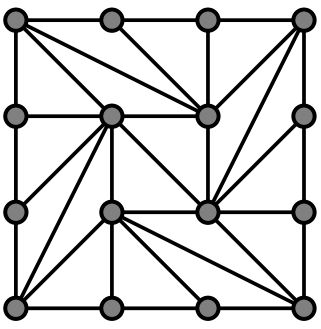
Lemma 8.3 *Given a point configuration* $\mathscr{A} \subset \mathbb{R}^d$ *and a weight vector* $\omega \in \mathbb{R}^{\mathscr{A}}$ *a set* F *is a face of* $\mathcal{S}_\omega(\mathscr{A})$ *if and only if there is a functional* $a_F \in (\mathbb{R}^d)^\star$ *and an* $\alpha_F \in \mathbb{R}$ *such that for all* $v \in \mathscr{A}$

$$\langle\, a_F, v \,\rangle + \omega_v \;\geq\; \alpha_F$$

and F *is the convex hull of those* v *that attain equality.*

Proof. This is a direct translation of the definition. □

Fig. 8.3: A lift of a regular triangulation.



Lemma 8.4 *Given a point configuration* $\mathscr{A} \subset \mathbb{R}^d$ *and a weight vector* $\omega \in \mathbb{R}^{\mathscr{A}}$ *define* $\omega' \in \mathbb{R}^{\mathscr{A}}$ *by* $\omega'_v := \Psi_\omega(v)$. *Then* $\operatorname{lift}(\omega) = \operatorname{lift}(\omega')$ *(and hence,* $\mathcal{S}_\omega(\mathscr{A}) = \mathcal{S}_{\omega'}(\mathscr{A})$ *as well as* $\Psi_\omega = \Psi_{\omega'}$*), and for all* $F \in \mathcal{S}_{\omega'}(\mathscr{A})$ *and all* $v \in \mathscr{A}$ *we have*

$$v \in F \iff \langle\, a_F, v \,\rangle + \omega'_v = \alpha_F\,, \tag{8.1}$$

where we use the certificates (a_F, α_F) *from Lemma 8.3.*

Fig. 8.4: A non-regular triangulation.

We will call a pair $(\mathcal{S}_{\omega'}(\mathscr{A}), \omega')$ satisfying (8.1) for all $F \in \mathcal{S}_{\omega'}(\mathscr{A})$ *tight*. If all $v \in \mathscr{A}$ are vertices of $\mathcal{S}_\omega(\mathscr{A})$, then $(\mathcal{S}_\omega(\mathscr{A}), \omega)$ is automatically tight.

Lemma 8.5 *Let* $\mathcal{S}_\omega(\mathscr{A})$ *and* $\mathcal{S}_{\omega'}(\mathscr{A})$ *be two regular subdivisions of the same point set* $\mathscr{A}$. *For* $\varepsilon > 0$ *small enough* $\mathcal{S}_{\omega-\varepsilon\omega'}(\mathscr{A})$ *is a regular refinement of* $\mathcal{S}_\omega(\mathscr{A})$. *In particular, if* $\mathcal{S}_{\omega'}(\mathscr{A})$ *is a triangulation, then* $\mathcal{S}_{\omega-\varepsilon\omega'}(\mathscr{A})$ *is one too.*

Proof. If

$$\langle\, a_F, a \,\rangle \;+\; \omega(a) \;-\; \alpha_F \;>\; 0$$

for some face F of $\mathcal{S}_\omega(\mathscr{A})$ and $a \in \mathscr{A}$, then also

$$\langle\, a_F, a \,\rangle \;+\; (\omega - \varepsilon\omega')(a) \;-\; \alpha_F \;>\; 0$$

for ε small enough. Thus, in $\mathcal{S}_\omega(\mathscr{A})$, the weight function at most subdivides within faces. Hence, $\omega - \varepsilon\omega'$ produces is a refinement of $\mathcal{S}_\omega(\mathscr{A})$.

Clearly, if ω' produces a triangulation of $\mathscr{A}$, then this is true also for the restriction to all faces of $\mathcal{S}_\omega(\mathscr{A})$. □

8.2 Pulling Triangulations

Pulling refinements are a useful tool for constructing regular triangulations.

Definition 8.6 (Pulling Refinements) *Consider a point configuration $\mathscr{A} \subset \mathbb{R}^d$ and $\mathcal{S}$ subdivision of $P = \operatorname{conv}(\mathscr{A})$. For $u \in \mathscr{A}$ we obtain the* pulling refinement $\operatorname{pull}(\mathcal{S}; u)$ *when we replace every face $F \in \mathcal{S}$ which contains u by the pyramids $\operatorname{conv}(u, F')$ where F' runs over all faces $F' \preceq F$ which do not contain u.*

The definition works mutatis mutandis for vector configurations and subdivisions of fans.

Fig. 8.5: A pulling refinement.

Here are some facts about the structure of pulling subdivisions. We say that a vertex v of a polytope P is an *apex* of P if all other vertices are contained in a facet of P.

Proposition 8.7 *Let $\mathscr{A}$ be a point configuration in $\mathbb{R}^d$ and $\mathcal{S}$ a subdivision of $\mathscr{A}$ (not necessarily regular).*

(1) Pulling preserves regularity.
(2) Pulling all points in $\mathscr{A}$ in some order results in a triangulation whose vertex set is all of $\mathscr{A}$.
(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.

Part (3) identifies the triangulation constructed back in Theorem 2.35 with the triangulation obtained by pulling the vertices in the given order.

Proof. (1): Let $\mathcal{S} = \mathcal{S}_\omega(\mathscr{A})$ be a regular subdivision of $P = \operatorname{conv}(\mathscr{A})$ induced by tight weights $\omega \in \mathbb{R}^{\mathscr{A}}$. Let $u \in \mathscr{A}$. Set $\omega'_u := \omega_u - \varepsilon$ and $\omega'_v := \omega_v$ for all $v \in \mathscr{A} \setminus \{u\}$. We claim that then, for small enough $\varepsilon > 0$, the pulling refinement $\operatorname{pull}(\mathcal{S}; u)$ is induced by the weights ω'.

To prove the claim, we will show that every face of $\operatorname{pull}(\mathcal{S}; u)$ lifts to a lower face of $\operatorname{lift}(\omega')$. Then we show that these faces cover P, and hence, all lower faces of $\operatorname{lift}(\omega')$ project to faces of $\operatorname{pull}(\mathcal{S}; u)$.

A face F of $\operatorname{pull}(\mathcal{S}; u)$ is either

- a face of $\mathcal{S}$ not containing u or
- it is of the form $\operatorname{conv}(u, F')$ where $F' \preceq G \in \mathcal{S}$ with $u \in G \setminus F'$.

In the former case we have $\omega|_F = \omega'|_F$ so that $\operatorname{lift}(\omega|_F) = \operatorname{lift}(\omega'|_F)$ which, for small enough ϵ, still is a lower face of $\operatorname{lift}(\omega')$. (This imposes finitely many upper bounds on ϵ.)

In the latter case, there are certificates

$$(a_{F'}, \alpha_{F'}) \quad \text{and} \quad (a_G, \alpha_G) \in (\mathbb{R}^d)^\star \times \mathbb{R}\,.$$

For the new weight ω' (and ε small enough) we have

$$\langle a_{F'}, u \rangle \;+\; \omega'_u \;-\; \alpha_{F'} \;>\; 0 \quad \text{and} \tag{8.2}$$

$$\langle a_G, u \rangle \;+\; \omega'_u \;-\; \alpha_G \;<\; 0\,. \tag{8.3}$$

Thus, there are coefficients $\lambda, \mu > 0$ with $\lambda + \mu = 1$ such that

$$\lambda \left[\langle a_{F'}, u \rangle + \omega'_u - \alpha_{F'} \right] \;+\; \mu \left[\langle a_G, u \rangle + \omega'_u - \alpha_G \right] \;=\; 0\,.$$

Then $\lambda(a_{F'}, \alpha_{F'}) + \mu(a_G, \alpha_G)$ is a certificate for the face $F := \operatorname{conv}(F', u)$ of $\mathcal{S}_{\omega'}(\mathscr{A})$: for all $v \in \mathscr{A}$ we have

$$\lambda \left[\langle a_{F'}, v \rangle + \omega'_v - \alpha_{F'} \right] \;+\; \mu \left[\langle a_G, v \rangle + \omega'_v - \alpha_G \right] \;\geq\; 0$$

with equality for $v \in F'$ and for $v = u$, while for $v \notin F'$ and $v \neq u$ we have a stricly positive summand.

