Ehrhart theory for real dilates of polytopes

Tiago Royer

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências

Programa: Ciência da Computação
Orientador: Prof. Dr. Sinai Robins

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro da CAPES

São Paulo, março de 2018

Ehrhart theory for real dilates of polytopes

Esta versão da dissertação/tese contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 15/02/2018. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Abstract

ROYER, T. **Ehrhart theory for real dilates of polytopes**. 2017. 80 pp. Master Thesis — Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2017.

The Ehrhart function $L_P(t)$ of a polytope P is defined to be the number of integer points in the dilated polytope tP. Classical Ehrhart theory is mainly concerned with integer values of t; in this master thesis, we focus on how the Ehrhart function behaves when the parameter t is allowed to be an arbitrary real number. There are three main results concerning this behavior in this thesis.

Some rational polytopes (like the unit cube $[0,1]^d$) only gain integer points when the dilation parameter t is an integer, so that computing $L_P(t)$ yields the same integer point count than $L_P(\lfloor t \rfloor)$. We call them *semi-reflexive polytopes*. The first result is a characterization of these polytopes in terms of the hyperplanes that bound them.

The second result is related to the Ehrhart theorem. In the classical setting, the Ehrhart theorem states that $L_P(t)$ will be a quasipolynomial whenever P is a rational polytope. This is also known to be true with real dilation parameters; we obtained a new proof of this fact starting from the chraracterization mentioned above.

The third result is about how the real Ehrhart function behaves with respect to translation in this new setting. It is known that the classical Ehrhart function is invariant under integer translations. This is far from true for the real Ehrhart function: not only there are infinitely many different functions $L_{P+w}(t)$ (for integer w), but under certain conditions the collection of these functions identifies P uniquely.

Keywords: Ehrhart theory, rational polytopes, semi-rational polytopes, real polytopes.

Resumo

ROYER, T. **Teoria de Ehrhart para fatores reais de dilatação**. 2017. 80 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2017.

A função de Ehrhart $L_P(t)$ de um politopo P é definida como sendo o número de pontos com coordenadas inteiras no politopo dilatado tP. A teoria de Ehrhart clássica lida principalmente com valores inteiros de t; esta dissertação de mestrado foca em como a função de Ehrhart se comporta quando permitimos que o parâmetro t seja um número real arbitrário. São três os resultados principais desta dissertação a respeito deste comportamento.

Alguns politopos racionais (como o cubo unitário $[0,1]^d$) apenas ganham pontos inteiros quando o parâmetro de dilatação t é um inteiro, de tal forma que computar $L_P(t)$ devolve a mesma contagem de pontos que $L_P(\lfloor t \rfloor)$. Eles são chamados de *politopos semi-reflexivos*. O primeiro resultado desta dissertação é uma caracterização destes politopos em termos de suas descrições como interseção de semi-espaços.

O segundo resultado é relacionado ao teorema de Ehrhart. No contexto clássico, o teorema de Ehrhart afirma que $L_P(t)$ será um quasi-polinômio sempre que P for um politopo racional. Sabe-se que este teorema generaliza para parâmetros reais de dilatação; nesta dissertação é apresentada uma nova demonstração deste fato, baseada na caracterização mencionada acima.

O terceiro resultado é sobre como a função real de Ehrhart se comporta com respeito à translação neste novo contexto. Sabe-se que a função de Ehrhart clássica é invariante sob translações por vetores com coordenadas inteiras. Por outro lado, a função real de Ehrhart está bem longe de ser invariante: não só existem infinitas funções $L_{P+w}(t)$ distintas, mas também, sob certas condições, esta coleção de funções identifica P unicamente.

Palavras-chave: Teoria de Ehrhart, politopos racionais, politopos semi-racionais, politopos reais.

Contents

Chapter 1

Introduction

Given a polytope $P \subseteq R^d$, the function $L_P(t)$ is defined (for integer $t > 0$) as the number of integral points in tP; that is,

$$L_P(t) = \#(tP \cap \mathbb{Z}^d).$$

Here, $\#(A)$ is the number of elements in the set A and $tP = \{tx \mid x \in P\}$ is the dilation of P by t.

Ehrhart theory is the study of this function and its properties. The two main results of this area are the Ehrhart and Reciprocity Theorems. If P is a d-dimensional polytope whose vertices are integral points (an *integral* polytope), the Ehrhart Theorem states that $L_P(t)$ will be a polynomial of degree d in t. In this case, it makes sense to evaluate L_P for negative integers; then the Reciprocity Theorem states that $(-1)^d L_P(-t)$ is the number of integral points in the relative interior of tP.

A classical extension to this setting is to allow P to have rational coordinates. Then $L_P(t)$ will not be a polynomial anymore, but we can come close: the Ehrhart Theorem for rational polytopes states that we can still write $L_P(t)$ as

$$L_P(t) = c_d(t)t^d + \cdots + c_1(t)t + c_0(t),$$

but we must allow the $c_i(t)$ to be periodic functions in t. This kind of function is called a *quasi-polynomial*. Since each c_i is periodic, it still makes sense to evaluate L_P in negative integers, and again the Reciprocity Theorem holds.

This master thesis aims to investigate another extension: allowing the dilation parameter to be an arbitrary real number. There are some recent papers which started exploring this extension [1, 2, 5, 12, 14].

We will sometimes use the classical theorems to show results for real dilation parameters. To minimize confusion, we will denote real dilation parameters with the letter s, so that $L_P(t)$ denotes the classical Ehrhart function and $L_P(s)$ denotes the extension considered in this paper. Thus, $L_P(t)$ is just the restriction of $L_P(s)$ to integer arguments.

1.1 Rational polytopes

A polytope P is called *rational* if it can be written as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \tag{1.1}$$

where the a_i are integer vectors and b_i are integer numbers.

The *reflexive* polytopes forms a special class of rational polytopes. A polytope is reflexive if it is an integer polytope (that is, all of its vertices are integer vectors), and in the representation (1.1) all the b_i are 1.

In Chapter 3, we will define *semi-reflexive* polytopes to be the rational polytopes such that $L_P(s) = L_P(\lfloor s \rfloor)$ for all $s \geq 0$. We have the following characterization of semi-reflexive polytopes in terms of their hyperplane representation.

Theorem 1. *Let P be a rational polytope written as in* (1.1)*. Then P is semi-reflexive if and only if all a_i are integers and all b_i are either* 0 *or* 1*.*

The name "semi-reflexive" is justified as follows. Given a polytope P, define its dual P^* by

$$P^* = \{x \in \mathbb{R}^d \mid \langle x, y \rangle \leq 1 \text{ for all } y \in P\}.$$

Then we have the following.

Theorem 2. *P is a reflexive polytope if and only if both P and P^* are semi-reflexive polytopes.*

In Chapter 4, we will explore the following consequence of Theorem 1. If P is a semi-reflexive polytope, then we may compute $L_P(s)$ using only information for integer dilation parameters; that is, we may deduce $L_P(s)$ from $L_P(t)$. Ehrhart theorem, in turn, says that we may deduce $L_P(t)$ for all t from a finite set of values of t; this gives us a closed-form expression for $L_P(s)$. We will extend this conclusion for all rational polytopes P; that is, we will show how to obtain a closed-form expression for $L_P(s)$ for all rational polytopes P. This, in turn, gives a new proof of the real version of the Ehrhart theorem, stated below.

Theorem 3. *Let $P \subseteq \mathbb{R}^d$ be a rational polytope. Then there exists piecewise-polynomial periodic functions $c_0(s), \ldots, c_d(s)$ such that*

$$L_P(s) = c_d(s)s^d + \cdots + c_1(s)s + c_0(s).$$

This, in turn, will give us a new proof of the following theorem, by Linke [14, p. 1973].

Theorem 4 (Linke, 2011)**.** *Let P be a rational polytope, and write*

$$L_P(s) = c_d(s)s^d + \cdots + c_1(s)s + c_0(s).$$

Then for every s at which all the c_i are left (resp. right) continuous, all the c_i will be left (resp. right) differentiable, and

$$c_i'(s) = -(i+1)c_{i+1}(s).$$

In Section 3.3, we will explore another consequence of Theorem 1. The origin satisfies every linear restriction $\langle a, x\rangle \leq b$ in which $b \geq 0$; thus, every semi-reflexive polytope must contain the origin. This means that, if P is semi-reflexive and some integer translation $P + w$ does not contain the origin, then $P + w$ cannot be semi-reflexive and thus we will have $L_{P+w}(s) \neq L_{P+w}(\lfloor s \rfloor)$ for at least some s. Since $L_{P+w}(t) = L_P(t)$ for all integer w and t, this shows that the real Ehrhart function is not invariant under integer translations.

This assertion can be strenghtened as follows.

Theorem 5. *Let P be a rational polytope. Then there exists an integer vector w such that the functions $L_{P+kw}(s)$ are all distinct for $k \geq 0$.*

This is in sharp contrast with the classical Ehrhart function, where all the functions $L_{P+kw}(t)$ are the same.

In Chapter 5, we will make this distinction even sharper with the following theorem.

Theorem 6. *Let P and Q be two rational polytopes such that, for every integer translation vector w, we have $L_{P+w}(s) = L_{Q+w}(s)$. Then $P = Q$.*

In other words, if P is a rational polytope, then the Ehrhart functions $L_{P+w}(s)$ (for integer w) indentifies P uniquely, so we may reconstruct P from the Ehrhart function of its integer translates.

We may also see this theorem as a first step towards a positive answer for the following question: are any two polytopes with the same Ehrhart function piecewise unimodular images of each other? (This is a variation of Question 4.1 of Haase and McAllister [11].) Theorem 6 has a stronger hypothesis (that $P + w$ and $Q + w$ have the same Ehrhart function for all integer w), but has a stronger conclusion (the polytopes are actually the same, not even up to translation). This suggests that we might be able to drop some of that hypothesis and still conclude that the polytopes are piecewise unimodular images of each other.

1.2 Non-rational polytopes

Although Ehrhart theory is usually concerned with rational polytopes, there has been some effort in working with non-rational polytopes as well. For example, Borda [5] deals with simplices and cross-polytopes with algebraic coordinates; and [6] and [7] deal with arbitrary real polytopes and real dilations but for the solid-angle polynomial.

In the course of proving the theorems stated in Section 1.1, we will be able to extend some of those theorems to real polytopes. Interestingly, we always need to impose some dimensionality condition (like demanding the polytope to be full-dimensional) in order to avoid simple counter-examples.

We will extend the theorems in Chapters 3 and 5. For Theorem 1, we have the following extension.

Theorem 7. *Let P be a full-dimensional real polytope. Then $L_P(s) = L_P(\lfloor s \rfloor)$ for all s if and only if the polytope P can be written as in* (1.1) *where each b_i is either* 0 *or* 1*, and when $b_i = 1$ the vector a_i must be integral.*

For Theorem 5, we may also handle polytopes which have codimension 1.

Theorem 8. *Let $P \subseteq \mathbb{R}^d$ be a real polytope which is either full-dimensional or has codimension 1. Then there is an integral vector $w \subseteq \mathbb{R}^d$ such that the functions $L_{P+kw}(s)$ are different for all integers $k \geq 0$.*

The extension of Theorem 6 is more modest. A polytope P is *semi-rational* if it can be written as in (1.1) with the a_i being integral vectors; the b_i may be arbitrary real numbers. We have the following generalization.

Theorem 9. *Let P and Q be two semi-rational polytopes in $\mathbb{R}^d$, both having codimension 0 or 1. Suppose moreover that $L_{P+w}(s) = L_{Q+w}(s)$ for all integer w and all real $s > 0$. Then $P = Q$.*

And, finally, we may show another extension of Theorem 6 by stepping outside the realm of polytopes. A convex body $K \subseteq \mathbb{R}^d$ is called *symmetric* if, for all $x \in \mathbb{R}^d$, we have $x \in K$ if and only if $-x \in K$.

Theorem 10. *Let K and H be symmetric convex bodies, and assume that $L_{K+w}(s) = L_{H+w}(s)$ for all real $s > 0$ and all integer w. Then $K = H$.*

1.3 Notation and structure of the text

Chapter 2 provides a quick introduction to the area. Section 2.1 contains a quick recapitulation of the classical Ehrhart theory, and Section 2.2 defines the real Ehrhart function $L_P(s)$. (Since results of the classical setting are used in the discussion, we will use the letter s when working with real dilation parameters to minimize confusion.)

We will usually represent polytopes by their description as intersection of half-spaces. That is, we will write polytopes $P \subset \mathbb{R}^d$ as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

where a_i are vectors of $\mathbb{R}^d$ and b_i are real numbers. If P is a full-dimensional polytope, the number n may be chosen to be the number of facets in P. In this case, each hyperplane $\{x \mid \langle a_i, x \rangle = b_i\}$ intersects P in a facet, so that there is no redundant hyperplanes; that is, such representation is minimal. We will assume such representations are always minimal for full-dimensional polytopes.

In some sections, we will deal with specific classes of polytopes, and thus the vectors a_i and the numbers b_i will be appropriately restricted. These restrictions will be stated explicitly.

In Chapter 3 we will define semi-reflexive polytopes and prove Theorems 1 and 7, which characterizes them in terms of their hyperplane description. Here, the vectors a_i will often be scaled so that the right-hand sides b_i are either -1, 0 or 1.

To show the characterization, we will use the Iverson bracket, which is defined as follows. Given a proposition p, we define the number $[p]$ to be 1 if p is true, and 0 if p is false. For example, the number $\#(P \cap \mathbb{Z}^d)$ of integer points contained in P may be expressed as

$$\#(P \cap \mathbb{Z}^d) = \sum_{x \in \mathbb{Z}^d} [x \in P].$$

The characterizations are shown in section 3.1, and then used in section 3.1.2 to show some examples of semi-reflexive polytopes. Theorem 2, relating reflexive and semi-reflexive polytopes, is shown in Section 3.1.3. And, in section 3.2, semi-reflexive polytopes are used to construct an example of two distinct polytopes which have the same Ehrhart function.

Section 3.3 contains the proof of Theorems 8 and 5. Most of the time, we will be working with arbitrary polytopes on this section, so the vectors a_i will be assumed to be normalized.

Chapter 4, presents a different approach for showing the real Ehrhart theorem, based on a modification of the argument used to show the "if" part of Theorem 1. As a warm-up, section 4.1.1 proves this result for polytopes containing the origin. When extending for all rational polytopes, we use the "front body/back shell decomposition", developed in section 4.1.2. The proof of the real Ehrhart theorem is the subject of section 4.1.3. For completeness, section 4.1.4 contains a proof of the real reciprocity theorem.

In the same chapter, Section 4.2 provides a different proof of Theorem 4.

Chapter 5, in turn, is dedicated to show Theorems 6, 9 and 10.

Sections 5.2 and 5.3 deal with semi-rational polytopes, so in this section the a_i will be primitive integer vectors; that is, vectors a_i such that $\frac{1}{k}a_i$ is not an integer for any integer $k > 1$, or, equivalently, the greatest common divisor of all coordinates of a_i is 1.

In Section 5.2, we will show Theorem 9 just for full-dimensional semi-rational polytopes; this is Corollary 41. It turns out that showing this theorem for codimension one polytopes is actually harder than for full-dimensional ones; in fact, in Section 5.3.2, we will first show Corollary 45, which is a strengthened version of Corollary 41 that says that, for full-dimensional semi-rational polytopes P and Q, we have $P = Q$ even if $L_{P+w}(s) = L_{Q+w}(s)$ for s in a dense subset of $\mathbb{R}$. Then we will reduce semi-rational polytopes with codimension one, and rational polytopes with any dimension, to this corollary.

In these proofs, we will have to use limits with "restricted domains". If $D \subseteq \mathbb{R}$ is an unbounded set, then the expression

$$\lim_{\substack{s\to\infty \\ s\in D}} f(s) = l$$

means that, for every $\varepsilon > 0$, there is a number N such that, for all $s \in D$, if $s > N$ then $|f(s) - l| < \varepsilon$. For example, if $D = \{k\pi \mid k \in \mathbb{Z}\}$, then

$$\lim_{\substack{\theta\to\infty \\ \theta\in D}} \sin\theta = 0,$$

a limit which we will usually write as

$$\lim_{\substack{\theta\to\infty \\ \frac{\theta}{\pi}\in\mathbb{Z}}} \sin\theta = 0.$$

Note that this limit is undefined if the domain is bounded.

The relative volume of a semi-rational polytope P, denoted by $\mathrm{vol}_{\mathrm{r}}\, P$, is defined in Section 5.2.2.

Finally, section 5.4 shows Theorem 10.

Chapter 2

Preliminaries

This chapter provides a quick recapitulation of the classical Ehrhart theory and an introduction to real Ehrhart theory.

For more details, see the book by Grünbaum [10] for a reference on polytopes and the book by Beck and Robins [4] for a reference on classical Ehrhart theory.

2.1 Classical Ehrhart theory

As mentioned in the introduction, the *Ehrhart lattice-point enumerator* $L_P(t)$ of a polytope $P \subseteq \mathbb{R}^d$ is defined by $L_P(t) = \#(tP \cap \mathbb{Z}^d)$. We will agree that $L_P(0) = 1$. Let us look at some examples.

The simplest polytopes are the real intervals $[\alpha, \beta] \subseteq \mathbb{R}$ (where α and β are arbitrary real numbers). If we fix $P = [\alpha, \beta]$, we have

$$L_P(t) = \#([t\alpha, t\beta] \cap \mathbb{Z}) = \lfloor t\beta \rfloor - \lceil t\alpha \rceil + 1.$$

We can handle rectangles in higher dimensions using the fact that

$$(P \times Q) \cap (A \times B) = (P \cap A) \times (Q \cap B),$$

so that if $P \in \mathbb{Z}^d$ and $Q \in \mathbb{Z}^f$ we have

$$\begin{aligned} L_{P\times Q}(t) &= \#(tP \times tQ) \cap \mathbb{Z}^{d+f} \\ &= \#((tP \cap \mathbb{Z}^d) \times (tQ \cap \mathbb{Z}^f)) \\ &= \#(tP \cap \mathbb{Z}^d)\#(tQ \cap \mathbb{Z}^f) \\ &= L_P(t)L_Q(t). \end{aligned}$$

If $P = [\alpha_1, \beta_1] \times \cdots \times [\alpha_d, \beta_d]$, we may apply this calculation repeatedly to conclude that

$$L_P(t) = (\lfloor t\beta_1 \rfloor - \lceil t\alpha_1 \rceil + 1) \cdots (\lfloor t\beta_n \rfloor - \lceil t\alpha_n \rceil + 1).$$

Consider now the right triangle $\triangle = \mathrm{conv}\{(0,0),(0,2),(2,0)\}$ (Figure 2.1). The tth dilate of this triangle is defined by the intersection of the half-planes defined by the equations $x \geq 0$, $y \geq 0$, and $x + y \leq 2t$, so we could sum $2t - i$ for i between 0 and $2t$ ($2t - i$ is the number of integer points inside $t\triangle$ which lies in the vertical

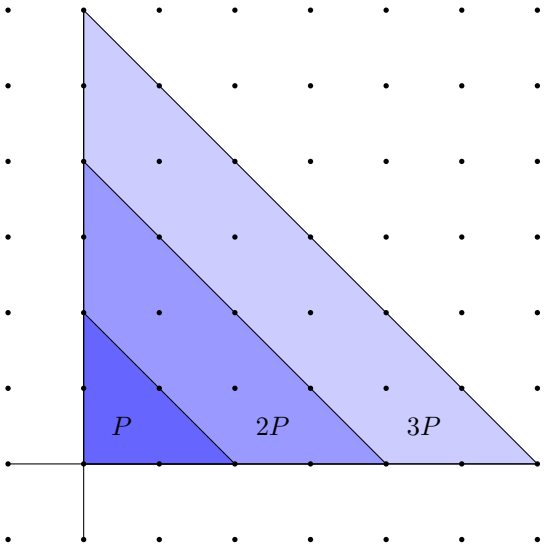


Figure 2.1: Polytope $P = \triangle = \text{conv}\{(0,0),(0,2),(2,0)\}$ and its integer dilates.

line $x = i$); or we could be smarter and notice this triangle takes half of the space of the square $[0, 2t] \times [0, 2t]$. Thus, if we take out the $2t + 1$ integer points which are in the diagonal edge, the remaining $(2t+1)^2 - (2t+1)$ points inside the square are evenly split between the triangle's inside and outside. But we will be lazy and use Pick's theorem below.

Theorem 11 (Pick's theorem)**.** *If A is the area of a polygon with integer vertices, B is the number of integer points in the polygon's boundary, and I is the number of integer points in the polygon's interior, then*

$$A = I + \frac{B}{2} - 1.$$

Since the total number of integer points in the polygon is $I + B$, rearranging terms in the equation gives $I + B = A + B/2 + 1$; in our case, $A = 2t^2$ and $B = 6t$, so $L_{\triangle}(t) = 2t^2 + 3t + 1$.

Incidentally, for any integral polygon P which has B integer points in its boundary, tP will have tB points in its boundary. The area scales quadratically, so if A is P's area then At^2 is tP's area. Using Pick's theorem again gives

$$L_P(t) = At^2 + \frac{B}{2}t + 1. \tag{2.1}$$

Therefore, for any integral polygon, its Ehrhart function is actually a polynomial; therefore, the function L_P is usually called the Ehrhart *polynomial* of P.

In higher dimensions, we do not get simple formulas for the Ehrhart function, but amazingly the Ehrhart function is still a polynomial.

Theorem 12 (Ehrhart's theorem)**.** *If $P \subseteq \mathbb{R}^d$ is an integral polytope, then $L_P(t)$ is a polynomial in t of degree d.*

Looking back at Equation (2.1), we see the leading coefficient is the area of the polygon. This is a consequence of a different interpretation of $L_P(t)$; instead of dilating the polytope, we may shrink the lattice:

$$L_P(t) = \#\left(P \cap \frac{1}{t}\mathbb{Z}^d\right).$$

Now if we divide this value by t^d, it becomes a Riemann sum of the indicator function of P (the corresponding subrectangles are all hypercubes with side $1/t$); as polytopes are Jordan-measurable, we have

$$\lim_{t\to\infty} \frac{L_P(t)}{t^d} = \operatorname{vol} P,$$

for any polytope $P \subseteq \mathbb{R}^d$. This allows us to conclude that the leading coefficient of the Ehrhart polynomial of P is always $\operatorname{vol} P$.

Analyzing again the 1-dimensional polytopes $[\alpha, \beta]$, if we use the identities $\lfloor x \rfloor = x - \{x\}$ and $\lceil x \rceil = x + \{-x\}$, we have

$$\begin{aligned} L_{[\alpha,\beta]}(t) &= t\beta - \{t\beta\} - (t\alpha + \{-t\alpha\}) + 1 \\ &= t(\beta - \alpha) + (1 - \{t\beta\} - \{-t\alpha\}). \end{aligned}$$

So, $L_{[\alpha,\beta]}(t)$ equals $(\operatorname{vol} P)t$ plus an error, which is always in the interval $(-1, 1]$. If α and β are rational numbers, this error term is a periodic function of t, because $\{-t\alpha\}$ and $\{t\beta\}$ will be periodic. This periodicity is not a coincidence: it happens for every rational polytope.

We define the *denominator* of a rational polytope P to be the least common multiple of the denominators of the coordinates of the vertices of P (after reducing each fraction to lowest terms). We have the following.

Theorem 13 (Ehrhart's Theorem for Rational Polytopes)**.** *Let $P \subseteq \mathbb{R}^d$ be a polytope with rational vertices. Then there are periodic functions $c_0(t), \ldots, c_{d-1}(t)$, each with period dividing the denominator of P, such that*

$$L_P(t) = (\operatorname{vol} P)t^d + c_{d-1}(t)t^{d-1} + \cdots + c_1(t)t + c_0(t).$$

Such functions are called *quasipolynomials*[1].

The Ehrhart lattice enumerator $L_P(t)$ was originally defined only for positive t. The expression above gives a natural extension of $L_P(t)$ to negative values: t^k is well-defined for negative t, and each $c_k(t)$ may be computed on negative integers respecting their periodicity. This raises the question to whether there is an interesting interpretation of the values given by $L_P(-t)$; it turns out that this expression enumerates the points in the interior of the polytope.

More formally, let P° be the relative interior[2] of P. Then we have the following.

[1] A quasipolynomial may also have a periodic leading coefficient, but most quasipolynomials we will meet have constant leading coefficient.

[2] Denote by $\operatorname{aff} P$ the *affine hull* of $P \subseteq \mathbb{R}^d$ (the set of all affine combinations of points in P). The *relative interior* P° of P is the set of all $x \in \mathbb{R}^d$ such that, for some open set U of $\mathbb{R}^d$ which contains x, we have $U \cap \operatorname{aff} P \subseteq P$.

Theorem 14 (Ehrhart-Macdonald Reciprocity Theorem)**.** *Let P be a rational polytope and $L_P(t)$ the associated Ehrhart quasipolynomial. Then*

$$L_P(-t) = (-1)^{\dim P} L_{P^\circ}(t),$$

where we use the quasipolynomial behavior to extend L_P to negative numbers.

2.2 Real dilations

When allowing for t to be an arbitrary real positive number, the Ehrhart function has now more information about the polytope, and so it becomes more "sensitive" to the shape of P.

(For simplicity, we will reserve t to be an integer, and use the letter s when talking about real dilates; so, for example, the function $L_P(t)$ is the restriction of the function $L_P(s)$ for integral values.)

A simple example of this extra sensitivity is the rectangle $P = [0,2] \times [0,1]$ and the triangle $\triangle = \text{conv}\{(0,0),(0,2),(2,0)\}$. Using Pick's theorem we can compute $L_P(t) = 2t^2 + 3t + 1$. This is the same polynomial we computed for $\triangle$ in section 2.1; that is, $L_P(t) = L_\triangle(t)$. However, for $s = 3/2$, it is easy to see that sP will contain 8 integer points ($sP = [0,3] \times [0,3/2]$ in this case), whereas $s\triangle = \text{conv}\{(0,0),(0,3),(3,0)\}$ will contain 10. (In our naming convention, this means $L_P(t) = L_\triangle(t)$ but $L_P(s) \neq L_\triangle(s)$.) This shows that $L_P(s)$ is a strictly stronger invariant than $L_P(t)$.

The easiest polytope to deal with is the rectangle $P = [\alpha_1, \beta_1] \times \cdots \times [\alpha_d, \beta_d]$. Even when α_i and β_i and s are real numbers, we have

$$L_P(s) = (\lfloor s\beta_1 \rfloor - \lceil s\alpha_1 \rceil + 1) \cdots (\lfloor s\beta_n \rfloor - \lceil s\alpha_n \rceil + 1).$$

Thus, in the specific case $P = [0,2] \times [0,1]$, we have

$$L_P(s) = (\lfloor 2s \rfloor + 1)(\lfloor s \rfloor + 1).$$

To calculate $L_\triangle(s)$, we could use the same brute-force method hinted in section 2.1, but again we will try to be smart. First, note that for any polytope $P \subseteq \mathbb{R}^d$ and positive real number α, we have

$$L_P(\alpha s) = \#(\alpha s P \cap \mathbb{Z}^d) = L_{\alpha P}(s);$$

therefore, we may define $\triangle' = \frac{1}{2}\triangle = \text{conv}\{(0,0),(1,0),(0,1)\}$ and compute $L_{\triangle'}$ instead.

The polytope $\triangle'$ has the interesting property that it will only "gain" new integer points when s is an integer; in other words, $L_{\triangle'}(s) = L_{\triangle'}(\lfloor s \rfloor)$ (so that when increasing from an integer k to the integer $k+1$ the value of $L_{\triangle'}$ will only change when s becomes the integer $k+1$). Therefore, we may use Pick's theorem again to obtain $L_{\triangle'}(t) = \frac{1}{2}t^2 + \frac{3}{2}t + 1$, and thus

$$\begin{aligned} L_\triangle(s) &= L_{2\triangle}(s) \\ &= L_{\triangle'}(2s) \\ &= L_{\triangle'}(\lfloor 2s \rfloor) \\ &= \frac{1}{2}\lfloor 2s \rfloor^2 + \frac{3}{2}\lfloor 2s \rfloor + 1. \end{aligned} \tag{2.2}$$

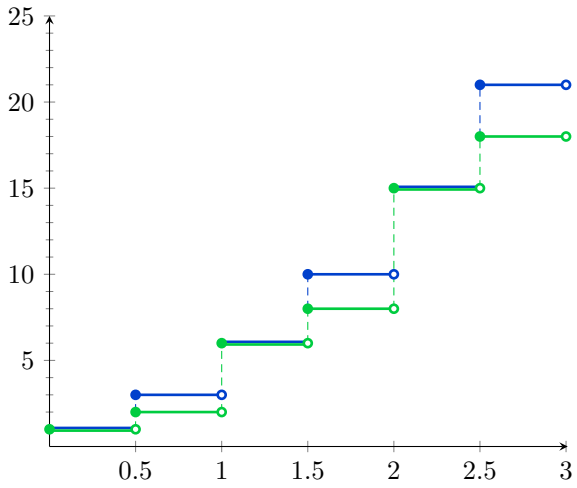


Figure 2.2: Graph of $L_{\triangle}(s)$ (blue) and $L_{[0,2]\times[0,1]}(s)$ (green).

