Rational Generating Functions and Lattice Point Sets

by

Kevin M. Woods

A dissertation submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
(Mathematics)
in The University of Michigan
2004

Doctoral Committee:

Professor Alexander Barvinok, Chair
Professor Richard Canary
Professor Sergey Fomin
Professor John Stembridge
Assistant Professor Satyanarayana Lokam

ACKNOWLEDGEMENTS

My thanks to the many people whose thoughts have contributed to this thesis and to my mathematical development, including Imre Bárány, Jesus De Loera, Ravi Kannan, Bernd Sturmfels, and Rekha Thomas. In particular, my collaborations with Tyrrell McAllister and Herb Scarf have been tremendously invaluable.

Many thanks to my doctoral committee, especially John Stembridge for his careful reading of this thesis. I am grateful to my fellow graduate students with whom I have grown as a mathematician, including Greg Blekherman, Long Dao, Tom Fiore, Bart Kastermans, and Han Peters.

I am forever indebted to the many people who have encouraged me in all of my pursuits, as a child, as an undergraduate at Wake Forest University, and as a graduate student. Foremost of these are my wife, Angela Roles, and parents, John and Carol Woods. Most of all, I am deeply grateful to my advisor, Alexander Barvinok, for his guidance and insight.

PREFACE

We will be interested in subsets of $\mathbb{Z}^k$ that may be very large and may seem to have quite complicated structure. A motivating example will be the set S of nonnegative integer combinations of given positive coprime integers $a_1, a_2, \ldots, a_d$. For example, if $d = 2$, $a_1 = 3$ and $a_2 = 7$, we have

$$S = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\},$$

and there is obviously some structure here (e.g., all sufficiently large integers are in the set), though it is hard to say exactly what that structure is. We will give one answer: the set can be encoded as a rational generating function (and a short one, at that).

More generally, the sets we will be interested in are projections of the set of integer points in a polytope. We will show that these sets can all be encoded as short rational generating functions. In addition, we can manipulate these functions to give us information about the set. For example, for the set S above, we can determine the number of integers not in S and the largest integer not in S. We will attack these questions from an algorithmic perspective: how can we answer them quickly?

In Chapter I, we define the relevant concepts (generating functions, polynomial time algorithms, etc.), state the Projection Theorem (Theorem 1.1.15), discuss previously known tools for finding and manipulating generating functions, and give

background information on the neighborhood complex (which will become important in Chapter IV). In Chapter II, we will prove the Projection Theorem (Theorem 1.1.15). In Chapter III, we examine several applications of Theorem 1.1.15, namely the Frobenius problem, Hilbert series for monomial ideals, neighbors and the neighborhood complex, Hilbert bases of cones, and aspects of algebraic integer programming. In Chapter IV, we examine the connection between generating functions and the neighborhood complex, and we consider possibilities for improving the algorithm for Theorem 1.1.15. In Chapter V, we examine the relation of these generating functions to logic, and in particular, we will define and discuss the Presburger arithmetic.

This dissertation is organized into chapters and each chapter into sections. Within a section, subheadings delineate important concepts. Subheadings, theorems, figures, etc., will all be numbered together within each section. For example, in Chapter 3, Section 2, Theorem 3.2.5 might follow Figure 3.2.4.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS . . . . . **ii**

PREFACE . . . . . **iii**

LIST OF FIGURES . . . . . **vii**

CHAPTER

I. Introduction and Background 1

1.1 Introduction 1
1.2 Rational Generating Functions 10
1.3 Neighbors and the Neighborhood Complex 21

II. The Projection Theorem 30

2.1 Outline 30
2.2 Lattice Width and Flatness Directions 36
2.3 Partitioning 41
2.4 Proof of Theorem 1.1.15 46

III. Applications 49

3.1 The Frobenius Problem 49
3.2 Hilbert Series for Monomial Ideals 52
3.3 Neighbors and Neighborhood Complexes 55
3.4 Hilbert Bases 57
3.5 Algebraic Integer Programming 61

IV. The Neighborhood Complex and Generating Functions 72

4.1 Introduction and Example 73
4.2 The General Case 78
4.3 The Euler Characteristic 80
4.4 Proof of Theorem 4.2.1 84
4.5 Examples 86
4.6 The Non-generic Case 92

V. Presburger Arithmetic 94

5.1 Presburger Arithmetic and Rational Generating Functions 95
5.2 Complexity and Presburger Arithmetic 99
5.3 Complexity, Presburger Arithmetic, and Rational Generating Functions . . . 103

BIBLIOGRAPHY **109**

LIST OF FIGURES

Figure

1.1.9 Example 1.1.8, triangle with vertices $(0,0)$, $(N,0)$, and (N,N) 7

1.1.10 Example 1.1.13, P is a triangle and $T(x,y) = x$ 7

1.1.11 Example 1.1.14 with $N = 3$, P is the parallelogram with vertices $(0, \pm\frac{1}{4})$ and $(6, 3 \pm \frac{1}{4})$, and $T(x,y) = x$ 8

1.2.4 Example of cone(P, v) 12

1.2.5 A unimodular cone, K 13

1.2.6 Triangulation of K into (a) unimodular cones and (b) signed unimodular cones . . 14

1.3.2 In Example 1.3.3, edges of $C(A)$ include (a) $\{(0,0),(0,1)\}$ and (b) $\{(0,0),(1,0)\}$. 22

1.3.8 Example 1.3.7, the neighborhood complex when $d = 2, n = 3$ 24

2.1.1 Example 2.1.2, $T(x,y) = (x+y, x-y)$, (a) $Q = P \cap \mathbb{Z}^2$ and (b) $S = T(Q)$ 31

2.1.4 Example 2.1.3, $T(x,y) = x$, (a) $\hat{S}$ and $T(\hat{S})$ and (b) S' and $T(S')$ 32

2.1.6 Example 2.1.5, for $\sigma = 2$ and $\pi(x,y) = x$, (a) $\hat{S}$ and $\pi(\hat{S})$, (b) a gap that doesn't appear in $\hat{S}$, (c) $\hat{S} \setminus (\hat{S}+1)$, and (d) $S' = \hat{S} \setminus (\hat{S}+1) \setminus (\hat{S}+2)$ and $\pi(S')$ 34

2.1.8 Example 2.1.7, $P = \text{conv}\{(5,0,\pm 5),(5,\pm 5,0)\}$, $T(x,y,z) = x$ 36

2.2.1 Convex B such that $B \cap \mathbb{Z}^2 = \emptyset$ 37

2.2.5 Illustration of Lemma 2.2.4 with $c = (0,1)$ 39

3.4.1 Example 3.4.2, Hilbert basis of cone K generated by $(N,1)$ and $(1,N)$ 58

3.4.3 Q, such that $Q \cap \mathbb{Z}^2 = Z \cap \mathbb{Z}^2 \setminus \{0\}$ 59

3.5.1 $\mathcal{N}$ for Example 3.5.2 62

3.5.7 An example of (a) Q_u and (b) $Q_u^{\bar{\tau}}$ 68

4.1.2 Neighborhood complex, C, for $T(x,y) = 2x + 5y$ 74

4.1.3 The complexes C_a 75

4.1.5 Bijection between integer points in Q and edges in the C_a 76

4.1.6 Example 4.1.7, $T(x, y, z) = 3x + 4y + 5z$, (a) C, (b) C_{15}, (c) C_{20}, (d) C_{25} 77

4.3.4 Example 4.3.6, P_1, with $X = \{-2, -1, 0, 1, 2\}$ 82

4.5.1 $Q_{\{0\}} = P$ and $Q_{\{0,1\}}$ in Example 4.5.2 86

4.5.5 $\bar{C}$ for $k = 1, d = 3$ in Example 4.5.7 89

CHAPTER I

Introduction and Background

1.1 Introduction

We would like to answer questions about certain interesting subsets of $\mathbb{Z}^k$, for some k. Let us start with an example.

Let $a_1, a_2, \ldots, a_d$ be positive coprime integers, and let

$$S = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d : \ \lambda_i \in \mathbb{Z}_{\geq 0} \text{ for all } i\}$$

be the set of all nonnegative integer combinations of $a_1, a_2, \ldots, a_d$. In other words, S is the additive semigroup (with zero) generated by $a_1, a_2, \ldots, a_d$. It is easy to see that all sufficiently large integers are in S. Sylvester and Frobenius asked several questions about this set. How many positive integers are not in S? What is the largest integer not in S? The answer to the latter question is called the *Frobenius number*.

Example 1.1.1. Let $d = 2$, and $a_1 = 3, a_2 = 7$. Then

$$S = \{0, 3, 6, 7, 9, 10, 12, 13, 14, \ldots\},$$

the number of positive integers not in S is 6, and the Frobenius number is 11.

We'd also like to say something about the structure of the set S.

We will examine these questions from an algorithmic viewpoint. In particular we will show that there is a quick algorithm which, given $a_1, a_2, \ldots, a_d$, answers these questions (we will shortly define "quick" precisely). For the particular question of finding the Frobenius number, a quick algorithm has already been found [Kan92], but for other questions no quick algorithm was previously known.

1.1.2 Generating functions

Our tool will be *generating functions*. For any subset $S \subset \mathbb{Z}_{\geq 0}$, we can define the generating function

$$f(S;x) = \sum_{s \in S} x^s.$$

This power series converges for x with $|x| < 1$, so we can talk about this function with impunity. We would like to find a short formula for $f(S;x)$.

In Example 1.1.1, we have $f(S;x) = 1 + x^3 + x^6 + x^7 + \cdots$. Of course this is far from a "short" formula: it is infinite! An obvious way to improve on this would be to write

$$f(S;x) = 1 + x^3 + x^6 + x^7 + x^9 + x^{10} + \frac{x^{12}}{1-x}.$$

We can do much better than this, however.

Indeed, for coprime a_1 and a_2, let S be the additive semigroup generated by a_1 and a_2, and let us examine $f(S;x)(1-x^{a_1})$. We have

$$\begin{aligned} f(S;x)(1-x^{a_1}) &= f(S;x) - x^{a_1} f(S;x) \\ &= \sum_{s \in S} x^s - \sum_{s \in S} x^{s+a_1} \\ &= \sum_{s \in S} x^s - \sum_{s-a_1 \in S} x^s \end{aligned}$$

$$= \sum_{\substack{s \in S, \\ s - a_1 \notin S}} x^s$$

$$= 1 + x^{a_2} + x^{2a_2} + \cdots + x^{(a_1-1)a_2}$$

$$= \frac{1 - x^{a_1 a_2}}{1 - x^{a_1}}.$$

Therefore $f(S;x) = \frac{1-x^{a_1 a_2}}{(1-x^{a_1})(1-x^{a_2})}$. In Example 1.1.1, we get

$$f(S;x) = \frac{1 - x^{21}}{(1-x^3)(1-x^7)}.$$

This result demonstrates nicely the main goal of this dissertation: to show that large and seemingly complicated sets can often be encoded by short rational functions.

Example 1.1.3. For $d = 3$ we also get a nice formula, that there exist positive integers $p_1, p_2, \ldots, p_5$ (which are quickly computable from a_1, a_2, a_3) such that

$$f(S;x) = \frac{1 - x^{p_1} - x^{p_2} - x^{p_3} + x^{p_4} + x^{p_5}}{(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})}.$$

This fact was proved by G. Denham [Den03] using algebraic results of J. Herzog [Her70]. It can also be seen geometrically (see Example 4.5.7 or [SW03]).

For $d = 4$ and higher, one would hope that we could find a similar formula, a rational function with a (small) number of monomials in the numerator and with denominator $\prod_i (1 - x^{a_i})$. There are examples (see [SW86]), however, where writing $f(S;x)$ in this form would require $\sqrt{t}$ monomials in the numerator, where $t = \min\{a_1, a_2, a_3, a_4\}$. This is "too many."

1.1.4 Quick algorithms

Let us be more precise. We define the *input size* of an algorithm to be the number of bits needed to encode the input into binary (as if we were going to give it to a

computer as data). In particular, the input size of an integer a is approximately $1 + \log_2|a|$ (the number of digits needed to write a in binary), and the input size of $a_1, a_2, \ldots, a_d$ is approximately $\sum_i (1 + \log_2 a_i)$.

We would like to find a "quick" algorithm which takes $a_1, a_2, \ldots, a_d$ as input, and outputs $f(S; x)$ in some nice form. An algorithm is called *polynomial time* if the number of steps it takes is bounded by a certain polynomial in the input size. Proving that an algorithm is polynomial time is generally regarded as proving that it is "quick," at least theoretically. See [Pap94] for general background on algorithms and computational complexity.

In general, this problem of finding a quick algorithm to compute $f(S; x)$ is hopeless. In fact, the easier problem of finding the largest integer not in S is itself NP-hard [RA96] (which means, basically, that there is very little hope that a polynomial time algorithm exists, see [Pap94] for a definition and more details). Rather than despair, we look at a subproblem and try to find a quick algorithm for that. A natural subproblem to examine is that of finding $f(S; x)$ for a given fixed d, where d is the number of generators of S. In Section 3.1, we will prove the following theorem which states that, for fixed d, there is a quick algorithm that finds $f(S; x)$, and furthermore, we can use $f(S; x)$ to quickly answer questions about S. We should conceptualize "for fixed d" to mean that, for small d, the algorithm is "quick," but as d increases, the algorithm rapidly slows down. This theorem originally appeared in [BW03].

Theorem 1.1.5. *Let d be fixed. Then there exists a constant $s = s(d)$ and a polynomial time algorithm which, given $a_1, a_2, \ldots, a_d$, computes $f(S; x)$ in the form*

$$f(S; x) = \sum_{i \in I} \alpha_i \frac{x^{p_i}}{(1 - x^{b_{i1}}) \cdots (1 - x^{b_{is}})},$$

where $\alpha_i \in \mathbb{Q}$, $p_i \in \mathbb{Z}$, and $b_{ij} \in \mathbb{Z} \setminus \{0\}$.

Furthermore, there is a polynomial time algorithm that computes the number of integers not in S and computes the largest integer not in S.

In particular, the number $|I|$ of fractions in the sum must be bounded by a polynomial in the input size, $\sum_i (1+\log_2 a_i)$ (otherwise, the algorithm could not even output $f(S;x)$ in polynomial time). This is much better than the $t = \min\{a_1, a_2, a_3, a_4\}$ fractions that might be required if we force all the denominators to be $\prod_i (1 - \mathbf{x}^{a_i})$, as t is exponential in the input size. This theorem shows that these complicated sets can be encoded by short rational functions.

Theorem 1.1.5 will follow from a general theorem which says that we may quickly find generating functions for certain sets of integer points. In particular, the sets we will be interested in are *projections of the set of integer points in a polytope* (some examples will follow shortly).

Let $S \subset \mathbb{Z}^k$ be a set of integer points, and define the *generating function*

$$f(S;\mathbf{x}) = \sum_{s=(s_1,\ldots,s_k)\in S} x_1^{s_1} x_2^{s_2} \cdots x_k^{s_k} = \sum_{s\in S} \mathbf{x}^s.$$

We must be careful that this generating function converges absolutely on some neighborhood in $\mathbb{C}^k$. For the most part, S will be a finite set, so this is not a problem, as $f(S;\mathbf{x})$ will be a Laurent polynomial. Our goal will be to quickly write $f(S;\mathbf{x})$ as a short rational generating function, as in Theorem 1.1.5.

1.1.6 Integer points in polyhedra

Let us first consider S, where S is the set of integer points in a polyhedron. Let $c_1, c_2, \ldots, c_n \in \mathbb{Z}^d$ be integer vectors and let $b_1, b_2, \ldots, b_n \in \mathbb{Z}$ be integers. Then we

can define a *rational polyhedron*, P, by

$$P = \left\{ x \in \mathbb{R}^d : \ \langle c_i, x \rangle \leq b_i \text{ for all } i \right\},$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^d$. We will be inputting P into an algorithm, so we must define its input size (the number of bits needed to encode P), which is roughly

$$nd + \sum_i \log_2 |b_i| + \sum_{i,j} \log_2 |c_{ij}|,$$

where $c_i = (c_{i1}, c_{i2}, \ldots, c_{id})$. In [BP99] it is proved that for fixed d, if P is a rational polyhedron not containing straight lines and $S = P \cap \mathbb{Z}^d$, then we can calculate $f(S; \mathbf{x})$ quickly as a short rational function.

Example 1.1.7. If $P = [0, N]$, then $S = P \cap \mathbb{Z} = \{0, 1, 2, \ldots, N\}$, and

$$f(S; x) = 1 + x + x^2 + \cdots + x^N = \frac{1 - x^{N+1}}{1 - x}.$$

Example 1.1.8. For a more complicated example, let $P \subset \mathbb{R}^2$ be the triangle with vertices $(0, 0)$, $(N, 0)$, and (N, N) (See Figure 1.1.9). Then

$$\begin{aligned} f(P \cap \mathbb{Z}^2; x, y) &= 1 + (x + xy) + (x^2 + x^2 y + x^2 y^2) + \cdots + (x^N + x^N y + \cdots + x^N y^N) \\ &= \frac{1 - y}{1 - y} + \frac{x - xy^2}{1 - y} + \frac{x^2 - x^2 y^3}{1 - y} + \cdots + \frac{x^N - x^N y^{N+1}}{1 - y} \\ &= \frac{1 + x + x^2 + \cdots + x^N}{1 - y} - \frac{y + xy^2 + x^2 y^3 + \cdots + x^N y^{N+1}}{1 - y} \\ &= \frac{1 - x^{N+1}}{(1 - x)(1 - y)} - \frac{y - x^{N+1} y^{N+2}}{(1 - xy)(1 - y)}. \end{aligned}$$

Again $f(S; \mathbf{x})$ can be written as a short rational generating function.

See Theorem 1.2.3 for a more precise statement of the general theorem and a sketch of a proof.