To finish the proof of our claim, we take a point $v \in P$ and show that it belongs to a face of $\operatorname{pull}(\mathcal{S}; u)$. Let $G \in \mathcal{S}$ be the face which contains v in its relative interior. If $u \notin G$, we have $G \in \operatorname{pull}(\mathcal{S}; u)$ and we are home. If $u \in G$, consider the ray from u through v. It hits the boundary of G in the relative interior of some face $F' \preceq G$. But then $v \in F := \operatorname{conv}(F', u)$ by construction, and $F \in \operatorname{pull}(\mathcal{S}; u)$.

(2): By definition, every face of $\operatorname{pull}(\mathcal{S}; u)$ which contains u is a pyramid with apex u. (In particular, u is a vertex of $\operatorname{pull}(\mathcal{S}; u)$.)

If $Q \in \mathcal{S}$ has v as an apex, then every face of Q containing v has v as an apex. Consequently, every face of $\operatorname{pull}(\mathcal{S}; u)$ inside Q and containing v still has v as an apex. After pulling all lattice points, all lattice points are vertices of the subdivision, and the cells have each of their vertices as apices. Hence, 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 maximal cell. □

Using pulling refinements (the fan version), we get unimodular triangulations of cones — this corresponds to resolution of singularities for toric varieties. It works like a charm, in arbitrary characteristic.

Theorem 8.8 *Every rational cone has a regular unimodular triangulation.*

Note that the remarkable claim in this theorem is the fact that we can make the triangulation *unimodular*. We already know that there are regular triangulations.

Proof. Given a rational cone C, we can, using pulling subdivisions on the vector configuration of primitive generators of C, find a triangulation $\mathcal{T}$ of C into simplicial cones. We will proceed by induction on lexicographically ordered pairs (D, N) where D is the maximal determinant D occuring in the triangulation and N is the number of cones of determinant D.

If $D = 1$ then the triangulation is unimodular.

If $D > 1$, we choose an inclusion-minimal cone $F \in \mathcal{T}$ of determinant D. Let $v_1, \ldots, v_k$ be the primitive generators of F. Pick one of the $D-1$ non-zero lattice vectors in the fundamental parallelepiped $\Pi(F)$: $u = \sum \lambda_j v_j$. (We have chosen F minimal so that all λ_j are positive.) If $v_1, \ldots, v_d$ are the primitive generators of a face G of $\mathcal{T}$ containing F, then G is subdivided into cones G_j $(j = 1, \ldots, k)$ where the generator v_j is replaced by u. As $\det(G_j) = \lambda_j \det(G) = \lambda_j D < D$ all the cones in $\mathrm{pull}(\mathcal{T}; u)$ have determinant $< D$. □

8.3 Compressed Polytopes

The notion of compressed polytopes was coined by Richard Stanley [54]. Surprisingly many well-known polytopes fall into this category.

Definition 8.9 *A lattice polytope $P \subset \mathbb{R}^d$ is* compressed *if all lattice points in P are vertices, and all pulling triangulations are unimodular.*

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 every point of P has lattice distance at most one from 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). The result was subsequently also proven by Ohsugi and Hibi [44] and by Sullivant [58].

Theorem 8.10 *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.

As a pulling triangulation of P induces a pulling triangulation on all faces of P, faces of compressed polytopes are compressed. In the same way, the facet-width-one property is inherited by faces.

Lemma 8.11 *If P has width one with respect to all its facets then the same is true for all faces of P.*

Proof. By induction on the codimension it is enough to consider a facet F of P. If G is a facet of F, there is a facet F' of P so that $G = F \cap F'$. Denote the primitive inner normal of F' to P by η. The restriction of η to $\operatorname{aff}(F)$ is an integral inner normal of G to F. (It might, a priori, not be primitive.) But at every point of $F \subset P$, η takes values in $[\langle \eta, G \rangle, \langle \eta, G \rangle + 1]$. That is, F has width one with respect to G. □

Proof (of Theorem 8.10). (2) $\Longrightarrow$ (1): Choose an ordering of the lattice points in P and let $\mathcal{T}$ be the corresponding pulling triangulation. The restriction of $\mathcal{T}$ to a face of P is the pulling triangulation induced by the restricted ordering of the lattice points. Thus, by induction on the dimension, the triangulations of the facets are unimodular.

Using the recursive description of Proposition 8.7(3) we see that every maximal simplex in $\mathcal{T}$ is the join of a unimodular simplex S in some facet with the first lattice point v_1 that was pulled. The facet width assumtion guarantees that v_1 is at distance one from S so that $\operatorname{conv}(S, v_1)$ is also unimodular.

The other implications are easy. □

Example 8.12 *Examples of compressed polytopes include*

(1) the Birkhoff polytope,
(2) order polytopes and hypersimplices,
(3) stable set polytopes of perfect graphs.

We can apply the above characterization of compressed polytopes to triangulate bigger polytopes using hyperplane arrangements.

Definition 8.13 *A collection $\mathscr{A} := \{a_1, \ldots, a_r\} \subset (\mathbb{Z}^d)^\star$ of functionals that span $(\mathbb{R}^d)^\star$ is said to form a* unimodular matrix *A if all $(d \times d)$–minors of the $r \times d$-matrix with rows a_i are either 0, 1 or -1.*

Such a collection induces an infinite arrangement of hyperplanes

$$\{v \in \mathbb{R}^d \,:\, \langle a_i, v \rangle = k\} \quad \text{for} \quad i = 1, \ldots, r \text{ and } k \in \mathbb{Z}\,,$$

The induced subdivision of $\mathbb{R}^d$ is the lattice dicing *of $\mathbb{R}^d$ by A.*

The notion *lattice dicing* was coined by [21].

Definition 8.14 *We call a lattice polytope P whose collection of primitive facet normals forms a unimodular matrix* facet unimodular.

The above hyperplane arrangement slices P into dicing cells. *We call this subdivision the* canonical subdivision *of a facet unimodular polytope.*

Lemma 8.15 *Let $P \subseteq \mathbb{R}^d$ be a facet unimodular polytope.*

(1) The cells of a lattice dicing are lattice polytopes.
(2) Canonical subdivisions are regular.
(3) Every face of a facet unimodular polytope is again facet unimodular in its own affine lattice. Canonical subdivisions induce canonical subdivisions on faces.

Exercise 8.1

The proof of this lemma ist left as Exercise 8.1.

Theorem 8.16 *Suppose that $P \subset \mathbb{R}^d$ 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. □

As a direct application of Theorem 8.16, flow polytopes as well as polytopes with facets in the root system of type A have regular unimodular triangulations. This method also shows that if P has a (regular) unimodular triangulation then so do all its integral dilates cP. You will work out the details in Exercise 8.2.

Theorem 8.17 *If P has a (regular) unimodular triangulation $\mathcal{T}$ then its dilation cP has one too, for every positive integer c.* □

Exercise 8.2

— a fact which we will prove with a different method in Theorem 8.17 below.

8.4 Special Simplices in Gorenstein Polytopes

The goal of this section is to prove the following theorem of Bruns and Römer.