Observe that $L_P(t) = L_{\triangle}(t) = 2t^2 + 3t + 1$, so for integer dilates the Ehrhart polynomials of P and $\triangle$ coincide, but their real counterparts do not (Figure 2.2).

This property that $\triangle'$ has raises an interesting problem: which polytopes also have this same property, namely, that $L_P(s) = L_P(\lfloor s \rfloor)$? This question is treated in the next section.

Chapter 3

Semi-reflexive polytopes

We will say that a rational polytope P is *semi-reflexive* if $L_P(s) = L_P(\lfloor s \rfloor)$ for all $s \geq 0$. In this chapter we will show Theorems 1 and 7, which characterize semi-reeflexive polytopes, and Theorem 2, which relates semi-reflexive and reflexive polytopes.

In this chapter, we will mostly deal with full-dimensional real polytopes. Thus, in the hyperplane description

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

the a_i will be arbitrary real vectors, rescaled so that the b_i are either -1, 0 or 1; and n is the number of facets in P.

3.1 Characterizing semi-reflexive polytopes in terms of their hyperplane description

The "if" part of both Theorems 1 and 7 is easy.

Theorem 15. *Let P be as in* (1.1)*. If every b_i is either* 0 *or* 1*, and a_i is integral whenever $b_i = 1$, then $L_P(s) = L_P(\lfloor s \rfloor)$.*

Proof.

$$L_P(s) = \sum_{x \in \mathbb{Z}^d} [x \in sP] = \sum_{x \in \mathbb{Z}^d} \prod_{i=1}^{n} \big[\langle a_i, x \rangle \leq s b_i\big].$$

If $b_i = 0$, the term $[\langle a_i, x \rangle \leq s b_i]$ reduces to $[\langle a_i, x \rangle \leq 0]$, which is constant for all s; thus $[\langle a_i, x \rangle \leq s b_i] = \big[\langle a_i, x \rangle \leq \lfloor s \rfloor\, b_i\big]$.

If $b_i = 1$, as x and a_i are integral, the number $\langle a_i, x \rangle$ is an integer, thus $[\langle a_i, x \rangle \leq s b_i] = \big[\langle a_i, x \rangle \leq \lfloor s \rfloor\, b_i\big]$ again.

Therefore,

$$\begin{aligned} L_P(s) &= \sum_{x\in\mathbb{Z}^d} \prod_{i=1}^{n} \left[\langle a_i, x\rangle \le s b_i\right] \\ &= \sum_{x\in\mathbb{Z}^d} \prod_{i=1}^{n} \left[\langle a_i, x\rangle \le \lfloor s\rfloor\, b_i\right] \\ &= \sum_{x\in\mathbb{Z}^d} \left[x \in \lfloor s\rfloor\, P\right] \\ &= L_P(\lfloor s\rfloor). \end{aligned}$$ □

For the other direction we need a lemma.

Denote the open ball with radius δ centered at x by $B_\delta(x)$; that is, if $x \in \mathbb{R}^d$, we have

$$B_\delta(x) = \{y \in \mathbb{R}^d \mid \|y - x\| < \delta\}.$$

Lemma 16. *Let K be a full-dimensional cone with apex 0, and let $\delta > 0$ be any value. Then there are infinitely many integer points $x \in K$ such that $B_\delta(x) \subset K$.*

That is, there are many points which are "very inside" K.

Proof. Choose x to be any rational point in the interior of the cone. By definition, there is some $\varepsilon > 0$ with $B_\varepsilon(x) \subseteq K$. For any $\lambda > 0$, we have

$$\lambda B_\varepsilon(x) = B_{\lambda\varepsilon}(\lambda x) \subseteq K.$$

For all sufficiently large λ, we have $\lambda\varepsilon > \delta$, so we just need to take the infinitely many integer λ such that λx is an integer vector. □

We will need the fact that these integral points are distant from the boundary only in the proof of Theorem 7. For the next theorem, existence of infinitely many such points would be enough.

Proposition 17. *Let P be a full-dimensional polytope. If $0 \notin P$, then $L_P(s)$ is not a nondecreasing function. In fact, $L_P(s)$ has infinitely many "drops"; that is, there are infinitely many points s_0 such that $L_P(s_0) > L_P(s_0 + \varepsilon)$ for sufficiently small $\varepsilon > 0$.*

Proof. Writing P as in (1.1), we conclude at least one of the b_i must be negative (because the vector 0 satisfies every linear restriction where $b_i \ge 0$). Equivalently (dividing both sides by b_i), there is a half-space of the form $\{x \mid \langle u, x\rangle \ge 1\}$ such that some facet F of P is contained in $\{x \mid \langle u, x\rangle = 1\}$.

Now, consider the cone $\bigcup_{\lambda>0} \lambda F$. The previous lemma says there is an integral point x_0 in this cone, and so by its definition we have $x_0 \in s_0 F$ for some $s_0 > 0$; thus, $x_0 \in s_0 P$. We will argue that, for all sufficiently small $\varepsilon > 0$, the polytopes $(s_0+\varepsilon)P$ do not contain any integral point which is not present in $s_0 P$ (Figure 3.1).

For small ε (say, $\varepsilon < 1$), all these polytopes are "uniformly bounded"; that is, there is some N such that $(s_0 + \varepsilon)P \subseteq [-N, N]^d$ for all $0 \le \varepsilon < 1$. Each integral x in $[-N, N]^d$ which is not in $s_0 P$ must violate a linear restriction of the form $\langle a_i, x\rangle \le s_0 b_i$; that is, $\langle a_i, x\rangle > s_0 b_i$ for some i. As we are dealing with real variables, we also have $\langle a_i, x\rangle > (s_0 + \varepsilon) b_i$ for all sufficiently small ε, say, for all

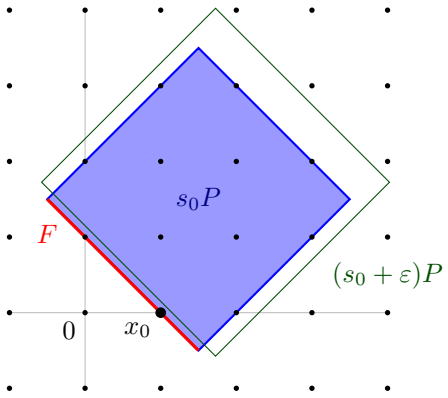


Figure 3.1: The polytope P, when dilated, loses the point x_0, but if the dilation is small enough then it does not gain any new integral point. Therefore, $L_P(s)$ will decrease from s_0 to $s_0 + \varepsilon$.

$\varepsilon < \delta_x$ for some $\delta_x > 0$. Now, as there is a finite number of such relevant integral x, we can take δ to be the smallest of all such δ_x; then if $0 < \varepsilon < \delta$ every integral point of $(s_0 + \varepsilon)P$ also appears in s_0P.

But the special restriction $\langle u, x\rangle \geq 1$, considered above, "dilates" to the linear restriction $\langle u, x\rangle \geq s_0 + \varepsilon$ in $(s_0 + \varepsilon)P$. Since x_0 satisfy this restriction with equality for $\varepsilon = 0$, for any $\varepsilon > 0$ we will have $x_0 \notin (s_0 + \varepsilon)P$. Therefore, not only the dilates $(s_0 + \varepsilon)P$ do not contain new integral points (for small enough ε), but actually these dilates lose the point x_0 if $\varepsilon > 0$. Thus, $L_P(s_0) > L_P(s_0 + \varepsilon)$ for all sufficiently small $\varepsilon > 0$.

Finally, there are infinitely many integral x_0 in the cone $\bigcup_{\lambda>0} \lambda F$; thus we have infinitely many different values of $\|x_0\|$ and hence of s_0, and the reasoning above shows $L_P(s)$ "drops" in every such s_0. □

A simple consequence of this proposition is that if s_0 is a point where $L_P(s)$ "drops", then in the interval $\big[\lfloor s_0\rfloor, \lfloor s_0\rfloor + 1\big)$ the function $L_P(s)$ will not be a constant function, so we cannot have $L_P(s) = L_P(\lfloor s\rfloor)$ for all s if P does not contain the origin.

A more interesting consequence comes from the observation that, if P is a full-dimensional polytope which contains 0, then $L_P(s)$ is a nondecreasing function. If v is any integer vector such that $0 \notin P+v$, then the proposition says $L_{P+v}(s)$ is not a nondecreasing function, and so $L_P(s)$ and $L_{P+v}(s)$ must be different functions, even though $L_P(t)$ and $L_{P+v}(t)$ are the same. We will explore this consequence in more details in Section 3.3.

Before continuing, we observe how this proposition may be extended to non-full-dimensional polytopes. For any polytope $P \subseteq \mathbb{R}^d$, if s is sufficiently small we have $sP \subseteq [-1, 1]^d$, so if P does not contain the origin we have

$$\lim_{s\to 0^+} L_P(s) = 0.$$

Since we agreed that $L_P(0) = 1$, the function $L_P(s)$ will not be nondecreasing for any polytopes which does not contain the origin, however we may not conclude anything about the infinitely many drops. For example, if $P =$

$\operatorname{conv}\{(1,\pi),(2,2\pi)\}$, then $L_P(s) = 0$ whenever $s > 0$, so L_P has only one drop — at $s = 0$.

We are now able to show that, for full-dimensional polytopes, the converse of Theorem 15 holds.

Theorem 7. *Let P be a full-dimensional real polytope. Then $L_P(s) = L_P(\lfloor s \rfloor)$ for all s if and only if the polytope P can be written as in* (1.1) *where each b_i is either* 0 *or* 1*, and when $b_i = 1$ the vector a_i must be integral.*

Proof. Since $0 \in P$, by the previous proposition, we know we can write P as in (1.1), with each b_i being nonnegative. By dividing each inequality by the corresponding b_i (if $b_i \neq 0$), we may assume each b_i is either 0 or 1. Now we must show that when $b_i = 1$, the vector a_i will be integral.

Let $\langle u, x\rangle \leq 1$ be one of the linear restrictions where $b_i = 1$. Using an approach similar to the proof of the previous proposition, we will show that u must be an integral vector.

Let F be the facet of P which is contained in $\{\langle u, x\rangle = 1\}$, and again define $K = \bigcup_{\lambda \geq 0} \lambda F$. Suppose u has a non-integer coordinate; first, we will find an integral point x_0 and a non-integer $s_0 > 0$ such that $x_0 \in s_0 F$.

By Lemma 16 (using $\delta = \frac{3}{2}$), there is some integral $y \in K$ such that $B_{\frac{3}{2}}(y) \subset K$. If $\langle u, y\rangle$ is not an integer, we may let $x_0 = y$ and $s_0 = \langle u, y\rangle$; then x_0 is an integral point which is in the relative interior of $s_0 F$. If $\langle u, y\rangle$ is an integer, as u is not an integral vector, some of its coordinates is not an integer, say the jth; then $\langle u, y+e_j\rangle$ will not be an integer, so (as $y + e_j \in B_{\frac{3}{2}}(y) \subset K$) we may let $x_0 = y + e_j$ and $s_0 = \langle u, y+e_j\rangle$ to obtain our desired integral point which is in a non-integral dilate of F.

We have $sP \subset s_0 P$ for $s < s_0$, but $x_0 \notin sP$ for any $s < s_0$, so $L_P(s) < L_P(s_0)$ for all $s < s_0$. As s_0 is not an integer (by construction), this shows that $L_P(\lfloor s_0 \rfloor) < L_P(s_0)$, a contradiction. □

Finally, using unimodular transforms, we may show the characterization for rational polytopes.

Theorem 1. *Let P be a rational polytope written as in* (1.1)*. Then P is semi-reflexive if and only if all a_i are integers and all b_i are either* 0 *or* 1*.*

Proof. The "if" part is Theorem 15, so assume that $L_P(s) = L_P(\lfloor s \rfloor)$. If P is full-dimensional, we just need to apply Theorem 7: if any of the a_i is non-integer, then it must be rational (because P is rational) and the corresponding b_i must be zero, so we may just multiply the inequality by the lcm of the denominators of the coordinates of a_i. Thus, assume that P is not full-dimensional.

By the discussion following Proposition 17, we must have $0 \in P$. Let $M = \operatorname{aff} P$, the affine hull of P. Since P contains the origin, M is a vector space; since P is rational, M is spanned by integer points. Let $\dim P$ be the dimension of P (and of M) and let d be the dimension of the ambient space (so that $P \subseteq \mathbb{R}^d$). Then there is a unimodular transform A which maps M to $\mathbb{R}^{\dim P} \times \{0\}^{d-\dim P}$.

If P is contained in the half-space

$$\{x \in \mathbb{R}^d \mid \langle a, x\rangle \leq b\},$$

then AP is contained in the half-space

$$\{x \in \mathbb{R}^d \mid \langle M^{-t} a, x\rangle \leq b\},$$

so applying unimodular transforms do not change neither the hypothesis nor the conclusions. Thus, let Q be the projection of AP to $\mathbb{R}^{\dim P}$; then Q is a semi-reflexive polytope (because $L_Q(s) = L_P(s)$), so we may apply Theorem 7 to conclude the proof. □

We finish this section by remarking that the hypothesis of P being either full-dimensional or rational is indeed necessary. For example, if H is the set of vectors which are orthogonal to $(\ln 2, \ln 3, \ln 5, \ln 7, \ldots, \ln p_d)$ (where p_d is the dth prime number) and $x = (x_1, \ldots, x_d)$ is an integral vector, $x \in H$ if and only if

$$x_1 \log 2 + \ldots x_d \log p_d = 0,$$

which (by applying e^x to both sides) we may rewrite as

$$2^{x_1} 3^{x_2} \ldots p_d^{x_d} = 1,$$

which is only possible if $x_1 = \cdots = x_d = 0$. That is, the only integral point in H is the origin. So, if $P \subseteq H$, then $L_P(s)$ will be a constant function, regardless of any other assumptions over P.

3.1.1 Interiors of polytopes

It is interesting to note there are results similar to Theorems 1 and 7, but for interiors of polytopes. More precisely:

Theorem 18. *Let P be a full-dimensional polytope written as in* (1.1)*. Then $L_{P^\circ}(s) = L_{P^\circ}(\lceil s \rceil)$ for all $s \geq 0$ if and only if all b_i is either 0 or 1, and a_i is integral whenever $b_i = 1$.*

In other words, $L_P(s) = L_P(\lfloor s \rfloor)$ if and only if $L_{P^\circ}(s) = L_{P^\circ}(\lceil s \rceil)$.

Proof. The proof is very similar to the proofs of the theorems 15, 17, and 7, so only the needed changes will be stated.

For Theorem 15, the case $b_i = 0$ is left unchanged, and when $b_i = 1$ we need to use $[n < x] = [n < \lceil x \rceil]$ to conclude that, in all cases, $[\langle a_i, x \rangle < s b_i] = \left[\langle a_i, x \rangle < \lceil s \rceil\, b_i\right]$.

For Proposition 17, we can use the same u, s_0 and x_0, but now we will show $L_{P^\circ}(s_0) < L_{P^\circ}(s_0 - \varepsilon)$. A point x which is in the interior of $s_0 P^\circ$ satisfy all linear restrictions of the form $\langle x, a_i \rangle < s_0 b_i$. For all sufficiently small $\varepsilon > 0$ we have $\langle x, a_i \rangle < (s_0 - \varepsilon) b_i$, and so every integer point in $s_0 P^\circ$ will also be present on $(s_0 - \varepsilon) P^\circ$. Now the linear restriction $\langle u, x \rangle > 1$ "shrinks" to $\langle u, x \rangle > 1 - \varepsilon$, and so the point x_0 (which satisfy $\langle u, x_0 \rangle = 1$) will be contained in $(s_0 - \varepsilon) P^\circ$, and thus $L_{P^\circ}(s_0 - \varepsilon) > L_{P^\circ}(s_0)$.

And for Theorem 7, we again can use the same s_0 and x_0 and also the face F, but now we will dilate P° instead of shrinking. As $sP \subseteq s'P$ for all $s \leq s'$, we also have $sP^\circ \subseteq s'P^\circ$ for all $s \leq s'$. Now $x_0 \in s_0 F$, so for all $\varepsilon > 0$ we will have $x_0 \in (s_0 + \varepsilon) P^\circ$, which thus show $L_P(s_0) < L_P(s_0 + \varepsilon)$. □

Thus, using essentially the same proof as of Theorem 1, we have the following characterization of semi-reflexive polytopes.

Theorem 19. *Let P be a rational polytope. Then P is semi-reflexive if and only if $L_{P^\circ}(s) = L_{P^\circ}(\lceil s \rceil)$ for all real $s \geq 0$.*

3.1.2 Examples of semi-reflexive polytopes

Here, we will use the "if" part of the characterization to provide some examples of semi-reflexive polytopes.

- The unit cube $P = [0,1]^d$. P may be represented by the inequalities $x_i \geq 0$ and $x_i \leq 1$, for all i.
- The standard simplex, which is defined by the inequalities $x_i \geq 0$ for all i, and $x_1 + \cdots + x_d \leq 1$.
- The cross-polytope. This polytope is defined by $|x_1| + \ldots |x_d| \leq 1$. Each of the 2^d vectors $(\alpha_1, \ldots \alpha_d) \in \{-1, 1\}^d$ gives a bounding inequality of the form $\alpha_1 x_1 + \cdots + \alpha_d x_d \leq 1$, all of which satisfy the characterization.
- Order polytopes [16]. Let $\prec$ be a partial order over the set $\{1, \ldots, d\}$. The order polytope for the partial order $\prec$ is the set of points $(x_1, \ldots, x_d) \in \mathbb{R}^d$ which satisfy $0 \leq x_i \leq 1$ for all i, and $x_i \leq x_j$ whenever $i \prec j$.
- Chain polytopes [16]. Let $\prec$ be a partial order over the set $\{1, \ldots, d\}$. The chain polytope for the partial order $\prec$ is the set of points $(x_1, \ldots, x_d) \in \mathbb{R}^d$ which satisfy $0 \leq x_i$ for all i, and $x_{i_1} + \cdots + x_{i_k} \leq 1$ for all chains $i_1 \prec i_2 \prec \cdots \prec i_k$.
- Quasi-metric polytopes [8]. Let G be a graph such that every vertex has degree 1 or 3. Identify its edge set with $\{1, \ldots, d\}$. The quasi-metric polytope $\mathcal{P}_G$ is defined to be the set of points $(x_1, \ldots, x_d) \in \mathbb{R}^d$ satisfying all inequalities of the form $x_i \leq x_j + x_k$ and $x_i + x_j + x_k \leq 1$, whenever i, j and k are the edges incident to a degree-3 vertex in G.
- And, as we will see in Section 3.1.3, all reflexive polytopes are also semi-reflexive.

3.1.3 Relation with reflexive polytopes

The hyperplane representation of Theorem 1 may be rewritten in matricial form as follows:

$$P = \{x \in \mathbb{R}^d \mid A_1 x \leq \mathbf{1}, A_2 x \leq 0\}, \tag{3.1}$$

where $\mathbf{1} = (1, \ldots, 1)$ is the all-ones vector, and A_1 and A_2 are integer matrices. We will use this representation to relate semi-reflexive and reflexive polytopes.

There are several equivalent definitions of reflexive polytopes (see e.g. [3, p. 185]). We mention two of them.

First, P is a reflexive polytope if it is an integer polytope which may be written as

$$P = \{x \in \mathbb{R}^d \mid Ax \leq \mathbf{1}\},$$

where $\mathbf{1} = (1, \ldots, 1)$ is the all-ones vector and A is an integer matrix. This definition make it obvious that every reflexive polytope is also semi-reflexive.

The second definition uses the dual P^* of a polytope P, defined by

$$P^* = \{x \in \mathbb{R}^d \mid \langle x, y \rangle \leq 1 \text{ for all } y \in P\}.$$

Then P is reflexive if and only if both P and P^* are integer polytopes.

We have the following relation between reflexive and semi-reflexive polytopes.

Theorem 2. *P is a reflexive polytope if and only if both P and P^* are semi-reflexive polytopes.*

Proof. If P is reflexive, then P^* is also reflexive, and thus both are semi-reflexive.

Now, suppose that P and P^* are semi-reflexive polytopes. This contains the implicit assumption that P^* is bounded, and thus P must contain the origin in its interior. Therefore, by Theorem 1, we must have

$$P = \{x \in \mathbb{R}^d \mid Ax \leq \mathbf{1}\}$$

for some integer matrix A. (The fact that 0 is in the interior of P allowed us to ignore A_2 in the representation (3.1).)

So, we just need to show that P has integer vertices. Since $(P^*)^* = P$, we may apply the same reasoning to P^* to write

$$P^* = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \langle a_i, x\rangle \leq 1\}$$

for certain integers $a_1, \ldots, a_n$. But these a_i are precisely the vertices of P, being, thus, an integral polytope. □

3.2 Application: two polytopes having the same Ehrhart function

Let P and Q be the 3-dimensional polytopes

$$P = \operatorname{conv}\left\{(0,0,0), (0,\tfrac{1}{2},\tfrac{1}{2}), (\tfrac{1}{2},0,\tfrac{1}{2}), (\tfrac{1}{2},\tfrac{1}{2},0)\right\}$$
$$Q = \operatorname{conv}\left\{(0,0,0), (0,\tfrac{1}{2},0), (\tfrac{1}{2},\tfrac{1}{2},0), (\tfrac{1}{2},0,0), (\tfrac{1}{4},\tfrac{1}{4},\tfrac{1}{2})\right\}$$

(Figure 3.2). First, we will show these two polytopes are semi-reflexive. Then, interpolating polynomials, we will show that $L_P(t) = L_Q(t)$. This will allow us to conclude their real Ehrhart functions are also the same.[1]

P is a tetrahedron, so each 3-element subset of its vertex set span a supporting hyperplane of P. Then we just need to look at the other point to determine the direction. We get the inequalities

$$\begin{aligned} x - y - z &\leq 0 \\ -x + y - z &\leq 0 \\ -x - y + z &\leq 0 \\ x + y + z &\leq 1 \end{aligned}$$

Theorem 13 says that

$$L_P(t) = (\operatorname{vol} P)t^3 + c_2(t)t^2 + c_1(t)t + c_0(t),$$

[1] P and Q are the quasi-metric polytopes associated with the graphs  and  , respectively. This specific example was taken from a paper by Fernandes, Pina, Ramírez Alfonsín, and Robins [8]. This paper shows that, if two $\{1,3\}$-graphs are equivalent under nearest-neighbor interchange operations, then the associated polytopes will have the same (integer) Ehrhart quasipolynomial. Since all these polytopes are semi-rational, this paper provides a whole family of rational polytopes with the same real Ehrhart function.

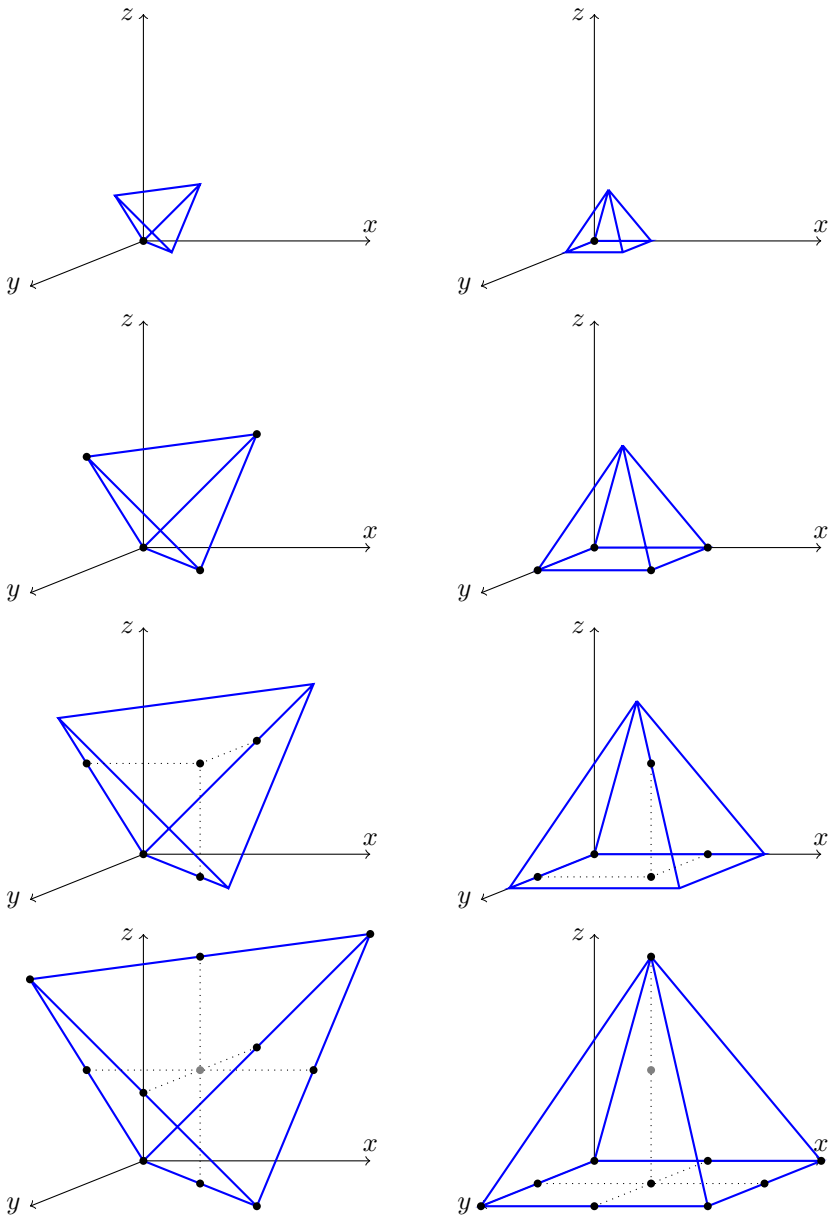


Figure 3.2: Polytopes P and Q and their dilates. The black points are integer points in the boundary of each dilate; the gray points are in the interior.

where each c_i has period 2. A different interpretation of the periodicity of the c_i is to look at each congruency class modulo 2 of t; since these functions will be constant in each congruency class, we know there are two polynomials p_0 and p_1 such that

$$L_P(t) = \begin{cases} p_0(t), & \text{if } t \equiv 0 \pmod 2; \\ p_1(t), & \text{if } t \equiv 1 \pmod 2. \end{cases}$$

To get the coefficients of p_0 and p_1, we will use polynomial interpolation. According to Theorem 14, we know $L_P(-t) = -L_{P^\circ}(t)$, so we may interpolate the points -3, -1, 1 and 3 to get the formula for p_1. Using the inequalities above to test all integral points in the cube $[0,1]^3$ (or looking at Figure 3.2), we get

$$\begin{aligned} p_1(-1) &= -L_{P^\circ}(-1) = 0 & \qquad p_1(1) &= L_P(1) = 1 \\ p_1(-3) &= -L_{P^\circ}(-3) = 0 & \qquad p_1(3) &= L_P(3) = 5 \end{aligned}$$

so polynomial interpolation allows us to determine that

$$p_1(t) = \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{11}{24}t + \frac{1}{4}.$$

To compute p_0, we will do the same thing. Interpolating, for example, at -4, -2, 2 and 4, we have

$$\begin{aligned} p_0(-2) &= -L_{P^\circ}(-2) = 0 & \qquad p_0(2) &= L_P(2) = 4 \\ p_0(-4) &= -L_{P^\circ}(-4) = -1 & \qquad p_0(4) &= L_P(4) = 11 \end{aligned}$$

so that

$$p_0(t) = \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{5}{6}t + 1.$$

Now let us compute $L_Q(t)$. The polytope Q has five vertices, so there are 10 hyperplanes to analyze. Two of them (each spanneed by two opposite vertices of the base together with the top vertex) yield "invalid" hyperplanes, and each of the four 3-set spanned by the vertices in the base yield the same hyperplane. We get the inequalities

$$\begin{aligned} -z &\le 0 \\ 2x + z &\le 1 \\ -2x + z &\le 0 \\ 2y + z &\le 1 \\ -2y + z &\le 0 \end{aligned}$$

Since the denominator of Q is 4, now we have four different polynomials q_0, q_1, q_2 and q_3 for each congruence class of t modulo 4. To compute, for example, q_1, we need to evaluate (say) $L_P(1) = q_1(1)$, $L_P(5) = q_1(5)$, $L_{P^\circ}(-3) = -q_1(-3)$ and $L_{P^\circ}(-7) = -q_1(-7)$, and then interpolate these values. (Now its better to use a computer to do this calculation.) We get

$$\begin{aligned} q_0(t) = q_2(t) &= \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{5}{6}t + 1, \\ q_1(t) = q_3(t) &= \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{11}{24}t + \frac{1}{4}. \end{aligned}$$

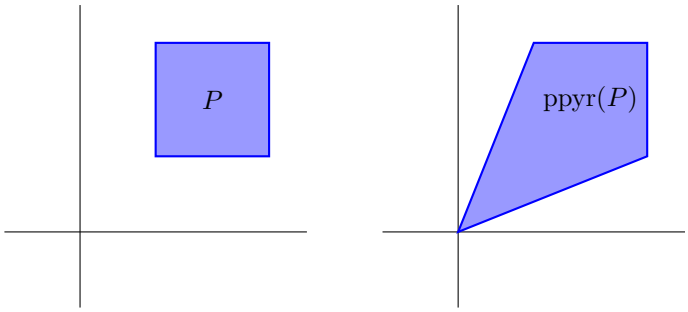


Figure 3.3: Pseudopyramid of a polytope.