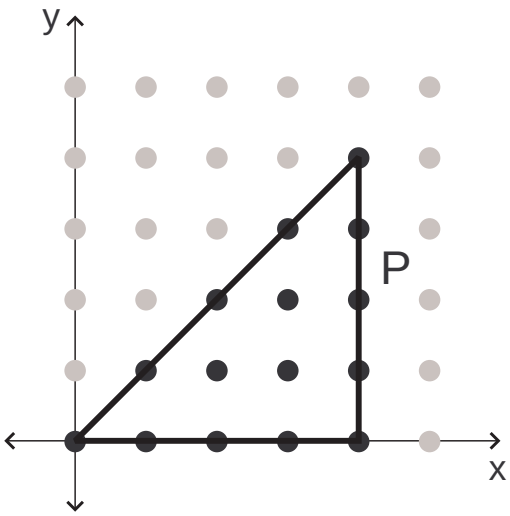


Figure 1.1.9: Example 1.1.8, triangle with vertices $(0,0)$, $(N,0)$, and (N,N)

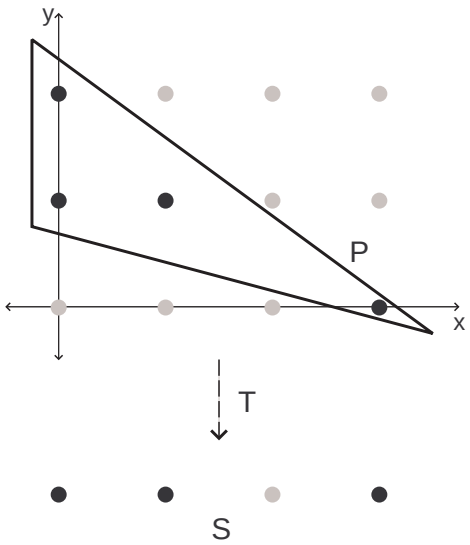


Figure 1.1.10: Example 1.1.13, P is a triangle and $T(x,y) = x$

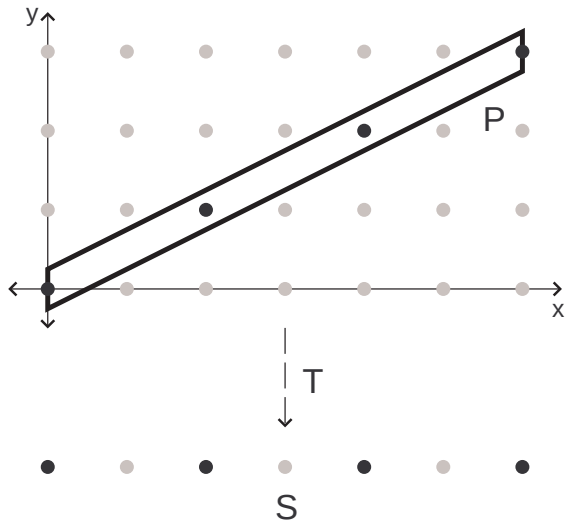


Figure 1.1.11: Example 1.1.14 with $N = 3$, P is the parallelogram with vertices $(0, \pm\frac{1}{4})$ and $(6, 3 \pm \frac{1}{4})$, and $T(x, y) = x$

1.1.12 Projections

Here we would like to find the generating function for the *projection* of the set of integer points in a rational polytope (that is, a *bounded* polyhedron). Let $T : \mathbb{R}^d \to \mathbb{R}^k$ be a linear transformation such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$. We will examine the set $S = T(P \cap \mathbb{Z}^d)$.

Example 1.1.13. Let P be the triangle pictured in Figure 1.1.10, and let $T : \mathbb{R}^2 \to \mathbb{R}$ be defined by $T(x, y) = x$. Then $S = T(P \cap \mathbb{Z}^2) = \{0, 1, 3\}$, and $f(S; x) = 1 + x + x^3$.

Example 1.1.14. For a more complicated example, let $P \subset \mathbb{R}^2$ be the parallelogram with vertices $(0, \pm\frac{1}{4})$ and $(2N, N \pm \frac{1}{4})$, and let $T : \mathbb{R}^2 \to \mathbb{R}$ be defined by $T(x, y) = x$ (See Figure 1.1.11, where $N = 3$). Then

$$f(S; x) = 1 + x^2 + x^4 + \cdots + x^{2N} = \frac{1 - x^{2N+2}}{1 - x^2}.$$

Again, in this case, $f(S; \mathbf{x})$ can be written as a short rational generating function.

In general, we can define the input size of T as

$$kd + \sum_{i,j} \log_2 |t_{ij}|,$$

where (t_{ij}) is the matrix of integers representing T. In Chapter II, we will prove the following theorem, which says that we can always calculate $f(S;\mathbf{x})$ as a short rational function, where $S = T(P \cap \mathbb{Z}^d)$. This theorem also originally appeared in [BW03].

Theorem 1.1.15. *Let d be fixed. Then there exists a constant $s = s(d)$ and a polynomial time algorithm which, given a rational polytope $P \subset \mathbb{R}^d$ and a linear transformation $T : \mathbb{R}^d \to \mathbb{R}^k$ such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$, computes $f(S;\mathbf{x})$ in the form*

$$f(S;\mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1-\mathbf{x}^{b_{i1}}) \cdots (1-\mathbf{x}^{b_{is}})},$$

where $S = T(P \cap \mathbb{Z}^d)$, $\alpha_i \in \mathbb{Q}$, $p_i \in \mathbb{Z}$, and $b_{ij} \in \mathbb{Z} \setminus \{0\}$.

As in Theorem 1.1.5, the number $|I|$ of fractions in the sum must be bounded by a polynomial in the input size. In Section 3.1, we will prove that Theorem 1.1.5 follows from Theorem 1.1.15. To give a flavor of the proof, note that the Frobenius set S can be written as $T(P \cap \mathbb{Z}^d)$, where P is the (unbounded) polyhedron

$$P = \left\{(\lambda_1, \lambda_2, \ldots, \lambda_d) \in \mathbb{R}^d : \ \lambda_i \geq 0 \text{ for all } i\right\}$$

and $T : \mathbb{R}^d \to \mathbb{R}$ is defined by

$$T(\lambda_1, \lambda_2, \ldots, \lambda_d) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d.$$

We cannot directly apply Theorem 1.1.15, as P is not bounded, but in Section 3.1 we will show how to apply it indirectly.

In Section 1.2, we will give the needed background on rational generating functions. In Section 1.3, we examine the concept of neighbors and the neighborhood complex associated to a matrix. This concept will not be needed for a proof of Theorem 1.1.15, but it will be central to Chapter IV.

In Chapter II, we will prove Theorem 1.1.15. In Chapter III, we examine several applications of Theorem 1.1.15, including the Frobenius problem. In Chapter IV, we examine the connection between generating functions and the neighborhood complex, and we consider possibilities for improving the algorithm from Theorem 1.1.15. In Chapter V, we examine the relation of these generating functions to logic, and in particular, we will define and discuss the Presburger arithmetic.

1.2 Rational Generating Functions

In this section, we discuss several useful results related to generating functions of the type

$$f(\mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1-\mathbf{x}^{a_{i1}})(1-\mathbf{x}^{a_{i2}})\cdots(1-\mathbf{x}^{a_{ik_i}})}, \tag{1.2.1}$$

where $\mathbf{x} \in \mathbb{C}^d$, $\alpha_i \in \mathbb{Q}$, $p_i, a_{ij} \in \mathbb{Z}^d$, and $a_{ij} \neq 0$ for all i, j. In general, we will assume that d is fixed and that there is a fixed upper bound, k, on the k_i. Theorem 1.2.3 will give us a nice collection of sets (the integer points in polyhedra) for which we can find a short rational generating function. A complete proof is given in [BP99]. The remaining theorems in this chapter give us operations which we can perform on generating functions. Most of these results were sketched in [BP99] and proved completely in [BW03].

1.2.2 Integer points in polyhedra, revisited

Suppose that $P \subset \mathbb{R}^d$ is a rational polyhedron, let $S = P \cap \mathbb{Z}^d$, and let

$$f(S; \mathbf{x}) = \sum_{a \in S} \mathbf{x}^a.$$

If P contains no straight lines, then $f(S; \mathbf{x})$ converges on a neighborhood $U \subset \mathbb{C}^d$. If P did contain straight lines, $f(S; \mathbf{x})$ as defined would not converge on any neighborhood in $\mathbb{C}^d$ (unless $P \cap \mathbb{Z}^d = \emptyset$), and it is convenient to define $f(S; \mathbf{x}) \equiv 0$. The following result states that, for fixed d, $f(S; \mathbf{x})$ can be found quickly as a short rational function.

Theorem 1.2.3. *(Theorem 4.4 of [BP99]) Fix d. Then there exists a polynomial time algorithm which, for any given rational polyhedron $P \subset \mathbb{R}^d$, computes $f(P \cap \mathbb{Z}^d; \mathbf{x})$ in the form*

$$f(P \cap \mathbb{Z}^d; \mathbf{x}) = \sum_{i \in I} \epsilon_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}})(1 - \mathbf{x}^{a_{i2}}) \cdots (1 - \mathbf{x}^{a_{id}})},$$

where $\epsilon_i \in \{-1, +1\}$, $p_i, a_{ij} \in \mathbb{Z}^d$, and $a_{ij} \neq 0$ for all i, j. In fact, for each i, $a_{i1}, a_{i2}, \ldots, a_{id}$ is a basis of $\mathbb{Z}^d$.

Sketch of Proof: The general idea is to express $f(P \cap \mathbb{Z}^d; \mathbf{x})$ in terms of generating functions for simpler sets, until the sets are simple enough to find the generating function directly. Given a vertex v of P, let $\text{cone}(P, v)$ be the *supporting* or *tangent cone* to P at v. This is the smallest cone with vertex v which contains P (see Figure 1.2.4). To be precise, if $P = \left\{x \in \mathbb{R}^d : \langle a_i, x \rangle \leq b_i \text{ for all } i \in I\right\}$, for some $a_i \in \mathbb{R}^d, b_i \in \mathbb{R}$, and I a finite index set, then let $I_v = \{i \in I : \langle a_i, v \rangle = b_i\}$, and define

$$\text{cone}(P, v) = \left\{x \in \mathbb{R}^d : \langle a_i, x \rangle \leq b_i \text{ for } i \in I_v\right\}.$$

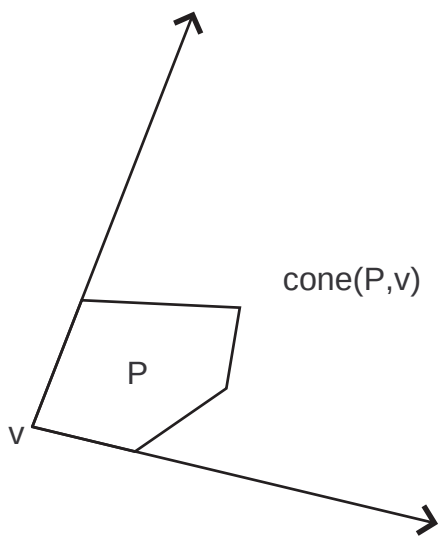


Figure 1.2.4: Example of cone(P, v)

Then Brion's Theorem ([Bri88], or see Section VIII.4 of [Bar02]) states that

$$f(P \cap \mathbb{Z}^d; \mathbf{x}) = \sum_{v \text{ a vertex of P}} f\big(\text{cone}(P, v) \cap \mathbb{Z}^d; \mathbf{x}\big).$$

Now we have reduced to the case of finding the generating function for a cone. We may triangulate a given cone(P, v) into simplicial cones in polynomial time, and then compute the generating function of each piece of the triangulation separately, so we only need to be able to find the generating function for cones K which are simplicial.

One particular type of simplicial cone for which it is easy to find the generating function is a *unimodular* cone, that is, a cone

$$K = \big\{x \in \mathbb{R}^d : \ \langle a_i, x\rangle \leq b_i \text{ for } i = 1, 2, \ldots, d\big\}$$

such that the $a_i \in \mathbb{Z}^d$ form a basis for $\mathbb{Z}^d$, and such that $b_i \in \mathbb{Q}$. Indeed, if $u_1, u_2, \ldots, u_d$ is the negative dual basis of $\mathbb{Z}^d$ so that $\langle u_i, a_j\rangle = -\delta_{ij}$, then

$$f(K \cap \mathbb{Z}^d; \mathbf{x}) = \mathbf{x}^v \prod_{i=1}^{d} \frac{1}{1 - \mathbf{x}^{u_i}},$$

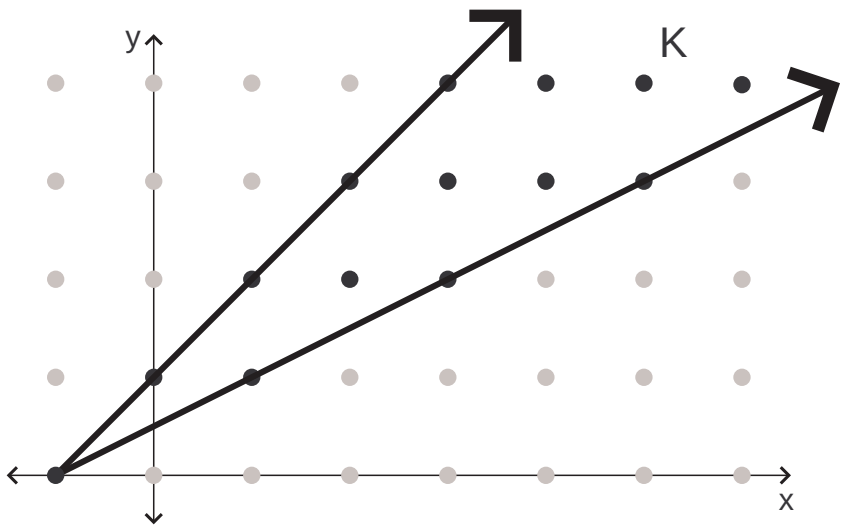


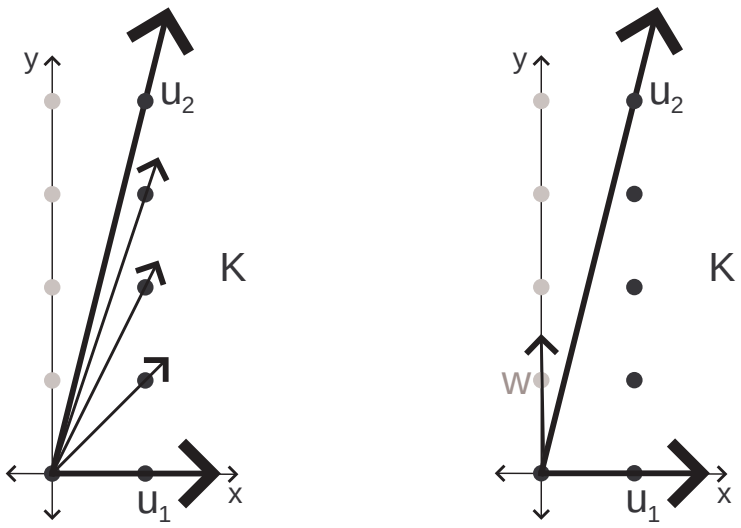
Figure 1.2.5: A unimodular cone, K

where $v = -\sum \lfloor b_i \rfloor u_i$ (see Lemma 4.1 of [BP99]). For example, if K is the unimodular cone K pictured in Figure 1.2.5, then $v = (-1, 0)$, $u_1 = (2, 1)$, and $u_2 = (1, 1)$, and so

$$\begin{aligned} f(K \cap \mathbb{Z}^d; x, y) &= x^{-1}(1 + x^2y + x^2y^4 + \cdots)(1 + xy + x^2y^2 + \cdots) \\ &= \frac{x^{-1}}{(1 - x^2y)(1 - xy)}. \end{aligned}$$

It is too much to hope that a simplicial cone could be divided into a polynomial number of unimodular cones, however. For example, if $K = \text{co}\{u_1, u_2\} \subset \mathbb{R}^2$ is the cone generated by the vectors $u_1 = (1, 0)$ and $u_2 = (1, n)$ (see Figure 1.2.6(a)), then a triangulation into unimodular cones would need n of them, the cone generated by $(1, i-1)$ and $(1, i)$ for each $1 \leq i \leq n$. This is exponential in the input size $O(\log n)$.

The key step in Barvinok's proof is showing that K can be represented as a short *signed* sum of unimodular cones. To be more precise, if $A \subset \mathbb{R}^d$, define the indicator



(a) **(b)**

Figure 1.2.6: Triangulation of K into (a) unimodular cones and (b) signed unimodular cones

function $[A] : \mathbb{R}^d \to \mathbb{R}$ by

$$[A](x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}.$$

Then there exists polynomially many unimodular cones $K_1, K_2, \ldots, K_n$ such that

$$[K] = \sum_{i=1}^{n} \pm [K_i].$$

For instance, in our example, if $w = (0, 1)$, then

$$[K] = [\text{co}\{w, u_1\}] - [\text{co}\{w, u_2\}] + [\text{co}\{u_2\}]$$

(see Figure 1.2.6(b)). The proof follows. □

The algorithm that we sketched has been implemented successfully, using the program LattE [DLHTY04].

1.2.7 Specialization (monomial substitution)

Now that we have a nice collection of generating functions that we can find, we would like to be able to manipulate them and to use them to answer questions

about the set. For example, if S is a finite set, and we have computed $f(S;\mathbf{x})$, then we would like to be able to compute $|S|$. This can be accomplished by specializing $f(S;\mathbf{x})$ at $(x_1, x_2, \ldots, x_d) = (1, 1, \ldots, 1)$. This is not as easy, however, as substituting $(1, 1, \ldots, 1)$ for $\mathbf{x}$, because $(1, 1, \ldots, 1)$ may be a pole of some of the fractions in the rational generating function as given. For example, if $S = \{0, 1, 2, \ldots, N\}$, then

$$f(S;x) = \frac{1}{1-x} - \frac{x^{N+1}}{1-x},$$

and 1 is a pole of the fractions.

Nevertheless, $(1, 1, \ldots, 1)$ is a regular point of $f(S;\mathbf{x})$, which is actually a polynomial (since S is finite), and so this specialization should be well-defined. This was first done in [Bar94] to count the number of integer points in a polyhedron.

More generally, let $f(\mathbf{x})$, with $\mathbf{x} \in \mathbb{C}^d$, be a rational function in the form (1.2.1), and let $l_1, l_2, \ldots, l_d \in \mathbb{Z}^n$ be integer vectors. These vectors define the *monomial map* $\phi : \mathbb{C}^n \to \mathbb{C}^d$ given by

$$\mathbf{z} = (z_1, z_2, \ldots, z_n) \mapsto (\mathbf{z}^{l_1}, \mathbf{z}^{l_2}, \ldots, \mathbf{z}^{l_d}).$$

If the image of ϕ does not lie entirely in the poles of $f(\mathbf{x})$, we can define the function $g : \mathbb{C}^n \to \mathbb{C}$ by

$$g(\mathbf{z}) = f\big(\phi(\mathbf{z})\big),$$

which is regular at almost every point in $\mathbb{C}^n$. Then $g(\mathbf{z})$ is $f(\mathbf{x})$ specialized at $x_i = \mathbf{z}^{l_i}$. In particular, if $l_i = 0$ for all i, then $g(\mathbf{z})$ is $f(1, 1, \ldots, 1)$. We have the following theorem, which states that, given $f(\mathbf{x})$ as a short rational generating function, we can find $g(\mathbf{z})$ quickly.