Theorem 8.18 *The $h^\star$-vector of a Gorenstein polytope with a regular unimodular triangulation is unimodal. That is, $1 = h_0^\star \leq \ldots \leq h^\star_{\lfloor s/2 \rfloor} \geq \ldots \geq h_s^\star$.*

This theorem and its proof are due to Bruns and Roemer [16]. For general Gorenstein polytopes the theorem fails, as shown by Payne and Mustata [41]. However, it is still open whether the following property might suffice.

Definition 8.19 *A lattice d-polytope $P \subseteq \mathbb{R}^d$ is said to possess the* integer decomposition property *(*IDP*) if for every $k \in \mathbb{Z}_{\geq 2}$ and for every lattice point $u \in kP \cap \mathbb{Z}^d$ there exist $v_1, \ldots, v_k \in P \cap \mathbb{Z}^d$ such that $u = v_1 + \cdots + v_k$.*

Equivalently, let $C \subset \mathbb{R}^{d+1}$ be the cone spanned by $P \times \{1\}$. Then P is IDP if and only if the semigroup of lattice points in C is generated by lattice points in $P \times \{1\}$. As Exercise 8.3 shows, being IDP is weaker than having a unimodular triangulation. Polytopes having the IDP-property are also called *integrally closed* or sometimes *normal*.

The central tool in the proof of Theorem 8.18 is the notion of a special simplex. The use of special simplices in this context had been pioneered by Athanasiadis [1]. Note that this notion of a *special* simplex is different from the special facets introduced in the classification of smooth reflexive polytopes.

Definition 8.20 *A simplex $S = \operatorname{conv}(v_1, \ldots, v_k)$ for $v_1, \ldots, v_k \in \subseteq P \cap \Lambda$ inside a polytope P is* special *if $S \cap F$ is a facet of S for all facets F of P.*

Example 8.21 *Here are some simple examples of special simplices.*

(1) The only special simplex in the unit simplex Δ is Δ itself
(2) See Figure 8.6 for two different special simplices in the unit cube. The reflexive cube $[-1.1]^d$ has also the origin as a special simplex.
(3) Figure 8.7 shows a special simplex in the tetrahedron with vertices $\mathbf{0}$, e_1, e_2 and $2e_3$. Note that also the tetrahedron itself is special.
(4) Figure 8.8 shows two special simplices in the bipyramid over a triangle.
(5) A special simplex in the Birkoff polytope for $(n \times n) -$ matrices is, for instance, the simplex spanned by the vertices corresponding to the permutations matrices for the permutations

$$i \longmapsto i + k \mod n \qquad \text{for } 1 \leq l \leq n\,.$$

Example 8.22 *If S is am $(r-1)$dimensional special simplex in a polytope P of codegree r, then S is necessarily unimodular. Otherwise, $kS \subseteq kP$ for some $k < r$ contains a lattice point.*

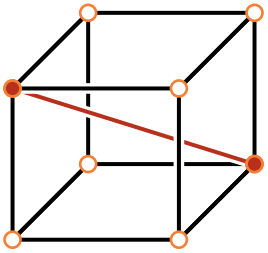
Lemma 8.23 *Let P be a Gorenstein polytope.*

If P has the IDP property, then P has a special simplex with $\operatorname{codeg}(P)$ many vertices.

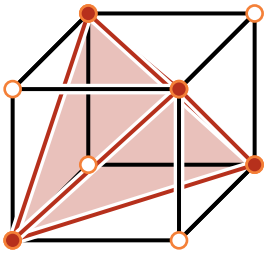
If P has a special simplex with $r = \operatorname{codeg}(P)$ many vertices, then its vertices have lattice distance zero or one from all facets.

Proof. Let $P \subset \mathbb{R}^d$ be a polytope with the IDP property and Gorenstein with degree s. Let $u_P \in C_P$ be the Gorenstein point in the cone over P.

Because P has the IDP property, we can write $u_P = v_1 + \ldots + v_r$ for $v_1, \ldots, v_r \in (\{1\} \times P) \cap \mathbb{Z}^{d+1}$. We claim that $S := \operatorname{conv}(v_1, \ldots, v_r)$ is a special simplex.



(a) A 1-dimensional special simplex



(b) A 2-dimensional special simplex

Fig. 8.6: Two special simplices in the unit cube

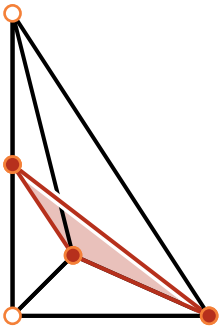


Fig. 8.7: A special simplex in a Lawrence prism

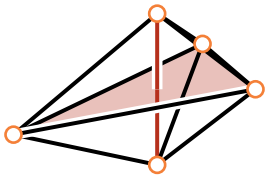


Fig. 8.8: Special simplices in a triangle bipyramid. Note that there may be more than one such.

Fig. 8.9

Every facet F of P is dual to a vertex w of the Gorenstein dual $\{1\} \times P^\vee$. Then $\langle w, v_i \rangle \geq 0$ for all $i = 1, \ldots, r$, and $\langle w, u_P \rangle = \sum \langle w, v_i \rangle = 1$. Thus, $\langle w, v_j \rangle = 1$ for exactly one index j. Hence $v_j \notin F$) for this j while $\langle w, v_i \rangle = 0$, that is, $v_i \in F$ for all $i \neq j$. Hence, $S \cap F$ contains all but one of the v_i. □

The punchline in the proof of Theorem 8.18 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.

Definition 8.24 *Let $S = \operatorname{conv}(v_1, \ldots, v_r) \subseteq \{1\} \times P$ be a special simplex. Denote by $\Gamma(P, S)$ the subcomplex of ∂P generated by faces of the form $F_1 \cap \ldots \cap F_r$ where F_i is a facet of C_P with $v_i \notin F_i$ for $i = 1, \ldots, r$.*

Lemma 8.25 *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 $\{\operatorname{conv}(S \cup F) \ : \ F \in \mathcal{T}\}$ 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 work in the cone $C_p \subset \mathbb{R}^{d+1}$ over $\{1\} \times P$. Add a 1-coordinate to the simplex vertices $\{1\} \times S = \operatorname{conv}(v_1, \ldots, v_r)$. The set of primitive facet normals of C_P is partitioned into sets $\mathscr{A}_1, \ldots, \mathscr{A}_r$ so that $\langle a, v_j \rangle = \delta_{ij}$ for $a \in \mathscr{A}_i$. Consider the concave piecewise linear function

$$\omega(x) := \min \left\{ \sum_{i=1}^{r} \langle a_i, x \rangle \ : \ a_i \in \mathscr{A}_i \text{ for } i = 1, \ldots, r \right\} .$$

We will prove the following.

(1) The domains of linearity of ω are $\operatorname{cone}(F \cup S)$ for $F \in \Gamma(P, S)$. This shows that these polytopes form a regular subdivision $\Gamma(P, S) \star S$ of P.
(2) If F is a (unimodular) simplex in Γ, then $\operatorname{conv}(S \cup F)$ is a (unimodular) simplex.
(3) The $\operatorname{conv}(S \cup F)$ cover P.
(4) The $\operatorname{conv}(S \cup F)$ and their faces form a polyhedral complex.
(5) If $\mathcal{T}$ is the restriction to $\Gamma(P, S)$ of a regular triangulation of P then $\mathcal{T} \star S$ is regular.

(1): To compute $\omega(x)$, we choose, for $i = 1, \ldots, r$, an element $a_i \in \mathscr{A}_i$ minimizing $\langle \cdot, x \rangle$. So the domains of linearity of ω are indexed by tuples $(a_1, \ldots, a_r) \in \prod_{i=1}^{r} \mathscr{A}_i$ and characterized by inequalities

$$\langle a_i, x \rangle \leq \langle a_i', x \rangle \text{ for all } a_i' \in \mathscr{A}_i \, . \tag{8.4}$$

A choice $(a_1, \ldots, a_r)$ determines a face F of $\Gamma(P,S)$. We claim that the set of points $x \in \{1\} \times P$ for which $\omega(x) = \sum_{i=1}^r \langle a_i, x \rangle$ agrees with $\operatorname{conv}(F \cup S)$. This then shows that these polytopes form a regular subdivision of P.