This shows that $L_P(t) = L_Q(t)$ for all integers t. Finally, using Theorem 1, it is clear from the inequalities above that both P and Q are semi-rational, and thus we may conclude that $L_P(s) = L_Q(s)$ for all s.

3.3 A digression: $L_P(s)$ is highly non-translation invariant

It is easy to show that both the integer and the real Ehrhart functions are invariant under unimodular transforms; that is, $L_P(s) = L_{AP}(s)$ for all unimodular transforms A. It is also easy to show that the integer Ehrhart function is invariant under integer translation; that is, $L_P(t) = L_{P+w}(t)$ for all integer vectors w.

One of the consequences of Theorem 17, mentioned after its proof, is that for full-dimensional polytopes P which contain the origin, $L_P(s)$ and $L_{P+v}(s)$ will be different functions for all vectors v which "take P out of the origin"; that is, all v such that $0 \notin P + v$. This section expands on this issue, and shows how bad behaved the real Ehrhart function can be with respect to translation.

We will first define an operation, called "pseudopyramid", that constructs a polytope $\text{ppyr}(P)$ from a polytope P. This operation will have the property that, if $\text{ppyr}(P)$ and $\text{ppyr}(Q)$ have different volumes, then $L_P(s)$ and $L_Q(s)$ differ in infinitely many points. Then we will show that, whenever P is a polytope which does not contain the origin and $v \in P$, all pseudopyramids $\text{ppyr}(P + \lambda v)$ (for $\lambda \geq 0$) will have different volumes.

Let $P \subseteq \mathbb{R}^d$ be any polytope. Define $\text{ppyr}(P)$ to be the convex hull of $P \cup \{0\}$, or, equivalently,

$$\text{ppyr}(P) = \bigcup_{0 \leq \lambda \leq 1} \lambda P$$

(Figure 3.3). The pseudopyramid is so called because it resembles the operation of creating a pyramid over a polytope. Note however that the pseudopyramid lives in the same ambient space as the polytope, whereas the pyramid over a polytope is a polytope in one higher dimension (that is, $\text{ppyr}(P) \subseteq \mathbb{R}^d$ while $\text{pyr}(P) \subseteq \mathbb{R}^{d+1}$).

The following lemma says that we may compute the Ehrhart function of P from the Ehrhart function of $\text{ppyr}\, P$.

Lemma 20. *Let P and Q be real polytopes such that $L_P(s) = L_Q(s)$. Then $L_{\text{ppyr}\, P}(s) = L_{\text{ppyr}\, Q}(s)$.*

Thus, if, for example, $\operatorname{ppyr} P$ and $\operatorname{ppyr} Q$ have different volumes, then these polytopes will have different Ehrhart functions and we will be sure that P and Q also have different Ehrhart functions.

Proof. First, we will define an operation, called "lifting", which we will use to reconstruct $L_{\operatorname{ppyr} P}(s)$ from $L_P(s)$.

Let $f : \mathbb{R} \to \mathbb{R}$ be any function which has a jump-discontinuity at a point s_0, and denote by $f(s_0^+)$ the limit of $f(s)$ as $s \to s_0$ with $s > s_0$. Define a function $g : \mathbb{R} \to \mathbb{R}$ by

$$g(s) = \begin{cases} f(s), & \text{if } s \le s_0; \\ f(s) - f(s_0^+) + f(s_0), & \text{if } s > s_0. \end{cases}$$

The function g is right-continuous at s_0 by construction. Call g the *result of lifting* f *at* s_0. For example, if f is the indicator function of $[0, 1]$, the result of lifting f at 1 is the indicator function of $[0, \infty)$.

If the discontinuity points of f are $s_0 < s_1 < s_2 < \dots$, we may successively lift the function at these points; that is, let $f_0 = f$ and for $k \ge 0$ let f_{k+1} be the result of lifting f_k at s_k. If $s < s_n$ for some n, then for all $k > n$ we have $f_k(s) = f_n(s)$, so that the functions f_k converge pointwise at every $s \in \mathbb{R}$. Let g be this pointwise limit; we will call g the *lifting* of f. (Figure 3.4d shows the graph of the lifting of the function depicted in Figure 3.4c.)

Fix the polytope P; we will show that $L_{\operatorname{ppyr} P}(s)$ is the lifting of $L_P(s)$.

Given a point x, define $\mathbb{1}_x(s) = [x \in sP]$ (the "indicator function" of x); that is, $\mathbb{1}_x(s) = 1$ if $x \in sP$ and 0 otherwise. Note we have $L_P = \sum_{x \in \mathbb{Z}^d} \mathbb{1}_x$.

Observe that $\mathbb{1}_x$ is the indicator function of a closed interval. If this interval is $[a, b]$, denote by $\mathbb{1}'_x$ the result of lifting $\mathbb{1}_x$ at b. If the interval is $\emptyset$ or $[a, \infty)$, just let $\mathbb{1}'_x = \mathbb{1}_x$. Since we have

$$s \operatorname{ppyr} P = \bigcup_{0 \le \lambda \le s} \lambda P,$$

we know that $x \in s \operatorname{ppyr} P$ whenever $s \ge a$, so we have $\mathbb{1}'_x(s) = [x \in s \operatorname{ppyr} P]$; therefore,

$$L_{\operatorname{ppyr} P} = \sum_{x \in \mathbb{Z}^d} \mathbb{1}'_x.$$

It is a simple exercise showing the lifting of a sum of finitely many functions is the sum of their liftings. Let $N > 0$ be fixed. If we look only for $s < N$, only finitely many of the functions $\mathbb{1}_x$ will be nonzero, so we may apply this result. If f is the lifting of $L_P(s)$, for $s < N$ we have

$$f(s) = \sum_{x \in \mathbb{Z}^d} \mathbb{1}'_x = L_{\operatorname{ppyr} P}(s).$$

As N was arbitrary, we conclude $L_{\operatorname{ppyr} P}$ is the lifting of L_P.

Finally, if $L_P(s) = L_Q(s)$, then their liftings $L_{\operatorname{ppyr} P}(s)$ and $L_{\operatorname{ppyr} Q}(s)$ will be equal. □

In order to use this lemma, we will decompose the pseudopyramid in several interior-disjoint pieces and show that some of them get "larger" when the polytope is translated. Since we have

$$\lim_{s \to \infty} \frac{L_{\operatorname{ppyr} P}(s)}{s^d} = \operatorname{vol} \operatorname{ppyr} P,$$

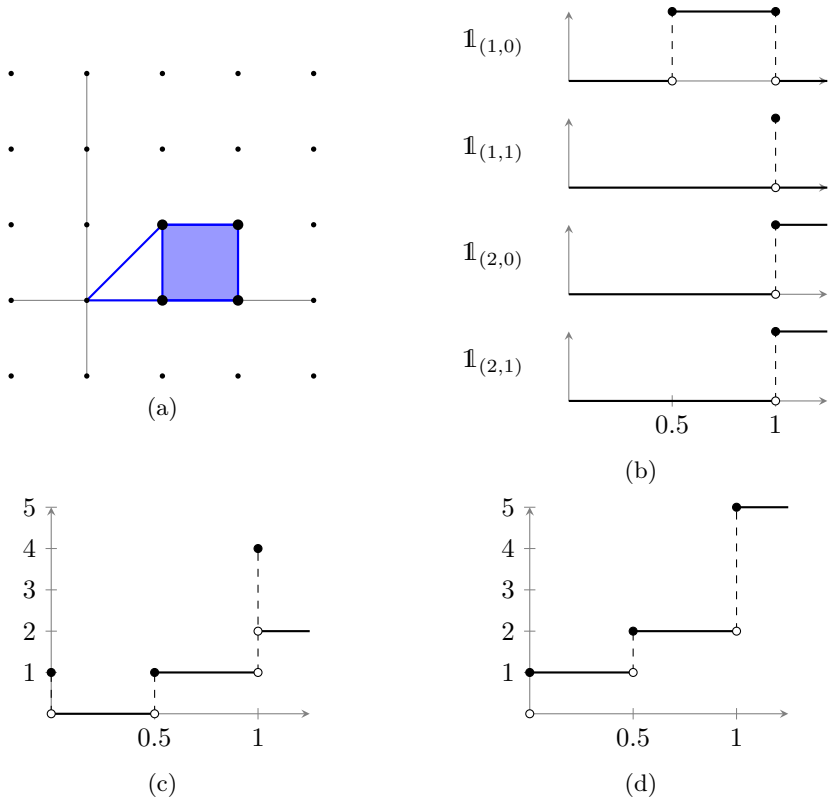


Figure 3.4: Computing $L_{\operatorname{ppyr} P}(s)$ from $L_P(s)$. (a): Polytope $P = [1,2] \times [0,1]$, and an outline of its pseudopyramid. (b): "Indicator functions" $\mathbb{1}_x(s)$ of the points $(1,0)$, $(1,1)$, $(2,0)$ and $(2,1)$. (c): Function $L_P(s)$. (d): Function $L_{\operatorname{ppyr} P}(s)$.

once we show that $\operatorname{ppyr} P$ and $\operatorname{ppyr}(P+w)$ have different volumes, Lemma 20 will guarantee that $L_P(s)$ and $L_{P+w}(s)$ are different.

If $P \subseteq \mathbb{R}^d$ is a full-dimensional polytope with n facets, write P as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \tag{1.1 revisited}$$

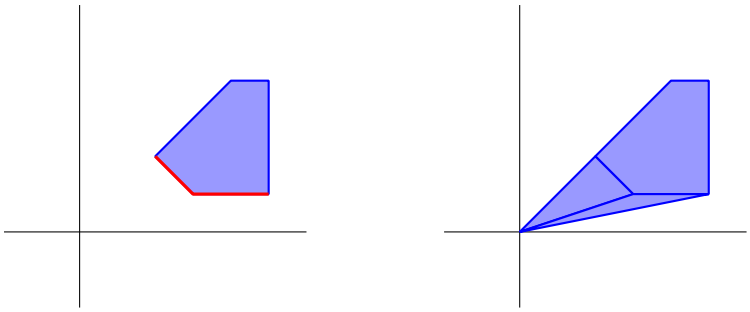
so that each of its facets F_i are defined by

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle = b_i\}.$$

Call F_i a *back facet* of P if $b_i < 0$ (Figure 3.5a). The pseudopyramid $\operatorname{ppyr} F_i$ will intersect P, but as $b_i < 0$ the interiors of these two full-dimensional polytopes are disjoint. This idea leads to the following decomposition lemma.

Lemma 21. *The pseudopyramid of a full-dimensional real polytope P is the interior-disjoint union of P and the pseudopyramids* $\operatorname{ppyr} F$ *of the back facets of P.*

Proof. Let P be the polytope we are decomposing. If $x \in \operatorname{ppyr}(P)$, then $x = \lambda y$ for some $y \in P$. If $x \in P$, great; otherwise we may assume y is in the boundary



(a) (b)

Figure 3.5: (a): Back facets (in red) of a polytope. (b): Decomposition of the pseudopyramid $\operatorname{ppyr} P$ of a polytope P in P and in pseudopyramids of its back facets.

of P (otherwise we may replace y by a shrunk version which is in the boundary). Then $\lambda' y \notin P$ for all $\lambda' < 1$, so y is "visible from the origin". Therefore $y \in F$ for some facet F of P which is contained in the back shell, and thus $x \in \operatorname{ppyr}(F)$, which is a polytope of the pseudopyramid decomposition.

This shows the pseudopyramid of P is the union of the pseudopyramid decomposition of P. Now we will show interior-disjointness.

If x is in the interior of a $\operatorname{ppyr}(F)$ for a back facet F of P, then x violates the linear restriction of F and thus is not contained in P. Besides, the "projection of x in the back shell of P" (that is, the shortest vector λx which is contained in P) is contained in the relative interior of the facet F, so it is not contained in any other facet of P, and thus x is not contained in any other pseudopyramid of a facet of P. □

For the next lemma, we will also need the fact that the volume of a pyramid is proportional to its height and to the area of its base; more specifically, a pyramid in $\mathbb{R}^d$ with height h and whose base has $(d-1)$-dimensional area A has volume $\frac{Ah}{d}$.

Lemma 22. *Let P be a full-dimensional real polytope which does not contain the origin and v any point of P. Then for any reals $\lambda > \mu \geq 0$, the functions $L_{P+\lambda v}(s)$ and $L_{P+\mu v}(s)$ will differ at infinitely many points.*

Proof. Write P as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\},$$

where n is the number of facets of P, so that each facet F_i can be written as

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle = b_i\}.$$

The facets of $P+\lambda v$ are of the form $F_i+\lambda v$. We will show that, for $\lambda > \mu \geq 0$, if $F_i+\mu v$ is a back facet of $P+\mu v$, then $F_i+\lambda v$ is also a back facet of $P+\lambda v$, and that the volume of $\operatorname{ppyr}(F_i+\mu v)$ is strictly smaller than the volume of $\operatorname{ppyr}(F_i+\lambda v)$ (Figure 3.6). The fact that P does not contain the origin will guarantee the

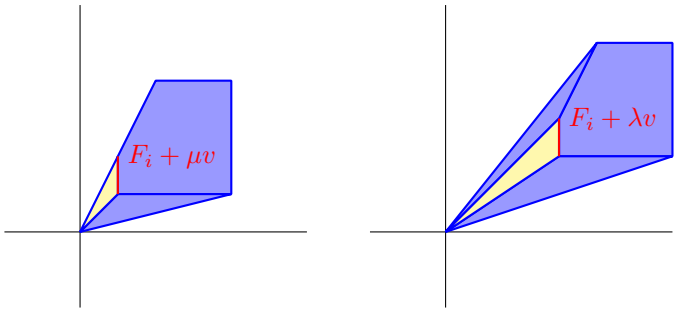


Figure 3.6: For $\lambda > \mu$ and $v \in P$, if $F_i + \mu v$ is a back facet of $P + \mu v$, then $F_i + \lambda v$ is also a back facet of $P + \lambda v$.

existence of at least one back facet. Since the volume of $P + \mu v$ and $P + \lambda v$ are the same, Lemma 21 will guarantee that the volume of $\mathrm{ppyr}(P + \mu v)$ is strictly smaller than the volume of $\mathrm{ppyr}(P + \lambda v)$, and thus by Lemma 20 the functions $L_{P+\mu v}(s)$ and $L_{P+\lambda v}(s)$ are different.

For any μ, we have

$$P + \mu v = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i + \mu\langle a_i, v\rangle\},$$

so that

$$F_i + \mu v = (P + \mu v) \cap \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle = b_i + \mu\langle a_i, v\rangle\}.$$

For all i, we know that

$$\langle a_i, v\rangle \leq b_i,$$

because v is contained in P, by assumption. If $F_i + \mu v$ is a back facet, we know that

$$b_i + \mu\langle a_i, v\rangle < 0.$$

Adding $\mu\langle a_i, v\rangle$ to both sides of the first inequality and using the latter gives $\langle a_i, v\rangle < 0$. Therefore, for $\lambda > \mu \geq 0$,

$$b_i + \lambda\langle a_i, v\rangle < b_i + \mu\langle a_i, v\rangle,$$

which shows that if $F_i + \lambda v$ is a back facet, then so is $F_i + \mu v$.

As P does not contain the origin, we know at least one of the b_i is negative, and thus P has at least one back facet F_i; therefore, applying the previous reasoning with $\mu = 0$ shows that all the polytopes $P + \lambda v$, for $\lambda \geq 0$, have $F_i + \lambda v$ as a back facet; that is, all these polytopes have back facets.

Since F_i is $(d-1)$-dimensional, the pseudopyramid $\mathrm{ppyr}(F_i + \mu v)$ is actually a pyramid. The height of this pyramid is the distance from the origin to the hyperplane

$$\{x \in \mathbb{R}^d \mid \langle a_i, x\rangle = b_i + \mu\langle a_i, v\rangle\}.$$

Without loss of generality we may assume a_i is unitary, so that this distance is

$$-\big(b_i + \mu\langle a_i, v\rangle\big).$$

As the bases of $\operatorname{ppyr}(F_i + \mu v)$ and $\operatorname{ppyr}(F_i + \mu v)$ have the same area, whenever $\lambda > \mu$ the volume of $\operatorname{ppyr}(F_i + \mu v)$ will be strictly smaller than the volume of $\operatorname{ppyr}(F_i + \lambda v)$.

As $P + \mu v$ has a back facet, by Lemma 21, the volume of $\operatorname{ppyr}(P + \lambda v)$ is strictly larger than the volume of $\operatorname{ppyr}(P + \mu v)$. Observe that there might exist some facet $F_j + \lambda v$ of $P + \lambda v$ such that $F_j + \mu v$ is not a back facet of $P + \mu v$; this is not a problem, because the back facets that do appear in $P + \mu v$ suffice to make the volume of $\operatorname{ppyr}(P + \lambda v)$ larger than $\operatorname{ppyr}(P + \mu v)$.

Finally, since

$$\lim_{s\to\infty} \frac{L_{\operatorname{ppyr}(P+\lambda v)}(s)}{s^d} = \operatorname{vol} \operatorname{ppyr}(P + \lambda v),$$

using Lemma 20, we conclude that the functions $L_{P+\lambda v}(s)$ and $L_{P+\mu v}(s)$ must be different. □

Theorem 8. *Let $P \subseteq \mathbb{R}^d$ be a real polytope which is either full-dimensional or has codimension 1. Then there is an integral vector $w \in \mathbb{R}^d$ such that the functions $L_{P+kw}(s)$ are different for all integers $k \geq 0$.*

Proof. If P is full-dimensional and does not contain the origin, then it contains a nonzero rational vector v. Let w be any nonzero multiple of v which is an integer vector; then Proposition 22 shows directly that all the functions $L_{P+kw}(s)$, for $k \geq 0$, are different.

If P is full-dimensional, but contains the origin, again it will contain a nonzero rational vector v. Now w not only needs to be a nonzero integer multiple of v, but also w must be large enough so that $P + w$ does not contain the origin (such a w always exist because P is bounded). Now Proposition 22 only shows that all the functions $L_{P+kw}(s)$ will be different for $k \geq 1$. But since $L_{P+kw}(s)$ is nondecreasing only for $k = 0$, because that is the only value of k for which $P + kw$ contains the origin, we must have $L_{P+wk}(s)$ distinct from $L_P(s)$ whenever $k \neq 0$; this completes the proof in this case.

And for the last case (if P has codimension 1), we will use Lemma 20 directly. As P is not full-dimensional, P is contained in a hyperplane H given by

$$H = \{x \in \mathbb{R}^d \mid \langle a, x\rangle = b\},$$

where a is a unit vector and $b \geq 0$.

Let w be any integer vector such that $\langle a, w\rangle > 0$. We have

$$P + kw \subseteq H + kw = \{x \in \mathbb{R}^d \mid \langle a, x\rangle = b + k\langle a, w\rangle\}.$$

As P is not full-dimensional, the pseudopyramid $\operatorname{ppyr}(P + kw)$ is actually a pyramid, whose base is $P + kw$. Let A be the $(d-1)$-dimensional area of P. As a is a unit vector, the height of this pyramid (which is the distance of $H + kw$ to the origin) is $b + \langle a, w\rangle$. Therefore, the volume of $\operatorname{ppyr}(P + kw)$ is

$$\operatorname{vol} \operatorname{ppyr}(P + kw) = \frac{1}{d} A(b + \langle a, w\rangle).$$

Since P has codimension 1, its area A is nonzero, so for $k \geq 0$ all these volumes are different. Thus, all functions $L_{P+kw}(s)$ are different in this case, too. □

If we assume the polytope is rational, we may drop the dimensionality assumption.

Theorem 5. *Let $P \subseteq \mathbb{R}^d$ be a rational polytope with any dimension. Then there is an integral vector $w \subseteq \mathbb{R}^d$ such that the functions $L_{P+kw}(s)$ are distinct for all integers $k \geq 0$.*

Proof. If P has codimension 0 or 1, use Theorem 8. Otherwise, P will be contained in a rational hyperplane passing through the origin, say, H. Then apply an affine transformation to P which maps H to $\mathbb{R}^{d-1} \times \{0\}$ and use this theorem for dimension $d-1$. □

We end this section by showing that, if we do not have the rationality hypothesis, then the dimension hypothesis is necessary. Let $M \subseteq \mathbb{R}^d$ be the $(d-2)$-dimensional affine space defined by

$$M = \{(\ln 2, \ln 3)\} \times \mathbb{R}^{d-2}.$$

That is, M is the set of all points $(x_1, \ldots, x_d)$ in $\mathbb{R}^d$ such that $x_1 = \ln 2$ and $x_2 = \ln 3$.

For any integer translation vector $w = (w_1, \ldots, w_d)$ and any real $s > 0$, we have

$$s(M + w) = \big\{\big(s(\ln 2 + w_1), s(\ln 3 + w_2)\big)\big\} \times \mathbb{R}^{d-2},$$

so if $s(M + w)$ contains an integer point $(x_1, \ldots, x_d)$, then $s(\ln 2 + w_1) = x_1$ and $s(\ln 3 + w_2) = x_2$. Since s, $\ln 2 + w_1$ and $\ln 3 + w_2$ are nonzero, we have $x_1, x_2 \neq 0$, too, and thus their ratio is

$$\frac{x_1}{x_2} = \frac{\ln 2 + w_1}{\ln 3 + w_2},$$

which, rearranging the terms, gives

$$x_1(\ln 3 + w_2) = x_2(\ln 2 + w_1).$$

Raising e to both sides of the equation then gives

$$\begin{aligned} (e^{\ln 3 + w_2})^{x_1} &= (e^{\ln 2 + w_1})^{x_2} \\ 3^{x_1} e^{w_2 x_1} &= 2^{x_2} e^{w_1 x_2} \\ \frac{3^{x_1}}{2^{x_2}} &= e^{w_1 x_2 - w_2 x_1} \end{aligned}$$

As e is a transcendental number, we must have $w_1 x_2 - w_2 x_1 = 0$, which shows $\frac{3^{x_1}}{2^{x_2}} = 1$. This is only possible if $x_1 = x_2 = 0$, a contradiction. Thus, $s(M + w)$ has no integer points.

Therefore, if P is any polytope contained in M, for any integer translation vector w and any real $s > 0$ the polytope $s(P + w)$ will contain no integer points, and thus $L_{P+w}(s) = 0$ for all $s > 0$ and all integer w. So, clearly these functions are all the same.

Chapter 4

Real Ehrhart theorem

The real Ehrhart theorem states that, if $P \subseteq \mathbb{R}^d$ is a rational polytope, then $L_P(s)$ may be written as

$$L_P(s) = c_d(s)s^d + \cdots + c_0(s),$$

where $c_i(s)$ are certain periodic functions of s.

In this chapter, we will use the fractional part function to give a new proof of the real Ehrhart theorem.

This chapter deals almost exclusively with rational polytopes, so in the hyperplane description

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

the a_i will always be integer vectors. Furthermore, we will assume that, for each i, the vector a_i and the integer b_i do not share common factors.

4.1 Step polynomials and real quasipolynomials

Theorem 13 says that whenever P is a rational polytope, the integer function $L_P(t)$ will be a quasipolynomial. The expressions we got for $L_{\triangle}(s)$ and $L_{[0,2]\times[0,1]}(s)$ in Section 2.2 can be rewritten to exhibit quasipolynomial behavior, using the identity $\lfloor x \rfloor = x - \{x\}$:

$$\begin{aligned} L_{[0,2]\times[0,1]}(s) &= (\lfloor 2s \rfloor + 1)(\lfloor s \rfloor + 1) \\ &= 2s^2 + \big(3 - 2\{s\} - \{2s\}\big)s + \{s\}\{2s\} - \{s\} - \{2s\} + 1. \\ L_{\triangle}(s) &= \frac{1}{2}\lfloor 2s \rfloor^2 + \frac{3}{2}\lfloor 2s \rfloor + 1 \\ &= 2s^2 + \big(3 - 2\{2s\}\big)s + \frac{1}{2}\{2s\}^2 - \frac{3}{2}\{2s\} + 1. \end{aligned}$$

The coefficients of s and the "constant term" are periodic functions of s (with period 1 here). The presence of terms of the form $\{\alpha s\}$ in our computations (as a "coefficient") is so ubiquitous it suggests that the functions $L_P(s)$ can always

be written as sums and products of constants, s, and terms of the form $\{\alpha s\}$ for certain numbers α. In other words, maybe $L_P(s)$ is always of the form

$$p_d(s)s^d + p_{d-1}(s)s^{d-1} + \cdots + p_1(s)s + p_0(s),$$

where each $p_i(s)$ is a polynomial over certain $\{\alpha_j s\}$. We will call a function f a *step polynomial*[1] over $\alpha_1, \ldots, \alpha_n$ provided there is a polynomial function p such that

$$f(t) = p(\{\alpha_1 t\}, \ldots, \{\alpha_n t\}).$$

For example, if $P = [\alpha_1, \beta_1] \times \cdots \times [\alpha_d, \beta_d]$, as

$$\lfloor s\beta_i \rfloor - \lceil s\alpha_i \rceil + 1 = (\beta_i - \alpha_i)s - \{\beta_i s\} - \{-\alpha_i s\} + 1,$$

$L_P(s)$ is a quasipolynomial in s whose coefficients are step polynomials over $-\alpha_1, \ldots, -\alpha_d, \beta_1, \ldots, \beta_d$.

The remainder of this section is dedicated to show that, whenever P is a rational polytope, the function $L_P(s)$ is, indeed, a quasi-polynomial whose coefficients are step polynomials.

4.1.1 Polytopes containing the origin

If $0 \in P$, we may try to mimick the procedure we used to obtain the formula (2.2) for $\triangle$. For example, let P be the polytope of Section 3.2. We know that

$$L_P(t) = \begin{cases} \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{5}{6}t + 1, & t \text{ is even;} \\ \frac{1}{24}t^3 + \frac{1}{4}t^2 + \frac{11}{24}t + \frac{1}{4}, & t \text{ is odd.} \end{cases}$$

Let us first find a closed-form expression for $L_P(t)$. The simplest 2-periodic step polynomial is $\{\frac{t}{2}\}$; we may create linear combinations of this step polynomial with the constant polynomial $p(t) = 1$ to get a closed form expression for the coefficients c_1 and c_0. In our case, we may write

$$c_1(t) = \frac{5}{6} - \frac{9}{12}\left\{\frac{t}{2}\right\} \qquad \text{and} \qquad c_0(t) = 1 - \frac{3}{2}\left\{\frac{t}{2}\right\}.$$

We may generalize this procedure using Lagrange's interpolation formula.