Theorem 1.2.8. *(Theorem 2.6 of [BW03]) Let us fix k, an upper bound on the k_i in (1.2.1). Then there exists a polynomial time algorithm, which, given $f(\mathbf{x})$ in the*

form (1.2.1) and a monomial map $\phi : \mathbb{C}^n \to \mathbb{C}^d$ *such that the image of* ϕ *does not lie entirely in the poles of* $f(\mathbf{x})$*, computes* $g(\mathbf{z}) = f\big(\phi(\mathbf{z})\big)$ *in the form*

$$g(\mathbf{z}) = \sum_{i \in I'} \beta_i \frac{\mathbf{z}^{q_i}}{(1 - \mathbf{z}^{b_{i1}})(1 - \mathbf{z}^{b_{i2}}) \cdots (1 - \mathbf{z}^{b_{is}})},$$

where $s \leq k$*,* $\beta_i \in \mathbb{Q}$*,* $q_i, b_{ij} \in \mathbb{Z}^n$*, and* $b_{ij} \neq 0$ *for all* i, j*.*

Sketch of proof: Again, we cannot simply substitute $\phi(\mathbf{z})$ in for $\mathbf{x}$, because $\phi(\mathbf{z})$, for generic $\mathbf{z}$, might be a pole of some of the fractions in the sum and yet be a regular point of $f(\mathbf{x})$. To solve this problem, we first change variables. Let $\mathbf{e}^s = (e^{s_1}, e^{s_2}, \ldots, e^{s_l})$ where $s = (s_1, s_2, \ldots, s_l)$, and define $F : \mathbb{C}^d \to \mathbb{C}$ and $G : \mathbb{C}^n \to \mathbb{C}$ so that

$$F(s) = f(\mathbf{e}^s) \text{ and } G(t) = g(\mathbf{e}^t).$$

In particular,

$$F(s) = \sum_{i \in I} \alpha_i \frac{\exp\langle s, p_i \rangle}{\big(1 - \exp\langle s, a_{i1} \rangle\big)\big(1 - \exp\langle s, a_{i2} \rangle\big) \cdots \big(1 - \exp\langle s, a_{ik_i} \rangle\big)}.$$

Let $\Phi : \mathbb{C}^n \to \mathbb{C}^d$ be defined by $\Phi(t) = \big(\langle t, l_1 \rangle, \langle t, l_2 \rangle, \ldots, \langle t, l_d \rangle\big)$ so that

$$G(t) = F\big(\Phi(t)\big).$$

Let $L \subset \mathbb{C}^d$ be the subspace which is the image of $\mathbb{C}^n$ under the linear map Φ. If we could rewrite $F(s)$ as

$$F(s) = \sum_{i \in I'} \beta_i \frac{\exp\langle s, q_i \rangle}{\big(1 - \exp\langle s, b_{i1} \rangle\big)\big(1 - \exp\langle s, b_{i2} \rangle\big) \cdots \big(1 - \exp\langle s, b_{ik_i} \rangle\big)}$$

in such a way that L was not orthogonal to any of the b_{ij}, then we would be allowed to simply substitute $\Phi(t)$ for s to compute $G(t) = F\big(\Phi(t)\big)$ (and then we could retrieve $g(\mathbf{z})$).

We do that as follows. Choose $v \in \mathbb{R}^d$ such that $\langle v, a_{ij} \rangle \neq 0$ for all i, j. Fix a regular point $s \in L$ of $F(s)$. We consider the function $F(s + \tau v)$ as a function of

$\tau \in \mathbb{C}$. We have that $F(s+\tau v)$ is analytic in a neighborhood of $\tau = 0$, and we would like to compute the constant term (in τ), which is exactly $F(s)$. We do this for each fraction in the sum.

Take a particular fraction in the sum,

$$h(\tau) = \frac{\exp\langle s+\tau v, p\rangle}{\big(1-\exp\langle s+\tau v, a_1\rangle\big)\big(1-\exp\langle s+\tau v, a_2\rangle\big)\cdots\big(1-\exp\langle s+\tau v, a_k\rangle\big)},$$

where $p, a_i \in \mathbb{Z}^d$. Assume, without loss of generality, that $a_1, a_2, \ldots, a_l$ are orthogonal to L for some l with $0 \le l \le k$ (these are the a_i we must do something about), and $a_{l+1}, a_{l+2}, \ldots, a_k$ are not orthogonal to L. In particular, $\langle s, a_i\rangle = 0$ for $1 \le i \le l$. Then

$$\tau^l h(\tau) = \exp\langle s,p\rangle \exp\{\tau\langle v,p\rangle\} \prod_{i=1}^{l} \frac{\tau}{1-\exp\{\tau\langle v,a_i\rangle\}} \times \prod_{i=l+1}^{k} \frac{1}{1-\exp\langle s+\tau v, a_i\rangle}.$$

Our goal, then, is to compute the coefficient of τ^l in the right hand side, which we can do by carefully writing the two products as power series expansions. The proof follows. □

1.2.9 Boolean combinations

Now we turn to another operation that we can perform on short rational generating functions. Let $S_1, S_2, \ldots, S_m \in \mathbb{Z}^d$ be finite sets. We say that S is a *Boolean combination* of $S_1, S_2, \ldots, S_m$ if it can be obtained from the S_i by taking intersections, unions, and set subtractions. Suppose we already know the rational generating functions $f(S_i; \mathbf{x})$ for each i. The following theorem states that we can find (quickly) the generating function for the Boolean combination S, using only the generating functions $f(S_i; \mathbf{x})$ (and no other information about these sets S_i). Note that it is very

important that we fix m, the number of sets we are taking a Boolean combination of.

Theorem 1.2.10. *(Corollary 3.7 of [BW03]) Let us fix m and k (an upper bound on the number of binomials in the denominator of any fraction of any $f(S_i;\mathbf{x})$). Then there exists an $s = s(k,m)$ and a polynomial time algorithm, which, for any finite sets $S_1, S_2, \ldots, S_m \subset \mathbb{Z}^d$ given by their generating functions $f(S_i;\mathbf{x})$ in the form (1.2.1) and any set $S \subset \mathbb{Z}^d$ defined as a Boolean combination of $S_1, S_2, \ldots, S_m$, computes $f(S;\mathbf{x})$ in the form*

$$f(S;\mathbf{x}) = \sum_{i \in I'} \gamma_i \frac{\mathbf{x}^{u_i}}{(1-\mathbf{x}^{v_{i1}})(1-\mathbf{x}^{v_{i2}})\cdots(1-x^{v_{is}})},$$

where $\gamma_i \in \mathbb{Q}$, $u_i, v_{ij} \in \mathbb{Z}^d$, and $v_{ij} \neq 0$ for all i, j.

Sketch of proof: We first discuss a binary operation on Laurent power series called the *Hadamard product*. Let $g_1(\mathbf{x})$ and $g_2(\mathbf{x})$ be Laurent power series given by

$$g_1(\mathbf{x}) = \sum_{m \in \mathbb{Z}^d} \alpha_m \mathbf{x}^m \text{ and } g_2(\mathbf{x}) = \sum_{m \in \mathbb{Z}^d} \beta_m \mathbf{x}^m.$$

Then the Hadamard product $g = g_1 \star g_2$ is defined to be the power series

$$g(\mathbf{x}) = \sum_{m \in \mathbb{Z}^d} \alpha_m \beta_m \mathbf{x}^m.$$

Note that if $S_1, S_2 \subset \mathbb{Z}^d$ and

$$g_1(\mathbf{x}) = \sum_{m \in S_1} \mathbf{x}^m \text{ and } g_2(\mathbf{x}) = \sum_{m \in S_2} \mathbf{x}^m,$$

then

$$(g_1 \star g_2)(\mathbf{x}) = \sum_{m \in S_1 \cap S_2} \mathbf{x}^m.$$

Therefore to compute the generating function for the intersection of two sets, we must compute the appropriate Hadamard product. Once we show we can compute

$f(S_1 \cap S_2; \mathbf{x})$ in polynomial time, then we use the facts that $f(S_1 \cup S_2; \mathbf{x}) = f(S_1; \mathbf{x}) + f(S_2; \mathbf{x}) - f(S_1 \cap S_2; \mathbf{x})$ and $f(S_1 \setminus S_2; \mathbf{x}) = f(S_1; \mathbf{x}) - f(S_1 \cap S_2; \mathbf{x})$ to finish the proof.

Note that we must be careful when talking about infinite Laurent power series expansions (and about Hadamard products) of rational functions. For example $\frac{1}{1-x}$ has two possible expansions as a Laurent power series,

$$1 + x + x^2 + x^3 + \cdots \text{ or } -x^{-1} - x^{-2} - x^{-3} - \cdots,$$

and these expansions converge on different neighborhoods in $\mathbb{C}$ (on $\|x\| < 1$ and $\|x\| > 1$, respectively). We must carefully expand $f(S_i; \mathbf{x})$ as Laurent power series which converge on a particular neighborhood, which we do as follows.

Suppose we have two *finite* sets S_1 and S_2, and we are given $f(S_1; \mathbf{x})$ and $f(S_2; \mathbf{x})$ as short rational generating functions

$$f(S_1; \mathbf{x}) = \sum_{i \in I_1} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}}) \cdots (1 - \mathbf{x}^{a_{ik}})} \text{ and}$$
$$f(S_2; \mathbf{x}) = \sum_{i \in I_2} \beta_i \frac{\mathbf{x}^{q_i}}{(1 - \mathbf{x}^{b_{i1}}) \cdots (1 - \mathbf{x}^{b_{ik}})}.$$

Let us choose a vector l such that $\langle l, a_{ij} \rangle, \langle l, b_{ij} \rangle \neq 0$. If $\langle l, a_{ij} \rangle > 0$ (and similarly for the b_{ij}), we may apply the identity

$$\frac{\mathbf{x}^p}{1 - \mathbf{x}^a} = -\frac{\mathbf{x}^{p-a}}{1 - \mathbf{x}^{-a}},$$

so that, without loss of generality $\langle l, a_{ij} \rangle, \langle l, b_{ij} \rangle < 0$ for all i, j. Then, if we expand $f(S_1; \mathbf{x})$ as a Laurent series convergent on a neighborhood of $(e^{l_1}, e^{l_2}, \ldots, e^{l_d})$ (and similarly for $f(S_2; \mathbf{x})$), we get

$$\sum_{i \in I_1} \alpha_i \sum_{\lambda_1, \ldots, \lambda_k \in \mathbb{Z}_{\geq 0}} \mathbf{x}^{p_i + \lambda_1 a_{i1} + \lambda_2 a_{i2} + \cdots + \lambda_k a_{ik}}.$$

This Laurent power series expansion is exactly $\sum_{m \in S_1} \mathbf{x}^m$.

Since the Hadamard product is bilinear,

$$f(S_1 \cap S_2; \mathbf{x}) = \sum_{i \in I_1, j \in I_2} \alpha_i \beta_j \left(\frac{\mathbf{x}^{p_i}}{(1-\mathbf{x}^{a_{i1}}) \cdots (1-\mathbf{x}^{a_{ik}})} \star \frac{\mathbf{x}^{q_j}}{(1-\mathbf{x}^{b_{j1}}) \cdots (1-\mathbf{x}^{b_{jk}})} \right).$$

The proof follows by the following lemma. □

Lemma 1.2.11. *Fix k (the maximum number of binomials in the denominators of the rational functions). Then there exists a polynomial time algorithm which, given $l \in \mathbb{Z}^d$ and functions*

$$g_1(\mathbf{x}) = \frac{\mathbf{x}^p}{(1-\mathbf{x}^{a_1}) \cdots (1-\mathbf{x}^{a_k})} \text{ and}$$
$$g_2(\mathbf{x}) = \frac{\mathbf{x}^q}{(1-\mathbf{x}^{b_1}) \cdots (1-\mathbf{x}^{b_k})}$$

such that $\langle l, a_i \rangle, \langle l, b_i \rangle < 0$, computes $g = g_1 \star g_2$ (where the Laurent power series are convergent on a neighborhood of $(e^{l_1}, e^{l_2}, \ldots, e^{l_d})$).

Sketch of proof: Let $P \subset \mathbb{R}^{2k}$ be a rational polyhedron defined by

$$P = \big\{(\xi_1, \ldots, \xi_{2k}) \in \mathbb{R}^{2k} : \; p + \xi_1 a_1 + \cdots + \xi_k a_k = q + \xi_{k+1} b_1 + \cdots + \xi_{2k} b_k \text{ and } \xi_i \geq 0 \text{ for all } i\big\}.$$

Then examining g_1 and g_2 as Laurent power series will yield that $g_1(\mathbf{x}) \star g_2(\mathbf{x})$ is

$$\mathbf{x}^p f(P \cap \mathbb{Z}^{2k}; \mathbf{z}), \text{ specialized at } z_1 = \mathbf{x}^{a_1}, \ldots, z_k = \mathbf{x}^{a_k}, z_{k+1} = 1, \ldots, z_{2k} = 1.$$

We use Theorems 1.2.3 and 1.2.8 to compute this. □

Note that if g and h are each a sum of N fractions with k binomials in the denominator, then $g \star h$ will be written as the sum of N^2 Hadamard products of fractions like the g_1 and g_2 in the statement of Lemma 1.2.11, and after taking the

Hadamard product, each fraction may now have $2k$ binomials in the denominator. These considerations make it vital that only a fixed number of boolean operations be performed in order to compute the generating function in polynomial time.

1.3 Neighbors and the Neighborhood Complex

Let A be an $n \times d$ matrix, and let a_i be the ith row of A. We will shortly define a simplicial complex $C = C(A)$ whose vertices are $\mathbb{Z}^d$. By a simplicial complex, we mean that C is a collection of finite subsets of $\mathbb{Z}^d$, and that if $s \in C$, then all subsets of s are also in C. This complex will contain infinitely many simplices s, and it will not, in general, be geometrically realizable in $\mathbb{R}^d$. This complex is called the *neighborhood complex* of A (it is also sometimes called the *complex of maximal lattice-free bodies* or the *Scarf complex*).

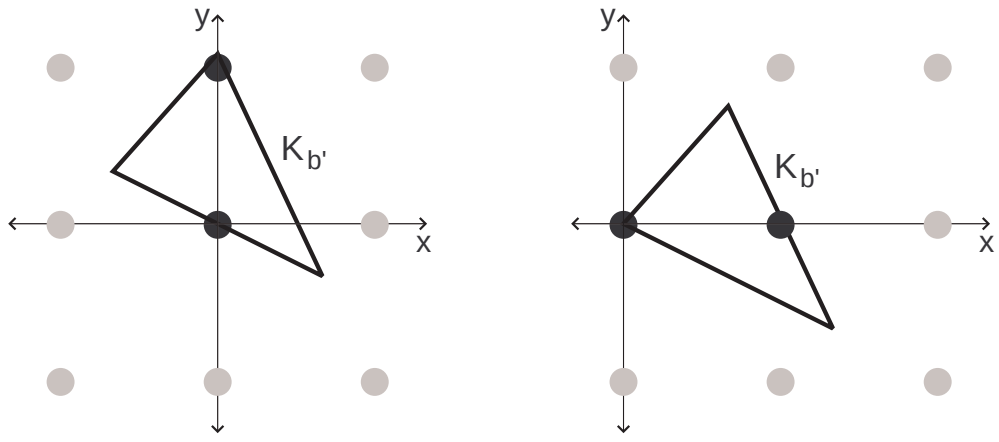
The neighborhood complex is closely related to the family of integer programs IP_A given by

$$\mathrm{IP}_A(b) = \min\langle a_n, x\rangle \text{ such that } \langle a_i, x\rangle \leq b_i \text{ for } 1 \leq i \leq n-1, \text{ and } x \in \mathbb{Z}^d, \tag{1.3.1}$$

as $b = (b_1, b_2, \ldots, b_{n-1})$ varies in $\mathbb{R}^{n-1}$. Theorem 1.1.15 will allow us to compute the generating function for the neighborhood complex (we will define this generating function precisely in Section 3.3). We introduce the complex here, because $C(A)$ will also be essential in formulating a different way to find generating functions for lattice point sets (see Chapter IV). We will not need anything in this section, however, for the proof of Theorem 1.1.15. For an excellent introduction to the neighborhood complex, see [Sca97].

Given $b' \in \mathbb{R}^n$, define the polyhedron

$$K_{b'} = \left\{x \in \mathbb{R}^d : \ Ax \leq b'\right\}.$$



(a) **(b)**

Figure 1.3.2: In Example 1.3.3, edges of $C(A)$ include (a) $\{(0,0),(0,1)\}$ and (b) $\{(0,0),(1,0)\}$

Note that this definition includes $\langle a_n, x\rangle \leq b'_n$ as a constraint, whereas in (1.3.1), $\langle a_n, x\rangle$ is the objective function. We will assume that $K_{b'}$ is bounded: this corresponds (excepting some degenerate cases) to the minimum existing in the integer programs $\mathrm{IP}_A(b)$ in (1.3.1). We say that $s = \{h^0, h^1, \ldots, h^k\} \subset \mathbb{Z}^d$ is a simplex of $C = C(A)$ if and only if there exists a b' such that $K_{b'}$ contains $h^0, h^1, \ldots, h^k$ but $K_{b'}$ contains no integer points in its interior. Then C is a simplicial complex (the same $K_{b'}$ which works for s works for all subsets of s), and C is invariant under translation by $\mathbb{Z}^d$.

Example 1.3.3. Let

$$A = \begin{bmatrix} 2 & 1 \\ -1 & -2 \\ -1 & 1 \end{bmatrix}.$$

Then Figure 1.3.2 shows that $\{(0,0),(0,1)\}$ and $\{(0,0),(1,0)\}$ are edges of $C(A)$.

This definition only works well if A is *generic* in the following sense: if b' is such that $K_{b'}$ contains no integer points in its interior, then no facet of $K_{b'}$ contains more than one integer point. The matrix A often fails to be generic when it is a small integer matrix, so it is important that we determine what definition of C to use in

the non-generic case, which we will do later in this section. For now, we assume that A is generic.

1.3.4 Test sets

For $x, y \in \mathbb{Z}^d$, we say that x *is a neighbor of* y if $\{x, y\}$ is an edge of C. Define N to be the set of neighbors of the origin. Then $y + N$ is the set of neighbors of y. The set N forms a *test set* for the family of integer programs $\mathrm{IP}_A(b)$, as the following proposition makes explicit.

Proposition 1.3.5. *(Theorem 3 of [Sca97]) Suppose, for a given b, that y is a feasible solution to the integer program $IP_A(b)$ in (1.3.1), that is, y satisfies the constraints $\langle a_i, y\rangle \leq b_i$, for $1 \leq i \leq n-1$. Then y is an optimal solution to $IP_A(b)$ if and only if there is no neighbor x of y such that both x is feasible and $\langle x, a_n\rangle < \langle y, a_n\rangle$.*

That is, to decide whether a feasible solution y is optimal, we only have to test the set of points $y + N$ to see if any of them are feasible and closer to optimal.

Because of the importance of neighbors to integer programming, much effort has been made to find some sort of structure in the set N and the complex C. For small dimensions, such structure has been found, and we will give some examples.

Example 1.3.6. When $d = 1$, C consists of vertices $\{i\}$, for $i \in \mathbb{Z}$, and edges $\{i, i+1\}$.