Observe that the elements of $\mathscr{A}_i$ agree along $\{1\} \times S$, and $\langle a_i', x \rangle \geq \langle a_i, x \rangle = 0$ along $x \in F$. This implies that $\omega(x) = \sum_{i=1}^r \langle a_i, x \rangle$ along $\operatorname{cone}(F \cup S)$.

Conversely, suppose $x \in \{1\} \times P$ so that $\omega(x) = \sum_{i=1}^r \langle a_i, x \rangle$. Set $x_\Gamma := x - \sum_{j=1}^r \langle a_j, x \rangle v_j$. For any $a_i' \in \mathscr{A}_i$ we have

$$\langle a_i', x_\Gamma \rangle \;=\; \langle a_i', x \rangle - \langle a_i, x \rangle \;\geq\; 0$$

by (8.4). Thus, $x_\Gamma \in C$. On the other hand, $\langle a_i, x_\Gamma \rangle = 0$ for all i so that $x_\Gamma \in \operatorname{cone} F$ and $x = x_\Gamma + \sum_{i=1}^r \langle a_i, x \rangle v_i \in \operatorname{cone} F + \operatorname{cone} S$.

(2): If $w_1, \ldots, w_s$ form a simplex T in $\Gamma(P,S)$, we want to show that the set

$$v_1, \ldots, v_r, w_1, \ldots, w_s$$

of vectors in $\mathbb{Z}^{d+1}$ generates the lattice. Let $x \in \mathbb{Z}^{d+1}$. Then

$$x \;=\; y \;+\; \sum_i \lambda_i v_i$$

for $y \in T$ and $\lambda_i \geq 0$ for $1 \leq i \leq r$. As $\operatorname{conv}(w_1, \ldots, w_s)$ belongs to a face of $\Gamma(P,S)$, there are $a_i \in \mathscr{A}_i$ for $i = 1, \ldots, r$ so that $\langle a_i, w_j \rangle = 0$ and $\langle a_i, v_j \rangle = \delta_{ij}$. Hence,

$$\lambda_i \;=\; \langle a_i, x \rangle \;\in \mathbb{Z}\,.$$

Thus,

$$y \;=\; x \;-\; \sum_i \lambda_i v_i \;\in T \cap \mathbb{Z}^{d+1}$$

and, as T is unimodular, $y = \sum_j \mu_j w_j$ for integral μ_j, $1 \leq j \leq s$.

(3): Every vertex u is either in S or in Γ as otherwise all facets containing u would also contain v_i for some fixed i. However, all facets containing v_i describe the tangent cone $\mathsf{T}_{v_i} P$ which has only one vertex.

(4): This follows immediately from the previous considerations.

(5): Suppose $\omega' \in \mathbb{R}^{\mathscr{A}}$ induces a triangulation of P which restricts to $\mathcal{T}$ along $\Gamma(P,S)$. Then the weights $\omega + \varepsilon\omega'$ for $\varepsilon > 0$ small enough will induce the triangulation $\mathcal{T} \star S$: by the pertubation Lemma 8.5, the resulting subdivision is a refinement of $\Gamma(P,S) \star S$ (induced by ω) so that every $\operatorname{conv}(F \cup S) = F \star S$ is subdivided according to ω'. Every subdivision of this join is the join of S with its restriction to F (cf. Exercise 8.4). □

Exercise 8.4

Lemma 8.26 *Let $\mathcal{T}$ be a regular triangulation of the polytope P so that all maximal simplices have a common vertex $v \in \operatorname{int} P$. Then $\mathcal{T}$ has the same h-vector as a simplicial polytope.* □

The proof of Theorem 8.18 uses h-vectors of triangulations (see § 3.4.4) and Theorem 3.40 by Betke-McMullen.

Proof (of Theorem 8.18). If the Gorenstein polytope P has a regular unimodular triangulation, then it is IDP (Exercise 8.3). By Lemma 8.23 P contains a special simplex S, and we can define the complex $\Gamma(P, S)$. By Lemma 8.25 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 $h^\star(P) = h^\star(\Gamma(P, S)) = h(\mathcal{T})$ by Theorem 3.40.

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 $\varepsilon > 0$, $Q := \{x \in L \ : \ \Phi(x) - \langle u, x \rangle \leq \varepsilon\}$ 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 7.25, see also Exercise 8.5.

Exercise 8.5

Corollary 8.27 *Let P_1, P_2 be reflexive. Then*

$$h^\star_{P_1 \circ P_2} \ = \ h^\star_{P_1} h^\star_{P_2}.$$

Proof. In this situation, $P := P_1 * P_2$ is also called the free join of P_1 and P_2. It's $h^\star$-polynomial is given by the product of those of P_1 and P_2 (Exercise 8.5). The origins in P_1 and P_2 form a special simplex S of P. As remarked in the proof (Exercise 8.6), projecting along the affine span of S does not change the $h^\star$-polynomial. Its image is the reflexive polytope $P_1 \circ P_2$. □

Exercise 8.6

8.5 Dilations

One of the first theorems about unimodular triangulations was proved in the early days of toric geometry by Knudsen, Mumford, and Water-

man [30]. They were interested in semi-stable reduction of families of algebraic varieties.

Theorem 8.28 ([30]) *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 8.17 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 8.28 we follow the strategy of the original ingenious proof [30] (we omit the regularity bit). Compare also [15, §§3.A&3.B].

Proof (Proof of Theorem 8.28). 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 $P \subset \mathbb{R}^d$ 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 8.29 and 8.33 below. The proofs occupy the remainder of this section. □

8.5.1 Composite Volume

For the induction step, we need some preparation. It is convenient to embed our lattice simplicial complex $\mathcal{S}$ on vertices $v_1, \ldots, v_N$ into $\mathbb{R}^N$ via $v_i \mapsto e_i$. For every face $F \in \mathcal{S}$ this yields a linear map $\varphi_F \colon \Lambda_F \to \mathbb{R}^N$, 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.

Lemma 8.29 *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 $F_1, \ldots, F_M$ 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 $i = 1, \ldots, M$, 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 $c_M \cdot \ldots \cdot c_1\mathcal{S}$. But now, the index $[\Lambda_{M+1} : \Lambda_M]$ is also less than V. So some $c_{M+1} \cdot \ldots \cdot c_1\mathcal{S}$ has a $\hat{\Lambda}$-unimodular triangulation. □

8.5.2 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, $\operatorname{star}(\mathcal{S}; F)$, of a face F of a simplicial complex $\mathcal{S}$ is the set of all faces that contain F. The closed star, $\overline{\operatorname{star}}(\mathcal{S}; F)$, contains additionally all faces of elements of $\operatorname{star}(\mathcal{S}; F)$. The boundary, $\partial \operatorname{star}(\mathcal{S}; F)$, of $\operatorname{star}(\mathcal{S}; F)$ is the difference $\overline{\operatorname{star}}(\mathcal{S}; F) \setminus \operatorname{star}(\mathcal{S}; F)$.

Lemma 8.30 *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. □

Lemma 8.31 *If $F \in \mathcal{S}$ is an inclusion minimal simplex of volume V, then there is a $c \le d$ so that $c \cdot \overline{\operatorname{star}}(\mathcal{S}; F)$ has a subdivision which induces the standard hypersimplicial subdivision on $c \cdot \partial \operatorname{star}(\mathcal{S}; F)$ 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 $m \in \operatorname{relint} cF$. As all non-$F$-coordinates of m vanish and all F-coordinates are less than one, we have $c < \dim F + 1$. Integrality implies $c \le d$. (We could use the symmetry of $\Pi(F)$ to obtain $c \le \lceil d/2 \rceil$.)

Subdivide the facets of $c \cdot \partial \operatorname{star}(\mathcal{S}; F)$ canonically into hypersimplices. Subdivide $c \cdot \overline{\operatorname{star}}(\mathcal{S}; F)$ into pyramids over these hypersimplices with apex m.