Lemma 23. *Any periodic function $f : \mathbb{Z} \to \mathbb{R}$ of period b can be written as a step polynomial over $\frac{1}{b}$.*

Proof. If t is an integer, all the possible values for $\{\frac{t}{b}\}$ are of the form $\frac{k}{b}$ for $0 \le k < b$. Therefore, the function

$$\left\{\frac{t}{b}\right\}\left(\left\{\frac{t}{b}\right\} - \frac{1}{b}\right)\cdots\left(\left\{\frac{t}{b}\right\} - \frac{b-1}{b}\right)$$

[1] This term was borrowed from Baldoni, Belini, Köppe and Vergne [1, p. 3]. They define a step polynomial to be a function of the form

$$f(t) = p\big((\zeta_1 t) \bmod q_1, \ldots, (\zeta_k t) \bmod q_k\big),$$

where $\zeta_i, q_i \in \mathbb{Z}$ and p is a polynomial. In our definition, we demand that $q_1 = \cdots = q_k = 1$.

is identically zero. If we leave out the factor $\left\{\frac{t}{b}\right\} - \frac{a}{b}$ in the expression above, we have a function $q_a(t)$ which is nonzero for $t \equiv a \pmod{b}$ and 0 otherwise. Each of these q_a is clearly a step function over $\frac{1}{b}$, so the fact that every periodic function can be written as a linear combination of these q_a finishes the proof. □

Since the polytope P satisfies the conditions of Theorem 15, we may apply it to the closed-form expression we got for $L_P(t)$. We have

$$\begin{aligned} L_P(s) &= L_P(\lfloor s \rfloor) \\ &= \frac{1}{24}\lfloor s \rfloor^3 + \frac{1}{4}\lfloor s \rfloor^2 + \left(\frac{5}{6} - \frac{9}{12}\left\{\frac{\lfloor s \rfloor}{2}\right\}\right)\lfloor s \rfloor + 1 - \frac{3}{2}\left\{\frac{\lfloor s \rfloor}{2}\right\}. \end{aligned}$$

The factors $\lfloor s \rfloor$ may be expanded using the identity $\lfloor s \rfloor = s - \{s\}$. To deal with the factors $\left\{\frac{\lfloor s \rfloor}{2}\right\}$, we will use the following lemma.

Lemma 24. *If b is a positive integer, then for all real s we have*

$$\left\{\frac{\lfloor s \rfloor}{b}\right\} = \left\{\frac{s}{b}\right\} - \frac{\{s\}}{b}.$$

Proof. The identity $x = \lfloor x \rfloor + \{x\}$ gives

$$\left\{\frac{\lfloor s \rfloor}{b}\right\} = \frac{\lfloor s \rfloor}{b} - \left\lfloor \frac{\lfloor s \rfloor}{b} \right\rfloor.$$

Now if $\lfloor \lfloor s \rfloor / b \rfloor = n$ then $\lfloor s \rfloor / b < n+1$, so $\lfloor s \rfloor < b(n+1)$, so $s < b(n+1)$, so $s/b < n+1$, so $\lfloor s/b \rfloor \le n$. The inequality $\lfloor s/b \rfloor \ge \lfloor \lfloor s \rfloor / b \rfloor$ then implies $\lfloor s/b \rfloor = n$, so $\lfloor \lfloor s \rfloor / b \rfloor = \lfloor s/b \rfloor$. Whence,

$$\begin{aligned} \left\{\frac{\lfloor s \rfloor}{b}\right\} &= \frac{\lfloor s \rfloor}{b} - \left\lfloor \frac{s}{b} \right\rfloor \\ &= \frac{s - \{s\}}{b} - \frac{s}{b} + \left\{\frac{s}{b}\right\} \\ &= \left\{\frac{s}{b}\right\} - \frac{\{s\}}{b}. \end{aligned}$$

□

Now, if we replace $\left\{\frac{\lfloor s \rfloor}{2}\right\}$ with $\left\{\frac{s}{2}\right\} - \frac{\{s\}}{2}$ in the expression we got for $L_P(s)$, we get

$$\begin{aligned} L_P(s) = \frac{1}{24}s^3 + \left(\frac{1}{4} - \frac{\{s\}}{8}\right)s^2 + \left(\frac{\{s\}^2 - \{s\}}{8} - \frac{3}{4}\left\{\frac{s}{2}\right\} + \frac{5}{6}\right)s + \\ - \frac{\{s\}^3}{24} - \frac{\{s\}^2}{8} - \frac{\{s\}}{12} - \frac{3}{2}\left\{\frac{s}{2}\right\} + \frac{3}{4}\{s\}\left\{\frac{s}{2}\right\} + 1. \end{aligned} \tag{4.1}$$

In this case, we had a semi-reflexive polytope; but, for example, when computing $L_{\triangleleft}(s)$, we had first to shrink $\triangleleft$ to a smaller polytope, which was semi-reflexive. In the general case, we will also shrink the polytope, as follows.

If P is the intersection of finitely many half-spaces of the form

$$H_i = \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \le b_i\},$$

where a_i and b_i have no common factors for any i, define the *numerator* of P to be the least common multiple of the b_i. If we divide P by a multiple kb_i of b_i, this modified half-space will read as

$$\frac{1}{kb_i}H = \{x \in \mathbb{R}^d \mid \langle ka_i, x\rangle \leq 1\}.$$

Therefore, if P contains the origin and m is its numerator, then $\frac{1}{m}P$ is semi-reflexive. This observation is the basis for the following theorem.

Proposition 25. *Let P be a rational polytope which contains the origin, and m and k its numerator and denominator, respectively. Then $L_P(s)$ is a quasipolynomial in s whose coefficients are step polynomials over m and $\frac{1}{k}$.*

Proof. As observed above, $\frac{1}{m}P$ is semi-refleixive, and thus by Theorem 1 we have $L_{\frac{1}{m}P}(s) = L_{\frac{1}{m}P}(\lfloor s \rfloor)$.

The denominator of $\frac{1}{m}P$ divides km, so Ehrhart's Teorem for rational polytopes now says that

$$L_{\frac{1}{m}P}(t) = c_d(t)t^d + \cdots + c_0(t)$$

for periodic functions $c_i(t)$ with period km. Applying Lemma 23 allows us to write each $c_i(t)$ as a step polynomial over $\frac{1}{km}$.

Now, $\lfloor s \rfloor$ is an integer, so we may plug $\lfloor s \rfloor$ into these step polynomials and obtain an expression for $L_{\frac{1}{m}P}(\lfloor s \rfloor)$ composed of sums and products of constants and the terms $\lfloor s \rfloor$ and $\left\{\frac{\lfloor s \rfloor}{km}\right\}$. Applying Lemma 24 now allows us to replace each $\left\{\frac{\lfloor s \rfloor}{km}\right\}$ by terms of the form $\left\{\frac{s}{km}\right\}$ and $\frac{\{s\}}{km}$. Using the identity $\lfloor s \rfloor = s - \{s\}$ now allows us to conclude that $L_{\frac{1}{m}P}(s)$ can be written as sums and products of constants and the terms s, $\{s\}$ and $\left\{\frac{s}{km}\right\}$.

Now, using the identity $L_P(s) = L_{\frac{1}{m}P}(ms)$, we get an expression for $L_P(s)$ with the terms s, $\{ms\}$ and $\left\{\frac{s}{k}\right\}$. This is precisely a quasipolynomial whose coefficients are step polynomials over m and $\frac{1}{k}$. □

To generalize this result for all rational polytopes P, even in one dimension, we will need to admit some more numbers over which the coefficients of $L_P(s)$ are step polynomials. For example, if $P = [1, 2]$,

$$\begin{aligned} L_P(s) &= \lfloor 2s \rfloor - \lceil s \rceil + 1 \\ &= s - \{2s\} - \{-s\} + 1, \end{aligned}$$

whose constant coefficient is a step polynomial over 2 and -1. In general, we will allow the coefficients of $L_P(s)$ to be step polynomials over m, $-m$ and $\frac{1}{k}$, where m and k are the numerator and the denominator of the polytope, respectively. (We know we need to allow negative numbers because, for example, the function $L_P(s)$ above is right-discontinuous at $s = 1$, and the functions $\{\alpha s\}$ cannot produce this kind of discontinuity if $\alpha > 0$.)

We will use the "front body/back shell decomposition", developed in the next section.

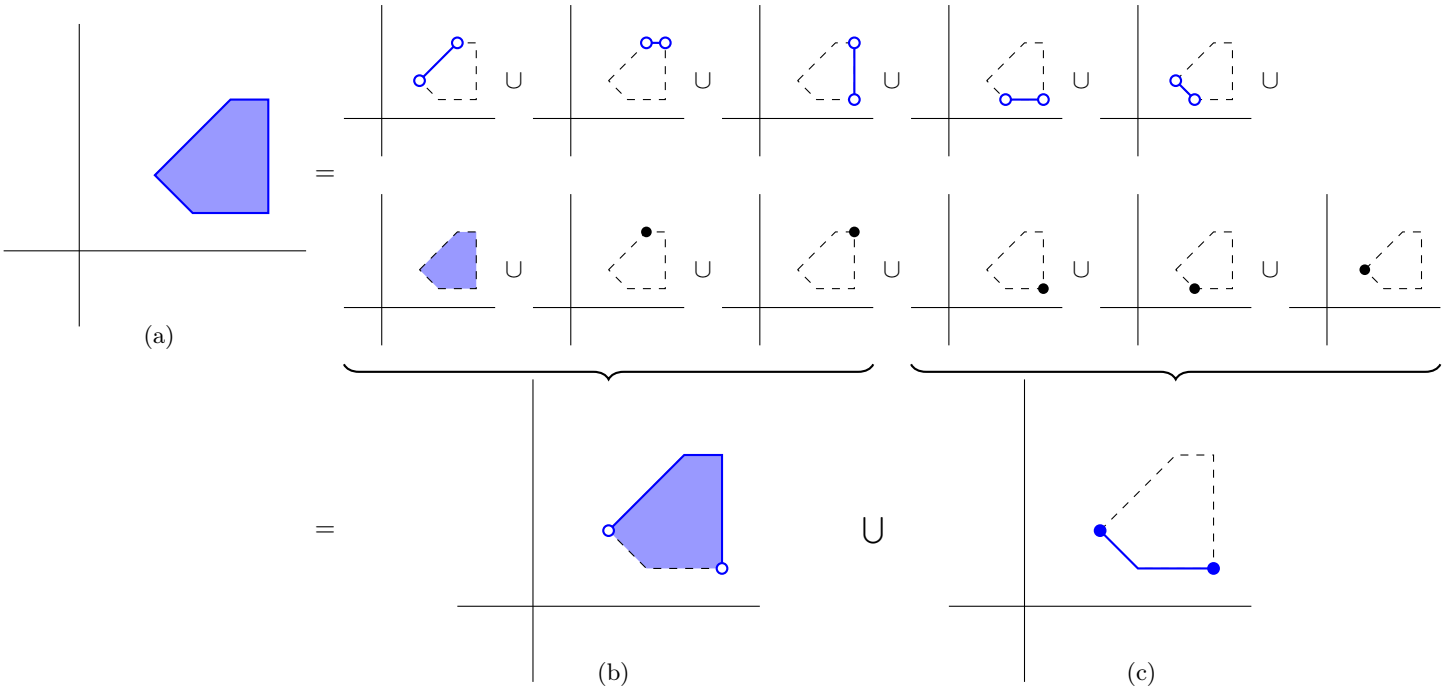


Figure 4.1: Decomposition of the polytope as the disjoint union of the interior of its faces (Lemma 28), and as the disjoint union of its front body and back shell (Proposition 26).
(a): Interiors of the faces of the polytope.
(b): The front body of the polytope; in this case, it is the union of the interiors of first three edges, the interior of the polytope, and the first two vertices.
(c): The back shell of the polytope; in this case, it is the union of the last two edges and the last three vertices.

4.1.2 Front body/back shell decomposition

Let P be any polytope, and write $P = \bigcap_{i=1}^{n} H_i^{\leq}$, where $H_i^{\leq}$ is the half-space

$$H_i^{\leq}\{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}.$$

Define $H_i^{<}$ analogously by

$$H_i^{<}\{x \in \mathbb{R}^d \mid \langle a_i, x\rangle < b_i\}.$$

In the proof of Theorem 15, the fact that $[n \leq b_i \lfloor s \rfloor] = [n \leq b_i s]$ when b_i is 0 or 1 allowed us to show $L_P(s) = L_P(\lfloor s \rfloor)$. For general polytopes, we may have to deal with negative b_i as well, and that relation is false in this case. However, we have an analogous relation if we replace the $\leq$ sign with $<$: $[n < b_i \lfloor s \rfloor] = [n < b_i s]$ if $b_i = -1$. Therfore, we will call by *front body* of the polytope P, denoted by $P^{\triangleright}$, the convex set

$$P^{\triangleright} = \bigcap_{\substack{1 \leq i \leq n \\ b_i \geq 0}} H_i^{\leq} \cap \bigcap_{\substack{1 \leq i \leq n \\ b_i < 0}} H_i^{<}. \tag{4.2}$$

That is, whenever $b_i < 0$, we replace the inequality $\langle a_i, x\rangle \leq b_i$ with the strict inequality $\langle a_i, x\rangle < b_i$ in the half-space intersection representation of the polytope (Figure 4.1b).

Recall that the back shell of the polytope is the set of nonzero points $x \in P$ which are "visible from the origin" (that is, the set of all $x \in P$ such that $\lambda x \notin P$ for all $0 \leq \lambda < 1$). We call it the "front body/back shell decomposition" due to the followith theorem.

Proposition 26. *A polytope is the disjoint union of its front body and its back shell.*

Proof. Let $x \in P$ be in the back shell. We know x satisfies every linear restriction of the form

$$\langle a_i, x\rangle \leq b_i,$$

which bounds the polytope. In the case where $b_i \geq 0$, we know that for all $0 \leq \lambda \leq 1$ the point λx will also satisfy these restrictions. But if $b_i \leq 0$, then for small enough λ the point λx will violate at least one of these inequalities. If x satisifes all these restrictions with strict inequality for all $b_i < 0$ (that is, $\langle a_i, x\rangle < b_i$ whenever $b_i < 0$), then for some $\lambda < 1$ sufficiently close to 1 the point λx will also satisfy all these restrictions. That would contradict the fact that x can be seen from the origin; therefore, for at least one i with $b_i < 0$, we must have

$$\langle a_i, x\rangle = b_i$$

(that is, x satisfy the linear restriction with equality). In the front body, this linear restriction is replaced by strict inequality, and thus now x violates it, so x is not in the front body.

Now, suppose $x \in P$ is not in the back shell; this means x cannot be seen from the origin, and thus for some $\lambda < 1$ we have $\lambda x \in P$. This means λx satisfies

$$\langle a_i, \lambda x\rangle \leq b_i$$

for all i, and so if $b_i < 0$ we have

$$\langle a_i, x\rangle \leq \frac{b_i}{\lambda} < b_i,$$

which shows x is in the front body. □

The lattice point enumerator $L_{P^\flat}(s)$ of the front body of a polytope is defined in the same way as for other sets. The next proposition asserts the front body of a polytope has the computational property we aimed for.

Proposition 27. *Let P be a polytope and $P^\flat$ be its front body, as in* (4.2)*. If all b_i are either* 0, 1 *or* -1 *and all a_i are integral, then for all $s \geq 0$ we have*

$$L_{P^\flat}(s) = L_{P^\flat}(\lfloor s \rfloor).$$

Proof. We saw in the proof of Theorem 15 that, whenever $b_i = 0$ or $b_i = 1$, we have $\big[\langle a_i, x\rangle \leq b_i s\big] = \big[\langle a_i, x\rangle \leq \lfloor s \rfloor\, b_i\big]$. If $b_i = -1$, for every integral point x,

using $[n < s] = [n < \lceil s \rceil]$ we have

$$\begin{aligned}\big[\langle a_i, x\rangle < b_i s\big] &= \big[\langle a_i, x\rangle < -s\big] \\ &= \big[\langle a_i, x\rangle < \lceil -s \rceil\,\big] \\ &= \big[\langle a_i, x\rangle < -\lfloor s \rfloor\,\big] \\ &= \big[\langle a_i, x\rangle < b_i \lfloor s \rfloor\,\big].\end{aligned}$$

Therefore,

$$\begin{aligned}L_{P^\supset}(s) &= \sum_{x\in\mathbb{Z}^d} [x \in sP^\supset] \\ &= \sum_{x\in\mathbb{Z}^d} \left(\prod_{\substack{1\le i\le n \\ b_i \ge 0}} \big[\langle a_i, x\rangle \le b_i s\big] \right) \left(\prod_{\substack{1\le i\le n \\ b_i < 0}} \big[\langle a_i, x\rangle < b_i s\big] \right) \\ &= \sum_{x\in\mathbb{Z}^d} \left(\prod_{\substack{1\le i\le n \\ b_i \ge 0}} \big[\langle a_i, x\rangle \le b_i \lfloor s \rfloor\,\big] \right) \left(\prod_{\substack{1\le i\le n \\ b_i < 0}} \big[\langle a_i, x\rangle < b_i \lfloor s \rfloor\,\big] \right) \\ &= \sum_{x\in\mathbb{Z}^d} [x \in \lfloor s \rfloor\, P^\supset] \\ &= L_{P^\supset}(\lfloor s \rfloor).\end{aligned}$$

□

We need one last property of the front body, which is a refinement of the decomposition of Proposition 26. We will use the following lemma.

Lemma 28. *Let $\mathcal{F}$ be the collection of all faces of a polytope P (including P itself). Then*

$$P = \bigcup_{F\in\mathcal{F}} F^\circ,$$

and this union is disjoint.

Proof. Without loss of generality, we may assume P to be full-dimensional. We will need to use the fact that the topological boundary of P is the union of all facets of P, and that any proper face of P is the intersection of some collection of facets of P (see [10, p. 27] for a proof).

We will use induction in the dimension of the polytope. The result is clearly true for 0-dimensional polytopes (single points).

If $x \in P$ is not in the interior of P, then it must be in the boundary of P, so $x \in F$ for some facet F of P. By induction in the dimension of the polytope, $x \in G^\circ$ for some face G of F, which is also a face of P. This shows that P is the union of the interiors of its faces.

Now we must show that the union is disjoint. If $x \in P$ is in the interior of P, then it cannot be in its topological boundary, so it will not be contained in any proper face of P — thus P° is disjoint from F° for all faces $F \neq P$.

So, suppose $x \in P$ is contained in the interiors of the faces F and G; then x is also in the interior of $F \cap G$. Since F and G are intersection of facets of P, so is $F \cap G$, and thus $F \cap G$ is a face of F. By induction, F is the disjoint union of

the interiors of its faces. As $x \in (F \cap G)^\circ$ and $x \in F^\circ$, we must have $F = F \cap G$. The same reasoning applied to G shows $G = F \cap G = F$. Thus, the union is disjoint. □

If a point in the back shell is in the relative interior of a face of P, then the whole face can be seen from the origin. Since every point of P is in the interior of some face, this means the back shell of the polytope is the union of interiors of certain faces of P. As a consequence, the remaining faces must form the front body of P. In other words, we have the following theorem.

Proposition 29. *For every polytope P there is a partition $\mathcal{F}' \cup \mathcal{F}''$ of the set of its faces such that $\bigcup_{F \in \mathcal{F}'} F^\circ$ is the front body $P^\supset$ of P and $\bigcup_{F \in \mathcal{F}''} F^\circ$ is the back shell of P.*

4.1.3 Real Ehrhart theorem

Before tackling the theorem for all rational polytopes, we will show the following results, which will allow us to perform some useful reductions.

Lemma 30. *Let P be a rational polytope and A a unimodular matrix. Then P and AP have the same numerator and denominator.*

Proof. Let $H = \{x \mid \langle u, x\rangle \leq \alpha\}$ be a half-space, where u and α are integers without a common factor. Then

$$\begin{aligned} AH &= \{Ax \mid \langle u, x\rangle \leq \alpha\} \\ &= \{x \mid \langle u, A^{-1}x\rangle \leq \alpha\} \\ &= \{x \mid \langle A^{-t}u, x\rangle \leq \alpha\}. \end{aligned}$$

As A is unimodular, A^{-t} has only integer entries, so $A^{-t}u$ is an integral vector. If $A^{-t}u$ and α had a common factor c, this means $\frac{1}{c}A^{-t}u$ is an integral vector, and thus $\frac{1}{c}u = A^t(\frac{1}{c}A^{-t}u)$ is also an integral vector, so u and α also shared this common factor. Therefore, $A^{-t}u$ and α have no common factors. This shows that the right-hand side of each inequality which bounds P is unchanged when we apply the linear operator P, even after dividing both sides by their common factors; so the least common multiple of all these α (which is the numerator of the polytope) is left unchanged.

For the denominator, let v be a vertex of P and define k and k' to be the least common multiple of the denominators of the coordinates of the vectors v and Av, respectively. Then kv is an integer and k divides every integer m such that mv is an integer, and same goes for k' and Av. As A has integer entries, $Akv = kAv$ must be an integer vector, and thus k' divides k. Since A^{-1} also has only integer entries, the vector $A^{-1}k'Av = k'v$ also is an integer vector, and thus k divides k'. Thus, $k = k'$. This shows A preserves least common multiples in the vertex level, and thus it must preserve the denominator of the whole polytope. □

We will denote the numerator and the denominator of a rational polytope P by $\operatorname{num} P$ and $\operatorname{den} P$, respectively. For the denominator we have the following.

Lemma 31. *Let P be a rational polytope and b a positive integer. Then* $\operatorname{den} \frac{1}{b}P$ *divides* $b \operatorname{den} P$.

Proof. The denominator of P is the least integer $\operatorname{den} P$ such that $(\operatorname{den} P)P$ is an integral polytope, so $\operatorname{den} P$ divides any integer k such that kP is an integral polytope. As $(b \operatorname{den} P)\frac{1}{b}P$ is an integral polytope, $\operatorname{den} \frac{1}{b}P$ divides $b \operatorname{den} P$. □

Theorem 3. *Let P be a rational polytope and m and k multiples of its numerator and denominator, respectively. Then both $L_P(s)$ and $L_{P^\circ}(s)$ are quasipolynomials whose coefficients are step polynomials over m, $-m$ and $\frac{1}{k}$.*

Proof. Let $P \subseteq \mathbb{R}^d$; we will show the theorem by induction on d. The interpretation for $d = 0$ is that a 0-dimensional polytope is a single point, so $L_P(s) = L_{P^\circ}(s) = 1$, which satisfies our requirements.

Assume now $d > 0$. First we will reduce to the case $m = 1$.

Consider $P' = \frac{1}{m}P$. Since m is a positive multiple of $\operatorname{num} P$, we have $\operatorname{num} P' = 1$, and by Lemma 31, $\operatorname{den} P'$ divides $m \operatorname{den} P$, so (as $\operatorname{den} P$ divides k) $\operatorname{den} P'$ divides mk. Therefore, if we let $m' = 1$ and $k' = km$, we may apply the theorem for P' with m' and k' to conclude both $L_{P'}(s)$ and $L_{(P')^\circ}(s)$ contain expressions of the form $\{\pm m's\}$ and $\{\frac{s}{k'}\}$. Since $L_P(s) = L_{P'}(ms)$ (and similarly for P°), the expressions $\{\pm m's\}$ become $\{\pm ms\}$ and the expressions $\{\frac{s}{k'}\}$ become $\{\frac{s}{k}\}$.

Therefore, we have solved the problem when $m \neq 1$, so henceforth assume $m = 1$. As $\operatorname{num} P$ must divide m, we must also have $\operatorname{num} P = 1$. We will now deal with the case when P is not full-dimensional.

In this case, $P \subseteq H$, where H is the hyperplane $\{x \mid \langle a, x\rangle = b\}$ for some integral a and integer b. We know b is either 0 or 1, as we are assuming $\operatorname{num} P = 1$ (the case $b = -1$ may be reduced to the case $b = 1$ by replacing a with $-a$).

If $b = 0$, H is a vector subspace, and so there is a unimodular matrix A such that $AH = \mathbb{R}^{d-1} \times \{0\}$.[2] Then AP may be regarded a polytope in $\mathbb{R}^{d-1}$ with the same numerator and denominator as P which satisfies $L_{AP}(s) = L_P(s)$ and $L_{(AP)^\circ}(s) = L_{P^\circ}(s)$, by Lemma 30; so we may just apply induction for this case.

If $b = 1$, $L_P(s)$ will be zero whenever s is not an integer, because the hyperplane sH will not contain any integer in this case. Let $p(s) = (1 - \{s\} - \{-s\})$; then $L_P(s) = p(s)L_P(\lfloor s \rfloor)$ and $L_{P^\circ}(s) = p(s)L_{P^\circ}(\lfloor s \rfloor)$ (because if s is an integer $\lfloor s \rfloor = s$ and if s is not an integer $p(s) = 0$). Now, by the Ehrhart Theorem for rational polytopes and integer t we know $L_P(t)$ and $L_{P^\circ}(t)$ are quasipolynomials with period $\operatorname{den} P$, so we can pretend the period is actually k (which is a multiple of $\operatorname{den} P$) and use Theorem 23 to write their coefficients as step polynomials in t over $\frac{1}{k}$. Then using Lemma 24 we conclude $L_P(\lfloor s \rfloor)$ and $L_{P^\circ}(\lfloor s \rfloor)$ are quasipolinomials whose coefficients are step polynomials over $m = 1$ and $\frac{1}{k}$, so as $L_P(s) = p(s)L_P(\lfloor s \rfloor)$ we have shown the theorem in this case.

Therefore, we have solved the case when P is not full-dimensional, so assume now $m = 1$ and P is full-dimensional.

Let $\mathcal{F}'$ and $\mathcal{F}''$ be the partition of the set of all faces of P given by Proposi-

[2] Proof: H, as a rational vector subspace, has dimension $d - 1$, so the set $H \cap \mathbb{Z}^d$ spans H. Now let $a_1, \ldots, a_{d-1}$ be a lattice basis for $H \cap \mathbb{Z}^d$, and pick a_d to be any vector of the canonical basis which is not in H; then the linear transform which maps the basis $\{a_1, \ldots, a_n\}$ to the canonical basis satisfies our requirements.

tion 29. We have the following:

$$L_{P^\supset}(s) = \sum_{F \in \mathcal{F}'} L_{F^\circ}(s)$$
$$L_P(s) = L_{P^\supset}(s) + \sum_{F \in \mathcal{F}''} L_{F^\circ}(s)$$
$$L_{P^\circ}(s) = L_{P^\supset}(s) - \sum_{\substack{F \in \mathcal{F}' \\ F \neq P}} L_{F^\circ}(s)$$

For a given face F of P, the Ehrhart's and Reciprocity Theorems for rational polytopes allows us to write, for integer t, the enumerator $L_{F^\circ}(t)$ as a quasipolynomial in t; and applying Theorem 23 again the coefficients of $L_{F^\circ}(t)$ are step polynomials over $\frac{1}{k}$. Therefore $L_{P^\supset}(t)$ is also one such quasipolynomial. Since $\operatorname{num} P = 1$, we satisfy the hypothesis of Proposition 27, and thus $L_{P^\supset}(s) = L_{P^\supset}(\lfloor s \rfloor)$. Now using Lemma 24 we conclude $L_{P^\supset}(s)$ is a quasipolynomial whose coefficients are step polynomials over $m = 1$ and $\frac{1}{k}$.

Finally, all proper faces F of P are not full-dimensional, so by induction $L_{F^\circ}(s)$ also are quasipolynomials whose coefficients are step polynomials over $\pm m$ and $\frac{1}{k}$. As $L_P(s)$ and $L_{P^\circ}(s)$ can both be obtained from $L_{P^\supset}(s)$ by adding or subtracting some appropriate $L_{F^\circ}(s)$, these two enumerators themselves are of this form. □

We note this provides some information on the rate of growth of $L_P(s)$. For any convex set $P \subset \mathbb{R}^d$, we know that

$$\lim_{s \to \infty} \frac{1}{s^d} L_P(s) = \operatorname{vol} P;$$

therefore, $L_P(s) = (\operatorname{vol} P)t^d + o(t^d)$. If P is a rational polytope, the theorem allows us to improve our estimates to

$$L_P(s) = (\operatorname{vol} P)t^d + O(t^{d-1}).$$

This also provides a weak counterpart to Proposition 8; as $\operatorname{vol} P = \operatorname{vol}(P + v)$, if P and v are rational then $L_P(s) - L_{P+v}(s) = O(t^{d-1})$, so that even though these two functions are different they are not "too different".