Example 1.3.7. When $d = 2, n = 3$, there exist $h^1, h^2 \in \mathbb{Z}^2$ such that the neighborhood complex consists of vertices $\{x\}$, for $x \in \mathbb{Z}^2$; edges $\{x, x+h^1\}$, $\{x, x+h^2\}$, and $\{x, x+h^1+h^2\}$; and triangles $\{x, x+h^1, x+h^1+h^2\}$ and $\{x, x+h^2, x+h^1+h^2\}$ (see Figure 1.3.8). Notice that these triangles exactly tile $\mathbb{Z}^2$ (see, for example, [Sca97]).

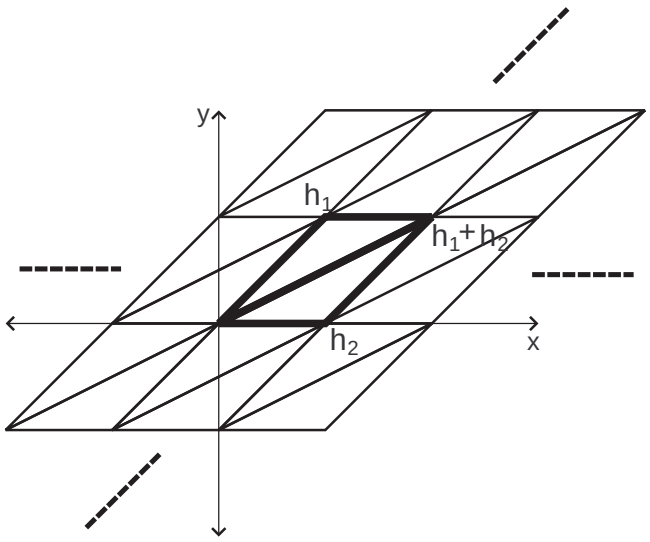


Figure 1.3.8: Example 1.3.7, the neighborhood complex when $d = 2, n = 3$

This is not true in higher dimensions, but C will still have a nice topology, as we will shortly discuss.

Example 1.3.9. When $d = 2, n > 3$, there may be exponentially many (in the input size of A) neighbors. Nevertheless, H. Scarf proved that the neighbors of the origin all lie on polynomially many intervals. In fact, Scarf used this [Sca81] to provide the first polynomial time algorithm for integer programming in two dimensions (H. Lenstra later discovered [Len83] a polynomial algorithm for any fixed d, using different methods). The neighborhood complex is 3-dimensional and its simplices of all dimensions can also be parametrized to lie on polynomially many intervals.

Example 1.3.10. When $d = 3, n = 4$, D. Shallcross [Sha92] showed that the neighbors of the origin have a nice form: they are the integer points in a union of 2-dimensional polyhedra.

For bigger d and n, however, little is known, though L. Lovász conjectured [Lov89] that the neighbors are the union of polynomially many intersections of lower dimen-

sional polyhedra with sublattices of $\mathbb{Z}^d$. In Proposition 3.3.1, we will show that the set of neighbors does have some structure, namely, it can be encoded as a short rational generating function using Theorem 1.1.15.

Even if the exact structure of the neighborhood complex is not known in higher dimensions, at least the topology is nice. We have the following theorem.

Theorem 1.3.11. *(Theorem 2 of [BSS98]) $C(A)$ is contractible.*

In fact, if we include some "ideal" simplices (which we will not discuss here), then C is homeomorphic to R^{n-1} (see [BSS98]). This theorem will come in handy in Chapter IV.

Another nice property of the neighborhood complex is that, if we fix d but let n be arbitrarily large, the dimension of the complex C is not too big. This has been discovered independently several times: by J.-P. Doignon [Doi73], D. Bell [Bel77], and H. Scarf [Sca77].

Proposition 1.3.12. *If $s = \{h^0, h^1, \ldots, h^k\}$ is a simplex in C, then $k \leq 2^d - 1$.*

Proof. Let $K_{b'}$, for some $b' \in \mathbb{R}^n$, be a polytope containing s but with no interior integer points. Then, because A is assumed generic, each facet of $K_{b'}$ contains at most one point from s. Suppose $k \geq 2^d$, that is, $|s| \geq 2^d + 1$. Then s contains two distinct points, h^i and h^j, such that $h^i_l \equiv h^j_l \pmod 2$, for all l. But then $(h^i + h^j)/2$ is an integer point in the interior of $K_{b'}$, which is a contradiction. □

If h is a neighbor of the origin, then Proposition 1.3.14 below will give a bound on the coordinates of h. To prove it, we need the following lemma.

Lemma 1.3.13. *(Part 1 of Theorem 1 from [CGST86]) Let A be an integral $n \times d$ matrix, let b and w be vectors such that $Ax \leq b$ has an integral solution and* $\max\{wx :$

$Ax \leq b\}$ exists, and let $\Delta(A)$ be the largest absolute value of the determinant of any square submatrix of A. Then for each optimal solution $\bar{x}$ to

$$\max\{wx : \ Ax \leq b\}$$

there exists an optimal solution z^* to

$$\max\{wx : \ Ax \leq b, x \text{ integral}\}$$

such that $\|\bar{x} - z^*\|_\infty \leq d\Delta(A)$.

Proposition 1.3.14. *Let A be a generic $n \times d$ matrix, and let $\Delta(A)$ be the largest absolute value of the determinant of any square submatrix of A. If h is a neighbor of the origin in $C(A)$, then $\|h\|_\infty \leq d\Delta(A)$.*

Proof. Let K_b be a polytope which contains only 0 and h, with both 0 and h on its boundary, and let i be an index such that $\langle a_i, h\rangle = b_i$. Let $b' \in \mathbb{Z}^n$ be such that

$$b'_j = b_j \text{ for } j \neq i, \text{ and } b'_i = b_i - \epsilon,$$

for some small $\epsilon > 0$. Then the only integer point in $K_{b'}$ is 0. Let

$$\bar{x} = h - \epsilon \frac{a_i}{\|a_i\|^2}.$$

Then 0 is the only optimal solution to the integer programming problem

$$\max\big\{\langle a_i, x\rangle : \ Ax \leq b', x \text{ integral}\big\},$$

whereas $\bar{x}$ is an optimal solution to the linear relaxation

$$\max\big\{\langle a_i, x\rangle : \ Ax \leq b'\big\}.$$

Then by Lemma 1.3.13, $\|\bar{x}\|_\infty \leq d\Delta(A)$. Taking $\epsilon \to 0$, the proof follows. □

1.3.15 Non-genericity

Finally, we turn to the case where A is not generic (that is, there exists a b' such that $K_{b'}$ contains no integer points in its interior but it contains more than one integer point on some facet). Assume that A is integral, which is the case we will be concerned about anyway. Suppose $K_{b'}$ is a polytope with no integer points in its interior, and suppose some facet, $\langle a_i, x\rangle = b'_i$, of $K_{b'}$ contains two or more integer points, $h^1, h^2, \ldots, h^m$, for some $m \geq 2$. To resolve the non-genericity, we want to choose one of the h^j to be in the simplex s. One way to resolve this is to use a lexicographical rule, which H. Scarf does in [Sca81]. He includes the h^j for which the following sequence is lexicographically minimal:

$$\Big(\langle a_1, h^j\rangle, \langle a_2, h^j\rangle, \ldots, \langle a_n, h^j\rangle\Big).$$

Here we use a slightly different approach developed in [SW03], which is to *perturb* things so that these "ties" don't occur. This approach is basically equivalent, but it is geometric so that useful facts such as Theorem 1.3.11 are still easy to prove. Rather than perturb $x \in \mathbb{Z}^d$ we perturb $Ax \in \mathbb{Z}^n$. We call $\phi : \mathbb{Z}^n \to \mathbb{R}^n$ a *proper perturbation* if the following 3 conditions hold (where $[a]_i$ means the ith coordinate of a):

1. If $c \neq d$, then $[\varphi(c)]_i \neq [\varphi(d)]_i$ for all i,

2. If $[\varphi(c)]_i < [\varphi(d)]_i$ for some i, then $c_i \leq d_i$, and

3. If $[\varphi(c)]_i < [\varphi(d)]_i$ for some i, then $[\varphi(c+e)]_i < [\varphi(d+e)]_i$ for all $e \in \mathbb{Z}^n$.

The first condition ensures that we will be in the generic case, the second ensures that the perturbation only "breaks ties" and doesn't change the natural ordering,

and the third condition will be needed to prove that the neighborhood complex is invariant under translation by $\mathbb{Z}^d$.

To prove that proper perturbations exist, we will construct an example of one.

Example 1.3.16. This example corresponds to the lexicographical tie-breaking rule used in [Sca81]. Given an integer i, let $f_i : \mathbb{Z} \to \mathbb{R}$ be a function such that

1. f_i is strictly increasing,
2. $f_i(0) = 0$ (and hence $f_i(x) < 0$ if $x < 0$), and
3. if $|x| > 0$ (hence $|x| \geq 1$), then $\frac{1}{2^{2i}} \leq |f_i(x)| < \frac{1}{2^{2i-1}}$.

Now define $\varphi : \mathbb{Z}^n \to \mathbb{R}^n$ by

$$\varphi(x) = x + (x_1 f_1(x_1) + x_2 f_2(x_2) + \cdots + x_n f_n(x_n)) \cdot \mathbf{1},$$

where $\mathbf{1}$ is the n-vector of ones. One can check that φ is a proper perturbation.

Given a proper perturbation φ, we can now define the neighborhood complex, C, on the vertices $\mathbb{Z}^d$, by saying $s = \{h^0, h^1, \ldots, h^k\}$ is in C if and only if for no $x \in \mathbb{Z}^d$ is

$$\varphi(Ax) < \max\big(\varphi(Ah^0), \varphi(Ah^1), \ldots, \varphi(Ah^k)\big),$$

where the maximum is taken coordinate-wise (that is, $[\max(x, y)]_i = \max(x_i, y_i)$). Note that if φ is the identity, then this is the definition of C in the generic case, because if b' is taken to be

$$b' = \max\big(Ah^0, Ah^0, \ldots, Ah^k\big),$$

then $K_{b'}$ is the smallest of all K_b containing s, and the condition that for no $x \in \mathbb{Z}^d$ is $Ax < b'$ is exactly the condition that $K_{b'}$ contains no integer points in its interior.

The complex C may be different for different φ, but many properties (including all of the theorems and propositions in this section) hold regardless of the choice of φ. The following lemma shows that C is invariant under translation by $\mathbb{Z}^d$.

Lemma 1.3.17. *If φ is a proper perturbation, then the neighborhood complex C, as defined above, is invariant under translation by $\mathbb{Z}^d$.*

Proof. Given $z \in \mathbb{Z}^d$, we have the following chain of implications:

$s = \{h^0, h^1, \ldots, h^k\} \in C$

$\Rightarrow$ for no $x \in \mathbb{Z}^d$ is $\varphi(Ax) < \max\big(\varphi(Ah^0), \varphi(Ah^1), \ldots, \varphi(Ah^k)\big)$

$\Rightarrow$ given $x \in \mathbb{Z}^d$, $\exists i$ such that $\forall j$ $[\varphi(Ax)]_i \geq [\varphi(Ah^j)]_i$

$\Rightarrow$ given $x \in \mathbb{Z}^d$, $\exists i$ such that $\forall j$ $[\varphi(Ax + Az)]_i \geq [\varphi(Ah^j + Az)]_i$

(by Property 3 of proper perturbations)

$\Rightarrow$ for no $x \in \mathbb{Z}^d$ is $\varphi\big(A(x+z)\big) < \max\Big(\varphi\big(A(h^0+z)\big), \varphi\big(A(h^1+z)\big), \ldots, \varphi\big(A(h^k+z)\big)\Big)$

$\Rightarrow s + z \in C.$

□

CHAPTER II

The Projection Theorem

In this chapter, we will prove Theorem 1.1.15. In Section 2.1, we give an outline of the proof and examine some special cases. In Section 2.2, we discuss some needed "flatness" results from the geometry of numbers. In Section 2.3, we examine an idea from parametric integer programming, developed by R. Kannan, L. Lovász, and H. Scarf in [KLS90] and [Kan92]. Finally, in Section 2.4, we combine these results to prove Theorem 1.1.15. The proof of Theorem 1.1.15 originally appeared in [BW03].

2.1 Outline

Suppose we are given a rational polytope $P \subset \mathbb{R}^d$ and a linear transformation $T : \mathbb{R}^d \to \mathbb{R}^k$, such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$. We would like to find $f(S; \mathbf{x})$ in polynomial time (for fixed d), where $S = T(P \cap \mathbb{Z}^d)$. The proof will by induction on $\dim(\ker(T))$. In this section we will prove the simplest two cases, where $\dim(\ker(T))$ is 0 or 1, and then we will outline the general proof.

Suppose that $\dim(\ker(T)) = 0$, so T is injective. The first step is to find $f(P \cap \mathbb{Z}^d; \mathbf{y})$, which we can do in polynomial time using Theorem 1.2.3. Now let $e_1, e_2, \ldots, e_d$ be the standard basis of $\mathbb{Z}^d$, and let $f_i = T(e_i)$, for each i. Then we obtain $f(S; \mathbf{x})$ from $f(P \cap \mathbb{Z}^d; \mathbf{y})$ by applying the monomial substitution $y_i = \mathbf{x}^{f_i}$, using Theorem 1.2.8.

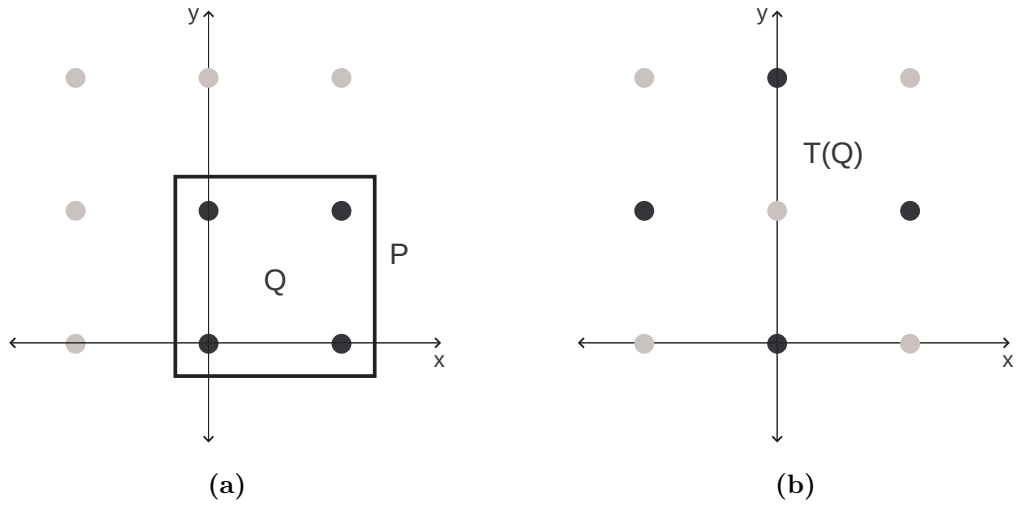


Figure 2.1.1: Example 2.1.2, $T(x, y) = (x + y, x - y)$, (a) $Q = P \cap \mathbb{Z}^2$ and (b) $S = T(Q)$

Example 2.1.2. Suppose $P \subset \mathbb{R}^2$ is the square pictured in Figure 2.1.1(a), let $Q = P \cap \mathbb{Z}^2$, and let $T : \mathbb{R}^2 \to \mathbb{R}^2$ be defined by $T(x, y) = (x + y, x - y)$. Then $S = T(Q)$ is pictured in Figure 2.1.1(b), $f(Q; x, y) = 1 + x + xy + y$, and

$$f(S; u, v) = f(Q; uv, uv^{-1}) = 1 + uv + u^2 + uv^{-1}.$$

Now suppose that $\dim(\ker(T)) = 1$. In Section 2.3, we will show that, without loss of generality, we may assume that $T(x_1, x_2, \ldots, x_d) = (x_1, x_2, \ldots, x_{d-1})$. Let $\hat{S} = P \cap \mathbb{Z}^d$. As before, we first find $f(\hat{S}; \mathbf{x}, x_d)$ using Theorem 1.2.3, where $\mathbf{x} = (x_1, x_2, \ldots, x_{d-1})$.

Example 2.1.3. Let P be as pictured in Figure 2.1.4(a), and let $T(x, y) = x$. Then

$$f(\hat{S}; x, y) = 1 + y + y^2 + x + xy + x^2y.$$

In general, if we were to apply the monomial substitution $x_d = 1$, $x_i = x_i$ for $1 \leq i \leq d - 1$, that is, if we were to specialize at $x_d = 1$, we would not quite get the generating function $f(S; \mathbf{x})$ that we want: the coefficient of $\mathbf{x}^a$ would be the

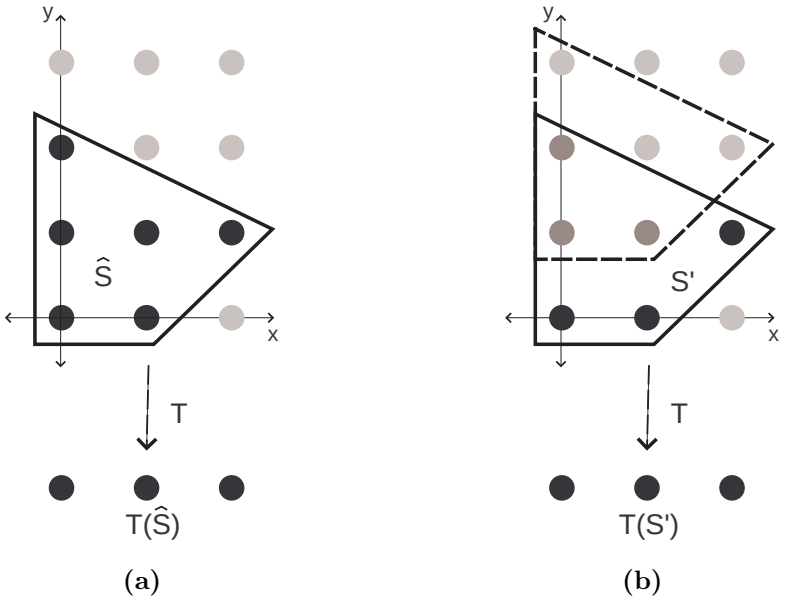


Figure 2.1.4: Example 2.1.3, $T(x, y) = x$, (a) $\hat{S}$ and $T(\hat{S})$ and (b) S' and $T(S')$

cardinality of the preimage $T^{-1}(a) \subset \hat{S}$. In Example 2.1.3, we would have

$$f(\hat{S}; x, 1) = 3 + 2x + x^2.$$

For this monomial substitution idea to work, we would need the map $T|_{\hat{S}}$ to be one-to-one.