Now, let G be a cell of a pulling triangulation refining this subdivision. Then $G = \operatorname{conv}(m, G')$ where G' lives inside cF' for some facet F' of $\partial \operatorname{star}(\mathcal{S}; F)$. There is a unique vertex v_j of F not in F', and the normalized volume of G equals $m_j \cdot V < V$. □

Lemma 8.32 *$d!\mathcal{S}$ 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 $c \cdot \overline{\operatorname{star}}(\mathcal{S}; F)$ as in Lemma 8.31. Now, $d! \cdot \overline{\operatorname{star}}(\mathcal{S}; F) = \frac{d!}{c} \cdot (c \cdot \overline{\operatorname{star}}(\mathcal{S}; F))$ 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:

Lemma 8.33 *Let V be a prime number, 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.

8.6 Problems

8.1. Prove Lemma 8.15

included on page 206

included on p

8.2. Prove Theorem 8.17 by using Theorem 8.16.

included on p

8.3. Show that a lattice polytope is integrally closed if it admits a unimodular triangulation.

included on page 210

8.4. Prove the last claim in the proof of Lemma 8.25.

included on page 210

8.5. Let $P \subset \mathbb{R}^n$ and $Q \subset \mathbb{R}^m$ be lattice polytopes. Show that the product of their $h^\star$-polynomials equals the $h^\star$-polynomial of the convex hull of $P \times \{\mathbf{0}\} \times \{0\}$ and $\{\mathbf{0}\} \times Q \times \{1\}$.

included on page 210

8.6. Use the methods of proof of Theorem 8.18 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 $h^\star$-polynomial.

Some Convex Geometry

A

Contents

We provide some results from general convex geometry.

A.1 Convex Bodies

Definition A.1 (Convex Body) *A* convex body *is a compact convex set* $K \subseteq \mathbb{R}^d$ *such that* int $K \neq \emptyset$. *It is centrally symmetric if for any* $x \in K$ *also* $-x \in K$.

A.2 Ellipsoids

Let $\mathcal{B}_\mathrm{d} := \{x \in \mathbb{R}^d \mid \|x\| = 1\}$ be the unit ball.

Definition A.2 (Ellipsoid) *Let* $T : \mathbb{R}^d \to \mathbb{R}^d$ *be an invertible linear transformation and* $t \in \mathbb{R}^d$. *The set*

$$E := E(T,t) := T(B) + t$$

is the ellipsoid *with center* t.

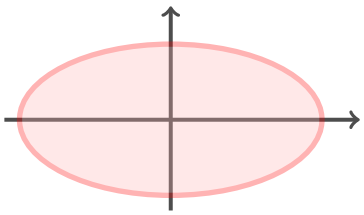


Fig. A.1: The ellipsoid for $T = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$ and $t = \mathbf{0}$

See Figure A.1 for an example. We can write the ellipsoid explicitely as

$$\begin{aligned} E &= \left\{ x \in \mathbb{R}^d \mid \langle T^{-1}(x-t), T^{-1}(x-t) \rangle \leq 1 \right\} \\ &= \left\{ x \in \mathbb{R}^d \mid \langle Q(x-t), x-t \rangle \leq 1 \right\} \end{aligned}$$

for the positive semidefinite matrix $Q = (TT^t)^{-1}$. We can also assume that T is positive definite, as any linear transformation T decomposes into a product $T = US$ for an orthogonal matrix U and a positive definite matrix S, and $U(\mathcal{B}_\mathrm{d}) = \mathcal{B}_\mathrm{d}$. In a basis of eigenvectors $u_1, \ldots, u_d$ with eigenvalues $\lambda_1, \ldots, \lambda_d$ for Q this takes the form

$$E = \left\{ x \in \mathbb{R}^d \mid \lambda_1(x_1 - t_1)^2 + \cdots + \lambda_d(x_d - t_d) \leq 1 \right\}.$$

The volume of the ellipsoid is

$$\operatorname{vol} E = |\det T| \operatorname{vol} \mathcal{B}_\mathrm{d} = \frac{\operatorname{vol} \mathcal{B}_\mathrm{d}}{\sqrt{\det Q}}.$$

Let K be a convex body and

$$\eta := \sup(\operatorname{vol} E : E \subseteq K \text{ ellipsoid}). \tag{A.1}$$

Theorem A.3 *Let $K \subseteq \mathbb{R}^d$ be a convex body. Then the supremum of (A.1) is attained, i.e. there is an ellipsoid $E \subseteq K$ such that* vol $E = \eta$. *E is called a* maximum volume ellipsoid.

Proof. Let $\mathcal{B}_\mathrm{d}$ be the unit ball. We define the set

$$S := \left\{ (T, a) \in \mathrm{Gl}(d) \times \mathbb{R}^d : T(\mathcal{B}_\mathrm{d}) + a \subseteq K \right\}.$$

Any ellipsoid $E \subseteq K$ is of the form $R = T(\mathcal{B}_\mathrm{d}) + a$ and

$$\operatorname{vol}(E) = |\det T| \cdot \operatorname{vol}(\mathcal{B}_\mathrm{d}). \tag{A.2}$$

K is compact, so there is $r > 0$ such that $\|x\| \leq r$ for all $x \in K$. Hence,

$$\|a\| \leq r \qquad \text{and} \qquad \|T\| \leq 2r \qquad \text{for all } (T, a) \in S. \tag{A.3}$$

Hence, S is a closed and bounded subset of $\mathrm{Gl}(d) \times \mathbb{R}^d$, and the map

$$(T, a) \longmapsto |\det T|$$

attains its maximum at some $(T_0, a_0) \in S$. As K is non-empty, we have $|\det T| > 0$ and $E_0 := T_0(\mathcal{B}_\mathrm{d}) + a_0$ is an ellipsoid of maximum volume.

Remark A.4 *The ellipsoid obtained in the previous theorem is in fact unique and is also called the* Löwner-John ellipsoid *or* John ellipsoid.

Essentially, for the uniqueness one shows first that, if there were two points (T_1, a_1) *and* (T_2, a_2) *attaining the maximum, then, if* $T_1 \neq T_2$, $\frac{1}{2}(T_1 + T_2)$ *generates an ellipsoid of strictly larger volume. So* $T_1 = T_2$, *and now, if* $a_1 \neq a_2$, *then* $\operatorname{conv}(T_1(\mathcal{B}_\mathrm{d}) + a_1, T_2(\mathcal{B}_\mathrm{d}) + a_2)$ *contains an ellipsoid of strictly larger volume.*

We can use the maximum volume ellipsoid of a convex body K to aaproximate K ap to a factor depending on the dimension alone. The following theroem is the key result of this section.

Theorem A.5 *Let* $K \subseteq \mathbb{R}^d$ *be a convex body and* E *a maximum volume ellipsoid in* K. *If the center of* E *is the origin, then* $K \subseteq d \cdot E$.

Using a translation we can of course always assume the the center of E is the origin.

Proof. By definition there is an invertible linear transformation T such that $E = T(\mathcal{B}_\mathrm{d})$. We can apply T^{-1} to both K and E, so that in the following we can assume that $E = \mathcal{B}_\mathrm{d}$.

We then need to show that there is no point $z \in K$ with $\|z\| \geq d$. Assume on the contrary that there is such a point $z \in K$ with $\|z\| > d$ and let

$$L \;:=\; \operatorname{conv}(\mathcal{B}_\mathrm{d} \cup \{z\}) \;\subseteq\; K\,.$$

We construct an ellipsoid inside L of volume larger than vol $\mathcal{B}_\mathrm{d}$.