4.1.4 Real Reciprocity theorem

Since the "components" of $L_P(s)$ and of $L_{P^\circ}(s)$ are only s, $\{\pm(\operatorname{num} P)s\}$ and $\{\frac{s}{\operatorname{den} P}\}$ and these functions are well-defined for negative s, we are ready to extend $L_P(s)$ and $L_{P^\circ}(s)$ to negative numbers. We will perform just one more sanity check before proceeding to prove a reciprocity theorem.

If $p_d(s)s^d + \cdots + p_0(s)$ is a quasipolynomial and p_d is not identically zero, we define the *degree* of this quasipolynomial to be d.

Lemma 32. *Let $p(s)$ and $q(s)$ be quasipolynomials in s of degree d whose coefficients have period k. If $p(s) = q(s)$ for all s in $[0, (d+1)k)$, then $p = q$.*

Proof. Let $p(s) = p_d(s)s^d + \cdots + p_0(s)$ and $q(s) = q_d(s)s^d + \cdots + q_0(s)$, where each p_i and q_i is a periodic function of period k; that is, $p_i(s + k) = p_i(s)$ and $q_i(s + k) = q_i(s)$ for all s.

Now, let $0 \leq s < k$ be fixed, and define for integer t the functions $\hat{p}(t) = p(s+kt)$ and $\hat{q}(t) = q(s+kt)$. By hypothesis, we have $\hat{p}(t) = \hat{q}(t)$ for all $0 \leq t \leq d$. But note that

$$\begin{aligned}\hat{p}(t) &= p(s+kt) \\ &= p_d(s+kt)(s+kt)^d + \cdots + p_0(s+kt) \\ &= p_d(s)(s+kt)^d + p_{d-1}(s)(s+kt)^{d-1} + \cdots + p_0(s),\end{aligned}$$

so $\hat{p}$ is a polynomial of degree $\leq d$; a similar reasoning shows $\hat{q}$ is also a polynomial of degree $\leq d$ with the same form. Since these two polynomials agree on $d+1$ points, they must be equal and thus have the same coefficients, which shows $p_i(s) = q_i(s)$ for all i.

Finally, since $s \in [0,k)$ was arbitrary, this means p_i agrees with q_i on $[0,k)$, and since these two functions have period k, this means $p_i = q_i$ for all i, from which the equality between p and q follows. □

Theorem 33. *Let P be any rational polytope and $L_P(s)$ and $L_{P^\circ}(s)$ their lattice point enumerators. Then if we regard $L_P(s)$ and $L_{P^\circ}(s)$ as quasipolynomials, their evaluation at negative integers yield*

$$L_P(-s) = (-1)^{\dim P} L_{P^\circ}(s)$$

for all real s.

The proof essentially follows the one by Linke [14, p. 1971].

Proof. We will use the Ehrhart-Macdonald reciprocity theorem for integer dilates.

First, let $s_0 = \frac{a}{b}$ be a rational number, with $b > 0$. For all positive s, we have $L_P(s) = L_{\frac{1}{b}P}(bs)$ and $L_{P^\circ}(s) = L_{(\frac{1}{b}P)^\circ}(bs)$, so by Lemma 32 these relations hold for all s. Then

$$\begin{aligned}L_P(-s_0) &= L_{\frac{1}{b}P}(-a) \\ &= (-1)^{\dim P} L_{(\frac{1}{b}P)^\circ}(a) \\ &= (-1)^{\dim P} L_{(P)^\circ}(s_0),\end{aligned}$$

where in the middle equality we used the Ehrhart-Macdonald reciprocity for the integer a.

This shows that the reciprocity law is valid for all rational s. Now, by theorem 3, $L_P(s)$ and $L_{P^\circ}(s)$ are quasipolynomials whose coefficients are step polynomials over a set of rational numbers; so, the coefficients (and thus the functions themselves) are continuous for every irrational number. Therefore, the validity of the reciprocity law for all real s follows by continuity. □

4.2 Linke's differential equation

As we saw, for example, with Proposition 8, looking at $L_P(s)$ for real s reveals some new behavior of this function. One of the most beautiful results of this nature is Linke's differential equation, which are satisfied by the coefficients of the quasipolynomial $L_P(s)$.

Theorem 4 (Linke, 2011[3]). *Let P be a rational polytope, and write*

$$L_P(s) = p_d(s)s^d + \cdots + p_1(s)s + p_0(s).$$

Then for every s at which all the p_i are left (resp. right) continuous, all the p_i will be left (resp. right) differentiable, and

$$p_i'(s) = -(i+1)p_{i+1}(s).$$

Proof. Let m be the numerator of P. A consequence of Theorem 3 is that if $s \in (\frac{a}{m}, \frac{a+1}{m})$ for some integer a, then all the coefficients p_i are continuous at s, and so there is a simple proof of the theorem for these s. The function $L_P(s)$ will be continuous in such an interval. As the image of $L_P(s)$ contain only integer numbers, for such a function to be continuous it must, in fact, be constant; that is, there is a number c such that

$$p_d(s)s^d + \cdots + p_1(s)r + p_0(s) = c$$

for all $s \in (\frac{a}{m}, \frac{a+1}{m})$. Now each p_i is a polynomial in this interval, so we may differentiate both sides of the above equation to get

$$p_d'(s)s^d + \Big(dp_d(s) + p_{d-1}'(s)\Big)s^{d-1} + \cdots + \Big(p_1(s) + p_0'(s)\Big) = 0.$$

Following the proof of Theorem 32, let $k = \operatorname{den} P$. Then each p_i has period k, so if we apply the above equation to all s of the form $s_0 + jk$ for some fixed $s_0 \in (\frac{a}{m}, \frac{a+1}{m})$ and all $j \in \mathbb{Z}$, the resulting polynomial in j will have infinitely many zeros, and thus its coefficients must all be zero; therefore,

$$p_i'(s_0) = -(i+1)p_{i+1}(s_0).$$

For all other cases, we will need the continuity hypothesis. Suppose all the p_i are left-continuous at s_0 (for right-continuity, the argument is the same); then the previous case guarantees that, for every sufficiently small $\varepsilon > 0$ (and all i), we have

$$p_i'(s_0 - \varepsilon) = -(i+1)p_{i+1}(s_0 - \varepsilon).$$

Since p_i is left-continuous at s (by hypothesis) and $\lim_{s \to s_0^-} p_i'(s)$ exists (by the above equation and the continuity of p_{i+1}), we know p_i is left-differentiable (and left-continuous) at s_0, and thus (by continuity) the differential equation still holds. □

As noted in the beginning of the proof, if m is the numerator of the polytope P, then (as a consequence of Theorem 3) the continuity condition is satisfied by every point which is not of the form $\frac{a}{m}$ for some integer a; therefore, the continuity condition demanded by the theorem might fail only for a countable, discrete set of points.

[3] This theorem first appeared in Linke's paper [14, p. 1973]. It claims that the differential equation is true whenever p_i is differentiable, but the proof contained in that paper does not address the cases where some p_i are continuous while the remaining are not. The statement is corrected in Linke's PhD thesis [13, p. 70]. (The theorem is stated here in a slightly different form; see discussion after the proof.)

The theorem is slightly different from Linke's [13]; specifically, $L_P(s)$ is demanded to be (one-sided) continuous in every point of the form $s_0 + jq$ for all integers $j \geq 0$, where q is the "rational denominator of P", the smallest positive rational number such that qP is an integer polytope. Applying Theorem 3 to qP and using the fact that $L_{qP}(s) = L_P(qs)$ allows us to conclude that the functions p_i have rational period q. If the condition of Theorem 4 is satisfied by some number s_0, by periodicity $L_P(s)$ will be continuous at all points of the form $s_0 + jq$. That is, the condition of Theorem 4 implies Linke's condition; the opposite implication can be shown as follows.

Denote by $p_i(s_0^-)$ the left-sided limit $\lim_{s \to s_0^-} p_i(s)$. We may rewrite the fact that $L_P(s)$ is left-continuous for every point of the form $s_0 + jq$ as

$$p_d(s_0)(s_0 + jq)^d + \cdots + p_0(s_0) = p_d(s_0^-)(s_0 + jq)^d + \cdots + p_0(s_0^-).$$

(Periodicity allowed us to replace $p_i(s_0 + jq)$ with $p_i(s_0)$ in the above formula.) Since this is a polynomial equality for integer $j \geq 0$, their coefficients must be the same; that is, $p_i(s_0) = p_i(s_0^-)$, which is precisely the continuity condition of Theorem 4.

Finally, we remark that merely assuming that $L_P(s)$ is continous at some s is not enough, because this does not guarantee the p_i will be continuous; for example, for the 3-dimensional polytope P of Section 3.2 (whose Ehrhart function was computed in (4.1)), $L_P(s)$ is continuous at 1 (in fact, $L_P(s) = 1$ for $s \in [0, 2)$), but p_2, p_1 and p_0 are discontinuous at 1.

Chapter 5

Reconstruction of polytopes

This chapter is dedicated to a reconstruction theorem. It states that, under certain conditions, the functions $L_{P+w}(s)$ identify the polytope P uniquely. We will show three versions of the theorem (Theorems 6, 9 and 10) by varying the "certain conditions".

In sections 5.2 and 5.3, the polytopes will usually be *semi-rational*; that is, in the hyperplane description

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

the a_i must be primitive integer vectors but the b_i are allowed to be arbitrary real numbers.

For full-dimensional polytopes, we will assume that n is the number of facets of P, so that the representation is minimal. In other words, each facet F_i of P may be written as

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle = b_i\}.$$

We will often use this representation in sections 5.2 and 5.3.

5.1 Motivation: Reconstructing real polytopes using real translation vectors

Recall that, in the course of proving Theorem 1, we proved Proposition 17, which says that $L_P(s)$ will not be nondecreasing if P does not contain the origin. If v is any real vector, we have $v \in P$ if and only if the polytope $P - v$ contains the origin. Together with proposition 17, we conclude that P contains v if and only if $L_{P-v}(s)$ is nondecreasing. Therefore, the set of functions $L_{P+v}(s)$ uniquely determines the polytope P. In other words, we have shown the following.

Theorem 34. *Let P and Q be two arbitrary real polytopes in $\mathbb{R}^d$. Suppose that $L_{P+v}(s) = L_{Q+v}(s)$ for all real v and all real $s > 0$. Then $P = Q$.*

If P and Q are full-dimensional, we can do slightly better by using only rational v. If $P \neq Q$, with both being full-dimensional, then there is some rational vector v which is contained in one but not in the other. Therefore, exactly one of $L_{P-v}(s)$

and $L_{Q-v}(s)$ will be nondecreasing, and so we cannot have $L_{P+v}(s) = L_{Q+v}(s)$ for all s. We thus have shown the following.

Theorem 35. *Let P and Q be two full-dimensional real polytopes in $\mathbb{R}^d$. Suppose that $L_{P+v}(s) = L_{Q+v}(s)$ for all rational v and all real $s > 0$. Then $P = Q$.*

This leads to the following question: is it possible to keep the conclusion $P = Q$ in the theorem above whilist using only integer translation vectos? This chapter is dedicated to showing that this question has a positive answer for some classes of polytopes.

5.2 Reconstruction of semi-rational polytopes

A polytope P is *semi-rational* if it can be written as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

where each a_i is an integer vector, and the b_i are arbitrary real numbers. (If we demand the b_i to be integers, too, then we recover the definition of a rational polytope.) Every real dilation and real translation of a rational polytope is a semi-rational polytope, but, for example, $P = [0, \sqrt{2}] \times [0, \sqrt{3}]$ is a semi-rational polytope which is not a translation nor a dilation of a rational polytope.

Suppose we know the directions a_i of each half-space, and also that we know $L_{P+w}(s)$ for all integer w and all real $s > 0$. This section will show how to extract each of the b_i from this information, effectively reconstructing the polytope.

Since we will need some technical lemmas, we will start discussing how to reconstruct just one specific b_i, but we will "collect" and prove each lemma where it is needed. The complete argument is the proof of Theorem 40.

5.2.1 Discontinuities of the Ehrhart function

We will extract information about the polytope P by analyzing the discontinuities of the various functions $L_{P+w}(s)$. This section discusses the meaning of these discontinuities.

Consider the polytope $P = [\frac{2}{3}, 1] \times [0, \frac{1}{3}]$ (Figure 5.1), whose Ehrhart function is

$$L_P(s) = \left(\lfloor s \rfloor - \left\lceil \frac{2}{3}s \right\rceil + 1\right)\left(\left\lfloor \frac{1}{3}s \right\rfloor + 1\right).$$

We will analyze what happens for the dilation parameters $s = 1$, $s = \frac{3}{2}$ and $s = 3$.

At $s = 1$, the polytope P is "gaining" a new integer point, namely, $(1, 0)$. This gain is marked in the Ehrhart function of P by a discontinuity: $L_P(s)$ is left-discontinuous at $s = 1$. It is a jump-discontinuity, and the magnitude of the jump is

$$L_P(1) - \lim_{s \to 1^-} L_P(s) = 1 - 0 = 1,$$

which is the number of points which P gains when reaching $s = 1$.

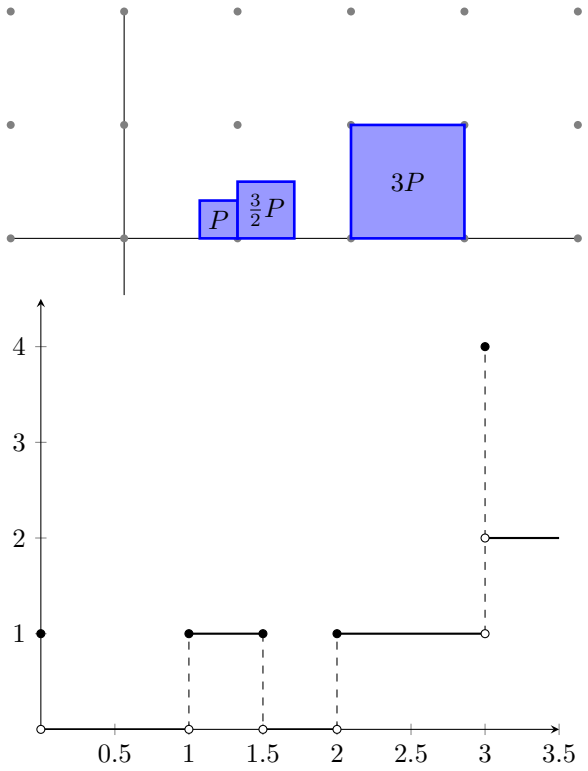


Figure 5.1: Polytope $P = [\frac{2}{3}, 1] \times [0, \frac{1}{3}]$ and its Ehrhart function.

At $s = \frac{3}{2}$, the polytope "loses" the integer point $(1, 0)$. Again this is marked in $L_P(s)$ by a discontinuity; we have a right-discontinuity at $s = \frac{3}{2}$, which is again a jump-discontinuity, and the magnitude of the jump is

$$L_P(\tfrac{3}{2}) - \lim_{s \to \frac{3}{2}^+} L_P(s) = 1 - 0 = 1,$$

again the number of points lost by P at $s = \frac{3}{2}$.

At $s = 3$, these two situations happen simultaneously. The polytope P gains the points $(2, 1)$, $(3, 1)$ and $(3, 0)$, and then immediately loses the points $(2, 1)$ and $(2, 0)$. The gain is marked by a left-discontinuity, with a jump of magnitude 3, and the loss is marked by a right-discontinuity, with a jump of magnitude 2.

Observe that these discontinuities are very regular: when gaining points, there is a left-discontinuity and the function $L_P(s)$ "jumps upwards", and when losing points, there is a right-discontinuity and the function $L_P(s)$ "jumps downwards". The magnitude of the jump is exactly the number of points gained or lost at that dilation parameter. We will now formalize how this behavior gives information about the facets of P.

Write P as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

where each a_i is a primitive integer vector, and let F_i be the ith facet of P; that is,

$$F_i = P \cap \{x \mid \langle a_i, x\rangle = b_i\}.$$

The facets F_i for which $b_i < 0$ were called *back facets* in Section 3.3. By analogy, we will call the facets F_i for which $b_i > 0$ by *front facets*. The relation between the magnitude of the discontinuities and the number of points in back and front facets is summarized by the following lemma.

Lemma 36. *Let P be a full-dimensional polytope and s_0 a discontinuity point of $L_P(s)$. If s_0 is a left-discontinuity, then the magnitude*

$$L_P(s_0) - \lim_{s \to s_0^-} L_P(s)$$

of the jump is the number of integral points contained in the front facets of s_0P. If s_0 is a right-discontinuity, then the magnitude

$$L_P(s_0) - \lim_{s \to s_0^+} L_P(s)$$

of the jump is the number of integral points contained in the back facets of s_0P.

Proof. In the hyperplane representation of P, if a point x_0 is not contained in s_0P, then it must violate at least one inequality; that is,

$$\langle a_i, x_0\rangle > s_0 b_i$$

for some i. Since this is a strict inequality, for any s sufficiently close to s_0 we also have

$$\langle a_i, x_0\rangle > s b_i,$$

and thus if $x \notin s_0P$ then $x \notin sP$ for all s sufficiently close to s_0.

This means that the difference between $L_P(s_0)$ and any of the limits

$$L_P(s_0^+) = \lim_{s \to s_0^+} L_P(s) \quad \text{and} \quad L_P(s_0^-) = \lim_{s \to s_0^-} L_P(s)$$

must be due to points $x_0 \in s_0P$.

Let x_0 be a point in s_0P. When considering the inequalities of sP for $s < s_0$, if $b_i \leq 0$ we have

$$\langle a_i, x_0\rangle \leq s_0 b_i \leq s b_i,$$

and thus all these inequalities are satisfied. Thus the only inequalities that might be violated are the ones when $b_i > 0$, which correspond to front facets.

Suppose then that x_0 is contained in the front facet of s_0P which is determined by the inequality $\langle a_i, x\rangle \leq s_0 b_i$. The point x_0 satisfies this inequality with equality; that is,

$$\langle a_i, x_0\rangle = s_0 b_i.$$

If $s < s_0$, as $b_i > 0$, we have

$$\langle a_i, x_0\rangle = s_0 b_i > s b_i,$$

which shows that $x_0 \notin sP$ for all $s < s_0$.

Conversely, if x_0 is not contained in any front facet of s_0P, it will satisfy

$$\langle a_i, x_0 \rangle < s_0 b_i$$

for all i with $b_i > 0$, and thus for all $s < s_0$ sufficiently close to s_0 the point x_0 will still satisfy the corresponding inequality for sP. Thus, $x_0 \in sP$ for all s close enough to s_0.

This means that the difference between $L_P(s_0)$ and $L_P(s_0^-)$ must be due to integer points in front facets of s_0P, and thus $L_P(s_0) - L_P(s_0^-)$ is the number of integer points in front facets of s_0P.

The analysis for $s > s_0$ is analogous. □

For example, the polytope $P = [\frac{2}{3}, 1] \times [0, \frac{1}{3}]$ (Figure 5.1) can be written as

$$\begin{aligned} P = \quad & \{(x,y) \in \mathbb{R}^2 \mid x \leq 1\} \\ & \cap \{(x,y) \in \mathbb{R}^2 \mid -x \leq \tfrac{2}{3}\} \\ & \cap \{(x,y) \in \mathbb{R}^2 \mid y \leq \tfrac{1}{3}\} \\ & \cap \{(x,y) \in \mathbb{R}^2 \mid -y \leq 0\}. \end{aligned}$$

This polytope has two front facets, namely $F_1 = \{1\} \times [0, \frac{1}{3}]$ (the right edge) and $F_3 = [\frac{2}{3}, 1] \times \{\frac{1}{3}\}$ (the upper edge), and one back facet, namely $F_2 = \{\frac{2}{3}\} \times [0, \frac{1}{3}]$ (the left edge). The bottom edge, $F_4 = [\frac{2}{3}, 1] \times \{0\}$, is contained in the x-axis, which is determined by the equation $y = 0$, and thus is neither a front facet nor a back facet.

At $s = 1$, the Ehrhart function $L_P(s)$ has a right-discontinuity, and the magnitude of the jump there is 1; this corresponds to sF_1 containing one integer point, namely, $(1, 0)$.

At $s = \frac{3}{2}$, the Ehrhart function $L_P(s)$ has a left-discontinuity, and the magnitude of the jump is also 1; this corresponds to sF_2 containing one integer point, again $(1, 0)$.

At $s = 3$, we have both a left and a right-discontinuity at $L_P(s)$. The left discontinuity has magnitude 3, which corresponds to the three points contained in $s(F_1 \cup F_3)$ (namely, $(2, 1)$, $(3, 1)$ and $(3, 0)$), and the right discontinuity has magnitude 2, which corresponds to the two points contained in sF_2 (namely, $(2, 1)$ and $(2, 0)$). Note that $(3, 1)$ is not counted twice, despite appearing in both F_1 and F_3, whereas $(2, 1)$ is counted both as an "entering point" (because it is contained in the front facet F_3) and as a "leaving point" (because it is contained in the back facet F_2).

5.2.2 Relative volumes of facets of a polytope

Let P be a full-dimensional polytope. In the proof of Lemma 22 and of Theorem 8, we used the fact that

$$\lim_{s \to \infty} \frac{L_P(s)}{s^d} = \operatorname{vol} P.$$

This may be shown by noting that

$$\begin{aligned}\frac{L_P(s)}{s^d} &= \frac{1}{s^d}\#\left(P \cap \frac{1}{s}\mathbb{Z}^d\right) \\ &= \sum_{x \in \frac{1}{s}\mathbb{Z}^d} \frac{1}{s^d}[x \in P].\end{aligned}$$

The last sum is, in fact, a Riemann sum for the indicator function of P, and the fact that P is Jordan-measurable guarantees that such a sum approaches $\operatorname{vol} P$ by letting $s \to \infty$.

We face problems when extending this notion to polytopes which are not full-dimensional. For example, consider the polytopes $F = \{1\} \times [0,1]$ and $F' = \operatorname{conv}\{(1,0),(0,1)\}$ (Figure 5.2). If s is an integer, we have $L_F(s) = L_{F'}(s) = s+1$, and $L_F(s) = L_{F'}(s) = 0$ otherwise. Therefore, the analogous limits

$$\lim_{s\to\infty} \frac{L_F(s)}{s} \quad \text{and} \quad \lim_{s\to\infty} \frac{L_{F'}(s)}{s}$$

do not exist.

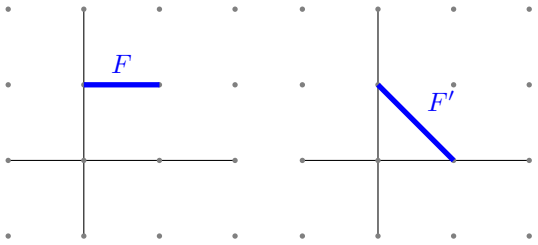


Figure 5.2: Two one-dimensional polytopes in R^2.

This problem may be solved by limiting the domain over which we take the limit. In these examples, we would have something like

$$\lim_{\substack{s\to\infty \\ s\in\mathbb{Z}}} \frac{L_F(s)}{s} = \lim_{\substack{s\to\infty \\ s\in\mathbb{Z}}} \frac{L_{F'}(s)}{s} = 1.$$

As expected, we do not get the lengths of F or F', but their "relative lengths". We will define the *relative volume* of a semi-rational polytope as follows.

If P is an l-dimensional semi-rational polytope contained in $\mathbb{R}^l \times \{(0,\dots,0)\}$, let P' be its projection to $\mathbb{R}^l$. The polytope P' will be a full-dimensional polytope, and thus we define the relative volume $\operatorname{vol}_r P$ to be $\operatorname{vol} P$.

If P is a l-dimensional semi-rational polytope in $\mathbb{R}^d$ such that the affine span $\operatorname{aff} P$ contains the origin, then $\operatorname{aff} P$ is a vector space, and since P is semi-rational, $\operatorname{aff} P$ is, in fact, a rational vector space (that is, H is generated by integer vectors). Let A be any unimodular transform on $\mathbb{R}^d$ which maps $\operatorname{aff} P$ to $\mathbb{R}^k \times \{(0,\dots,0)\}$. The relative volume of P is then defined to be $\operatorname{vol}_r AP$.

Finally, if P is an arbitrary semi-rational polytope, let $v \in \operatorname{aff} P$ be any vector, and define the relative volume of P to be $\operatorname{vol}_r(P - v)$.

We leave to the reader showing that this definition does not depend on the choices of A or v. This is an extension of the definition found in [4, chapter 5.4] to semi-rational polytopes.

We then have the following.

Lemma 37. *Let $P \subseteq \mathbb{R}^d$ be a semi-rational polytope. For each vector $v \in \mathbb{R}^d$, let $E_v \subseteq \mathbb{R}$ be the set of all s such that* aff $s(P+v)$ *contains integer points. Then whenever E_v is unbounded we have*

$$\lim_{\substack{s\to\infty \\ s\in E_v}} \frac{L_{F+v}(s)}{s^{\dim P}} = \operatorname{vol}_{\mathrm{r}} F,$$

and the limit is uniform in v.

A more precise (though less clear) way of expressing the above limit is: for every $\varepsilon > 0$, there is a $N > 0$ such that, for all vectors v and all $s > N$, if the affine span of $s(P+v)$ contains integer points, then

$$\left| \operatorname{vol}_{\mathrm{r}} F - \frac{L_{F+v}(s)}{s^{\dim P}} \right| < \varepsilon.$$

The uniformity in v will be important later.

Proof. If P is full dimensional, then

$$\begin{aligned} \frac{L_{P+v}(s)}{s^d} &= \frac{1}{s^d} \# \left((P+v) \cap \frac{1}{s}\mathbb{Z}^d \right) \\ &= \sum_{x \in \frac{1}{s}\mathbb{Z}^d} \frac{1}{s^d} [x + v \in P], \end{aligned}$$

which is a Riemann sum for the indicator function $\mathbb{1}_P$ of P. Since P is Jordan-measurable, any such sum may be made close to $\operatorname{vol} P$ just by making $\frac{1}{s}$ small, regardless of the choice of v. Thus

$$\lim_{s\to\infty} \frac{L_{P+v}(s)}{s^d} = \operatorname{vol} P = \operatorname{vol}_{\mathrm{r}} P,$$

and the limit is uniform in v.

Next, assume that $P \subseteq \mathbb{R}^d$ is l-dimensional, that aff P contains the origin, and that $v \in$ aff P. Let A be any unimodular transform which maps aff P to $\mathbb{R}^l \times \{(0, \ldots, 0)\}$, and let P' and v' be the projections of AP and Av to $\mathbb{R}^l$, respectively. Then $L_{P+v}(s) = L_{P'+v'}(s)$, so this case reduces to the previous.

Finally, let P be an arbitrary semi-rational polytope and v and arbitrary vector. Choose $v_0 \in$ aff P and define $P' = P - v_0$. Note that aff P' is the translation of aff P which passes through the origin.

Let $s \in E_v$ be fixed; that is, there exists an integer vector w in aff $s(P+v)$. Then $\frac{1}{s}w - v$ is contained in aff P, so if we let $u = \frac{1}{s}w - v - v_0$ we have

$$\begin{aligned} L_{P+v}(s) &= L_{P+v-\frac{1}{s}w}(s) \\ &= L_{P'-u}(s). \end{aligned}$$

Since $u \in$ aff P', this case follows from the previous. □

We are most interested in the case when the polytope has codimension 1, because this is the case of facets of full-dimensional polytopes (and Lemma 36

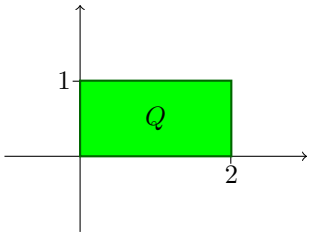


Figure 5.3: Rectangle $[0,2] \times [0,1]$.

already hinted that this case is important). Let F be a $(d-1)$-dimensional polytope in $\mathbb{R}^d$ and suppose F is contained in the hyperplane

$$H = \{x \in \mathbb{R}^d \mid \langle a, x\rangle = b\},$$

where a is a nonnegative integer vector and $b \in \mathbb{R}$ is arbitrary. We may assume a is a "primitive vector"; that is, there is no integer $k > 1$ such that $\frac{1}{k}a$ is integral, or, equivalently, the greatest common divisor of all entries of a is 1. As a consequence, the set of all possible values for $\langle a, x\rangle$, for integer x, is the set of all integers; that is,

$$\{\langle a, x\rangle \mid x \in \mathbb{Z}^d\} = \mathbb{Z}.$$

Therefore the hyperplane $s(H + v)$ has integer points if and only if $s(b + \langle a, v\rangle)$ is an integer. Thus, in this case, Lemma 37 reads

$$\lim_{\substack{s\to\infty \\ s(b+\langle a,v\rangle)\in\mathbb{Z}}} \frac{L_{F+v}(s)}{s^{d-1}} = \operatorname{vol}_{\mathrm{r}} F.$$

5.2.3 An example: reconstructing a rectangle

Let P be the polytope $[0,2] \times [0,1]$ (Figure 5.3). The facets of this polytope have normal vectors $a_1 = (1,0), a_2 = (0,1), a_3 = (-1,0), a_4 = (0,-1)$. For a given translation vector (m,l), its Ehrhart function is

$$L_{P+(m,l)}(s) = (\lfloor s(m+2)\rfloor - \lceil sm\rceil + 1)(\lfloor s(l+1)\rfloor - \lceil sl\rceil + 1).$$

In this section, we will show how to reconstruct the polytope P knowing only $a_1, \ldots, a_4$ and $L_{P+(m,l)}(s)$ for all integer m, l and all real $s > 0$.