To fix this, notice that the preimage $T^{-1}(a) \subset \hat{S}$ of any $a \in S$ is an interval of points $\{(a, b_0), (a, b_0 + 1), \ldots, (a, b_1)\}$, for some $b_0, b_1 \in \mathbb{Z}$. Let S' be the set $\hat{S} \setminus \big(\hat{S} + (0, 0, \ldots, 0, 1)\big)$ (see Figure 2.1.4(b)). Then the preimage of any $a \in S$ under the map $T|_{S'} : S' \to S$ is simply the point (a, b_0), and so the map $T|_{S'}$ is one-to-one (and onto S). To obtain $f(S'; \mathbf{x}, x_d)$, we use Theorem 1.2.10 together with the fact $f(\hat{S} + (0, 0, \ldots, 0, 1); \mathbf{x}, x_d) = x_d f(\hat{S}; \mathbf{x}, x_d)$. Now we compute $f(S; \mathbf{x})$ by specializing $f(S'; \mathbf{x}, x_d)$ at $x_d = 1$, using Theorem 1.2.8. In Example 2.1.3,

$$f(S'; x, y) = 1 + x + x^2 y \text{ and } f(S; x) = f(S'; x, 1) = 1 + x + x^2.$$

In the general case, where $\dim(\ker(T)) > 1$, we will proceed inductively on

$\dim(\ker(T))$. First we will choose (very carefully) a direction $w \in \ker(T) \setminus \{0\}$. Then let $\hat{T} : \mathbb{R}^d \to \mathbb{R}^k \oplus \mathbb{R}$ be the linear transformation

$$\hat{T}(x) = (T(x), \langle w, x \rangle),$$

and let $\pi : \mathbb{R}^k \oplus \mathbb{R} \to \mathbb{R}^k$ be the projection

$$\pi(x, \xi) = x.$$

Then $T = \pi \circ \hat{T}$. Furthermore, $\dim(\ker(\hat{T})) = \dim(\ker(T)) - 1$. Let $\hat{S} = \hat{T}(P \cap \mathbb{Z}^d)$, so that $\pi(\hat{S}) = S$. By the induction hypothesis, we may find $f(\hat{S}; \mathbf{x}, x_{k+1})$ in polynomial time.

$\hat{S}$ will not be as nice as it was in the case where $\dim(\ker(T)) = 1$, where $\hat{S}$ was the set of integer points in a polytope.

Example 2.1.5. Suppose $\hat{S}$ is as in Figure 2.1.6(a), with $\pi(x, y) = x$. Then $\hat{S}$ is not the set of integer points in a polytope.

In general, then, the preimage $\pi^{-1}(a) \subset \hat{S}$, for $a \in S$, will not be an interval of points $\{(a, b_0), (a, b_0 + 1), \ldots, (a, b_1)\}$ as it was before. We will prove, however, that (for the appropriate choice of w) the preimage will be similar to an interval in that it will not have large "gaps." To be concrete, there exists a constant $\sigma = \sigma(d)$ depending only on d, such that if (a, b_0) and (a, b_1) are in $\hat{S}$ and $b_1 - b_0 > \sigma$, then there is a b with $b_0 < b < b_1$ such that $(a, b) \in \hat{S}$. In Example 2.1.5 (see Figure 2.1.6(a)), $\sigma = 2$ works, because gaps as large as in Figure 2.1.6(b) (where $b_1 - b_0 = 3 > 2$) do not occur.

Then, generalizing what we did in the $\dim(\ker(T)) = 1$ case, define $\hat{S} + i$ to be $\hat{S} + (0, 0, \ldots, 0, i)$, and let

$$S' = \hat{S} \setminus \bigcup_{i=1}^{\sigma} (\hat{S} + i).$$

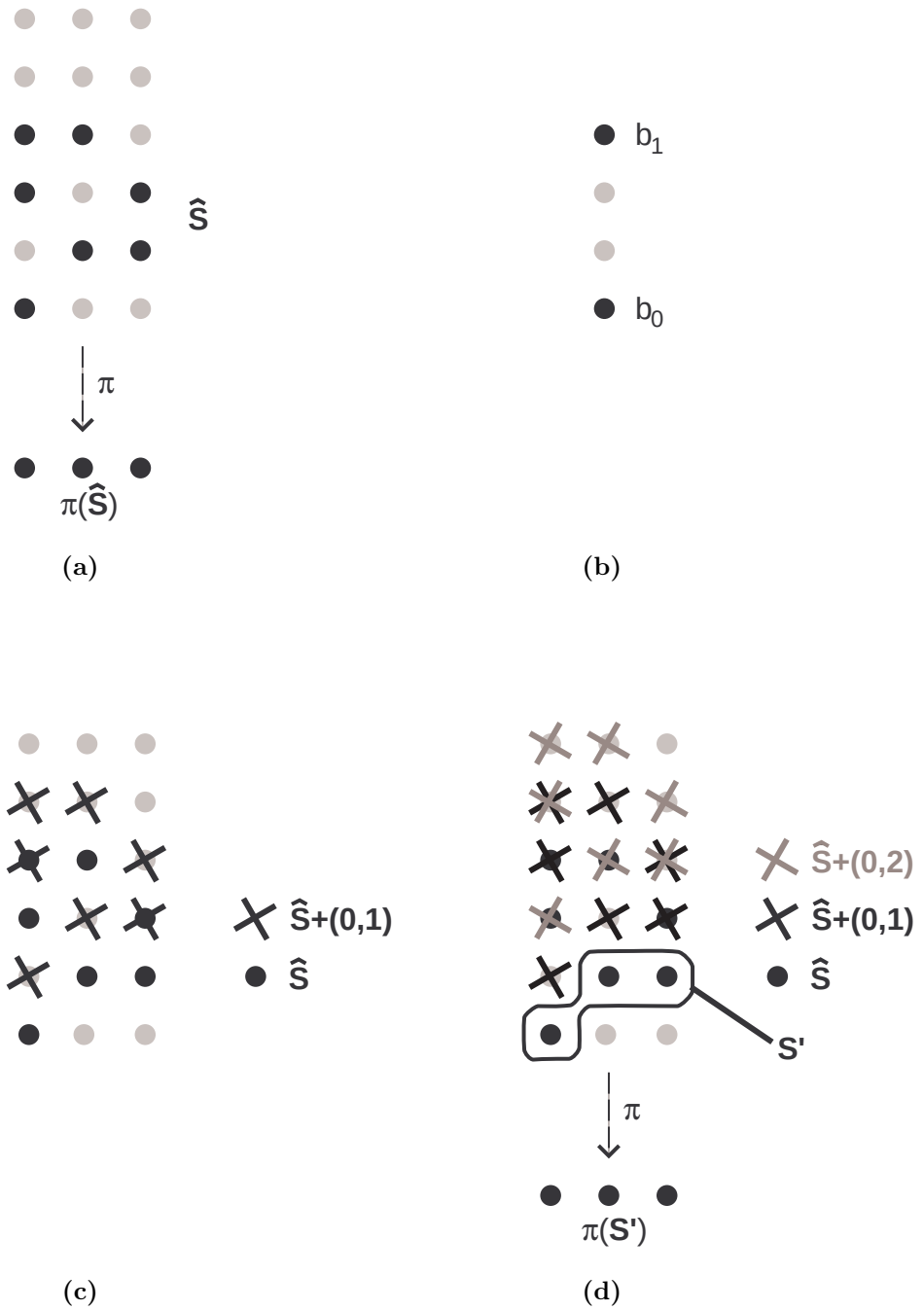


Figure 2.1.6: Example 2.1.5, for $\sigma = 2$ and $\pi(x, y) = x$, (a) $\hat{S}$ and $\pi(\hat{S})$, (b) a gap that doesn't appear in $\hat{S}$, (c) $\hat{S} \setminus (\hat{S} + 1)$, and (d) $S' = \hat{S} \setminus (\hat{S} + 1) \setminus (\hat{S} + 2)$ and $\pi(S')$

In Example 2.1.5 (with $\sigma = 2$), Figure 2.1.6(c) shows $\hat{S} \setminus (\hat{S} + 1)$, and Figure 2.1.6(d) shows $S' = \hat{S} \setminus (\hat{S} + 1) \setminus (\hat{S} + 2)$. Note that, in this case, the map $\pi : S' \to S$ is one-to-one. This is true in general, because for any $a \in S$, there is exactly one point (a, b_0) in S', given by $b_0 = \min\{b : \ (a, b) \in \hat{S}\}$. We may find $f(S'; \mathbf{x}, x_{k+1})$ using Theorem 1.2.10 (since σ is fixed, for fixed d), and then we specialize at $x_{k+1} = 1$, using Theorem 1.2.8, to compute $f(S; \mathbf{x})$.

There is one more complication. It is not possible to choose the same w for every point $a \in S$, and expect the preimage to not have large gaps. We will have to do the following. We will partition $T(P) \subset \mathbb{R}^k$ into pieces $Q'_1, Q'_2, \ldots, Q'_n$ in a particular way. Each piece Q'_i will be the relative interior of a polytope Q_i (these Q_i will not all be full dimensional), and n will be bounded by a polynomial in the input. Each Q'_i will have an associated w_i which will be used, as before, to define the linear transformation

$$\hat{T}_i : Q_i \to \mathbb{R}^k \oplus \mathbb{R}, \text{ with } \hat{T}_i(x) = (T(x), \langle w_i, x \rangle).$$

We will use the process outlined above to calculate $f(Q'_i \cap S; \mathbf{x})$, for each i, and then we have

$$f(S; \mathbf{x}) = \sum_{i=1}^{n} f(Q'_i \cap S; \mathbf{x}).$$

The Q_i will be calculated based on the shapes of the preimages $T^{-1}(a) \subset P$.

Example 2.1.7. If $P \subset R^d$ is the convex hull of $(-5, 0, \pm 5)$ and $(5, \pm 5, 0)$ and $T(x, y, z) = x$ (see Figure 2.1.8), then the preimages $T^{-1}(x) \subset P$ are rectangles. For $-5 \leq x < 0$, these rectangles are thinnest in the y-direction, and for $0 < x \leq 5$, these rectangles are thinnest in the z-direction. A possible partition of $T(P)$ into Q'_i, where Q'_i are relative interiors of polytopes, would be

$$Q'_1 = (-5, 0), Q'_2 = (0, 5), Q'_3 = \{-5\}, Q'_4 = \{0\}, Q'_5 = \{5\},$$

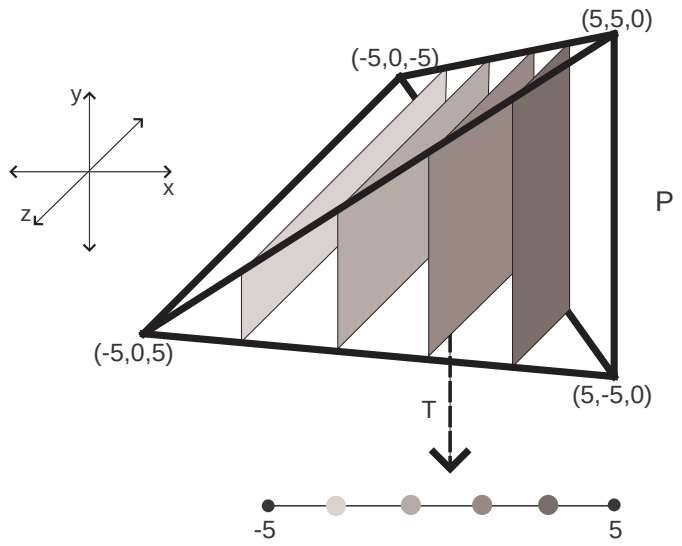


Figure 2.1.8: Example 2.1.7, $P = \text{conv}\left\{(5, 0, \pm 5), (5, \pm 5, 0)\right\}$, $T(x, y, z) = x$

and we could have $w_1 = w_3 = w_4 = (0, 1, 0)$ and $w_2 = w_5 = (0, 0, 1)$.

In general, w_i should be a direction in which $T^{-1}(a) \subset P$ is "flat," for $a \in Q_i$. We will go through the specifics of how to partition $T(P)$, in general, in Section 2.3.

2.2 Lattice Width and Flatness Directions

In this section, we develop the geometric theory which tells us that, if w (see outline of proof, Section 2.1) is chosen so that it is a "flat" direction of $T^{-1}(a) \subset P$, for a given $a \in \mathbb{R}^k$, then $\pi^{-1}(a) \subset \hat{S}$ will have small gaps, as desired. Section 2.3 will then tell us how to find these directions.

Let $\Lambda \subset \mathbb{R}^d$ be a d-dimensional lattice, and let Λ^* be the dual lattice

$$\Lambda^* = \{c \in \mathbb{R}^d : \ \langle c, \lambda \rangle \in \mathbb{Z} \text{ for all } \lambda \in \Lambda\},$$

where $\langle \cdot, \cdot \rangle$ is the standard inner product on $\mathbb{R}^d$. We will be mainly concerned with the case $\Lambda = \Lambda^* = \mathbb{Z}^d$.

Let B be a convex body (that is, a convex, compact set). If B were centrally

(a) **(b)**

Figure 2.2.1: Convex B such that $B \cap \mathbb{Z}^2 = \emptyset$

symmetric, and if B contained no nonzero lattice points, then Minkowski's Theorem (see Section VII.3 of [Bar02], for example) would give a bound

$$\operatorname{vol} B \leq 2^d \det \Lambda,$$

where $\det \Lambda$ is the cardinality of $\mathbb{Z}^d/\Lambda$.

2.2.2 Flatness

We will be concerned with convex bodies that are not necessarily centrally symmetric. In this case, B could contain no lattice points and yet have arbitrarily large volume, as in Figure 2.2.1. Notice that, for this to happen, B must be flat like a pancake.

Let us be more precise. Given a convex body $B \subset \mathbb{R}^d$ and a vector $c \in \Lambda^* \setminus \{0\}$, define the *width* of B along c to be

$$\operatorname{width}(B, c) = \max_{x \in B} \langle c, x \rangle - \min_{x \in B} \langle c, x \rangle.$$

Then define the *lattice width* of B to be

$$\text{width}(B) = \min_{c \in \Lambda^* \setminus \{0\}} \text{width}(B, c).$$

We have the following theorem which says that if a convex body contains no lattice points, it must be "flat" in some direction.

Theorem 2.2.3. *(The Flatness Theorem) There exists a constant $\omega(d)$ which depends only on d such that, if B is a convex body and $B \cap \Lambda = \emptyset$, then width$(B) \leq \omega(d)$.*

For an elementary proof, see Section VI.8 of [Bar02]. The best known value for ω is $O(d^{\frac{3}{2}})$ (see [BLPS99]), though it is conjectured to be $O(d)$. Our constant $\sigma(d)$ (see outline of proof, Section 2.1) will be $\lceil 2\omega(d) \rceil$.

For any $\alpha \in \mathbb{R}_{\geq 0}$ and any $b \in \mathbb{R}^d$, it is clear that

$$\text{width}(\alpha B + b, c) = \alpha \cdot \text{width}(B, c),$$

and so

$$\text{width}(\alpha B + b) = \alpha \cdot \text{width}(B).$$

The following technical lemma will help us (see Figure 2.2.5 for an illustration with $c = (0, 1)$).

Lemma 2.2.4. *Let $B \subset \mathbb{R}^d$ be a convex body, let $c \in \mathbb{R}^d \setminus \{0\}$, and let*

$$\gamma_{\min} = \min_{x \in B} \langle c, x \rangle \text{ and } \gamma_{\max} = \max_{x \in B} \langle c, x \rangle.$$

Let γ_1, γ_2 be numbers such that $\gamma_{\min} < \gamma_1 < \gamma_2 < \gamma_{\max}$. Then there exists a point $x_0 \in B$ and a number $0 < \alpha < 1$ such that, for

$$A = \alpha(B - x_0) + x_0 = \alpha B + (1 - \alpha)x_0,$$

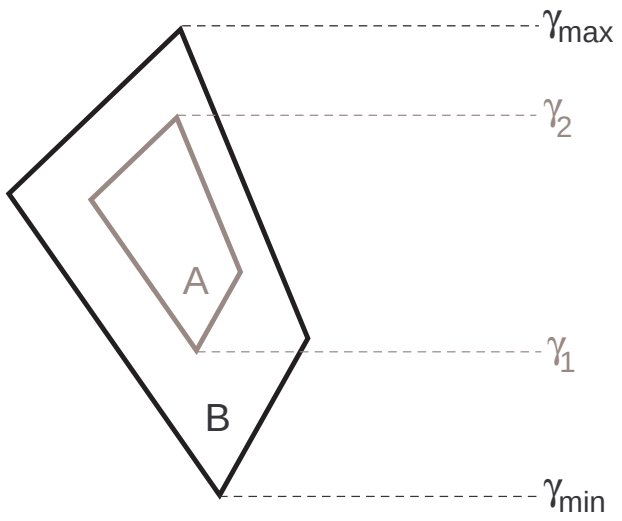


Figure 2.2.5: Illustration of Lemma 2.2.4 with $c = (0, 1)$

one has $A \subset B$ *and*

$$\min_{x \in A} \langle c, x \rangle = \gamma_1 \text{ and } \max_{x \in A} \langle c, x \rangle = \gamma_2.$$

Proof. By translating and dilating B, we may assume without loss of generality that $\gamma_{\min} = 0$ and $\gamma_{\max} = 1$. Since

$$0 < \frac{\gamma_1}{1 - \gamma_2 + \gamma_1} < 1,$$

we may choose $x_0 \in B$ such that $\langle c, x_0 \rangle = \frac{\gamma_1}{1-\gamma_2+\gamma_1}$. Let $\alpha = \gamma_2 - \gamma_1$. Then, for $A = \alpha B + (1 - \alpha)x_0$, we have

$$\min_{x \in A} \langle c, x \rangle = \alpha \cdot 0 + (1 - \alpha) \frac{\gamma_1}{1 - \gamma_2 + \gamma_1} = \gamma_1$$

and

$$\max_{x \in A} \langle c, x \rangle = \alpha \cdot 1 + (1 - \alpha) \frac{\gamma_1}{1 - \gamma_2 + \gamma_1} = \gamma_2,$$

as desired. Furthermore, $A \subset B$, since B is convex. □

2.2.6 Small gaps

We will use the following theorem to show that, if we choose $w \in \ker(T)$ (see outline of proof, Section 2.1) such that $T^{-1}(a) \subset P$ is flat enough in the direction of w, that is, such that

$$\text{width}(T^{-1}(a), w) \leq 2 \cdot \text{width}(T^{-1}(a)),$$

for a given $a \in \mathbb{R}^k$, then $\pi^{-1}(a) \subset \hat{S}$ will have small gaps, that is, gaps of size at most $\sigma(d) = \lceil 2\omega(d) \rceil$. This is crucial to the proof of Theorem 1.1.15.

Theorem 2.2.7. *Let $B \subset \mathbb{R}^d$ be a convex body, and let $\Lambda \subset \mathbb{R}^d$ be a lattice. Let $c \in \Lambda^*$ be a nonzero vector. Let us consider the map:*

$$\phi : B \cap \Lambda \to \mathbb{Z}, \text{ given by } \phi(x) = \langle c, x \rangle,$$

and let $Y = \phi(B \cap \Lambda)$. Hence $Y \subset \mathbb{Z}$ is a finite set.