Using a linear transformation we can assume that $z = me_1$. For parameters a, b and ε we consider the ellipsoid

$$F_d \;:=\; \left\{ x \in \mathbb{R}^d \mid \frac{1}{a^2}(x_1 - \varepsilon)^2 + \frac{1}{b^2}\sum_{i=2}^{d} x_i^2 \;\leq\; 1 \right\}.$$

This is symmetric in the last $d-1$ coordinated. Hence, it suffices to consider the case $d = 2$, *i.e.*

$$F \;:=\; \left\{ x \in \mathbb{R}^d \mid \frac{1}{a^2}(x_1 - \varepsilon)^2 + \frac{x_2^2}{b^2} \;\leq\; 1 \right\}.$$

See Figure A.2 for a sketch of the setting. Now clearly an ellipsoid of maximum volume in F will touch at the point $(-1, 0)$. Plugging this into the defining equation we obtain

$$a \;=\; \varepsilon + 1\,. \tag{A.4}$$

The tangent to F at a point (u, v) is given by the equation

$$\frac{u - \varepsilon}{a^2}(x_1 - \varepsilon) \;+\; \frac{v}{b^2}x_2 \;=\; 1\,. \tag{A.5}$$

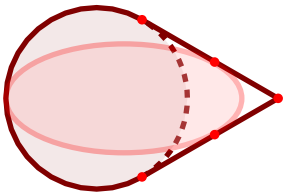


Fig. A.2: A sketch of the setting for the proof of Theorem A.5.

and, as (u, v) is on the boundary of F,

$$1 \;=\; \frac{(u-\varepsilon)^2}{a^2} \;+\; \frac{v^2}{b^2} \tag{A.6}$$

Now we want to determine the particular tangent to the ellipsoid that also passes through me_1 and touches the unit ball, *i.e.* the boundary segment of L added in the convex hull of $\mathcal{B}_\mathrm{d}$ with me_1. This line touches the unit ball in a point (p, q) and can thus also be written as

$$px_1 \;+\; qx_2 \;=\; 1\,. \tag{A.7}$$

It passes through me_1 and $p^2 + q^2 = 1$, so

$$\frac{u-\varepsilon}{a^2} \;=\; \frac{1}{m-\varepsilon} \qquad p \;=\; \frac{1}{m} \qquad q \;=\; \frac{\sqrt{m^2-1}}{m}\,. \tag{A.8}$$

From (A.7) we deduce that the slope of the tangent is $-1/\sqrt{m^2-1}$. Computing the slope from (A.5) we obtain

$$-\frac{1}{\sqrt{m^2-1}} \;=\; -\frac{u-\varepsilon}{a^2}\frac{b^2}{v}\,.$$

Squaring and first using (A.6) and then the first equation of (A.8) we obtain

$$\begin{aligned}\frac{1}{m^2-1} \;&=\; \frac{(u-\varepsilon)^2}{a^4}b^2\left(1-\frac{(u-\varepsilon)^2}{a^2}\right)^{-1}\\ &=\; \frac{1}{(m-\varepsilon)^2}b^2\left(1-\frac{a^2}{(m-\varepsilon)^2}\right)^{-1}\end{aligned}$$

Using (A.4) and solving for b^2 gives

$$b^2 \;=\; \frac{(m-\varepsilon)^2 \;-\; (1+\varepsilon)^2}{m^2-1}\,.$$

Now let us return to the ellipsoid F_d in dimension d. Its volume is

$$\mathrm{vol}\; F_d \;=\; ab^{d-1}\,\mathrm{vol}\;\mathcal{B}_\mathrm{d}\;.$$

Now

$$ab^{d-1} \;=\; (1+\varepsilon)\left(\frac{(m-\varepsilon)^2 \;-\; (1+\varepsilon)^2}{m^2-1}\right)^{(d-1)/2}$$

As a function in ε its derivative at 0 is

$$1-\frac{d-1}{2}\frac{2}{m-1} \;=\; \frac{m-d}{m-1}\,.$$

Hence, for $m > d$ and small ε the volume of F_d is larger than that of $\mathcal{B}_\mathrm{d}$. □

From the proof of Theorem A.6 it becomes pretty obvious that we can get a larger ellipsoid inside L if K is centrally symmetric and we use the knowledge that also $-z$ is in K and we can thus replace L by $L := \operatorname{conv}(\mathcal{B}_d \cup \{\pm z\})$. With essentially the same proof this leads to the following approximation of a centrally symmetric convex body K by an ellipsoid.

Theorem A.6 *Let $K \subseteq \mathbb{R}^d$ be a* centrally symmetric *convex body and E a maximum volume ellipsoid in K. If the center of E is the origin, then $K \subseteq \sqrt{d} \cdot E$.*

Exercise A.4

The proof is left to the reader as Exercise A.4.

A.3 Problems

A.1. Let C_d be the cube defined by $|x_i| \leq 1$. Prove that the maximum volume ellipsoid is the unit ball.

included on page 219

A.2. Let $\Delta_d \subseteq \mathbb{R}^{d+1}$ be the d-dimensional simplex defined as the convex hull of the unit vectors. Prove that a maximum volume ellipsoid is the ball in the affine hull of Δ_d with center $1/(d+1)\mathbf{1}$.
Deduce that the bound of Theorem A.6 is best possible.

included on page 219

A.3. Let K be a centrally symmetric convex body. Prove that then also a maximum volume ellipsoid is centrally symmetric (and in particular centered at the origin).

included on page 219

A.4. Prove Theorem A.6.

Solutions to some Exercises

B

B.1 Solutions for Chapter 4

4.13. $\mathrm{ca}(P;w)$ attained for η, can assume $v := w + \eta \in \partial P$. If v is not a vertex of P, then there is a $v' \in \mathbb{R}^d \setminus \{\mathbf{0}\}$ so that $v \pm v' \in P$. compute the defining quotient ... can decrease the dimension of the carrier face of v.
Alternative proof: $\max\{\lambda > 0 \ : \ w - \lambda(v-w) \in P\}$ is a linear optimization problem. It has a basic optimal solution.

4.11. (1) Let A, B and C be the vertices of the triangle realising $\mathrm{sbc}(2,i)$ for an interior point L and assume the smallest coefficient is at vertex C. We can transform the triangle so that A is the origin and B is on the x-axis and $C = (c_1, c_2)$ is in the positive orthant. Then $\mathit{smallestbary}(2,i) = \frac{1}{c_2}$, so that $\mathrm{sbc}(2,i)$ is realized by a triangle with maximal height and i interior lattice points.
This is obtained if $B = (2,0)$ and $c_1 = 0$. In this case $c_2 = 2i+2$, so $\mathrm{sbc}(2,i) = \frac{1}{2i+2}$.
(2)
(3)

B.2 Solutions for Chapter 6

6.2. This is equivalent to $\det(\Lambda) \cdot \det(\Lambda^*) = 1$.

References to software packages (citations starting with an "S") are listed in the software section of the references.

[1] Christos A. Athanasiadis. *Ehrhart polynomials, simplicial polytopes, magic squares and a conjecture of Stanley*. J. Reine Angew. Math., 583 (2005), pp. 163–174. doi: 10.1515/crll.2005.2005.583.163. url: https://doi.org/10.1515/crll.2005.2005.583.163 (cit. on p. 207)

[2] Margherita Barile, Dominique Bernardi, Alexander Borisov, and Jean-Michel Kantor. *On empty lattice simplices in dimension 4*. Proc. Amer. Math. Soc., 139:12 (2011), pp. 4247–4253. doi: 10.1090/S0002-9939-2011-10859-1. arXiv: 0912.5310 [math.AG]. url: http://dx.doi.org/10.1090/S0002-9939-2011-10859-1 (cit. on p. 122)

[3] A. I. Barvinok. *Computing the Ehrhart polynomial of a convex lattice polytope*. Discrete Comput. Geom., 12:1 (1994), pp. 35–48. doi: 10.1007/BF02574364. url: http://dx.doi.org/10.1007/BF02574364 (cit. on pp. 148, 149)

[4] Alexander Barvinok. *A course in convexity*. Graduate Studies in Mathematics (vol. 54). American Mathematical Society (Providence, RI), 2002, x+366 pages (cit. on p. 45)