Let F_1, F_2, F_3 and F_4 be the facets of P associated with a_1, a_2, a_3 and a_4, respectively (so that, for example, $F_1 = P \cap \{(x,y) \mid x = 2\}$). First, we will gather information about the facet F_1.

Let us define a list of vectors w_k by $w_k = ka_1 = (k,0)$. We will extract data about F_1 by analyzing the discontinuities of the functions $L_{P+w_k}(s)$.

We know that there exist some real numbers b_1, b_2, b_3, b_4 such that the points (x,y) in the polytope are bounded by the linear inequalities

$$\begin{aligned}
\langle a_1, (x,y)\rangle &\le b_1 \\
\langle a_2, (x,y)\rangle &\le b_2 \\
\langle a_3, (x,y)\rangle &\le b_3 \\
\langle a_4, (x,y)\rangle &\le b_4,
\end{aligned}$$

which translates to

$$\begin{aligned} x &\leq b_1 \\ y &\leq b_2 \\ -x &\leq b_3 \\ -y &\leq b_4. \end{aligned}$$

In the polytope $s(P + w_k)$, these inequalities become

$$\begin{aligned} x &\leq s(b_1 + k) \\ y &\leq sb_2 \\ -x &\leq s(b_3 - k) \\ -y &\leq sb_4. \end{aligned}$$

We know from theorem 36 that all discontinuities of $L_{P+w_k}(s)$ are caused by points passing through the facets of $P + w_k$. Moreover, the left-discontinuities are caused exclusively by points passing through front facets. We know that, for k large enough (larger than b_3), the right-hand side of the inequality defining $F_3 + w_k$ (which is $b_3 - k$) will be negative, and thus $F_3 + w_k$ will be a back facet of $P + w_k$. Therefore, if we analyze only the left-discontinuities of $L_{P+w_k}(s)$, we will eventually get data regarding only F_1, F_2 and F_4; that is, we eliminated the interference of F_3 in our analysis.

Observe that we do not know whether F_2 and F_4 are front facets or not, so the data we get may or may not include information about these facets. But since we are trying to get data about F_1, and for large enough k the facet $F_1 + w_k$ will be a front facet, this will not be a problem.

The function $L_{P+w_k}(s)$ is

$$L_{P+w_k}(s) = (\lfloor s(k+2) \rfloor - \lceil sk \rceil + 1)(\lfloor s \rfloor + 1).$$

It has a left-discontinuity whenever s is of the form $\frac{n}{k+2}$ for some integer n. If s itself is an integer, the jump in the discontinuity has size $3s+1$ (that is, $L_{P+w_k}(s) - L_{P+w_k}(s^-) = 3s + 1$). Otherwise, if s is not an integer, the jump has size $\lfloor s \rfloor + 1$.

Back to the linear inequalities. Consider the function $L_{F_1+w_k}(s)$. According to Lemma 37, we have

$$\lim_{\substack{s \to \infty \\ s(b_1+k) \in \mathbb{Z}}} \frac{L_{F_1+w_k}(s)}{s} = \operatorname{vol}_{\mathrm{r}} F_1.$$

A direct consequence of this is that, if $\operatorname{vol}_{\mathrm{r}} F_1 > 0$ (that is, F_1 is not a lower-dimensional face), the function $L_{F_1+w_k}(s)$ will eventually be positive for all large enough s with the form $\frac{n}{b_1+k}$. This means that the distance between any two consecutive discontinuities caused by F_1 in $P + w_k$ (which is $\frac{1}{b_1+k}$) should get smaller as k increases; that is, the discontinuities caused by F_1 get closer as k increases.

If we repeat the analysis for F_2 and F_4, we learn that these facets cause discontinuities for s of the form $\frac{n}{b_2}$ and $\frac{n}{b_4}$. Thus, these discontinuities do not get closer for large k.

Analyzing $L_{P+w_k}(s)$, we have found two types of left-discontinuities: whenever s is an integer, the jump has size $3s + 1$, and whenever s is of the form $\frac{n}{k+2}$, but

is not an integer, the jump has size $\lfloor s \rfloor + 1$. Observe that only this second class of inequalities get closer together, and thus cannot be caused by the stationary F_2 and F_4; therefore, these discontinuities are caused by F_1.

(More precisely: the left-discontinuities caused by F_2 and F_4 must happen in integer multiples of $\frac{1}{b_2}$ and $\frac{1}{b_4}$. Simply by taking k large enough, we will find some multiples of $\frac{1}{k+2}$ which are not multiples of either $\frac{1}{b_2}$ nor $\frac{1}{b_4}$, and thus these discontinuities must be caused by F_1.)

Finally, since $F_1 + w_k$ causes discontinuities of the form $\frac{n}{b_1+k}$ and the discontinuities we observe in $L_{P+w_k}(s)$ are of the form $\frac{n}{2+k}$, we conclude that $b_1 = 2$. Therefore, we know precisely where the supporting hyperplane of F_1 lies.

Observe we can also recover the relative volumee of F_1: since the discontinuities caused solely by F_1 have size $\lfloor s \rfloor + 1$, Lemma 37 says that $\operatorname{vol}_{\mathrm{r}} F_1 = 1$.

Repeating this analysis for F_2, F_3 and F_4 gives us the values of b_2, b_3 and b_4, thus reconstructing the whole polytope.

Dealing with extraneous information

In the example, we assumed that all facets $F_1, \ldots, F_4$ were actual facets and not degenerate faces. What if were told that the facet normals included the vector $a_5 = (-1, -1)$?

When gathering information for F_1 and F_2, the "facet" F_5 would also eventually become a back facet, so the same argument as before is valid. However, this extra facet messes up the analysis for F_3 and F_4. For example, if we define $w_k = (-k, 0)$ (when trying to extract information about F_3), the supporting hyperplane of F_5 is

$$\{(x, y) \in \mathbb{R}^2 \mid -x - y = -k + b_5\},$$

so the discontinuities caused by F_5 come closer together at the same rate as the discontinuities caused by F_3, and thus we cannot properly separate them.

But we can make progress if we analyze F_5 first. As before, let $w_k = ka_5 = (-k, -k)$. Here, the inequality corresponding to $F_5 + w_k$ is

$$-x - y \leq 2k + b_5,$$

so we get discontinuities for s of the form $\frac{n}{2k+b_5}$. However, the function $L_{P+w_k}(s)$ is

$$L_{P+w_k}(s) = (\lfloor sk \rfloor - \lceil s(k-2) \rceil + 1)(\lfloor sk \rfloor - \lceil s(k-1) \rceil + 1),$$

and this function only has left-discontinuities for s of the form $\frac{n}{k}$. That is, we expect that the spacing between consecutive discontinuities approaches $\frac{1}{2k}$ for large k, but we only get a spacing of $\frac{1}{k}$. This contradicts Lemma 37, unless $\operatorname{vol}_{\mathrm{r}} F_5 = 0$. But this means that F_5 is a degenerate facet; this allows us to conclude that a_5 is not the direction of any facet of P.

So, the plan for showing Theorem 6 goes like this: given two polytopes P and Q and the functions $L_{P+w}(s)$ and $L_{Q+w}(s)$ for all integer w, we will first write P and Q over the same set of facet normals $a_1, \ldots, a_n$, even if some of the represented facets are degenerate; then we will go through the procedure outlined above in order to extract the right-hand sides $b_1, \ldots, b_n$ of the linear inequalities. (Here, the ability of pruning out extraneous vectors, like a_5 in the example, allows us to not worry about the degenerat facets.) This information uniquely determines P and Q, so if $L_{P+w}(s) = L_{Q+w}(s)$, we will have $P = Q$.

The hard part of extracting the $b_1, \ldots, b_n$ will be isolating the interference of other facets when analyzing a specific facet. In Section 5.2.4 we will prove a technical lemma which will allow us to do this isolation, and in Section 5.2.5 we will prove another technical lemma which will give us the right-hand sides b_i using the (properly isolated) information given by the previous step.

5.2.4 Isolating the facet with the largest vector

Again, write P as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

where each a_i is a primitive integer vector.

A consequence of Lemma 36 is that all discontinuities of $L_P(s)$ are caused by integer points passing through facets of P. We will focus now on the left-discontinuities, which are caused by integer points passing through front facets of P.

Let F_i be the ith facet; that is,

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle = b_i\}.$$

If $b_i > 0$, so that F_i is a front facet, then F_i is "eligible" for causing left-discontinuities on P. Such discontinuities will only be caused by F_i if sb_i is an integer; moreover, for small values of s, it might happen that sF_i is too small to contain integer points. However, as long as F_i is not a "degenerate facet" (that is, F_i has codimension 1), its relative volume will be positive; thus Lemma 37 guarantees that, for all large enough s, the polytope sF_i will contain integer points whenever sb_i is an integer.

Therefore, the discontinuities of the function $L_P(s)$ give some clues about b_i; that is, s may only be a left-discontinuity point if sb_i is an integer for some $b_i > 0$, and eventually all such s are left-discontinuity points. The problem is that these discontinuities give clues for all b_i at once, so we need a way of isolating such clues for each b_i.

We will look at the discontinuities of $L_{P+w}(s)$, for a certain infinite collection of integer w. If we choose $w_k = ka_1$, for example, then the left-discontinuities of $L_{P+w_k}(s)$ occur only when $s(b_i + k\langle a_i, a_1 \rangle)$ is an integer. For larger k, the spacing between discontinuity points of $L_{P+w_k}(s)$ decreases. For now, assume that a_1 has the largest norm among all a_i; then the factor $\langle a_1, a_i \rangle$ will be largest for $i = 1$, and thus (for all arbitrarily large k) the discontinuities coming from the facet $F_1 + w_k$ will be the closest among all facets of $P + w_k$.

However, the fact these discontinuities are interleaved (or even overlapping) is what makes things difficult. We will use the following technical lemma; it essentially provides us with a "window" $(\alpha_k, \alpha_k + \epsilon_k)$ where we can, at least infinitely often, be sure only the discontinuities stemming from a_1 appear.

Lemma 38. *Let $a_1, \ldots, a_n$ be primitive integer vectors in $\mathbb{R}^d$, with $\|a_1\| \geq \|a_i\|$ for all i. Then there is an integer vector w_0 and a sequence $(\alpha_k, \alpha_k + \epsilon_k)$ of intervals such that, for all possible choice of real numbers $b_1, \ldots, b_n$, the following properties are true:*

1. $\langle a_i, w_0 \rangle \neq 0$ *for all* i*;*
2. $\langle a_1, w_0 \rangle > 0$*;*
3. $\alpha_k > k$ *for all* k*;*
4. $\lim_{k\to\infty} |\alpha_k - k| = 0$*;*
5. $\lim_{k\to\infty} \epsilon_k = 0$*;*
6. *For all sufficiently large* k*, there is either one or two distinct values of* s *in* $(\alpha_k, \alpha_k + \epsilon_k)$ *such that*
$$s(b_1 + k\langle a_1, w_0 \rangle)$$
is an integer; and
7. *There exists infinitely many* k *such that, for all* $i \geq 2$ *such that* $\langle a_i, w_0 \rangle > 0$*, there is no* $s \in (\alpha_k, \alpha_k + \epsilon_k)$ *such that*
$$s(b_i + k\langle a_i, w_0 \rangle)$$
is an integer.

Before proving the lemma, let us see what these properties mean, intuitively.

Properties 3, 4 and 5 says that the numbers $s \in (\alpha_k, \alpha_k + \epsilon_k)$ are of the form $k + \delta$, where δ is a positive value which approaches zero for large k. This will guarantee the hypothesis of Lemma 39.

Define $w_k = kw_0$, so that the interval $(\alpha_k, \alpha_k + \epsilon_k)$ is an "interesting interval" of discontinuities in $L_{P+w_k}(s)$. We are assuming we know the vectors a_i, but not the right-hand sides b_i. Property 1 guarantees that, for all sufficiently large k, the right-hand sides $b_i + \langle a_i, w_k \rangle$ will have the sign of $\langle a_i, w_0 \rangle$, so we know that all left-discontinuities of $L_{P+w_k}(s)$ are caused by the a_i for which $\langle a_i, w_0 \rangle > 0$. Property 2 says that a_1 is one of these vectors which causes the left-discontinuity.

Define V_k to be the sum of the magnitudes of all left-discontinuities of $L_{P+w_k}(s)$ which happen in the interval $(\alpha_k, \alpha_k+\epsilon_k)$. Property 6 says that, for all large enough k, at least one of these discontinuities is caused by F_1; Lemma 37 and the fact that the values in $(\alpha_k, \alpha_k + \epsilon_k)$ are approximately k says that this discontinuity has magnitude of approximately $k^{d-1} \operatorname{vol}_{\mathrm{r}} F_1$. (Here we use the uniformity in w claimed by that lemma.)

Intuitively, each V_k equals $k^{d-1} \operatorname{vol}_{\mathrm{r}} F_1$ plus some positive garbage. Properties 6 and 7 allows us to handle this garbage.

We may categorize the V_k in three cases: the *good* case, where $L_{P+w_k}(s)$ has just a single discontinuity in $(\alpha_k, \alpha_k + \epsilon_k)$; the *not-so-good* case, where there is two discontinuities of about the same magnitude, and the *bad* case, which is the remaining cases. Property 6 says that, in the good and the not-so-good case, V_k is approximately $k^{d-1} \operatorname{vol}_{\mathrm{r}} F_1$ and $2k^{d-1} \operatorname{vol}_{\mathrm{r}} F_1$, respectively, and Property 7 says that either the good or the not-so-good case happen infinitely often.

Therefore, at least one of the following limits is true (that is, exists and equals the expression in the right-hand side):

$$\lim_{\substack{k\to\infty \\ V_k \text{ good}}} \frac{V_k}{k^{d-1}} = \operatorname{vol}_{\mathrm{r}} F_1 \qquad \text{or} \qquad \lim_{\substack{k\to\infty \\ V_k \text{ not-so-good}}} \frac{V_k}{k^{d-1}} = 2 \operatorname{vol}_{\mathrm{r}} F_1.$$

Therefore, if we know $a_1, \ldots, a_n$ and $L_{P+w}(s)$ for all integer w, then we can determine $\mathrm{vol}_{\mathrm{r}} F_1$. Later, we will see how to do some sort of induction to get the values of $\mathrm{vol}_{\mathrm{r}} F_i$ for the remaining i, too; this is why Lemma 38 was stated directly in terms of the vectors a_i, without referring to the polytope.

Proof of Lemma 38. First, choose an integral vector $w' \in \{a_1\}^\perp$ which is not orthogonal to any of the vectors a_i, for $a_i \neq \pm a_1$ (such a w' exist because the intersections $\{a_1\}^\perp \cap \{a_i\}^\perp$, where the "forbidden" w' falls, have codimension 2, and thus their union are a proper subset of $\{a_1\}^\perp$).

Since

$$\langle a_1, a_i \rangle < \|a_1\| \, \|a_i\| \leq \|a_1\|^2 ,$$

for all large enough $\tau > 0$ we have

$$\tau \|a_1\|^2 > \langle a_i, w' + \tau a_1 \rangle.$$

So, choose $\tau > 0$ to be an integer so large that the above equation is satisfied, and also that

$$\langle a_i, w' + \tau a_1 \rangle \neq 0$$

for all i. (If $\langle a_i, a_1 \rangle = 0$, then any τ will do, due to the choice of w'; otherwise, we may just make τ large, because the other terms in the expression are constant.)

Define $w_0 = \tau a_1 + w'$. This definition of w_0 satisfies conditions 1 and 2.

Define $\epsilon_k = \frac{1}{k}\epsilon_0$, where ϵ_0 is a value (to be determined later) which satisfies

$$\frac{1}{\langle a_1, w_0 \rangle} < \epsilon_0 < \frac{2}{\langle a_1, w_0 \rangle}. \tag{5.1}$$

This suffice to get property 6: note that $s(b_1 + k\langle a_1, w_0 \rangle)$ is an integer if and only if $s = \frac{m}{b_1 + k\langle a_1, w_0 \rangle}$ for some integer m. Therefore, any open interval in $\mathbb{R}$ whose length is larger than $\frac{1}{b_1 + k\langle a_1, w_0 \rangle}$ is guaranteed to contain at least one of these. The first inequality guarantees that

$$\frac{1}{b_1 + k\langle a_1, w_0 \rangle} < \frac{\epsilon_0}{k} = \epsilon_k$$

for all large enough k. Since $(\alpha_k, \alpha_k + \epsilon_k)$ has lenght ϵ_k, this guarantees that, for all large enough k, at least one s in this interval satisfies $s(b_1 + k\langle a_1, w_0 \rangle) \in \mathbb{Z}$.

Now, any open interval which contains three distinct numbers s of the form $\frac{n}{b_1 + k\langle a_1, w_0 \rangle}$, for integer n, must have length larger than $\frac{2}{b_1 + k\langle a_1, w_0 \rangle}$. Here, the second inequality in (5.1) guarantees that

$$\epsilon_k = \frac{\epsilon_0}{k} < \frac{2}{b_1 + k\langle a_1, w_0 \rangle}$$

for all large enough k. This shows that, once we define ϵ_0 properly (satisfying inequality (5.1)), we satisfy both properties 6 and 5.

Property 7 will be the hardest. We will define α_k to be a value which is a bit greater that k, so that the values of the interval $(\alpha_k, \alpha_k + \epsilon_k)$ are of the form $k + \delta$, where δ is "small, but not too small". The value δ will lie in $(\alpha_k - k, \alpha_k - k + \epsilon_k)$. We will make $\alpha_k - k + \epsilon_k$ close to 0, so that δ will be small, but we will make sure $\alpha_k - k$ stays some "safe distance" from 0, so that δ is not "too small".

We want to control when $s(b_i + k\langle a_i, w_0\rangle)$ is an integer. If $s = k + \delta$, this number is

$$(k+\delta)(b_i + k\langle a_i, w_0\rangle) = k^2\langle a_i, w_0\rangle + \delta b_i + kb_i + \delta k\langle a_i, w_0\rangle.$$

If we can guarantee that this value is distant from an integer for all $i > 2$, we get property 7.

The first term of the above expression, $k^2\langle a_i, w_0\rangle$, will always bee an integer, so we have nothing to do.

We will choose α_k and ϵ_k so that $\alpha_k - k$ is proportional to $\frac{1}{k}$. As $\epsilon_k = \frac{\epsilon_0}{k}$ is also proportional to $\frac{1}{k}$, and δ is "sandwiched" between these two values, the value of δ will be proportional to $\frac{1}{k}$, too. This means that the second term, δb_i, will tend to zero for large k.

The third term, kb_i, will be dealt with in an indirect way. By the "simultaneous Dirichlet's approximation theorem", for each N there is a $k \in \{1, \ldots, N^n\}$ such that all numbers kb_i are within $\frac{1}{N}$ of an integer. By choosing larger and larger N, we guarantee the existence of arbitrarily large k where all the distance of kb_i to the nearest integer is made arbitrarily small. (This indirect attack to kb_i is the responsible for the phrase "there exist infinitely many k" in the condition 7, as opposed to something like "for all large enough k".)

So, the difficulties rests upon the fourth term, $\delta k\langle a_i, w_0\rangle$. We want to place it in the interval $(\varepsilon, 1-\varepsilon)$ for some $\varepsilon > 0$, so that this term is always at least within ε of the nearest integer. Since for the other three terms the distance to the nearest integer gets arbitrarily small, but this fourth term stays distant, we can guarantee that $(k+\delta)(\langle a_i, w_0\rangle k + b_i)$ is not an integer.

We will determine a suitable $\varepsilon > 0$ later. Let $\varepsilon' > 0$ be such that, for $i \geq 2$, we have $\langle a_i, w_0\rangle > \varepsilon'$ whenever $\langle a_i, w_0\rangle > 0$, and $\langle a_i, w_0\rangle < \tau \|a_1\|^2 - \varepsilon'$ for all $i \geq 2$.

Define

$$\alpha_k = k + \frac{1}{k}\frac{\varepsilon}{\varepsilon'}.$$

Observe that this definition of α_k clearly satisfies conditions 3 and 4. We have $\delta > \frac{1}{k}\frac{\varepsilon}{\varepsilon'}$, and thus

$$\delta k\langle a_i, w_0\rangle > \delta k\varepsilon' > \varepsilon.$$

Define

$$\epsilon_0 = \frac{1-\varepsilon}{t\|a_1\|^2 - \varepsilon'} - \frac{\varepsilon}{\varepsilon'}.$$

Then since $\epsilon_k = \frac{\epsilon_0}{k}$, we get

$$\delta < \alpha_k - k + \epsilon_k = \frac{1}{k}\frac{1-\varepsilon}{t\|a_1\|^2 - \varepsilon'},$$

and thus

$$\delta k\langle a_i, w_0\rangle < \delta k(t\|a_1\|^2 - \varepsilon') < 1 - \varepsilon.$$

This show that, regardless of the value of $\varepsilon > 0$, the definitions of α_k and ϵ_k guarantee that, if $s = k + \delta \in (\alpha_k, \alpha_k + \epsilon_k)$, then $\delta k\langle a_i, w_0\rangle \in (\varepsilon, 1-\varepsilon)$. The other terms in $s(b_i + k\langle a_i, w_0\rangle)$ will approximate integer values, thus showing property 7.

Now we will choose $\varepsilon > 0$ so that the definition of ϵ_0 satisfy inequality (5.1).

The inequality $\frac{1}{\langle a_1, w_0\rangle} < \epsilon_0$ can be rewritten as follows:

$$\begin{aligned} \epsilon_0 &> \frac{1}{\langle a_1, w_0\rangle} \\ \frac{1-\varepsilon}{\tau\|a_1\|^2 - \varepsilon'} - \frac{\varepsilon}{\varepsilon'} &> \frac{1}{\tau\|a_1\|^2} \\ \frac{1}{\tau\|a_1\|^2 - \varepsilon'} &> \frac{1}{\tau\|a_1\|^2} + \varepsilon\left(\frac{1}{\varepsilon'} + \frac{1}{\tau\|a_1\|^2 - \varepsilon'}\right). \end{aligned}$$

Analogously, the inequality $\epsilon_0 < \frac{2}{\langle a_1, w_0\rangle}$ can be rewritten as

$$\frac{1}{\tau\|a_1\|^2 - \varepsilon'} < \frac{2}{\tau\|a_1\|^2} + \varepsilon\left(\frac{1}{\varepsilon'} + \frac{1}{\tau\|a_1\|^2 - \varepsilon'}\right).$$

As $\varepsilon' > 0$ is a small value, it is clear that

$$\frac{1}{\tau\|a_1\|^2} < \frac{1}{\tau\|a_1\|^2 - \varepsilon'} < \frac{2}{\tau\|a_1\|^2},$$

so an $\varepsilon > 0$ satisfying both inequalities above does exist. This guarantees condition 6, finishing the proof of the lemma. □

5.2.5 Pseudo-Diophantine equations

We will now show how to recover b_1. From the discussion preceding the proof of Lemma 38, we have a sequence of values V_k from which we extract $\mathrm{vol_r}\, F_1$. The V_k represent the values of some discontinuities of $L_{P+w_k}(s)$ which we know are due to points passing through F_1. We are interested in these discontinuities.

For simplicity, we will assume that there are infinitely many good V_k. For all large enough k for which V_k is good, there is precisely one real number s_k in the interval $(\alpha_k, \alpha_k + \epsilon_k)$ which corresponds to a discontinuity of $L_{P+w_k}(s)$, and this discontinuity was caused by F_1. That is, we have infinitely many equations of the following form: there is some integer m_k such that

$$s_k(b_1 + k\langle a_1, w_0\rangle) = m_k.$$

The following lemma asserts that there is exactly one solution for b_1 of this infinite set of "semi-Diophantine equations".

Lemma 39. *Let $s_l \in \mathbb{R}$, $k_l \in \mathbb{Z}$ be given for each integer $l > 0$, where the s_l are non-integer numbers such that $\{s_l\}$ approaches zero for $l \to \infty$. Then the infinite system of equations*

$$s_l(b + k_l) = m_l, \qquad l > 0$$

for $b \in \mathbb{R}$ and $m_l \in \mathbb{Z}$, has at most one solution.

Proof. Without loss of generality, we may assume all s_l and all k_l are different. Let $(b, m_1, m_2, m_3, \dots)$ be a solution for this system of equations. If we did not have the integrality constraint on m_l, then all the solutions of this infinite system of equations would have the form

$$(b + \lambda, m_1 + s_1\lambda, m_2 + s_2\lambda, \dots), \qquad \lambda \in \mathbb{R}.$$

The integrality constraint dictates that $m_l + s_l\lambda$ is an integer, say m_l'; thus for some integer $\nu_l = m_l' - m_l$ we have $s_l\lambda = \nu_l$.

Assume b is irrational; then all s_l are also irrational. Since

$$\lambda = \frac{\nu_1}{s_1} = \frac{\nu_2}{s_2},$$

so we know that $\frac{s_1}{s_2} = \frac{\nu_1}{\nu_2}$ is a rational number. Since $b = \frac{m_1}{s_1} - k_1 = \frac{m_2}{s_2} - k_2$, we have

$$\begin{aligned} k_2 - k_1 &= \frac{m_1}{s_1} - \frac{m_2}{s_2} \\ s_1(k_2 - k_1) &= m_1 - \frac{s_1}{s_2} m_2. \end{aligned}$$

Since $k_1 \neq k_2$, the above equation shows that s_1 is rational; this is a contradiction, unless $\nu_2 = 0$, which amounts to $\lambda = 0$. Therefore, if b is irrational, we indeed have at most one solution.

Assume now that b is rational. Therefore, all s_l are rational, so we may write $s_l = \frac{p_l}{q_l}$ for relatively prime p_l, q_l.

For $m_l + s_l\lambda$ to be an integer, λ must be a rational number, say, $\lambda = \frac{p}{q}$. The number $s_l\lambda$ must also be an integer, say r; that is,

$$p_l p = q_l q r.$$

Reducing both sides modulo q_l gives

$$p_l p \equiv 0 \mod q_l;$$

as p_l and q_l are relatively prime, this shows that q_l divides p.

Finally, since we assumed that no s_l is an integer, but the distance of s_l to the nearest integer approaches zero as $l \to \infty$, we must have $\lim_{l\to\infty} q_l = \infty$. So p is a multiple of arbitrarily large numbers, thus the only possibility is $p = 0$, which implies $\lambda = 0$, from which the lemma follows. □

The fact that each s_k is contained in $(\alpha_k, \alpha_k + \epsilon_k)$, together with properties 3, 4 and 5 from Lemma 38, guarantees that the fractional part $\{s_k\}$ of s_k, although never zero, approaches zero as $k \to \infty$. Therefore, we are in position to apply the lemma, which thus determines b_1 uniquely.

5.2.6 Piecing together the semi-rational case

Throughout the last sections, we argued how we could obtain b_1 and $\mathrm{vol_r}\, F_1$ if we knew $a_1, \ldots, a_n$ and $L_{P+w}(s)$ for all integer w and all real $s > 0$. During this discussion, we collected some lemmas, which we now will use to show how to obtain the remaining b_i.

Theorem 40. *Let $a_1, \ldots, a_n \in \mathbb{R}^d$ be primitive integer vectors and for each integer w let $f_w(s)$ be a function on $\mathbb{R}$. Then there is at most one set of numbers $b_1, \ldots, b_n$ such that*

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}$$

is a full-dimensional semi-rational polytope, that $f_w(s) = L_{P+w}(s)$ *for all* $s > 0$ *and all integer* w*, and that the polytopes* F_i *defined by*

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle = b_i\}$$

are faces of P*.*

Observe that here we are not assuming that n is the number of facets of P; in particular, every facet of P will be an F_i for some i, but some of the F_i might be lower-dimensional faces of P. For example, the facet F_5 of the example in Section 5.2.3 is a lower-dimensional face of the polytope P. We will have to take care to detect when a face F_i is a codimension 1 facet or not; this will be important in the proof of Corollary 41.