Suppose that

$$\text{width}(B, c) \leq 2 \cdot \text{width}(B).$$

Then, for any $y_1, y_2 \in Y$ such that $y_2 - y_1 > 2\omega(d)$, there exists a $y \in Y$ such that $y_1 < y < y_2$.

Proof. Suppose there is no such y. Then for some small ϵ, $0 < \epsilon < \frac{1}{2}$, let $\gamma_1 = y_1 + \epsilon$ and $\gamma_2 = y_2 - \epsilon$, so $[\gamma_1, \gamma_2] \cap Y = \emptyset$. Using Lemma 2.2.4, choose $x_0 \in B$ and $\alpha > 0$ such that for $A = \alpha(B - x_0) + x_0$, we have

$$\min_{x \in A} \langle c, x \rangle = \gamma_1 \text{ and } \max_{x \in A} \langle c, x \rangle = \gamma_2.$$

Since $A \subset B$ and $[\gamma_1, \gamma_2] \cap Y = \emptyset$, we have $A \cap \Lambda = \emptyset$. Then by the Flatness Theorem (Theorem 2.2.3),

$$\text{width}(A) \leq \omega(d).$$

Since $A = \alpha(B - x_0) + x_0$, we know

$$\text{width}(A, c) = \alpha\text{width}(B, c) \leq 2\alpha \cdot \text{width}(B) = 2 \cdot \text{width}(A).$$

Therefore,

$$y_2 - y_1 - 2\epsilon = \gamma_2 - \gamma_1 = \text{width}(A, c) \leq 2 \cdot \text{width}(A) \leq 2\omega(d),$$

for all $\epsilon > 0$, and so $y_2 - y_1 \leq 2\omega(d)$, a contradiction. □

The following corollary will help us construct the set S' whose projection $\pi : S' \to S$ is one-to-one (see outline of proof, Section 2.1).

Corollary 2.2.8. *Let $Y \subset \mathbb{Z}$ be the set of Theorem 2.2.7 and let $m = \lceil 2\omega(d) \rceil$. If $Y \neq \emptyset$, then the set*

$$Z = Y \setminus \bigcup_{l=1}^{m} (Y + l)$$

consists of a single point.

Proof. By Theorem 2.2.7, that point is z, where $z = \min\{y : \ y \in Y\}$. □

2.3 Partitioning

Let $T : \mathbb{R}^d \to \mathbb{R}^k$ be a linear transformation such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$. Let

$$P = \{x \in \mathbb{R}^d : \ Ax \leq b\}$$

be a rational polytope in $\mathbb{R}^d$, for some $n \times d$ integer matrix A and some $b \in \mathbb{Z}^n$. For $a \in \mathbb{R}^k$, consider the fiber $T^{-1}(a) \cap P$. We will transform these fibers so that they lie in $\mathbb{R}^r$, where $r = \dim(\ker(T))$. We need the following lemma.

Lemma 2.3.1. *There is a polynomial time algorithm which, given a linear transformation $T : \mathbb{R}^d \to \mathbb{R}^k$ such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$ with $r = \dim(\ker(T))$, computes linear transformations $T_1 : \mathbb{R}^d \to \mathbb{R}^d$, $T_2 : \mathbb{R}^d = \mathbb{R}^{d-r} \oplus \mathbb{R}^r \to \mathbb{R}^{d-r}$, and $T_3 : \mathbb{R}^{d-r} \to \mathbb{R}^k$ such that*

1. $T = T_3 \circ T_2 \circ T_1$,

2. T_1 *is a unimodular transformation (that is,* $T_1(\mathbb{Z}^d) = \mathbb{Z}^d$*),*

3. $T_2 : \mathbb{R}^d = \mathbb{R}^{d-r} \oplus \mathbb{R}^r \to \mathbb{R}^{d-r}$ *is given by* $T_2(x, y) = x$*, and*

4. T_3 *is injective with* $T_3(\mathbb{Z}^{d-r}) \subset \mathbb{Z}^k$.

Proof. Let M be the $k \times d$ integer matrix which represents T. We first show how to transform M into a lower triangular matrix (that is, a matrix such that $M_{ij} = 0$ for $j > i$) in polynomial time, using elementary (integer) column operations. Begin by transforming the first row of M, using elementary operations on all columns, into

$$\begin{bmatrix} M'_{11} & 0 & 0 & \cdots & 0 \end{bmatrix},$$

where $M'_{11} = \gcd(M_{11}, M_{12}, \ldots, M_{1d})$. This requires at most d applications of the Euclidean algorithm. Then, using elementary operations on all but the first column, we may transform the second row into

$$\begin{bmatrix} M'_{21} & M'_{22} & 0 & \cdots & 0 \end{bmatrix},$$

where $M'_{21}, M'_{22} \in \mathbb{Z}$. Continuing gives us the desired lower triangular matrix. We have decomposed M into

$$M = M'C,$$

where M' is a $k \times d$ lower triangular matrix, and C is the $d \times d$ unimodular (that is, $|\det(C)| = 1$) matrix determined by the column operations. Let M'' be the $k \times (d-r)$ matrix formed by the first $d-r$ columns of M' (these are exactly the nonzero columns of M'). Then define $T_1 : \mathbb{R}^d \to \mathbb{R}^d$ by

$$T_1(x) = Cx,$$

define $T_2 : \mathbb{R}^d = \mathbb{R}^{d-r} \oplus \mathbb{R}^r \to \mathbb{R}^{d-r}$ by

$$T_2(x, y) = x,$$

and define $T_3 : \mathbb{R}^{d-r} \to \mathbb{R}^k$ by

$$T_3(x) = M''x.$$

Then $T = T_3 \circ T_2 \circ T_1$, and these maps have the desired properties. □

We may assume, without loss of generality, that the map T_3 from Lemma 2.3.1 is the identity map $\mathbb{R}^{d-r} \to \mathbb{R}^{d-r}$: otherwise, apply the following lemma with $T' = T_3$ and $S' = T_2 \circ T_1(P \cap \mathbb{Z}^d)$.

Lemma 2.3.2. *Fix d and k. There is a polynomial time algorithm which, given an injective linear transformation $T' : \mathbb{R}^d \to \mathbb{R}^k$ such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$ and a rational generating function $f(S'; \mathbf{x})$ in the form*

$$f(S'; \mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}})(1 - \mathbf{x}^{a_{i2}}) \cdots (1 - \mathbf{x}^{a_{ik_i}})}$$

with $k_i \leq k$, computes $f(T'(S'); \mathbf{y})$ in the same form.

Proof. Let $e_1, e_2, \ldots, e_d$ be the standard basis of $\mathbb{Z}^d$, and let $f_i = T'(e_i)$, for each i. Then we obtain $f(T'(S'); \mathbf{y})$ from $f(S'; \mathbf{x})$ by applying the monomial substitution $y_i = \mathbf{x}^{f_i}$, using Theorem 1.2.8. □

Now let T_1 and T_2 be given as in Lemma 2.3.1, and assume, without loss of generality, the T_3 is the identity transformation. Let $P' = T_1(P)$. If $P = \left\{x \in \mathbb{R}^d : Ax \leq b\right\}$, and if C is the $d \times d$ matrix defined in the proof of Lemma 2.3.1, then P' is the polytope

$$P' = \left\{y \in \mathbb{R}^d : \ AC^{-1}y \leq b\right\}.$$

Since T_1 is a unimodular transformation, it bijectively maps $P \cap \mathbb{Z}^d$ to $P' \cap \mathbb{Z}^d$, and so

$$T(P \cap \mathbb{Z}^d) = T_2(P' \cap \mathbb{Z}^d).$$

Therefore we may assume, without loss of generality, that T_1 is the identity, that is, that $T = T_2$ is the map $\mathbb{R}^d = \mathbb{R}^k \oplus \mathbb{R}^{d-k} \to \mathbb{R}^k$ given by $T(x, y) = x$.

Then we may identify the fibers $T^{-1}(a) \cap P$, for $a \in \mathbb{R}^k$, with

$$P_a = \big\{y \in \mathbb{R}^{d-k} : \ (a, y) \in P\big\}.$$

If $P = \big\{x \in \mathbb{R}^d : \ Ax \leq b\big\}$, let B be the $n \times k$ matrix formed by the first k columns of A, and let B' be the $n \times (d-k)$ matrix formed by that last $d-k$ columns of A. Then P_a is the polytope

$$\big\{y \in \mathbb{R}^{d-k} : \ B'y \leq b - Ba\big\}.$$

2.3.3 Kannan's partitioning lemma

We have the following lemma, a rephrasing of Part 3 of Lemma 3.1 of [Kan92]. In essence, it states that we may partition $Q = T(P)$ into polynomially many (in the input size of P and T, for fixed d) rational polytopes Q_i, and for each i we may find a direction $w_i \in \mathbb{Z}^{d-k}$ such that, for all $a \in Q_i$, the lattice width of P_a is almost attained at w_i.

Lemma 2.3.4. *Let us fix d. Then there exists a polynomial time algorithm, which, for any rational polytope $P \subset \mathbb{R}^d$ and a linear transformation $T : \mathbb{R}^k \oplus \mathbb{R}^{d-k} \to \mathbb{R}^k$ with $T(x, y) = x$, constructs rational polytopes $Q_1, Q_2, \ldots, Q_m \subset \mathbb{R}^k$ and vectors $w_1, w_2, \ldots, w_m \in \mathbb{Z}^{d-k}$ such that (when P_a is defined as above)*

1. *For each $i = 1, 2, \ldots, m$ and every $a \in Q_i$, either*

(a) $\text{width}(P_a, w_i) \leq 2 \cdot \text{width}(P_a)$ *or*

(b) $\text{width}(P_a, w_i) \leq 1$*;*

2. *The relative interiors* $\text{int}(Q_i)$ *are pairwise disjoint and*

$$\bigcup_{i=1}^{m} \text{int}(Q_i) = T(P).$$

2.3.5 Patching together

To prove Theorem 1.1.15, we will first prove that we can find $f(S \cap Q_i; \mathbf{x})$, for each i. If we could then use these to find $f(S \cap \text{int}\, Q_i; \mathbf{x})$, we would have

$$f(S; \mathbf{x}) = \sum_i f(S \cap \text{int}\, Q_i; \mathbf{x}),$$

since $T(P)$ is the disjoint union of the $\text{int}\, Q_i$. The following lemma allows us to do this "patching" together.

Lemma 2.3.6. *Let us fix d and k. There exists a polynomial time algorithm which, given a rational polytope Q and a rational generating function $f(S \cap Q; \mathbf{x})$ in the form*

$$f(S \cap Q; \mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}})(1 - \mathbf{x}^{a_{i2}}) \cdots (1 - \mathbf{x}^{a_{ik_i}})}$$

with $k_i \leq k$, computes $f(S \cap \text{int}\, Q; \mathbf{x})$ in the form

$$f(S \cap \text{int}\, Q; \mathbf{x}) = \sum_{i \in I'} \beta_i \frac{\mathbf{x}^{q_i}}{(1 - \mathbf{x}^{b_{i1}})(1 - \mathbf{x}^{b_{i2}}) \cdots (1 - \mathbf{x}^{b_{is}})},$$

where $s \leq 2k$.

Proof. It suffices to calculate $f(\text{int}\, Q \cap \mathbb{Z}^d; \mathbf{x})$, because

$$S \cap \text{int}\, Q = (S \cap Q) \cap (\text{int}\, Q \cap \mathbb{Z}^d),$$

and we could then apply Theorem 1.2.10. Recall that, for a set $A \subset \mathbb{R}^d$, we define the indicator function $[A] : \mathbb{R}^d \to \mathbb{R}$ by

$$[A](x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}.$$

We have the following consequence of the Euler-Poincaré theorem (see, for example, Section VI.3 of [Bar02]):

$$[\operatorname{int} Q] = (-1)^{\dim Q} \sum_F (-1)^{\dim F} [F],$$

where the sum is taken over all faces of Q, including Q itself. Therefore

$$f(\operatorname{int} Q \cap \mathbb{Z}^d; \mathbf{x}) = (-1)^{\dim Q} \sum_F (-1)^{\dim F} f(F \cap \mathbb{Z}^d; \mathbf{x}).$$

The number of faces of Q is bounded by a polynomial in the input size (since d is fixed), and we may calculate a description of each face (which are also polyhedra) in polynomial time. Therefore we may apply Theorem 1.2.3 to calculate $f(F \cap \mathbb{Z}^d; \mathbf{x})$ for each face F, and the proof follows. □

2.4 Proof of Theorem 1.1.15

In this section we will finally prove Theorem 1.1.15.

Theorem 1.1.15. *Let d be fixed. Then there exists a constant $s = s(d)$ and a polynomial time algorithm which, given a rational polytope $P \subset \mathbb{R}^d$ and a linear transformation $T : \mathbb{R}^d \to \mathbb{R}^k$ such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$, computes $f(S; \mathbf{x})$ in the form*

$$f(S; \mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{b_{i1}}) \cdots (1 - \mathbf{x}^{b_{is}})},$$

where $\alpha_i \in \mathbb{Q}$, $p_i \in \mathbb{Z}$, and $b_{ij} \in \mathbb{Z} \setminus \{0\}$.

Proof. We prove it by induction on the dimension of $\ker(T)$. The case $\dim(\ker(T)) = 0$ was already proved in Section 2.1. We showed in Section 2.3 that we may assume, without loss of generality, that $T : \mathbb{R}^d = \mathbb{R}^k \oplus \mathbb{R}^{d-k} \to \mathbb{R}^k$ is the map $T(x, y) = x$.

Let $Q_1, Q_2, \ldots, Q_m$ be the polytopes in $\mathbb{R}^k$ constructed in Lemma 2.3.4. Then it is sufficient to compute $f(S \cap Q_i)$ for each i, because then we may use Lemma 2.3.6 to patch them together and find $f(S; \mathbf{x})$.

Let us fix a particular i. From Lemma 2.3.4, we have a direction $w_i \in \mathbb{R}^{d-k}$ such that, for $a \in Q_i$, either $\text{width}(P_a, w_i) \leq 2 \cdot \text{width}(P_a)$ or $\text{width}(P_a, w_i) \leq 1$, where $P_a = \left\{ y \in \mathbb{R}^{d-k} : \ (a, y) \in P \right\}$. Let us consider the linear transformation

$$\hat{T} : \mathbb{R}^k \oplus \mathbb{R}^{d-k} \to \mathbb{R}^k \oplus \mathbb{R}, \text{ given by } \hat{T}(x, y) = (x, \langle w_i, y \rangle)$$

and the projection

$$\pi : \mathbb{R}^k \oplus \mathbb{R} \to \mathbb{R}^k, \text{ given by } \pi(x, \xi) = x,$$

so that $T = \pi \circ \hat{T}$.

Let $\hat{S} = \hat{T}(P \cap Q_i \cap \mathbb{Z}^d)$, so that $\pi(\hat{S}) = S \cap Q_i$. Since $\dim(\ker(\hat{T})) = d - k - 1$, we can compute $f(\hat{S}; \mathbf{x}, x_{k+1})$ in polynomial time, by the induction hypothesis. Now we must use $f(\hat{S}; \mathbf{x}, x_{k+1})$ to compute $f(S \cap Q_i; \mathbf{x})$. To do this, we will find a subset $S' \subset \hat{S}$ such that the projection $\pi : S' \to S \cap Q_i$ is a bijection. After computing $f(S'; \mathbf{x}, x_{k+1})$, we obtain $f(S \cap Q_i; \mathbf{x})$ by specializing at $x_{k+1} = 1$, using Theorem 1.2.8.

For $l \in \mathbb{Z}$, define $\hat{S} + l$ to be translation along the last coordinate, so that $\hat{S} + l = \hat{S} + (0, 0, \ldots, 0, l)$. Note that

$$f(\hat{S} + l; \mathbf{x}, x_{k+1}) = x_{k+1}^l f(\hat{S}; \mathbf{x}, x_{k+1}).$$

Let $\sigma = \sigma(d-k) = \lceil 2\omega(d-k) \rceil$, where $\omega(d-k)$ is the constant in the Flatness Theorem (Theorem 2.2.3). Then we define

$$S' = \hat{S} \setminus \bigcup_{l=1}^{\sigma} (\hat{S} + l).$$

We can compute $f(S';\mathbf{x},x_{k+1})$ using Theorem 1.2.10, since (without loss of generality) $\sigma(d-k)\leq\sigma(d)$, which is constant for fixed d. It remains to show that the projection $\pi : S' \to S\cap Q_i$ is a bijection. Fix some $a\in S\cap Q_i$. We want to show that a has a unique preimage in S', and we will use Corollary 2.2.8. Let

$$B = P_a = \{y\in\mathbb{R}^{d-k} :\ (a,y)\in P\}.$$

Let $\phi : B\cap\mathbb{Z}^{d-k}\to\mathbb{Z}$ be given by

$$\phi(y) = \langle w_i, y\rangle,$$

and let $Y = \phi(B\cap\mathbb{Z}^{d-k})$, as in the statement of Theorem 2.2.7. Let $\hat{S}_a$ be the preimage $\pi^{-1}(a)\subset\hat{S}$. Then

$$\hat{S}_a = \{(a,\langle w_i,y\rangle) :\ y\in P_a\cap\mathbb{Z}^{d-k}\} = \{a\}\times Y.$$

Let

$$Z = Y\setminus\bigcup_{l=1}^{\sigma}(Y+l),$$

as in the statement of Corollary 2.2.8. Then $\{a\}\times Z$ is the preimage of a under the map $\pi : S'\to S$. Therefore we must show that Z consists of a single point.

By Lemma 2.3.4, either $\text{width}(P_a,w_i)\leq 2\cdot\text{width}(P_a)$ or $\text{width}(P_a,w_i)\leq 1$. If $\text{width}(P_a,w_i)\leq 2\cdot\text{width}(P_a)$, then Z consists of a single point, by Corollary 2.2.8. If $\text{width}(P_a,w_i)\leq 1$, then Y consists of a single point (or perhaps 2 points), and therefore Z is again a single point.

Therefore the map $\pi : S'\to S\cap Q_i$ is a bijection, and so we may obtain $f(S\cap Q_i;\mathbf{x})$ by specializing $f(S';\mathbf{x},x_{k+1})$ at $x_{k+1}=1$, using Theorem 1.2.8. $\square$

CHAPTER III

Applications

We turn now to several applications of Theorem 1.1.15.

3.1 The Frobenius Problem

As in Chapter 1, let $a_1, a_2, \ldots, a_d$ be positive coprime integers, and let

$$S = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d : \ \lambda_i \in \mathbb{Z}_{\geq 0}\}$$

be the set of all nonnegative integer combinations of $a_1, a_2, \ldots, a_d$. We now have the tools to prove Theorem 1.1.5.