[5] Alexander Barvinok. *Integer points in polyhedra*. Zurich Lectures in Advanced Mathematics. European Mathematical Society (EMS), Zürich, 2008, viii+191 pages. doi: 10.4171/052 (cit. on p. 108)

[6] Alexander I. Barvinok and James E. Pommersheim. *An algorithmic theory of lattice points in polyhedra*. In: *New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97)*. Cambridge Univ. Press (Cambridge), 1999, pp. 91–147 (cit. on p. 148)

[7] Victor Batyrev and Benjamin Nill. *Combinatorial aspects of mirror symmetry*. In: *Integer points in polyhedra — geometry, number theory, representation theory, algebra, optimization, statistics*. Ed. by Matthias Beck, Christian Haase, Bruce Reznick, Michèle Vergne, Volkmar Welker, and Ruriko Yoshida. Contemp. Math. (Vol. 452). Papers from the AMS-IMS-SIAM Joint Summer Research Conference held in Snowbird, UT, June 11–15, 2006. Amer. Math. Soc. (Providence, RI), 2008, pp. 35–66. doi: 10.1090/conm/452/08770. arXiv: math/0703456 [math.CO] (cit. on p. 137)

[8] Victor V. Batyrev. *Dual polyhedra and mirror symmetry for Calabi–Yau hypersurfaces in toric varieties*. J. Alg. Geom., 3 (1994), pp. 493–535 (cit. on p. 181)

[9] Matthias Beck and Frank Sottile. *Irrational proofs for three theorems of Stanley*. European J. Combin., 28:1 (2007), pp. 403–409. doi: 10.1016/j.ejc.2005.06.003. arXiv: math/0501359 [math.CO] (cit. on pp. 74, 79)

[10] Ulrich Betke, Martin Henk, and Jörg M. Wills. *Successive-minima-type inequalities*. Discrete Comput. Geom., 9:2 (1993), pp. 165–175. doi: 10.1007/BF02189316. url: http://dx.doi.org/10.1007/BF02189316 (cit. on p. 104)

[11] Ulrich Betke and Peter McMullen. *Lattice points in lattice polytopes*. Monatsh. Math., 99:4 (1985), pp. 253–265. doi: 10.1007/BF01312545 (cit. on p. 80)

[12] Louis J. Billera and Carl W. Lee. *Sufficiency of McMullen's conditions for f-vectors of simplicial polytopes*. Bull. Amer. Math. Soc. (N.S.), 2:1 (1980), pp. 181–185 (cit. on p. 29)

[13] Alexandr A. Borisov. *Convex lattice polytopes and cones with few lattice points inside, from a birational geometry viewpoint*. arXiv:math/0001109[math.AG]. 2000 (cit. on p. 109)

[14] Alexandr A. Borisov and Lev A. Borisov. *Singular toric Fano varieties*. Mat. Sb., 183:2 (1992), pp. 134–141. doi: 10.1070/SM1993v075n01ABEH003385. url: http://dx.doi.org/10.1070/SM1993v075n01ABEH003385 (cit. on p. 109)

[15] Winfried Bruns and Joseph Gubeladze. *Polytopes, Rings, and K-Theory*. Monographs in Mathematics. XIV, 461 p. 52 illus. Springer-Verlag, 2009 (cit. on p. 211)

[16] Winfried Bruns and Tim Römer. *h-vectors of Gorenstein polytopes*. J. Combin. Theory Ser. A, 114:1 (2007), pp. 65–76. doi: 10.1016/j.jcta.2006.03.003. url: http://dx.doi.org/10.1016/j.jcta.2006.03.003 (cit. on p. 206)

[17] Vladimir I. Danilov and Askol'd G. Khovanskii. *Newton polyhedra and an algorithm for computing Hodge–Deligne numbers*. Math. USSR Izvestiya, 29:2 (1987), pp. 279–298 (cit. on p. 181)

[18] Jesús A. De Loera, Raymond Hemmecke, and Matthias Köppe. *Algebraic and geometric ideas in the theory of discrete optimization*. MOS-SIAM Series on Optimization (vol. 14). Society for Industrial and Applied Mathematics (SIAM) (Philadelphia, PA), 2013, xx+322 pages (cit. on pp. 75, 155)

[19] Jesus deLoera, Francisco Santos, and Jörg Rambau. *Triangulations*. Algorithms and Computation in Mathematics (vol. 25). Springer, 2010 (cit. on pp. 32, 200)

[20] Jan Draisma, Tyrrell B. McAllister, and Benjamin Nill. *Lattice width directions and Minkowski's 3^d-theorem* (Jan. 2009). eprint: 0901.1375 (cit. on p. 104)

[21] Robert M. Erdahl and Sergej S. Ryshkov. *On lattice dicing*. English. Eur. J. Comb., 15:5 (1994), pp. 459–481. doi: 10.1006/eujc.1994.1049 (cit. on p. 205)

[22] Israel M. Gel′fand, Michael M. Kapranov, and Andrei V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston Inc. (Boston, MA), 1994, x+523 pages. doi: 10.1007/978-0-8176-4771-1 (cit. on p. 200)

[23] Roland Grinis and Alexander Kasprzyk. *Normal forms of convex lattice polytopes*. Jan. 2013. arXiv: 1301.6641 [math.CO] (cit. on p. 145)

[24] Martin Grötschel, László Lovász, and Alexander Schrijver. *Geometric algorithms and combinatorial optimization*. Second. Algorithms and Combinatorics (vol. 2). Springer-Verlag (Berlin), 1993, xii+362 pages (cit. on p. 102)

[25] Christian Haase and Günter M. Ziegler. *On the maximal width of empty lattice simplices*. Eur. J. Comb., 21:1 (2000), pp. 111–119 (cit. on p. 122)

[26] Martin Henk. *Successive minima and lattice points*. Rend. Circ. Mat. Palermo (2) Suppl.,: 70, part I (2002). IV International Conference in "Stochastic Geometry, Convex Bodies, Empirical Measures & Applications to Engineering Science", Vol. I (Tropea, 2001), pp. 377–384. eprint: math.MG/0204158 (cit. on p. 103)

[27] Douglas Hensley. *Lattice vertex polytopes with interior lattice points*. Pacific J. Math., 105:1 (1983), pp. 183–191. doi: 10.2140/pjm.1983.105.183 (cit. on p. 115)

[28] Lutz Hille and Harald Skarke. *Reflexive polytopes in dimension 2 and certain relations in $SL_2(\mathbb{Z})$*. English. J. Algebra Appl., 1:2 (2002), pp. 159–173. doi: 10.1142/S0219498802000124 (cit. on p. 179)

[29] Ravindran Kannan and Achim Bachem. *Polynomial algorithms for computing the Smith and Hermite normal forms of an integer matrix*. SIAM J. Comput., 8:4 (1979), pp. 499–507. doi: 10.1137/0208040. url: https://doi.org/10.1137/0208040 (cit. on p. 148)

[30] George R. Kempf, Finn F. Knudsen, David Mumford, and Bernard Saint–Donat. *Toroidal Embeddings I*. Lecture Notes in Mathematics (vol. 339). Springer–Verlag, 1973 (cit. on p. 211)

[31] Matthias Köppe and Sven Verdoolaege. *Computing Parametric Rational Generating Functions with a Primal Barvinok Algorithm*. Electronic journal of Combinatorics, 15 (2008) (cit. on p. 74)

[32] Maximilian Kreuzer and Harald Skarke. *Classification of reflexive polyhedra in three dimensions*. Adv. Theor. Math. Phys., 2:4 (1998), pp. 853–871 (cit. on p. 140)

[33] Maximilian Kreuzer and Harald Skarke. *Complete classification of reflexive polyhedra in four dimensions*. Adv. Theor. Math. Phys., 4:6 (2000), pp. 1209–1230 (cit. on pp. 140, 194)