Proof. Order the vectors a_i by lenght, in nonincreasing order; that is,

$$\|a_1\| \geq \|a_2\| \geq \cdots \geq \|a_n\|.$$

For each i, we will determine whether F_i is a facet of P or not (that is, whether F_i has codimension 1), and, in the case it is a facet, we will determine $\operatorname{vol}_{\mathrm{r}} F_i$ and b_i. Then, given b_i for the facets of P, the polytope is completely determined; since then b_i is the smallest real number such that

$$P \subseteq \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\},$$

this determines the remaining b_i (which are associated with lower dimensional faces of P).

We will proceed by induction, so assume that, for some $j \geq 1$, we have determined everything for the faces F_i with $i < j$.

By Lemma 36, all discontinuities of the function $L_{P+w}(s)$ are due to integer points passing through the facets of P. If s_0 is a point of left-discontinuity of $L_{P+w}(s)$, let $F_{i_1}+w, \ldots, F_{i_l}+w$ be the front facets of $P+w$ such that $s_0(b_i+\langle a_i, w\rangle)$ is an integer; that is, $F_{i_1}, \ldots, F_{i_l}$ are the facets which caused the discontinuity at s_0. Then Lemma 37 says that if U is the magnitude of this discontinuity, then $\frac{U}{s_0^{d-1}}$ is approximately $\operatorname{vol}_{\mathrm{r}} F_{i_1} + \cdots + \operatorname{vol}_{\mathrm{r}} F_{i_l}$.

Here, the fact that Lemma 37 asserts that the limit is uniform in the translation vector w guarantees that the number $\frac{U}{s^{d-1}}$ will approximate $\operatorname{vol}_{\mathrm{r}} F_{i_1} + \cdots + \operatorname{vol}_{\mathrm{r}} F_{i_l}$ just by making s large, regardless of w.

Let $S(x) = 0^{d-1} + 1^{d-1} + \cdots + \lfloor x \rfloor^{d-1}$ for $x \geq 0$ and $S(x) = -S(-x)$ for $x \leq 0$, and define

$$g_w(s) = f_w(s) - \sum_{i=1}^{j-1} S(s(b_i + \langle a_i, w\rangle))\gamma_i,$$

where γ_i is $\operatorname{vol}_{\mathrm{r}} F_i$, if F_i is a facet of P, and zero otherwise.

If $x = s(b_i+\langle a_i, w\rangle)$ is a positive integer, then the term $S(x)\operatorname{vol}_{\mathrm{r}} F_i$ will cause a left-discontinuity of magnitude $x^{d-1}\operatorname{vol}_{\mathrm{r}} F_i$; if x is a negative integer, then the term $S(x)\operatorname{vol}_{\mathrm{r}} F_i$ will cause a right-discontinuity of magnitude $x^{d-1}\operatorname{vol}_{\mathrm{r}} F_i$. Subtracting these values from f_w "cleans" the function from the influence of the discontinuities caused by F_i, for $i < j$.

In terms of $\frac{U}{s^{d-1}}$, this says that, if V is the magnitude of the left discontinuity at s_0 of g_w, then $\frac{V}{s_0^{d-1}}$ approximates the sum of the $\operatorname{vol}_{\mathrm{r}} F_{i_m}$ for which $i_m \geq j$.

Since we know whether F_i is a facet or not, and we know $\operatorname{vol}_{\mathrm{r}} F_i$ and b_i in the case it is, we may construct the function g_w, so we may work with the "cleaner" V instead of with U. (Note that removing the terms $S(x) \operatorname{vol}_{\mathrm{r}} F_i$ does not perfectly eliminate the influence of the facets F_i, because the magnitudes of the jumps only approximate $s^{d-1} \operatorname{vol}_{\mathrm{r}} F_i$. Therefore, there might be some "residual" discontinuities of order $O(s^{d-2})$ in g_w. Since we will always divide the magnitude of the discontinuities by s^{d-1}, we may safely ignore these residual discontinuities.)

Use Lemma 38 with the vectors $a_j, \ldots, a_n$ to get appropriate w_0, α_k and ϵ_k.

Define V_k to be sum of the magnitudes of the left-discontinuities of the function g_k in the interval $(\alpha_k, \alpha_k + \epsilon_k)$. We will first determine whether F_j is a facet or not.

Property 6 says that, if F_j is a facet (so that its $(d-1)$-dimensional volume is nonzero), the value of $\frac{V_k}{k^{d-1}}$ must be at least $\operatorname{vol}_{\mathrm{r}} F_j$. Property 7 says that, for arbitrarily many k, the value of $\frac{V_k}{k^{d-1}}$ will be either $\operatorname{vol}_{\mathrm{r}} F_j$ or $2 \operatorname{vol}_{\mathrm{r}} F_j$. Conversely, if F_j is not a facet, then this number will approach zero. Therefore, F_j is a facet if and only if

$$\liminf_{k\to\infty} \frac{V_k}{k^{d-1}} > 0.$$

If F_j is not a facet, there is nothing more to do, so assume that F_j is a facet of P.

Let us say that a value V_k is *good* if the interval $(\alpha_k, \alpha_k + \epsilon_k)$ contains exactly one discontinuity; *not-so-good*, if the interval contains exactly two discontinuities, and the magnitude of the jump in both cases is approximately the same (that is, their ratio is close to 1); and *bad* otherwise.

If V_k is good, then we know from Lemma 37 that V_k is approximately $k^{d-1} \operatorname{vol}_{\mathrm{r}} F_j$. If V_k is not-so-good, we know at least one of the two discontinuities must have a magnitude of approximately $k^{d-1} \operatorname{vol}_{\mathrm{r}} F_j$, so the other discontinuity must also have that magnitude, and thus V_k is approximately $2k^{d-1} \operatorname{vol}_{\mathrm{r}} F_j$.

Property 7 of Lemma 38 says that there are infinitely many V_k which are either good or not-so-good. This means that at least one of the limits

$$\liminf_{\substack{k\to\infty \\ V_k \text{ good}}} \frac{V_k}{k^{d-1}} \qquad \text{and} \qquad \frac{1}{2} \liminf_{\substack{k\to\infty \\ V_k \text{ not-so-good}}} \frac{V_k}{k^{d-1}}$$

exists and equals $\operatorname{vol}_{\mathrm{r}} F_j$.

If either one of the limits do not exist (which happens only if there is only finitely many good V_k or finitely many not-so-good V_k, respectively), or both limits agree, then we know for sure the value of $\operatorname{vol}_{\mathrm{r}} F_j$. It might happen that both limit exists, but their values are different; this happens if there are infinitely many good and not-so-good V_k, but either of these have some associated "garbage". For good V_k, we know that there is a single discontinuity in $(\alpha_k, \alpha_k + \epsilon_k)$, but it might happen that this discontinuity is due to F_j and some other facets F_i for $i > j$. A similar problem happens with the not-so-good V_k. In this case, we will have "dirty" V_k, which will make the limits larger than $\operatorname{vol}_{\mathrm{r}} F_j$.

However, property 7 does guarantee that there will be infinitely many "clean" V_k, so in the event that both limits exist and differ, the smallest value is the correct one (because that's where the infinitely many "clean" V_k appeared).

To recover b_j, we will handle these cases separately.

Assume first that the "infinitely many good V_k" gave the correct value. Looking in the intervals $(\alpha_k, \alpha_k + \epsilon_k)$ for which the corresponding V_k approximate

$k^{d-1} \operatorname{vol}_{\mathrm{r}} F_j$, we get an infinite number of $s_k \in (\alpha_k, \alpha_k + \epsilon_k)$ which we know are discontinuities provoked by F_j. That is, there is a sequence of integers m_k such that

$$s_k(b_j + k\langle a_j, w_0\rangle) = m_k$$

for all these k. By properties 3, 4 and 5 of Lemma 38, we have that $\{s_k\}$ approaches zero for these k, and thus we may apply Lemma 39 to determine b_j uniquely.

Now assume that the correct limit is the "infinitely many not-so-good V_k". Let s_k and s'_k (with $s_k < s'_k$) be the two discontinuities which happen in $(\alpha_k, \alpha_k, \epsilon_k)$, when V_k is not-so-good and approximates $2 \operatorname{vol}_{\mathrm{r}} F_j$. The main difficulty of this case is that, for each k, we know at least one of s_k and s'_k is a point of discontinuity caused by F_j, but it might not be both.

Call the case where both are discontinuities caused by F_j the *nice* case. Since these two are consecutive discontinuities, we have

$$s'_k - s_k = \frac{1}{b_j + k\langle a_j, w_0\rangle};$$

rearranging this equation gives

$$b_j = \frac{1}{s'_k - s_k} - k\langle a_j, w_0\rangle.$$

In a non-nice case, the distance between s'_k and s_k is smaller than in the nice case (because in any open interval with length larger than $\frac{1}{b_j + k\langle a_j, w_0\rangle}$ lies a point of discontinuity of F_j); that is,

$$s'_k - s_k < \frac{1}{b_j + k\langle a_j, w_0\rangle}.$$

If k is large enough, this translates to

$$b_j < \frac{1}{s'_k - s_k} - k\langle a_j, w_0\rangle.$$

Due to properties 6 and 7, together with the current assumption that there are only finitely many good V_k, we know that the nice case happens infinitely often; therefore,

$$b_j = \limsup_{\substack{k\to\infty \\ V_k \text{ not-so-good}}} \frac{1}{s'_k - s_k} - k\langle a_j, w_0\rangle.$$

Therefore, if F_j is a facet of P, both when there are infinitely many good V_k and when there are infinitely many not-so-good V_k we can compute $\operatorname{vol}_{\mathrm{r}} F_j$ and b_j.

Now apply induction on j to finish the proof. □

Corollary 41. *Let P and Q be two full-dimensional semi-rational polytopes such that $L_{P+w}(s) = L_{Q+w}(s)$ for all integer w and all real $s > 0$. Then $P = Q$.*

In other words, the functions $L_{P+w}(s)$ for all integer w form a complete set of invariants in the class of full-dimensional semi-rational polytopes.

Proof. If a is a primitive integer vector such that

$$P \cap \{x \in \mathbb{R}^d \mid \langle a, x\rangle = b\}$$

is a facet of P, then, as Q is a bounded set, for some appropriate b' we have

$$Q \subseteq \{x \in \mathbb{R}^d \mid \langle a, x\rangle \leq b'\}.$$

This means we can write

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}$$
$$Q = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq c_i\},$$

where $a_1, \ldots, a_n$ are primitive integer vectors, and $b_1, \ldots, b_n, c_1, \ldots, c_n$ are real numbers.

That is, by possibly adding some redundant vectors, we can write P and Q as intersection of hyperplanes using the same set of normal vectors. Now just apply Theorem 40 (assuming knowledge of the vectors $a_1, \ldots, a_n$) to conclude that $P = Q$. □

5.3 Codimension one polytopes

Corollary 41 says that the functions $L_{P+w}(s)$ form a complete set of invariants in the class of full-dimensional semi-rational polytopes. There exists a simple example which shows that full-dimensionality is needed: consider again the affine space M defined in Section 3.3 by

$$M = \{(\ln 2, \ln 3)\} \times \mathbb{R}^{d-2}.$$

For any real $s > 0$ and any integer w, the affine space $s(M + w)$ has no integer points, and thus if P and Q are any polytopes which are contained in M then $L_{P+w}(s) = L_{Q+w}(s) = 0$ for all w and all $s > 0$.

P and Q may be chosen to be semi-rational in the example above, so we know that the analogue of Corollary 41 for codimension 2 semi-rational polytopes is false. This leaves open the possibility that the analogue for semi-rational codimension 1 polytopes, or for rational polytopes of any dimension, is true. In this section we will show that both these analogues are indeed true.

The general idea is to reduce to the full-dimensional case, but we will need to do some adjustments. For example, if P is a $(d-1)$-dimensional polytope contained in $\mathbb{R}^{d-1} \times \{\frac{1}{2}\}$, let $P' = P - (0, \ldots, 0, \frac{1}{2})$, and P'' be the projection of P' to $\mathbb{R}^{d-1}$. The polytope P'' is, indeed, a full-dimensional polytope in $\mathbb{R}^{d-1}$, and if $w = (w_1, \ldots, w_{d-1})$ is an integer vector we know that

$$L_{P'+w}(s) = L_{P''+(w_1,\ldots,w_{d-1},0)}(s)$$

for all s. Therefore, if we can compute $L_{P'+w}(s)$ for all w whose last coordinate is zero, we may use Corollary 41 for P'', and conclude P'' is uniquely identified. (We will see later how to distinguish between two translates of the same polytope.)

The problem is that, just by using $L_{P+w}(s)$, we cannot compute $L_{P'+w}(s)$ for all s. Let $w = (w_1, \ldots, w_d)$ be an integer vector. Then

$$P + w \subseteq \mathbb{R}^{d-1} \times \{w_d + \tfrac{1}{2}\},$$

so $L_{P+w}(s)$ will be nonzero only for s of the form $\frac{m}{w_d+\frac{1}{2}}$ for some integer m. In this case, we have

$$L_{P+w}(s) = L_{P'+w'}(s),$$

for $w' = (w_1, \ldots, w_{d-1}, 0)$.

Thus, we may compute $L_{P''+w}(s)$ only for s of the form $\frac{2m}{2w_d+1}$; that is, instead of knowing the value of $L_{P''+w}(s)$ for all s, we know it just for a dense subset of $\mathbb{R}$.

Since each $L_P(s)$ is piecewise constant, this is still enough information to compute the one-sided limits $L_P(s^+)$ and $L_P(s^-)$ for all $s > 0$, and as each $L_P(s)$ is lower semicontinuous, we can fully reconstruct most of its discontinuities. In particular, if s_0 is either a right-discontinuity or a left-discontinuity, but no both, of $L_P(s)$, we know that $L_P(s_0)$ is the largest of $L_P(s_0^-)$ and $L_P(s_0^+)$. However, this is not enough to recover $L_P(s_0)$ if s_0 is both a left- and right-discontinuity; this happens, for example, at $s_0 = 3$ with the square of Figure 5.1.

In order to use Corollary 41, we will strengthen its proof to work with knowledge of $L_{P+w}(s)$ only for densely many s. More specifically, we will modify Lemma 38 so that the choice of w_0 avoids these overlapping discontinuities, at least in the window $(\alpha_k, \alpha_k + \epsilon_k)$ in which we analyze $L_{P+kw_0}(s)$.

5.3.1 Avoiding overlapping discontinuities

Again, write P as

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle \leq b_i\}, \qquad \text{(1.1 revisited)}$$

and let F_i be the corresponding facets of P.

The facet $F_i + w_k$ may only trigger a discontinuity at s if

$$s = \frac{m}{b_i + \langle a_i, w_k\rangle}$$

for some integer m. Therefore, if $F_i + w_k$ and $F_j + w_k$ both trigger a discontinuity at s, then we must have, for integers m_i, m_j,

$$s = \frac{m_i}{b_i + \langle a_i, w_k\rangle} = \frac{m_j}{b_j + \langle a_j, w_k\rangle}.$$

If we divide both m_i and m_j by their greatest common divisor, we obtain a "primitive" number s such that all other simultaneous discontinuity points of $F_i + w_k$ and $F_j + w_k$ are integer multiples of s. So, assume m_i and m_j are relatively prime.

From this equation, it is clear that if both $F_i + w_k$ and $F_j + w_k$ trigger a discontinuity, we must either have both b_i and b_j rational, or both irrational. We will first deal with the irrational case, which is easier.

Assume for now that b_i and b_j are both irrational. We may rewrite the above equation as

$$b_j = \frac{m_i}{m_j} b_i + \frac{m_i}{m_j}\langle a_j, w_k\rangle - \langle a_i, w_k\rangle.$$

If there is a $k' \neq k$ for which $F_i + w_{k'}$ and $F_j + w_{k'}$ also have overlapping discontinuities, then there is also two coprime integers m_i', m_j' such that

$$b_j = \frac{m_i'}{m_j'} b_i + \frac{m_i'}{m_j'}\langle a_j, w_{k'}\rangle - \langle a_i, w_{k'}\rangle.$$

In both cases, we wrote b_j as a rational combination of b_i and 1. Thinking of $\mathbb{R}$ as a vector space over $\mathbb{Q}$, we know b_i and 1 are linearly independent, and thus this representation of b_j is unique. Therefore,

$$\frac{m_i'}{m_j'} = \frac{m_i}{m_j} \qquad \text{and} \qquad \frac{m_i}{m_j}\langle a_j, w_k\rangle - \langle a_i, w_k\rangle = \frac{m_i'}{m_j'}\langle a_j, w_{k'}\rangle - \langle a_i, w_{k'}\rangle.$$

Since the pairs (m_i, m_j) and (m_i', m_j') are of coprime numbers, the first of these two equations give $m_i = \pm m_i'$ and $m_j = \pm m_j'$; we may assume $m_i = m_i'$ and $m_j = m_j'$. Using these identities and expanding $w_k = kw_0$, the second equation may be rearranged to

$$k\langle m_i a_j - m_j a_i, w_0\rangle = k'\langle m_i a_j - m_j a_i, w_0\rangle.$$

Since we assumed that $k' \neq k$, we must have

$$\langle m_i a_j - m_j a_i, w_0\rangle = 0,$$

which means that w_0 is orthogonal to $m_i a_j - m_j a_i$.

Therefore, if we guarantee that w_0 is not orthogonal to $m_i a_j - m_j a_i$, we are sure that $F_i + w_k$ and $F_j + w_k$ will have overlapping discontinuities for at most one k.

Ideally, we would like to make w_0 non-orthogonal to $m_i a_j - m_j a_i$ for all possible choices of m_i, m_j and all a_i, a_j. That would add an infinite number of restrictions on w_0, which might make the choice of w_0 impossible (for example, if $a_1 = (1, 0)$ and $a_2 = (0, 1)$, then the only possible choice would be $w_0 = 0$).

Fortunately, there is at most one problematic m_i and m_j which must be avoided for each pair of irrationals b_i and b_j. So, for convenience, call the "dependence index" between any two irrational numbers b_i and b_j to be $\max\{|m_i|, |m_j|\}$, where m_i and m_j are coprime numbers such that $b_i = \frac{m_i}{m_j} b_j + r$ for some rational number r. (This is well-defined because if m_i and m_j exist, then they are unique, up to signs.) If no such integers m_i and m_j exist, let the dependence index be zero.

If N is larger than the dependence index between any two irrational numbers in $\{b_1, \ldots, b_n\}$, making w_0 not orthogonal to any vector of the form $m_i a_j - m_j a_i$ with $|m_i|, |m_j| \leq N$ guarantees that the discontinuities of $F_i + w_k$ and $F_j + w_k$ will overlap for at most one k.

This solves the irrational clashes, so now assume b_i and b_j are rational.

Here, clashes are unavoidable. The goal is to make them happen outside $(\alpha_k, \alpha_k + \epsilon_k)$. This will be accomplished by showing that, if s is a simultaneous discontinuity point for any k, then the denominator of s is bounded. The

interval $(\alpha_k, \alpha_k + \epsilon_k)$ contains points of the form $k + \delta$ for small, positive δ, and as k gets large, δ gets small. This will guarantee no discontinuity clashes happen inside this interval.

Write $b_i = \frac{p_i}{q_i}$. The "primitive clash equation" reads

$$s = \frac{q_i m_i}{p_i + q_i \langle a_i, w_k \rangle} = \frac{q_j m_j}{p_j + q_j \langle a_j, w_k \rangle},$$

which may be rewritten as

$$m_i q_i (p_j + q_j \langle a_j, w_0 \rangle k) = m_j q_j (p_i + q_i \langle a_i, w_0 \rangle k).$$

This is an equation of the form $\zeta m_i = \xi m_j$, where $\zeta = q_i p_j + q_i q_j \langle a_j, w_0 \rangle k$ and $\xi = q_j p_i + q_j q_i \langle a_i, w_0 \rangle k$. All solutions are of the form

$$(m_i, m_j) = \left(\frac{\xi}{\gcd(\zeta, \xi)} l, \frac{\zeta}{\gcd(\zeta, \xi)} l \right),$$

for some integer l. Since we are looking for the "primitive" solution, we will take $l = 1$.

The following lemma guarantees that the denominator of the primitive solution is bounded, as a function of k.

Lemma 42. *Let ζ, ξ, γ, η be integers such that the vectors (ζ, γ) and (ξ, η) are linearly independent. Then the sequence $\{\gcd(\zeta k + \gamma, \xi k + \eta)\}_{k=1}^{\infty}$ is periodic.*

Proof. By swapping (ζ, γ) and (ξ, η) and multiplying them by -1, if needed, we may assume that $\zeta \geq \xi \geq 0$.

If $\xi = 0$, then the sequence has only terms of the form

$$\gcd(\zeta k + \gamma, \eta).$$

Since $\eta \neq 0$ (due to the linear independence restriction), we have

$$\gcd(\zeta k + \gamma, \eta) = \gcd(\eta, (\zeta k + \gamma) \bmod \eta),$$

from which periodicity is clear.

If $\zeta, \xi > 0$, we have

$$\gcd(\zeta k + \gamma, \xi k + \eta) = \gcd(\xi k + \eta, (\zeta - \xi) k + \gamma - \eta),$$

so if we let $\zeta' = \xi$, $\xi' = \zeta - \xi$, $\gamma' = \eta$, and $\eta' = \gamma - \eta$, then $\zeta', \xi' \geq 0$ and $\zeta' + \xi' < \zeta + \xi$, so we may apply induction in $\zeta + \xi$ to conclude that the sequence is periodic. □

In our case, we have $\zeta = q_i q_j \langle a_i, w_0 \rangle$, $\xi = q_i q_j \langle a_i, w_0 \rangle$, $\gamma = q_j p_i$ and $\eta = q_i p_j$. For the vectors (ζ, γ) and (ξ, η) to be linearly dependent, there must exist some rational number r such that $r\zeta = \xi$ and $r\gamma = \eta$. That is,

$$\frac{q_i q_j \langle a_i, w_0 \rangle}{q_i q_j \langle a_j, w_0 \rangle} = \frac{\xi}{\zeta} = r = \frac{\eta}{\gamma} = \frac{q_i p_j}{q_j p_i}$$

Rearranging the equation gives

$$\langle w_0, p_j q_i a_i - p_i q_j a_j \rangle = 0.$$

Therefore, if we can guarantee that w_0 is not orthogonal to $p_j q_i a_j - p_i q_j a_j$, for all i and j (with $i \neq j$), we will make sure that

$$\frac{m_i}{p_i + q_i \langle a_i, w_k \rangle}$$

will have only finitely many distinct values. As s is a multiple of this value, this gives a bound on the denominator of s; so, for large enough k, no such s will appear in $(\alpha_k, \alpha_k + \epsilon_k)$.

We may use the same trick that deals with the irrational case: we will add a parameter N to the lemma, and make w_0 orthogonal to all $\tau_j a_j - \tau_i a_i$ for any pair τ_i, τ_j with $|\tau_i|, |\tau_j| \leq N^2$.

The modified lemma is the following.

Lemma 43. *Let $N \geq 0$ be some integer number, and let $a_1, \ldots, a_n$ be primitive integer vectors in $\mathbb{R}^d$, with $\|a_1\| \geq \|a_i\|$ for all i. Then there is an integer vector w_0 and a sequence $(\alpha_k, \alpha_k + \epsilon_k)$ of intervals such that, for all possible choice of real numbers $b_1, \ldots, b_n$, all the properties enumerated in Lemma 38 are true, and also the following one:*

8. *If the numerator and the denominator of all rational b_i is smaller than or equal to N, and the "dependence index" between any two irrational b_i is smaller than or equal to N, then for all sufficiently large k there will be no $s \in (\alpha_k, \alpha_k + \epsilon_k)$*

Proof. In the choice of the vector w_0, in the beginning of the lemma, there was already a (finite) list of integer vectors such that w_0 was made non-orthogonal (namely, all vectors a_i for $i = 1, \ldots, n$). Now, add to that list all vectors of the form

$$\tau_i a_j - \tau_j a_i,$$

for all pairs of integers τ_i, τ_j such that $|\tau_i|, |\tau_j| \leq N^2$.

Primitiveness of the vectors a_i guarantee that none of these vectors is the zero vector, and as we are limiting the coefficients by N^2 we still have a finite list.

Now choose w_0, α_k and ϵ_k in the same way as in the proof of Lemma 38 except that, now, the list of vectors not orthogonal to w_0 is larger. This will guarantee all the properties of that lemma.

Finally, property 8 follows from the discussion above. □

5.3.2 Piecing together the semi-rational case, but avoiding discontinuity clashes

The improved Lemma 43 guarantees that, for large enough k, there will not be discontinuities overlapping in $(\alpha_k, \alpha_k + \epsilon_k)$, and thus the other lemmas may be used. So we can prove the following improved version of Theorem 40.

Theorem 44. *Let $a_1, \ldots, a_n \in \mathbb{R}^d$ be primitive integer vectors and for each integer w let $f_w(s)$ be a function on $\mathbb{R}$. Then there is at most one set of numbers $b_1, \ldots, b_n$ such that*

$$P = \bigcap_{i=1}^{n} \{x \in \mathbb{R}^d \mid \langle a_i, x \rangle \leq b_i\}$$

is a full-dimensional semi-rational polytope, that $f_w(s) = L_{P+w}(s)$ *for all integer* w *and all* s *in a dense subset of* $\mathbb{R}$*, and that the polytopes* F_i *defined by*

$$F_i = P \cap \{x \in \mathbb{R}^d \mid \langle a_i, x\rangle = b_i\}$$

are faces of P*.*

Proof. Write $b_i = \frac{p_i}{q_i}$ whenever b_i is rational, and let N be so large that $N \geq |p_i|$ and $N \geq |q_i|$, and that N is larger than the dependence index between any two irrational numbers in $\{b_1, \ldots, b_n\}$. Use Lemma 43 with this N, and property 8 will guarantee that, for all large enough k, we still know precisely where the discontinuities of $L_{P+w}(s)$ happen and what are their magnitudes.

Thus the remainder of the proof is identical. □

Corollary 45. *Let* P *and* Q *be two full-dimensional semi-rational polytopes such that* $L_{P+w}(s) = L_{Q+w}(s)$ *for all integer* w *and all real* $s > 0$ *in a dense subset of* $\mathbb{R}$*. Then* $P = Q$*.*

Proof. Analogous to the proof of 41. □

5.3.3 Semi-rational polytopes with codimension 0 and 1

Now we may show Corollary 41 for semi-rational polytopes which have codimension 0 and 1.

Theorem 9. *Let* P *and* Q *be two semi-rational polytopes in* $\mathbb{R}^d$*, both having codimension* 0 *or* 1*. Suppose moreover that* $L_{P+w}(s) = L_{Q+w}(s)$ *for all integer* w *and all real* $s > 0$*. Then* $P = Q$*.*

Proof. If their codimensions do not match, then $L_P(s)$ and $L_Q(s)$ will be different, so we may assume either both have codimension 0 or both have codimension 1. In the first case, P and Q are full-dimensional, so we may use Corollary 45 directly. Thus, assume both P and Q have codimension 1.

Let H, H' satisfy

$$P \subseteq H = \{x \in \mathbb{R}^d \mid \langle a, x\rangle = b\}$$
$$Q \subseteq H' = \{x \in \mathbb{R}^d \mid \langle a', x\rangle = b'\}.$$

If we had $a \neq a'$, we could choose some vector w which is orthogonal to a but not to a', and then $\operatorname{vol}\operatorname{ppyr}(Q+kw)$ would increase for large k (because the height of the pseudopyramid would increase, whereas the area of the base do not change) but $\operatorname{vol}\operatorname{ppyr}(P+kw)$ would stay the same (because neither the height nor the area of the base would change). Since $\operatorname{vol}\operatorname{ppyr}(P+kw)$ is determined by $L_{P+kw}(s)$ (by Lemma 20), we know this cannot happen.

This shows $a = a'$, and using Lemma 37 both $L_P(s)$ and of $L_Q(s)$ must exhibit discontinuities for all large enough s, which shows $b = b'$. Thus, $H = H'$.