Theorem 1.1.5. *Let d be fixed. Then there exists a constant $s = s(d)$ and a polynomial time algorithm which, given $a_1, a_2, \ldots, a_d$, computes $f(S; x)$ in the form*

$$f(S; x) = \sum_{i \in I} \alpha_i \frac{x^{p_i}}{(1 - x^{b_{i1}}) \cdots (1 - x^{b_{is}})},$$

where $\alpha_i \in \mathbb{Q}$, $p_i \in \mathbb{Z}$, and $b_{ij} \in \mathbb{Z} \setminus \{0\}$.

Furthermore, there is a polynomial time algorithm that computes the number of positive integers not in S and computes the largest integer not in S.

Proof. We would like to apply Theorem 1.1.15. Suppose we let P be the polyhedron $\mathbb{R}^d_{\geq 0}$ and let $T : \mathbb{R}^d \to \mathbb{R}$ be defined by

$$T(\lambda_1, \lambda_2, \ldots, \lambda_d) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d.$$

Then we do have that $S = T(P \cap \mathbb{Z}^d)$. Unfortunately, we cannot directly apply Theorem 1.1.15, because P is unbounded; the theorem requires that P be a polytope. This problem will occur quite often in these applications. The key to fixing this problem is that the unbounded part of S will generally have a simple structure. In this case, we know that every sufficiently large integer is in S. We take some bound N on the largest integer not in S. For example, in [EG72], it is shown that $N = \lceil 2t^2/d \rceil$ works, where $t = \max\{a_1, a_2, \ldots, a_d\}$. It is important that this bound be polynomial in the a_i (that is, that $\log N$ be polynomial in the input size).

Now let

$$P' = \big\{(\lambda_1, \lambda_2, \ldots, \lambda_d) \in \mathbb{R}^d : \ \lambda_i \geq 0, \text{for all } i, \text{ and } \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d \leq N\big\}.$$

Then P' *is* bounded, and S is the disjoint union of $T(P' \cap \mathbb{Z}^d)$ and $\{N+1, N+2, \ldots\}$. Using Theorem 1.1.15, we may find $f(T(P' \cap \mathbb{Z}^d); x)$ in polynomial time, and then

$$f(S; x) = f(T(P' \cap \mathbb{Z}^d); x) + \frac{x^{N+1}}{1-x}.$$

Now we turn to computing the number of positive integers not in S and the largest integer not in S. Let S' be the set of positive integers which are not in S. Then $S' = \mathbb{Z}_{\geq 0} \setminus S$, and so

$$f(S'; x) = \frac{1}{1-x} - f(S; x).$$

Specializing $f(S'; x)$ at $x = 1$ (using Theorem 1.2.8) gives the number of positive integers not in S.

Note that the largest integer not in S is the degree of $f(S'; x)$ as a polynomial. We also have an explicit bound on the degree, in particular $\lceil 2t^2/d \rceil$, where $t = \max\{a_1, a_2, \ldots, a_d\}$. We can then find the largest integer not in S using the following lemma, and the proof is finished. $\square$

Lemma 3.1.1. *For fixed s, there is a polynomial time algorithm which, given a generating function $f(S;x)$ in the form*

$$f(S;x) = \sum_{i \in I} \alpha_i \frac{x^{p_i}}{(1-x^{b_{i1}}) \cdots (1-x^{b_{is}})},$$

where $\alpha_i \in \mathbb{Q}$, $p_i \in \mathbb{Z}$, and $b_{ij} \in \mathbb{Z} \setminus \{0\}$, and given a known bound N on the degree of $f(S;x)$, computes the degree of $f(S;x)$.

Proof. Let n be the degree of $f(S;x)$. We will find n using a binary search. Let $m_0 = 0$ and $M_0 = N$. Then we know that

$$m_0 \leq n \leq M_0.$$

Let $a_0 = \lceil (M_0 + m_0)/2 \rceil$. We would like to decide whether

$$m_0 \leq n \leq a_0 - 1 \text{ or } a_0 \leq n \leq M_0.$$

To do this, let $I_0 = \{a_0, a_0 + 1, \ldots, M_0\}$. Then we know

$$f(I_0;x) = \frac{x^{a_0} - x^{M_0+1}}{1-x}.$$

Let $g_0(x) = f(S \cap I_0; x)$, which we can find in polynomial time, by Theorem 1.2.10. Using Theorem 1.2.8, we may specialize at $x = 1$, and compute $g_0(1) = |S \cap I_0|$.

If $g_0(1) = 0$, then $S \cap I_0$ is empty, and we know

$$m_0 \leq n \leq a_0 - 1.$$

In this case, we let $m_1 = m_0$ and $M_1 = a_0 - 1$, and repeat the process.

If $g_0(1) > 0$, then $S \cap I_0$ is nonempty, and we know

$$a_0 \leq n \leq M_0.$$

In this case, we let $m_1 = a_0$ and $M_1 = M_0$, and repeat the process.

The size of the interval $[m_i, M_i]$ is cut in half at each step of the algorithm, so after $\log N$ repetitions, we will have $m_i = M_i$, and this number is n, the degree of $f(S; x)$. $\square$

3.2 Hilbert Series for Monomial Ideals

Let $a_1, a_2, \ldots, a_d \in \mathbb{Z}^k_{\geq 0}$ be given, and let

$$S = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d : \ \lambda_i \in \mathbb{Z}_{\geq 0}, \text{ for all } i\}.$$

We would like to find $f(S; \mathbf{x})$. This is a generalization of the Frobenius problem, which corresponds to the case $k = 1$.

We may also think of $f(S; \mathbf{x})$ as a *Hilbert series*. Let R be a $\mathbb{Z}^k$-graded ring over a field, for some k (we will provide an example shortly). Then the set of elements of R that are homogeneous of degree s, for a given $s \in \mathbb{Z}^k$, form a vector space over the field. Define $\dim_s$ to be the dimension of this vector space. Then the Hilbert series, $H_{\mathbb{Z}^k}(\mathbf{z})$ is defined to be the generating function

$$H_{\mathbb{Z}^k}(\mathbf{z}) = \sum_{s \in \mathbb{Z}^k} \dim_s \cdot \mathbf{z}^s,$$

where $\mathbf{z} \in \mathbb{C}^k$. See Section 10.4 of [Eis95], for example, for more background on Hilbert series.

Example 3.2.1. Let R be the polynomial ring $\mathbb{C}[x, y]$. We may think of R as having a $\mathbb{Z}$-grading given by $\deg(x^a y^b) = a + b$. Then the degree i homogeneous part of R is $\mathbb{C}x^i + \mathbb{C}x^{i-1}y + \mathbb{C}x^{i-1}y^2 + \cdots + \mathbb{C}y^i$, and $\dim_i = i + 1$. Then

$$H_{\mathbb{Z}}(z) = 1 + 2z + 3z^2 + \cdots = \frac{1}{(1-z)^2}.$$

Note that $H_{\mathbb{Z}}(z)$ can be written nicely as a short rational generating function.

Example 3.2.2. We may also think of $R = \mathbb{C}[x, y]$ as having a $\mathbb{Z}^2$-grading given by $\deg(x^a y^b) = (a, b)$. In this case, the degree (a, b) homogeneous part of R is $\mathbb{C}x^a y^b$, and $\dim_{(a,b)} = 1$. Then

$$H_{\mathbb{Z}^2}(z_1, z_2) = 1 + z_1 + z_2 + z_1^2 + z_1 z_2 + z_2^2 + \cdots = \frac{1}{(1 - z_1)(1 - z_2)}.$$

Note that $H_{\mathbb{Z}}(z) = H_{\mathbb{Z}^2}(z, z)$.

Now let R be the monomial ring $\mathbb{C}[\mathbf{x}^{a_1}, \mathbf{x}^{a_2}, \ldots, \mathbf{x}^{a_d}]$, where $a_i \in \mathbb{Z}^k_{\geq 0}$ for all i, and $\mathbf{x} = (x_1, x_2, \ldots, x_k)$ (see, for example, [BS98]). Let R have the standard $\mathbb{Z}^k$-grading defined above. For $s \in \mathbb{Z}^k$, $\mathbf{x}^s$ is in R if and only if, for some $\lambda_1, \lambda_2, \ldots, \lambda_d \in \mathbb{Z}_{\geq 0}$, we have

$$\mathbf{x}^s = (\mathbf{x}^{a_1})^{\lambda_1} (\mathbf{x}^{a_2})^{\lambda_2} \cdots (\mathbf{x}^{a_d})^{\lambda_d} = \mathbf{x}^{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d}.$$

Then $\mathbf{x}^s$ is in R if and only if $s \in S$, where

$$S = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d : \ \lambda_i \in \mathbb{Z}_{\geq 0} \text{ for all } i\}.$$

Therefore

$$H_{\mathbb{Z}^k}(\mathbf{z}) = f(S; \mathbf{z}).$$

We have the following proposition, from [BW03], which says that we can find $f(S; \mathbf{x})$ in polynomial time.

Proposition 3.2.3. *(from Section 7.3 of [BW03]) Let $a_1, a_2, \ldots, a_d \in \mathbb{Z}^k_{\geq 0}$ be given. Let*

$$S = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d : \ \lambda_i \in \mathbb{Z}_{\geq 0} \textit{ for all } i\},$$

let R be the $\mathbb{Z}^k$-graded ring

$$\mathbb{C}[\mathbf{x}^{a_1}, \mathbf{x}^{a_2}, \ldots, \mathbf{x}^{a_d}],$$

and let $H_{\mathbb{Z}^k}(\mathbf{z})$ be the Hilbert series for R. Then $f(S;\mathbf{z}) = H_{\mathbb{Z}^k}(\mathbf{z})$, and we may compute this generating function in polynomial time (for fixed d), in the form given in Theorem 1.1.15.

Sketch of proof: The full proof is given in Section 7.3 of [BW03], but we will sketch it here. Let $T : \mathbb{R}^d \to \mathbb{R}^k$ be defined by

$$T(\lambda_1, \lambda_2, \ldots, \lambda_d) = \lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_d a_d.$$

Then $S = T(\mathbb{Z}^d_{\geq 0})$. As in Theorem 1.1.5, we cannot directly apply Theorem 1.1.15, because $\mathbb{R}^d_{\geq 0}$ is an *unbounded* polyhedron. Again, though, the infinite part of S is "uninteresting." In this case,

$$g(S;\mathbf{z}) := f(S;\mathbf{z})(1-\mathbf{z}^{a_1})(1-\mathbf{z}^{a_2})\cdots(1-\mathbf{z}^{a_d})$$

is a polynomial, and we may compute a specific bound, L, on the degree of g (see Section 7.3 of [BW03]).

Now if $\Delta \subset \mathbb{R}^k$ is the simplex

$$\Delta = \left\{(\mu_1, \mu_2 \ldots, \mu_k) \in \mathbb{R}^k_{\geq 0} : \ \mu_1 + \mu_2 + \cdots + \mu_k \leq L\right\},$$

then $P = T^{-1}(\Delta)$ is now a polytope, and we may compute $f(S';\mathbf{z})$, where $S' = T(P \cap \mathbb{Z}^d)$. If we let

$$g(S';\mathbf{z}) = f(S';\mathbf{z})(1-\mathbf{z}^{a_1})(1-\mathbf{z}^{a_2})\cdots(1-\mathbf{z}^{a_d}),$$

then

$$g(S;\mathbf{z}) = g(S';\mathbf{z}) \star f(\Delta \cap \mathbb{Z}^k;\mathbf{z}),$$

where $\star$ is the Hadamard product (see Section 1.2). Using Theorem 1.2.3 and Theorem 1.2.10, we may compute $g(S;\mathbf{z})$, and hence we may compute $f(S;\mathbf{z})$. $\square$

3.3 Neighbors and Neighborhood Complexes

In Section 1.3, we introduced the neighborhood complex. Suppose we are given an $n \times d$ integer matrix A such that the polyhedron

$$K_b = \left\{x \in \mathbb{R}^d : \ Ax \leq b\right\}$$

is bounded, for any $b \in \mathbb{R}^n$. Recall that (for generic A) we say $\{h^0, h^1, \ldots, h^k\} \subset \mathbb{Z}^d$ is a k-dimensional simplex in the neighborhood complex, $C = C(A)$, if, for some $b \in \mathbb{R}^d$, the polytope K_b contains $h^0, h^1, \ldots, h^k$ but contains no integer points in its interior. Also recall, by Proposition 1.3.12, that the maximal simplices of C have dimension at most $2^d - 1$. Given $1 \leq k \leq 2^d - 1$, define the generating function

$$g_k(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k) = \sum_{\{0, h^1, h^2, \ldots, h^k\} \in C} \mathbf{x}_1^{h^1} \mathbf{x}_2^{h^2} \cdots \mathbf{x}_k^{h^k},$$

where $\mathbf{x}_i \in \mathbb{C}^d$. We would like to find this generating function, and the following proposition says we can.

Proposition 3.3.1. *Fix d. There is a polynomial time algorithm that, given a (generic) $n \times d$ integer matrix A, computes $g_k(\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_k)$ in the form given in Theorem 1.1.15, for all $1 \leq k \leq 2^d - 1$.*

Remark: This is true for non-generic matrices A (as defined in Section 1.3) as well, but, for the sake of clarity, we prove it here for generic A.

Proof. Choose k with $1 \leq k \leq 2^d - 1$. Let $a_1, a_2, \ldots, a_n$ be the rows of A, and let $h^0 = 0$ throughout. Given $(h^1, h^2, \ldots, h^k) \in (\mathbb{R}^d)^k$, we want to know the $b = (b_1, b_2, \ldots, b_n)$ such that K_b is the smallest polytope (among all $K_{b'}$ with $b' \in \mathbb{R}^n$) that contains $h^0, h^1, h^2, \ldots, h^k$. Then we would have that $\{h^0, h^1, h^2, \ldots, h^k\}$ is in C if and only if K_b has no integer points in its interior. We know that

$$b_i = \max\left\{\langle a_i, h^j \rangle : \ 0 \leq j \leq k\right\}.$$

We will first divide up $(\mathbb{R}^d)^k$ into M pieces, where M is polynomial in the input size, such that on a particular piece, we know, for each i, at which j this maximum is achieved.

We do this as follows. We define $n\binom{k+1}{2}$ hyperplanes $H_{ij_1j_2}$, for $1 \leq i \leq n$ and $0 \leq j_1 < j_2 \leq k$, by

$$H_{ij_1j_2} = \left\{(h^1, h^2, \ldots, h^k) \in (\mathbb{R}^d)^k : \ \langle a_i, h^{j_1}\rangle = \langle a_i, h^{j_2}\rangle\right\}.$$

These hyperplanes cut $(\mathbb{R}^d)^k$ into polyhedral pieces. At first glance, it might seem that there could be $2^{n\binom{k+1}{2}}$ full-dimensional pieces in this decomposition, which would be exponential in the input size, but in fact there are at most $\Phi(dk, n\binom{k+1}{2})$, where

$$\Phi(D, N) = \binom{N}{0} + \binom{N}{1} + \cdots + \binom{N}{D}.$$

This can be proved by induction on D and N, see for example Section 6.1 of [Mat02]. $\Phi(dk, n\binom{k+1}{2})$ is a polynomial in n, since d is fixed and $k \leq 2^d - 1$.

Now let us take a particular piece, P, the closure of one of the cells of the decomposition. It is enough to calculate the generating function for $\{0, h^1, h^2, \ldots, h^k\} \in C$ such that $h = (h^1, h^2, \ldots, h^k) \in P$, because we can patch these pieces together using Lemma 2.3.6 to find $g_k(\mathbf{x}_1, \mathbf{x}_2 \ldots, \mathbf{x}_k)$. Furthermore, Proposition 1.3.14 gives a bound on $\|h^j\|_\infty$ such that $\{0, h^1, h^2, \ldots, h^k\} \in C$, so we need only look at a bounded portion, P', of P. For each i with $1 \leq i \leq n$, let j_i be the j where the maximum

$$\max\left\{\langle a_i, h^j\rangle : \ 0 \leq j \leq k\right\}$$

is achieved, for every $h = (h^1, h^2, \ldots, h^k) \in P'$. Then if we take $b_i = \langle a_i, h^{j_i}\rangle$, for $1 \leq i \leq n$, K_b is the smallest polytope (of the $K_{b'}$ such that $b' \in \mathbb{R}^n$) containing $0 = h^0, h^1, h^2, \ldots, h^k$.

Then $\{0, h^1, h^2, \ldots, h^k\}$ is in C if and only K_b contains no integer points in its interior, that is, if and only if $K_{b-1} \cap \mathbb{Z}^d = \emptyset$, where $b-1 = (b_1-1, b_2-1, \ldots, b_n-1)$. Define

$$K(h) = K_{b-1},$$

and note that $b-1$ is a linear function of h, for $h \in P'$.

Define Q to be the polytope

$$Q = \left\{(h, x) \in (\mathbb{R}^d)^k \times \mathbb{R}^d : \ h \in P' \text{ and } x \in K(h)\right\},$$

and let $T : (\mathbb{R}^d)^k \oplus \mathbb{R}^d \to (\mathbb{R}^d)^k$ be defined by

$$T(h, x) = h.$$

Then $T\left(Q \cap \left[(\mathbb{Z}^d)^k \times \mathbb{Z}^d\right]\right)$ is exactly the $h \in P'$ such that $K(h)$ is nonempty, that is, the h such that $\{0, h^1, \ldots, h^k\}$ is *not* in C. Then the generating function we are looking for is

$$f\left(P' \cap (\mathbb{Z}^d)^k; \mathbf{x}\right) - f\big(T(Q \cap \left[(\mathbb{Z}^d)^k \times \mathbb{Z}^d\right]); \mathbf{x}\big),$$

which we may compute using Theorems 1.1.15 and 1.2.3. The proof follows. □

Note that there are other types of test sets, including Schrijver's universal test set and Graver's test set (see [Tho95]), which can also be defined. The methods used in this chapter can be applied to see that these also have short rational generating functions.

3.4 Hilbert Bases

Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}^d$ be linearly independent vectors, and let K be the cone generated by $a_1, a_2, \ldots, a_n$, that is,

$$K = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n : \ \lambda_1, \ldots, \lambda_n \in \mathbb{R}_{\geq 0}\}.$$

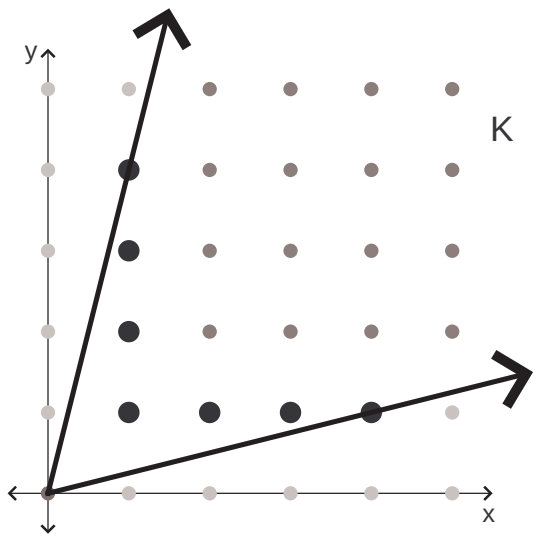


Figure 3.4.1: Example 3.4.2, Hilbert basis of cone K generated by $(N, 1)$ and $(1, N)$

We will assume that K is pointed, that is, that 0 is a vertex of K. We say that a set $B \subset K \cap \mathbb{Z}^d$ is a *Hilbert basis* if every point in $K \cap \mathbb{Z}^d$ can be written as a nonnegative integer combination of the points in B. Hilbert bases are closely related to the study of toric varieties (see [Ewa96] or [Ful93]) and of total dual integrality in integer programming (see Section 22.3 of [Sch86]).