[34] Maximilian Kreuzer and Harald Skarke. *PALP: a package for analysing lattice polytopes with applications to toric geometry*. Comput. Phys. Comm., 157:1 (2004), pp. 87–106. doi: 10.1016/S0010-4655(03)00491-0. url: http://dx.doi.org/10.1016/S0010-4655(03)00491-0 (cit. on p. 140)

[35] J. C. Lagarias. *Knapsack public key cryptosystems and Diophantine approximation (extended abstract)*. In: *Advances in cryptology (Santa Barbara, Calif., 1983)*. Plenum, New York, 1984, pp. 3–23 (cit. on p. 168)

[36] J. C. Lagarias, H. W. Lenstra Jr., and C.-P. Schnorr. *Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice*. Combinatorica, 10:4 (1990), pp. 333–348. doi: 10.1007/BF02128669. url: https://doi.org/10.1007/BF02128669 (cit. on p. 107)

[37] Jeffrey C. Lagarias and Günter M. Ziegler. *Bounds for lattice polytopes containing a fixed number of interior points in a sublattice*. English. Can. J. Math., 43:5 (1991), pp. 1022–1035 (cit. on p. 115)

[38] A. K. Lenstra, H. W. Lenstra Jr., and L. Lovász. *Factoring polynomials with rational coefficients*. Math. Ann., 261:4 (1982), pp. 515–534. doi: 10.1007/BF01457454. url: http://dx.doi.org/10.1007/BF01457454 (cit. on pp. 159, 167, 168)

[39] P. McMullen. *The numbers of faces of simplicial polytopes*. Israel J. Math., 9 (1971), pp. 559–570. doi: 10.1007/BF02771471. url: http://dx.doi.org/10.1007/BF02771471 (cit. on p. 29)

[40] David R. Morrison and Glenn Stevens. *Terminal quotient singularities in dimensions three and four*. Proc. Amer. Math. Soc., 90:1 (1984), pp. 15–20. doi: 10.2307/2044659 (cit. on p. 118)

[41] Mircea Musta and Sam Payne. *Ehrhart polynomials and stringy Betti numbers*. Math. Ann., 333:4 (2005), pp. 787–795. doi: 10.1007/s00208-005-0691-x. eprint: math/0504486 (math.AG) (cit. on p. 206)

[42] Phong Q. Nguyen and Brigitte Vallée, eds. *The LLL algorithm*. Information Security and Cryptography. Survey and applications. Springer-Verlag, Berlin, 2010, xiv+496 pages. doi: 10.1007/978-3-642-02295-1. url: http://dx.doi.org/10.1007/978-3-642-02295-1 (cit. on p. 160)

[43] Mikkel Øbro. *Classification of smooth Fano polytopes*. PhD thesis. University of Aarhus, 2007. url: pure.au.dk/portal/files/41742384/imf_phd_2008_moe.pdf (cit. on p. 194)

[44] Hidefumi Ohsugi and Takayuki Hibi. *Convex polytopes all of whose reverse lexicographic initial ideals are squarefree*. English. Proc. Am. Math. Soc., 129:9 (2001), pp. 2541–2546 (cit. on p. 204)

[45] Oleg Pikhurko. *Lattice points in lattice polytopes*. English. Mathematika, 48:1-2 (2001), pp. 15–24 (cit. on p. 115)

[46] Bjorn Poonen and Fernando Rodriguez-Villegas. *Lattice polygons and the number 12*. Amer. Math. Monthly, 107:3 (2000), pp. 238–250 (cit. on p. 179)

[47] Herbert E. Scarf. *Integral polyhedra in three space*. Math. Oper. Res., 10 (1985), pp. 403–438 (cit. on p. 118)

[48] Claus-P. Schnorr. *A hierarchy of polynomial time lattice basis reduction algorithms*. Theoret. Comput. Sci., 53:2-3 (1987), pp. 201–224. doi: 10.1016/0304-3975(87)90064-8. url: http://dx.doi.org/10.1016/0304-3975(87)90064-8 (cit. on p. 167)

[49] Alexander Schrijver. *Combinatorial optimization. Polyhedra and efficiency (3 volumes)*. English. Algorithms and Combinatorics 24. Berlin: Springer., 2003 (cit. on p. 102)

[50] Alexander Schrijver. *Theory of linear and integer programming*. English. Wiley-Interscience Series in Discrete Mathematics. A Wiley-Interscience Publication. Chichester: John Wiley & Sons Ltd., 1986 (cit. on pp. 25, 102, 172)

[51] P. R. Scott. *On convex lattice polygons*. Bull. Austral. Math. Soc., 15:3 (1976), pp. 395–399 (cit. on p. 12)

[52] András Seb. *An introduction to empty lattice simplices*. In: *Integer programming and combinatorial optimization (Graz, 1999)*. Ed. by Gérard Cornuéjols, Rainer E. Burkard, and Gerhard J. Woeginger. Lecture Notes in Comput. Sci. (Vol. 1610). Springer (Berlin), 1999, pp. 400–414. doi: 10.1007/3-540-48777-8_30. url: http://dx.doi.org/10.1007/3-540-48777-8_30 (cit. on p. 118)

[53] Richard P. Stanley. *A monotonicity property of h-vectors and h^*-vectors*. European J. Combin., 14:3 (1993), pp. 251–258. doi: 10.1006/eujc.1993.1028. url: http://dx.doi.org/10.1006/eujc.1993.1028 (cit. on p. 79)

[54] Richard P. Stanley. *Decompositions of rational convex polytopes*. Ann. Discrete Math., 6 (1980). Combinatorial mathematics, optimal designs and their applications (Proc. Sympos. Combin. Math. and Optimal Design, Colorado State Univ., Fort Collins, Colo., 1978), pp. 333–342 (cit. on p. 204)

[55] Richard P. Stanley. *The number of faces of a simplicial convex polytope*. Adv. in Math., 35:3 (1980), pp. 236–238. doi: 10.1016/0001-8708(80)90050-X (cit. on p. 29)

[56] Arne Storjohann. *Faster Algorithms for Integer Lattice Basis Reduction*. 1996 (cit. on p. 167)

[57] Bernd Sturmfels. *Gröbner bases and convex polytopes*. Univ. Lecture Series (vol. 8). American Mathematical Society (Providence, RI), 1996, xii+162 pages (cit. on p. 200)

[58] Seth Sullivant. *Compressed polytopes and statistical disclosure limitation*. Tohoku Math. J. (2), 58:3 (2006). Preprint arXiv:math.CO/0412535, pp. 433–445. url: http://projecteuclid.org/getRecord?id=euclid.tmj/1163775139 (cit. on p. 204)

[59] Sven Verdoolaege, Rachid Seghir, Kristof Beyls, Vincent Loechner, and Maurice Bruynooghe. *Counting integer points in parametric polytopes using Barvinok's rational functions*. Algorithmica, 48:1 (2007), pp. 37–66. doi: 10.1007/s00453-006-1231-0. url: https://doi.org/10.1007/s00453-006-1231-0 (cit. on p. 148)

[60] G. K. White. *Lattice tetrahedra*. Canadian J. Math., 16 (1964), pp. 389–396. doi: 10.4153/CJM-1964-040-2. url: https://doi.org/10.4153/CJM-1964-040-2 (cit. on p. 118)

[61] J. Zaks, M. A. Perles, and J. M. Wilks. *On lattice polytopes having interior lattice points*. Elem. Math., 37:2 (1982), pp. 44–46 (cit. on p. 116)

[S1] Jesús A. De Loera, Raymond Hemmecke, Ruriko Yoshida, and Jeremy Tauzer. `lattE`. http://www.math.ucdavis.edu/~latte/. 2005 (cit. on p. 148)

[S2] Matthias Köppe. *Latte macchiato – An improved version of Latte*. http://www.math.uni-magdeburg.de/~mkoeppe/latte/. 2007 (cit. on p. 148)

[S3] Sven Verdoolaege. `barvinok`. http://barvinok.gforge.inria.fr/. 2007 (cit. on p. 148)