Now using unimodular transforms we may assume that

$$H = \{x \in \mathbb{R}^d \mid x_d = b\}.$$

We have $P - (0, \ldots, 0, b) \in \mathbb{R}^{d-1} \times \{0\}$, and analogously for Q, so we may define $P' \subseteq \mathbb{R}^{d-1}$ to be the projection of $P - (0, \ldots, 0, b)$ to $\mathbb{R}^{d-1}$, and analogously for Q. We will show that $P' = Q'$, which implies $P = Q$.

Let $w' = (w_1, \ldots, w_{d-1})$ be given. If s is of the form

$$s = \frac{m}{b + w_d}$$

for some integers m and w_d, let $w = (w_1, \ldots, w_d)$ and then

$$\begin{aligned} L_{P+w}(s) &= \#(s(P+w) \cap \mathbb{Z}^d) \\ &= \#\big((s(P+w) - (0, \ldots, 0, m)) \cap \mathbb{Z}^d\big) \\ &= \#(s(P'+w') \cap \mathbb{Z}^{d-1}) \\ &= L_{P'+w'}(s). \end{aligned}$$

Analogously, we have $L_{Q+w}(s) = L_{Q'+w'}(s)$.

This shows that $L_{P'+w'}(s) = L_{Q'+w'}(s)$ for all integer $w' \in \mathbb{R}^{d-1}$ and all $s > 0$ of the form $\frac{m}{b+w_d}$, which form a dense subset of $\mathbb{R}$. Therefore, P' and Q' satisfy the hypothesis of Corollary 45, and thus $P' = Q'$, which shows $P = Q$. □

5.3.4 All the way down with the rationals

As a last bonus from Corollary 45, we may extend Theorem 9 for all dimensions, if we restrict ourselves to rational polytopes.

Theorem 6. *Let P and Q be two rational polytopes in $\mathbb{R}^d$. Suppose that $L_{P+w}(s) = L_{Q+w}(s)$ for all integer w and all real $s > 0$. Then $P = Q$.*

Proof. Measuring rate of growth of $L_P(s)$ and $L_Q(s)$ gives the dimension of both polytopes, so we may assume both have the same dimension. If they have codimension 0 or 1, then we may apply Theorem 9 directly. So, assume their dimension is smaller than $d - 2$.

Let $M = \operatorname{aff} P$, and let H be the translate of M which passes through the origin. Define M' and H' analogously for Q. If $H \neq H'$, let $w \in H \setminus H'$; then the relative volume of $\operatorname{ppyr}(P + kw)$ will stay the same, whereas the relative volume of $\operatorname{ppyr}(Q + kw)$ will increase for large k (we may measure the relative volume for $P + kw$ and $Q + kw$ because these polytopes are rational, and thus there are dilations of them which will contain integer points.)

This shows $H = H'$, and a similar reasoning as before shows $M = M'$. Now let A be a unimodular transform which maps M to a subset of $\mathbb{R}^{d-1} \times \{0\}$; apply A to both P and Q, project the unimodular images to $\mathbb{R}^{d-1}$, and use this theorem for $d - 1$ to conclude $P = Q$. □

5.4 Reconstruction of symmetric convex bodies

A *convex body* is a full-dimensional compact convex set. A convex K body is *symmetric* if $x \in K$ if and only if $-x \in K$.

In this section, we will show yet another version of Theorems 6 and 9, but for symmetric convex bodies.

We first observe that Lemma 20, about pseudopyramids, still holds for convex bodies, with the same proof. As a consequence, whenever we know $L_K(s)$, we may assume that we know $\operatorname{vol}\operatorname{ppyr} K$. More formally, we have the following.

Lemma 46. *Let K and H be convex bodies, and suppose that $L_K(s) = L_H(s)$ for all $s > 0$. Then $\operatorname{vol}\operatorname{ppyr} H = \operatorname{vol}\operatorname{ppyr} K$.*

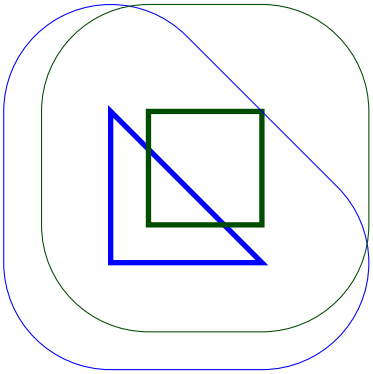


Figure 5.4: Hausdorff distance between two convex sets. The thick lines are the boundaries of the sets K and H; the thin lines are the boundaries of the sets K_λ and H_λ.

5.4.1 Aleksandrov's projection theorem and Hausdorff distances

The punchline is Aleksandrov's projection theorem. Let $K \subseteq \mathbb{R}^d$ be a convex body (that is, a covex, compact set with nonempty interior). For any unit vector v, we will denote by $V_K(v)$ the $(d-1)$-dimensional area of the orthogonal projection of K in $\{v\}^\perp$.

For example, let $K = [0,1] \times [0,1] \subseteq \mathbb{R}^2$, $v = (0,1)$ and $v' = (\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$. Then $V_K(v) = 1$ and $V_K(v') = \sqrt{2}$.

A convex body K is said to be *symmetric* if $x \in K$ if and only if $-x \in K$. An importan reconstruction theorem for symmetric convex bodies is Aleksandrov's projecion theorem (see e.g. [9, p. 115]).

Theorem 47 (Aleksandrov's projection theorem)**.** *Let K and H be two symmetric convex bodies in $\mathbb{R}^d$ such that $V_K(v) = V_H(v)$ for all unit vectors v. Then $K = H$.*

So, the goal is to compute the function V_K using the Ehrhart functions L_{K+w}. The two main tools are the Hausdorff distance and pseudopyramids.

For $\lambda \geq 0$ and $x \in \mathbb{R}^d$, denote by $B_\lambda(x)$ the ball with radius λ centered at x. If K is a convex body and $\lambda \geq 0$, define K_λ by

$$K_\lambda = \bigcup_{x \in K} B_\lambda(x).$$

The Hausdorff distance $\rho(K, H)$ between two convex bodies K and H is defined to be (Figure 5.4)

$$\rho(K, H) = \inf\{\lambda \geq 0 \mid K \subseteq H_\lambda \text{ and } H \subseteq K_\lambda\}.$$

It can be shown that the set of convex sets in $\mathbb{R}^d$ is a metric space under the Hausdorff distance and that the Euclidean volume is continuous in this space (see e.g. [9, p. 9]), but we just need the following special case of this theory.

Lemma 48. *Let K and $A_1, A_2, \ldots$ be convex bodies. If $\lim_{i\to\infty} \rho(K, A_i) = 0$, then $\lim_{i\to\infty} \operatorname{vol} A_i = \operatorname{vol} K$.*

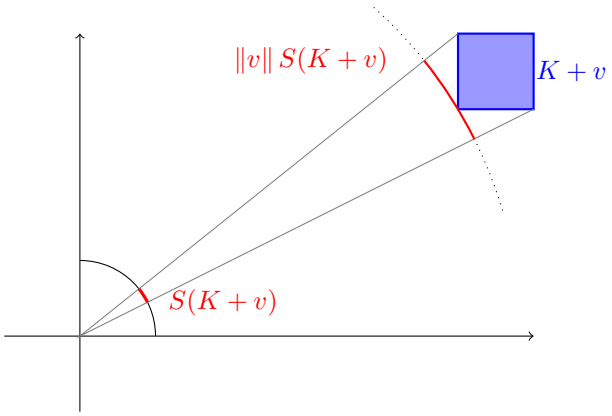


Figure 5.5: Spherical projection of $K + v$.

5.4.2 Approximating spherical projections

Given a convex body K, define its spherical projection $S(K)$ by (Figure 5.5)

$$S(K) = \left\{ \frac{x}{\|x\|} \,\middle|\, x \in K \text{ and } x \neq 0 \right\}.$$

The connection between pseudopyramid volumes and areas of projections can be seen in Figure 5.5. The set $\|v\|\, S(K+v)$ is a dilation of the projection $S(K+v)$ of K. Note that the shape of $\|v\|\, S(K+v)$ "looks like" the orthogonal projection of K in $\{v\}^\perp$; that is, the area of $\|v\|\, S(K+v)$ approximates $V_K(v)$.

If the pseudopyramid were an actual pyramid (with base $\|v\|\, S(K+v)$), then using the formula $v = \frac{Ah}{d}$ for the volume of a pyramid would allow us to discover what is the area of the projection, which would give an approximation to $V_K(v)$. We will show that this formula is true "in the infinity"; that is, using limits, we can recover the area of the projection using taller and taller pseudopyramids.

For convex bodies K, the set $S(K)$ is a manifold[1]. If K does not contain the origin in its interior, then $S(K)$ may be parameterized with a single coordinate system; that is, there is a set $U \subseteq \mathbb{R}^{d-1}$ and a continuously differentiable function $\varphi : U \to S(K)$ which is a bijection between U and $S(K)$. Since we want to move P towards infinity, this shall always be the case if the translation vector is long enough. In this case, we define its area to be [15, p. 126]

$$\begin{aligned} \operatorname{area} S(K) &= \int_U \|D_1\varphi \times \cdots \times D_{d-1}\varphi\| \\ &= \int_U \left\| \frac{\partial \varphi}{\partial x_1} \times \cdots \times \frac{\partial \varphi}{\partial x_{d-1}} dx_1 \ldots dx_{d-1} \right\|. \end{aligned}$$

The following theroem states that the spherical projection approximates, in a sense, the orthogonal projection, for large enough translation vectors.

[1] Technically, $S(K)$ will be a manifold-with-corners (see [15, p. 137]). However, their interiors relative to the $(d-1)$-dimensional sphere S^{d-1} are manifolds, and since we are dealing with areas there will be no harm in ignoring these boundaries.

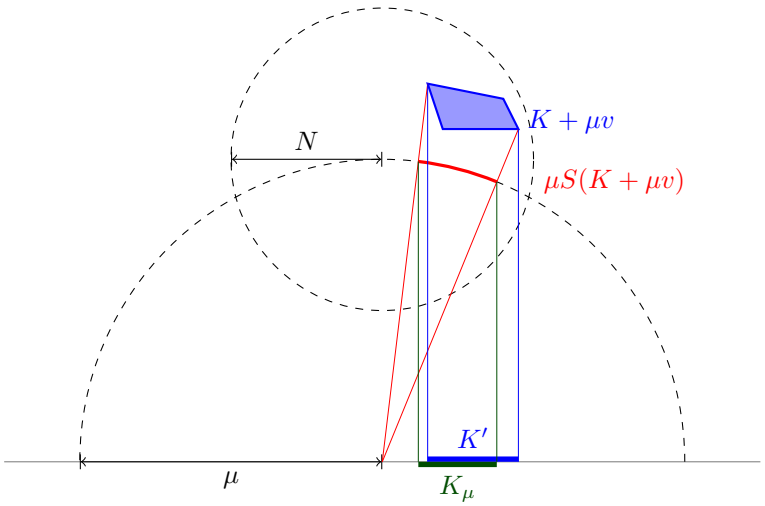


Figure 5.6: The spherical projection $\mu S(K + \mu v)$, when projected orthogonally to the plane $x_d = 0$ (the set K_μ), approaches the volume of the projection K'.

Theorem 49. *Let v be a unit vector and $K \subseteq \mathbb{R}^d$ a convex body. Then*

$$\lim_{\mu \to \infty} \mu^{d-1} \operatorname{area} S(P + \mu v) = V_K(v).$$

Proof. By rotating all objects involved if needed, we may assume that $v = (0, \ldots, 0, 1)$. Let N be large enough that $K \subseteq B_N(0)$; we will assume that $\mu > N$, so that $K + \mu v$ lies strictly above the hyperplane $x_d = 0$.

Let K' be the orthogonal projection of K into $\{v\}^\perp$. We will think of K' as being a subset of $\mathbb{R}^{d-1}$. Denote by K_μ the projection of the set $\mu S(K + \mu v)$ on $\mathbb{R}^{d-1}$ (Figure 5.6); that is, first project $K + \mu v$ to the sphere with radius μ, then discard the last coordinate. Note this is similar to project it to the hyperplane $x_d = 0$. We will show that, as μ goes to infinity, both the Hausdorff distance between K_μ and K' and the difference between the volume of K_μ and the area of $\mu S(K + \mu v)$ tend to zero.

First, let us bound the Hausdorff distance between K' and K_μ. If $x \in K + \mu v$, then x gets projected to a point $x_0 \in K'$ by just discarding the last coordinate; however, to be projected to a point $x_1 \in K_\mu$, first we replace x by $x' = \frac{\mu}{\|x\|} x$ to get a point $x' \in \mu S(K + \mu v)$, and then the last coordinate of x' is discarded. Note that $x_1 = \frac{\mu}{\|x\|} x_0$; therefore, the distance between these two points is

$$\|x_0 - x_1\| = \left| 1 - \frac{\mu}{\|x\|} \right| \|x_0\| = \frac{|\,\|x\| - \mu|}{\|x\|} \|x_0\|$$

We have $x \in K + \mu v \subseteq B_N(\mu v)$, so $\mu - N \leq \|x\| \leq \mu + N$. As $v = (0, \ldots, 0, 1)$ and x_0 is x without its last coordinate, we have $\|x_0\| \leq N$ (because, in $\mathbb{R}^{d-1}$, we have $x_0 \in B_N(0)$). So, the distance between x_0 and x_1 is at most $\frac{N^2}{\mu - N}$.

Every point in K' and in K_μ can be obtained through these projections. This means that, given any point x_0 in one of the sets, we may find another point x_1 in the other set which is at a distance of at most $\frac{N^2}{\mu + N}$ from the former, because

we can just pick a point x whose projection is x_0; then its other projection x_1 will be close to x_0. Thus

$$\rho(K', K_\mu) \leq \frac{N^2}{\mu - N},$$

so by Theorem 48 the volumes of K_μ converges to $\operatorname{vol} K'$.

Now, let us relate $\operatorname{vol} K_\mu$ with $\mu^{d-1} \operatorname{area} S(K + \mu v)$. If $y = (y_1, \ldots, y_d)$ is a point in $\mu S(K + \mu v)$, we know that $\|y\| = \mu$ and that $y_d > 0$ (because we are assuming $\mu > N$). Therefore, if we define $\varphi : K_\mu \to \mu S(K + \mu v)$ by

$$\varphi(y_1, \ldots, y_{d-1}) = \left(y_1, \ldots, y_{d-1}, \sqrt{\mu^2 - y_1^2 - \cdots - y_{d-1}^2}\right),$$

then φ will be a differentiable bijection between K_μ and $\mu S(K + \mu v)$, so that φ is a parametrization for $\mu S(K + \mu v)$.

For the partial derivatives, we have $\frac{\partial \varphi_i}{\partial y_j} = [i = j]$ if $i < d$; that is, the partial derivatives behave like the identity. For $i = d$, we have

$$\frac{\partial \varphi_d}{\partial y_j} = \frac{y_j}{\sqrt{\mu^2 - y_1^2 - \cdots - y_{d-1}^2}}.$$

Now, by definition of N, we have

$$\left|\frac{\partial \varphi_d}{\partial y_j}\right| \leq \frac{N}{\sqrt{\mu^2 - N^2}},$$

so the vectors $D_i \varphi$ converge uniformly to e_i for large μ. Since the generalized cross product is linear in each entry, the vector $D_1\varphi \times \cdots \times D_{d-1}\varphi$ converges uniformly to e_d, and thus the number

$$\begin{aligned} |\operatorname{vol} K_\mu - \operatorname{area} \mu S(K + \mu v)| &= \left| \int_{K_\mu} 1 - \int_{K_\mu} \|D_1\varphi \times \cdots \times D_{d-1}\varphi\| \right| \\ &\leq \int_{K_\mu} \left| 1 - \|D_1\varphi \times \cdots \times D_{d-1}\varphi\| \right| \end{aligned}$$

converges to zero.

Now, since $\operatorname{area}(\mu S(K + \mu v)) = \mu^{d-1} \operatorname{area} S(K + \mu v)$, combining these two convergence results gives the theorem. □

5.4.3 Limit behavior of pseudopyramids

Now we will show how to use the pseudopyramids to compute these projections.

Let K be a pseudopyramid. Define the *outer radius* $R(K)$ of K to be the smallest number such that the ball of radius $R(K)$ around the origin contains K. That is,

$$R(K) = \inf\{R \geq 0 \mid K \subseteq B_R(0)\}.$$

Define the *front shell* of K to be the set of points in the boundary of K which are not contained in any facet passing through the origin; that is, the set of points x in the boundary of K such that λx is contained in the interior of K for all $0 < \lambda < 1$. Define, then, the *inner radius* $r(K)$ of K to be the largest number

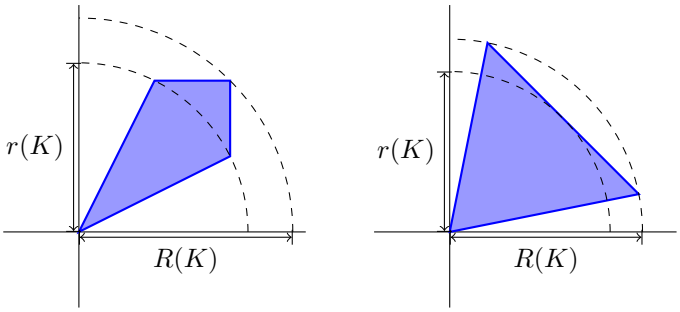


Figure 5.7: Inner and outer radius for two pseudopyramids.

such that the ball of radius $r(K)$ around the origin contains no points of the front shell of K (Figure 5.7). Note that this is equivalent to $r(K)S(K)$ to be contained in K; that is,

$$r(K) = \sup\{r \geq 0 \mid rS(K) \subseteq K\}.$$

We have the following relation between these radii and the area of the spherical projection.

Lemma 50. *Let $K \subseteq \mathbb{R}^d$ be a convex body which does not contain the origin. Then*

$$\frac{\operatorname{vol} \operatorname{ppyr} K}{R(\operatorname{ppyr} K)^d} \leq \frac{\operatorname{area} S(K)}{d} \leq \frac{\operatorname{vol} \operatorname{ppyr} K}{r(\operatorname{ppyr} K)^d}.$$

Proof. Denote by S_μ the set

$$S_\mu = \bigcup_{0 \leq \lambda \leq \mu} \lambda S(P).$$

By the definition of $r(\operatorname{ppyr} P)$ and of $R(\operatorname{ppyr} P)$, we have

$$S_{r(\operatorname{ppyr} P)} \subseteq \operatorname{ppyr} P \subseteq S_{R(\operatorname{ppyr} P)}.$$

Let $U \subseteq \mathbb{R}^{d-1}$ and $\varphi : U \to S(P)$ be such that φ is a parametrization of $S(P)$; we know such U and φ exist because we are assuming P does not contain the origin. Define now the function $\psi : U \times (0, \mu] \to S_\mu$ by

$$\psi(x, \lambda) = \lambda \varphi(x).$$

Then ψ is a bijection between $U \times (0, \mu]$ and $S_\mu \setminus \{0\}$, so we may compute the volume of S_μ using change of variables [15, p. 67]:

$$\begin{aligned} \operatorname{vol} S_\mu &= \int_{S_\mu} 1 \\ &= \int_{\psi(U \times (0,\mu])} 1 \\ &= \int_{U \times (0,\mu]} |\det \psi'|. \end{aligned}$$

Since

$$\psi'(x,\lambda) = \begin{bmatrix} | & & | & | \\ \lambda D_1\varphi(x) & \cdots & \lambda D_{d-1}\varphi(x) & \varphi(x) \\ | & & | & | \end{bmatrix},$$

we have, by the definition of the cross product,

$$\det \psi'(x,\lambda) = \lambda^{d-1}\langle D_1\varphi(x) \times \cdots \times D_{d-1}\varphi(x), \varphi(x)\rangle.$$

Each of the vectors $D_i\varphi(x)$ is a tangent vector at the point $\varphi(x)$ in the sphere. Since the $D_i\varphi(x)$ are linearly independent, their cross product is a multiple of the normal vector of the surface at that point. In this case, the vector $\varphi(x)$ is itself the unit normal, so the above inner product is $\pm$ the length of the cross product; that is,

$$|\det \psi'(x,\lambda)| = \lambda^{d-1} \|D_1\varphi(x) \times \cdots \times D_{d-1}\varphi(x)\|.$$

Therefore, the volume of S_μ is

$$\begin{aligned} \operatorname{vol} S_\mu &= \int_{U\times(0,\mu]} \lambda^{d-1} \|D_1\varphi(x) \times \cdots \times D_{d-1}\varphi(x)\| \\ &= \frac{\mu^d}{d} \int_U \|D_1\varphi(x) \times \cdots \times D_{d-1}\varphi(x)\| \\ &= \frac{\mu^d}{d} \operatorname{area} S(P). \end{aligned}$$

Now combining this result with the inclusions between S_μ and $\operatorname{ppyr} P$ gives the theorem. □

This lemma, combined with Lemma 49, shows how to calculate the volume of the orthogonal projection knowing only the volumes of the pseudopyramids.

Lemma 51. *Let $K \subseteq \mathbb{R}^d$ be a convex body, and v any unit vector. Then*

$$\lim_{\mu\to\infty} \frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{\mu} = \frac{V_K(v)}{d}.$$

Proof. Let N be large enough so that $K \subseteq B_N(0)$. For any μ, as v is a unit vector, we have $K + \mu v \subseteq B_{N+\mu}(0)$, so

$$R(\operatorname{ppyr}(K+\mu v)) \le \mu + N.$$

Since all the points in the front shell of $\operatorname{ppyr}(K+\mu v)$ are points of K, all of them must have norm greater or equal to $\mu - N$. Therefore, no origin-centered ball with radius smaller than that can contain these points. Thus,

$$r(\operatorname{ppyr}(K+\mu v)) \ge \mu - N.$$

Using these two inequalities and Proposition 50 gives

$$\frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{(\mu+N)^d} \le \frac{\operatorname{area} S(K+\mu v)}{d} \le \frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{(\mu-N)^d},$$

which may be rewritten as

$$\frac{(\mu-N)^d}{\mu^d}\frac{\mu^{d-1}\operatorname{area} S(K+\mu v)}{d} \le \frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{\mu} \le \frac{(\mu+N)^d}{\mu^d}\frac{\mu^{d-1}\operatorname{area} S(K+\mu v)}{d}.$$

Now Theorem 49 and the squeeze theorem finish the proof. □

For example, for $K = [0,1]^2$ and $v = (1,0)$, we have $\operatorname{vol}\operatorname{ppyr}(K+\mu v) = 1 + \frac{\mu}{2}$, so $\lim_{\mu\to\infty} \frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{\mu} = \frac{1}{2}$, which is precisely one-half of the area of $\{0\}\times[0,1]$, the projection K' of K on the y-axis. This highlights that, for large μ, the pseudopyramid $\operatorname{ppyr}(K+\mu v)$ "behaves like" an actual pyramid, with height μ and base K'.

5.4.4 Piecing everything together

Theorem 10. *Let K and H be symmetric convex bodies, and assume that $L_{K+w}(s) = L_{H+w}(s)$ for all real $s > 0$ and all integer w. Then $K = H$.*

Proof. By Lemma 46, we have $\operatorname{vol}\operatorname{ppyr}(K+w) = \operatorname{vol}\operatorname{ppyr}(H+w)$ for all integer w.

If w is a nonzero integer vector, let $v = \frac{w}{\|w\|}$; then, by Lemma 51, we have

$$\begin{aligned}\frac{V_K(v)}{d} &= \lim_{\mu\to\infty}\frac{\operatorname{vol}\operatorname{ppyr}(K+\mu v)}{\mu}\\ &= \lim_{\mu\to\infty}\frac{\operatorname{vol}\operatorname{ppyr}(H+\mu v)}{\mu}\\ &= \frac{V_H(v)}{d}\end{aligned}$$

This shows that, whenever v is a multiple of a rational vector, we have $V_K(v) = V_H(v)$. Since the functiosn V_K and V_H are continuous, we have $V_K = V_H$, and thus by Aleksandrov's projection theorem we conclude that $K = H$. □

Chapter 6

Final Remarks

Theorem 9 assumes knowledge of $L_{P+w}(s)$ for all integer w and guarantees that P is uniquely determined, as long as P is a full-dimensional semirational polytope. We mention two open questions regarding this theorem.

The first question (already hinted in Section 1.2) whether we may extend Theorems 9 and 10 to all convex bodies. We have the following conjecture.

Conjecture 52. *Let P and Q be two full-dimensional convex bodies such that $L_{P+w}(s) = L_{Q+w}(s)$ for all integer w and all real $s > 0$. Then $P = Q$.*

The second question is whether we need to know L_{P+w} for *all* w. For the sake of naming, let us call a certain set $W \subseteq \mathbb{Z}^d$ a *witness set* if $L_{P+w}(s) = L_{Q+w}(s)$ for all $w \in W$ implies $P = Q$; for example, Theorem 6 says that $W = \mathbb{Z}^d$ is a witness set for the class of rational polytopes.

Question 53. *Does there exist a finite witness set (for example, for the class of rational polytopes)?*

Bibliography

[1] Velleda Baldoni, Nicole Berline, Matthias Köppe, and Michèle Vergne. Intermediate sums on polyhedra: Computation and real Ehrhart theory. *Mathematika*, 59(1):1–22, 2013. doi:10.1112/S0025579312000101.

[2] Velleda Baldoni, Nicole Berline, Jesús Antonio De Loera, Matthias Köppe, and Michèle Vergne. Intermediate sums on polyhedra II: bidegree and Poisson formula. *Mathematika*, 62(3):653–684, 2016. doi:10.1112/S0025579315000418.

[3] Matthias Beck, Beifang Chen, Lenny Fukshansky, Christian Haase, Allen Knutson, Bruce Reznick, Sinai Robins, and Achill Schürmann. Problems from the Cottonwood Room. In *Integer points in polyhedra—geometry, number theory, algebra, optimization*, volume 374 of *Contemporary Mathematics*, pages 179–191. American Mathematical Society, Providence, RI, 2005. doi:10.1090/conm/374/06905.

[4] Matthias Beck and Sinai Robins. *Computing the Continuous Discretely: Integer-Point Enumeration in Polyhedra*. Undergraduate Texts in Mathematics. Springer, New York, second edition, 2015. doi:10.1007/978-1-4939-2969-6.

[5] Bence Borda. Lattice points in algebraic cross-polytopes and simplices. 2016. Preprint. URL: http://arxiv.org/abs/1608.02417.

[6] David Desario and Sinai Robins. Generalized solid-angle theory for real polytopes. *Quarterly journal of mathematics*, 62(4), 2011.

[7] Ricardo Diaz, Quang-Nhat Le, and Sinai Robins. Fourier transforms of polytopes, solid angle sums, and discrete volume. 2016. Preprint. URL: https://arxiv.org/abs/1602.08593.

[8] Cristina Gomes Fernandes, José Coelho de Pina, Jorge Luis Ramírez Alfonsín, and Sinai Robins. Polytopes attached to cubic graphs, and their Ehrhart quasi-polynomials. In preparation.

[9] Richard J. Gardner. *Geometric tomography*, volume 58 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, New York, second edition, 2006.

[10] Branko Grünbaum. *Convex polytopes*, volume 221 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2003. doi:10.1007/978-1-4613-0019-9.

[11] Christian Haase and Tyrrell B. McAllister. Quasi-period collapse and $\mathrm{GL}_n(\mathbb{Z})$-scissors congruence in rational polytopes. In *Integer points in polyhedra—geometry, number theory, representation theory, algebra, optimization, statistics*, volume 452 of *Contemporary Mathematics*, pages 115–122. American Mathematical Society, Providence, RI, 2008. doi:10.1090/conm/452/08777.

[12] Martin Henk and Eva Linke. Note on the coefficients of rational Ehrhart quasi-polynomials of Minkowski-sums. *Online Journal of Analytic Combinatorics*, (10):12, 2015.

[13] Eva Linke. *Ehrhart polynomials, successive minima, and an Ehrhart theory for rational dilates of a rational polytope.* PhD thesis, Otto-von-Guericke-Universität Magdeburg, 2011.

[14] Eva Linke. Rational Ehrhart quasi-polynomials. *Journal of Combinatorial Theory, Series A*, 118(7):1966–1978, 2011. doi:10.1016/j.jcta.2011.03.007.

[15] Michael Spivak. *Calculus on Manifolds: A Modern Approach to Classical Theorems of Advanced Calculus.* W. A. Benjamin, 1965.

[16] Richard Peter Stanley. Two poset polytopes. *Discrete & Computational Geometry*, 1(1):9–23, 1986.