We call B a *minimal Hilbert basis* if no points from B are superfluous (that is, none can be written as a sum of other points in B). When K is pointed, there is a unique minimal Hilbert basis (see Section 16.4 of [Sch86]). This unique basis can be defined as the set of *indecomposable* elements of $K \cap \mathbb{Z}^d$, that is, the set of points v which cannot be written as $v = v_1 + v_2$, where v_1 and v_2 are nonzero integer points in K.

The cardinality of B can be exponentially large in the input size of $a_1, a_2, \ldots, a_n$.

Example 3.4.2. Let $n = d = 2$, $a_1 = (N, 1)$ and $a_2 = (1, N)$ (see Figure 3.4.1).

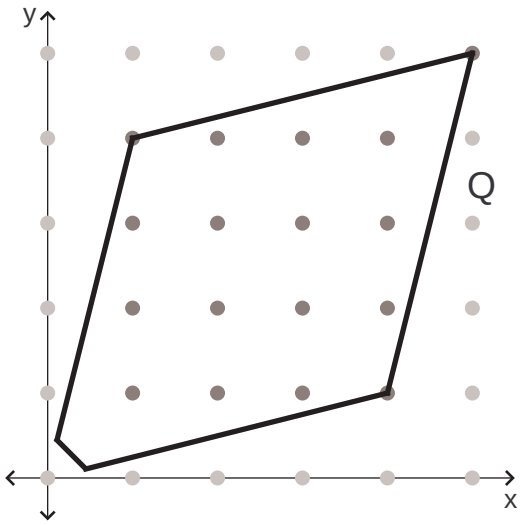


Figure 3.4.3: Q, such that $Q \cap \mathbb{Z}^2 = Z \cap \mathbb{Z}^2 \setminus \{0\}$

Then the minimal Hilbert basis is

$$B = \big\{(1,1),(2,1),\ldots,(N,1),(1,2),(1,3),\ldots,(1,N)\big\},$$

which contains $2N-1$ elements. Nevertheless, $f(B;\mathbf{x})$ is can be written as a short rational generating function,

$$\begin{aligned} f(B;x,y) &= (xy + x^2y + \cdots + x^Ny) + (xy^2 + xy^3 + \cdots + xy^N) \\ &= \frac{xy - x^{N+1}y}{1-x} + \frac{xy^2 - xy^{N+1}}{1-y}. \end{aligned}$$

In fact, we have the following proposition, which says that $f(B;\mathbf{x})$ can always be written as a short rational generating function.

Proposition 3.4.4. *For fixed d, there is a polynomial time algorithm which, given $a_1, a_2, \ldots, a_n \in \mathbb{Z}^d$ such that 0 is a vertex of K (the cone generated by $a_1, a_2, \ldots, a_n$), computes $f(B;\mathbf{x})$ in the form given in Theorem 1.1.15, where B is the minimal Hilbert basis of K.*

Proof. Let Z be the *zonotope* generated by $a_1, a_2, \ldots, a_n$, that is,

$$Z = \{\lambda_1 a_1 + \lambda_2 a_2 + \cdots + \lambda_n a_n : \ 0 \leq \lambda_i \leq 1 \text{ for all } i\}.$$

We will show that $B \subset Z$. Indeed, suppose $v \in K \cap \mathbb{Z}^d$ but $v \notin Z$. Then $v = \sum_i \lambda_i a_i$, where $\lambda_i \geq 0$, for all i, and $\lambda_j > 1$, for some j. Therefore

$$v = (v - a_j) + a_j$$

is a decomposition of v into nonzero integer vectors in K, and so $v \notin B$.

We construct a polytope Q (such as the one pictured in Figure 3.4.3, continuing Example 3.4.2) so that

$$Q \cap \mathbb{Z}^d = Z \cap \mathbb{Z}^d \setminus \{0\}.$$

For example, take some $l \in \mathbb{Z}^d$ such that $\langle l, a_i \rangle > 0$, for all i (which we can do since K is pointed). Then

$$Q = Z \cap \{x \in \mathbb{R}^d : \ \langle l, x \rangle \geq 1\}$$

works.

Now let $P = Q \times Q$ and let $T : \mathbb{R}^d \oplus \mathbb{R}^d \to \mathbb{R}^d$ be defined by $T(x, y) = x + y$. Let $S_1 = T(P \cap \mathbb{Z}^{2d})$. Then S_1 is exactly the set of *decomposable* elements of $K \cap \mathbb{Z}^d$, and we may compute $f(S_1; \mathbf{x})$ using Theorem 1.1.15. Let $S_2 = Q \cap \mathbb{Z}^d$, which we may compute using Theorem 1.2.3. Then $B = S_2 \setminus S_1$, and $S_1 \subset S_2$, and so

$$f(B; \mathbf{x}) = f(S_2; \mathbf{x}) - f(S_1; \mathbf{x}),$$

and the proof follows. □

As usual, once we have obtained $f(B; \mathbf{x})$, we may compute $|B|$ and other quantities.

3.5 Algebraic Integer Programming

In this section, we will examine some applications of Theorem 1.1.15 to algebraic integer programming. For definitions of algebraic terms used in this section, see [Eis95], for example. Throughout we will fix an $m \times n$ integer matrix A and an integer vector $c \in \mathbb{Z}^n$. For $b \in \mathbb{Z}^m$, we have an integer program

$$IP_{A,c}(b) = \min\big\{\langle c, u\rangle : \ u \in \mathbb{N}^n \text{ and } Au = b\big\},$$

where $\mathbb{N} = \{0, 1, 2, \ldots\}$. We will assume that we have chosen A such that the set $\{u \in \mathbb{R}^n_{\geq 0} : \ Au = b\}$ is bounded for all b. Note that this is a different formulation of the integer programming problem than we used in Section 1.3, but it is easy to go from one formulation to the other. We are interested in this family of integer programs, as b varies and A and c remain fixed.

If A were chosen at random in $\mathbb{R}^{m\times n}$, then, with probability one, for each b there would be a unique u which achieves the optimum $IP_{A,c}(b)$. We are constraining A to be integral, however, so this will often not happen. To combat this problem, we will assume that we have a total order $\prec$ on $\mathbb{N}^n$ such that

1. if $\langle c, u\rangle < \langle c, v\rangle$, then $u \prec v$
2. if $u \prec v$, then, for all $w \in \mathbb{N}^n$, $u + w \prec v + w$.

The first condition ensures that $\prec$ only "breaks ties" between u and v such that $\langle c, u\rangle = \langle c, v\rangle$, and the second condition is needed to ensure that these ties are broken consistently. For example, a possible order $\prec$ would be $u \prec v$ if either

- $\langle c, u\rangle < \langle c, v\rangle$, or
- $\langle c, u\rangle = \langle c, v\rangle$ and u precedes v lexicographically.

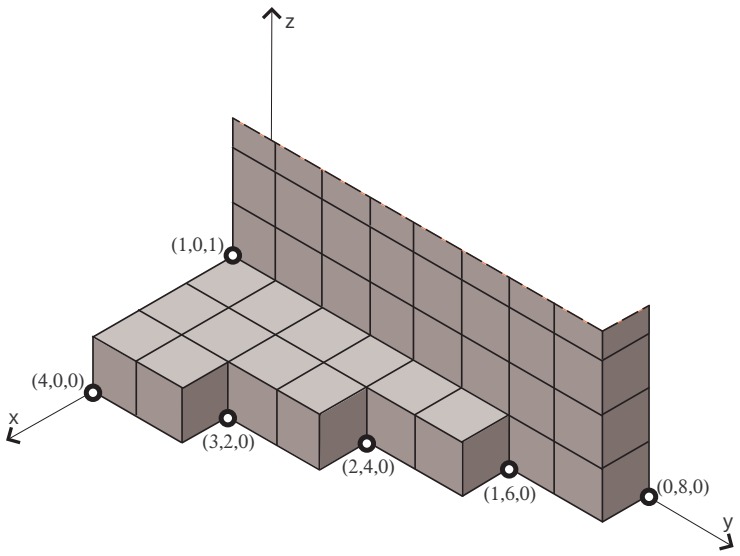


Figure 3.5.1: $\mathcal{N}$ for Example 3.5.2

We can now formulate the integer programming problem as a problem with a unique optimum:

$$IP_{A,\prec}(b) = \text{ the minimum } u \in \mathbb{N}^n \text{ (with respect to } \prec) \text{ such that } Au = b.$$

We will define some subsets of $\mathbb{N}^n$ based on this family of integer programs. Let $\mathcal{O}$ be the set of $u \in \mathbb{N}^n$ which are optimal in the appropriate integer program $IP_{A,\prec}(Au)$. Let $\mathcal{N} = \mathbb{N}^n \setminus \mathcal{O}$ be the set of u which are not optimal. $\mathcal{N}$ is an ideal, that is, if $u \in \mathcal{N}$ (i.e., there exists a $v \in \mathbb{N}^n$ such that $Au = Av$ and $v \prec u$) then $u + w \in \mathcal{N}$ for all $w \in \mathbb{N}^n$ (because $A(u + w) = A(v + w)$, and $v + w \prec u + w$). Let $\mathcal{M}$ be the set

$$\mathcal{M} = \{u \in \mathcal{N} : \ u - w \notin \mathcal{N}, \text{ for any } w \in \mathbb{N}^n \setminus \{0\}\}.$$

Then $\mathcal{M}$ is a minimal set of generators for the ideal $\mathcal{N}$.

Example 3.5.2. Consider the integer programming family

$$\min 10000x + 100y + z : \ (x, y, z) \in \mathbb{N}^3 \text{ and } 2x + 5y + 8z = b,$$

as b varies in $\mathbb{Z}$ (see [Tho03] for a more thorough treatment of this example). The ideal $\mathcal{N}$ is generated by

$$\mathcal{M} = \Big\{(0,8,0),(1,6,0),(2,4,0),(3,2,0),(4,0,0),(1,0,1)\Big\}.$$

Figure 3.5.1 is a picture of $\mathcal{N}$. Integer points on the pictured surface, as well as points on the near side of the surface, are in $\mathcal{N}$ (the dotted line depicts where the surface has been cut off: in reality, it continues to infinity). Integer points hidden by the surface are in $\mathcal{O}$, which consists of twelve points $(p,q,0)$ and eight infinite rays of points $(0,i,j)$, where $0 \leq i \leq 7$ and $j \in \mathbb{N}$. The six labelled points are the set $\mathcal{M}$.

The family $IP_{A,\prec}(b)$ is closely related to some algebraic objects. Define the ideal I_A of $k[x_1, x_2, \ldots, x_n]$ by

$$I_A = \langle \mathbf{x}^u - \mathbf{x}^v : \ u, v \in \mathbb{N}^n \text{ and } Au = Av \rangle.$$

Let $\text{in}_\prec(I_A)$ be the initial ideal of I_A with respect to the order $\prec$, and let $\mathcal{G}$ be the reduced Gröbner basis for I_A with respect to $\prec$. Then we have the following proposition relating $IP_{A,\prec}$ to these algebraic objects (see [Tho03] or Chapter 5 of [Stu96] for these facts plus a general overview of these relationships).

Proposition 3.5.3. *Let $\mathcal{O}, \mathcal{N}, \mathcal{M}, I_A, in_\prec(I_A)$, and $\mathcal{G}$ be defined as above. Then*

1. $\mathcal{G} = \{\mathbf{x}^u - \mathbf{x}^v : \ u \in \mathcal{M}, v \in \mathcal{O}, \text{ and } Au = Av\}$,
2. *if $u \in \mathbb{N}^n$, and if $\mathbf{x}^{u^*}$ is the (unique) normal form for $\mathbf{x}^u$ with respect to $\mathcal{G}$, then u^* is the optimal solution to $IP_{A,\prec}(Au)$,*
3. *The set $\{u - v : \ (\mathbf{x}^u - \mathbf{x}^v) \in \mathcal{G}\}$ forms a test set for the family of integer programs $IP_{A,c}(b)$ (see Section 1.3 for discussion of test sets), and*
4. *$u \in \mathcal{N}$ if and only if $\mathbf{x}^u \in in_\prec(I_A)$.*

Theorem 1.1.15 has several applications to the algebraic study of integer programs.

Theorem 3.5.4. *(Theorem 1 of [DLHH$^+$04]) Let n and m be fixed. Then there is a polynomial time algorithm which, given an $m \times n$ integer matrix A and a term order $\prec$, computes*

$$f(\mathcal{G}; \mathbf{y}, \mathbf{z}) = \sum_{(\mathbf{x}^u - \mathbf{x}^v) \in \mathcal{G}} \mathbf{y}^u \mathbf{z}^v$$

as a short rational generating function, where $\mathcal{G}$ is the reduced Gröbner basis of I_A. Furthermore, given $f(\mathcal{G}; \mathbf{y}, \mathbf{z})$ and any monomial $\mathbf{x}^a$, the following tasks can be performed in polynomial time:

1. *Decide whether $\mathbf{x}^a$ is in normal form with respect to $\mathcal{G}$,*
2. *Perform one step of the division algorithm modulo $\mathcal{G}$, and*
3. *Compute the normal form of $\mathbf{x}^a$ modulo $\mathcal{G}$.*

Remark: The algorithm takes as input a term order of $\mathbb{N}^n$. We may assume that one is given by a nondegenerate $n \times n$ integer matrix W, so that

$$u \prec v \text{ if and only if } Wu \text{ lexicographically precedes } Wv.$$

Sketch of proof: By Proposition 3.5.3,

$$f(\mathcal{G}; \mathbf{x}, \mathbf{y}) = \sum_{\substack{u \in \mathcal{M}, v \in \mathcal{O}, \\ Au = Av}} \mathbf{x}^u \mathbf{y}^v.$$

We will first compute separately

$$m(\mathbf{x}) = \sum_{u \in \mathcal{M}} \mathbf{x}^u \text{ and } o(\mathbf{y}) = \sum_{v \in \mathcal{O}} \mathbf{y}^v.$$

Along the way, we will also compute

$$n(\mathbf{x}) = \sum_{u \in \mathcal{N}} \mathbf{x}^u \text{ and } h(\mathbf{x}, \mathbf{y}) = \sum_{\substack{u, v \geq 0, \\ Au = Av}} \mathbf{x}^u \mathbf{y}^v.$$

Computing $h(\mathbf{x}, \mathbf{y})$ is easy. It is the generating function for the integer points in a polyhedron, so we may use Theorem 1.2.3 to find it in polynomial time. To compute $n(\mathbf{x})$, recall that we input the term order $\prec$ as a $n \times n$ integer matrix W, and we say

$$u \prec v \text{ if and only if } Wu \text{ lexicographically precedes } Wv.$$

Define

$$P = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^n : \ x, y \geq 0, Ax = Ay, Wy \text{ lexicographically precedes } Wx\}.$$

P is an unbounded polyhedron (except that parts of its boundary are open, a technicality which we will not discuss). Let T be the projection $T : \mathbb{R}^n \oplus \mathbb{R}^n \to \mathbb{R}^n$, given by $T(x, y) = x$. Then $\mathcal{N}$, the set of non-optimal u, is $T(P \cap \mathbb{Z}^{2n})$. We then use Theorem 1.1.15 (we must deal with the fact that P is unbounded, using a similar method as in the proof of Proposition 3.2.3) to calculate $n(\mathbf{x})$.

Now we can compute

$$o(\mathbf{x}) = \left(\prod_{i=1}^{n} \frac{1}{1 - x_i} \right) - n(\mathbf{x}).$$

Also, we have

$$\mathcal{M} = \mathcal{N} \setminus \left(\bigcup_{i=1}^{n} \{u : \ u - e_i \in \mathcal{N}\} \right),$$

where e_i is the standard basis vector. Since

$$f\big(\{u : \ u - e_i \in \mathcal{N}\} ; \mathbf{x} \big) = x_i \cdot n(\mathbf{x}),$$

we may calculate $m(\mathbf{x})$ as a boolean combination of known generating functions, using Theorem 1.2.10.

Finally, to compute $f(\mathcal{G}; \mathbf{x}, \mathbf{y})$ itself. Let

$$H(\mathbf{x}; \mathbf{y}) = m(\mathbf{x}) \cdot o(\mathbf{y})$$

be the generating function for the set of (u, v) such that $u \in \mathcal{M}$ and $v \in \mathcal{O}$. Then, since $f(\mathcal{G}; \mathbf{x}, \mathbf{y})$ is the generating function for the set

$$\begin{aligned}&\big\{(u,v):\ u\in\mathcal{M}, v\in\mathcal{O}, Au=Av\big\}\\ =&\big\{(u,v):\ u\in\mathcal{M}, v\in\mathcal{O}\big\}\cap\big\{(u,v):\ u,v\in\mathbb{N}^n, Au=Av\big\},\end{aligned}$$

and we have computed $H(\mathbf{x}, \mathbf{y})$ and $h(\mathbf{x}, \mathbf{y})$, we may compute $f(\mathcal{G}; \mathbf{x}, \mathbf{y})$ as a boolean combination, using Theorem 1.2.10. □

Let us more closely examine $\mathcal{O}$, the set of u which are optimal in their integer program. If $u \in \mathbb{N}^n$ and $\tau \subset \{1, 2, \ldots, n\}$, then we say that (u, τ) is an *admissible pair* if

$$S_{u,\tau} := \{u + w :\ w \in \mathbb{N}^n \text{ and } w_i = 0 \text{ for } i \notin \tau\}$$

is contained in $\mathcal{O}$. We say that (u, τ) is a *standard pair* if (u, τ) is a admissible pair and there is no admissible pair (u', τ') such that $S_{u,\tau} \subsetneq S_{u',\tau'}$. There are a finite number of standard pairs, and the sets $S_{u,\tau}$, such that (u, τ) is a standard pair, cover all of $\mathcal{O}$. In Example 3.5.2, the standard pairs are

1. the twelve pairs $\big((p, q, 0), \emptyset\big)$, where $S_{u,\emptyset}$ is the point u and
2. the eight pairs $\big((0, i, 0), \{3\}\big)$, for $0 \leq i \leq 7$, where $S_{u,\{3\}}$ is the ray in the positive z direction with endpoint u.

Then we have the following proposition (Theorem 1.3 of [HT99]).

Proposition 3.5.5. *For $\tau \subset \{1, 2, \ldots, n\}$, let p_τ be the prime ideal $\langle x_j :\ j \notin \tau\rangle$. Then*

1. *p_τ is an associated prime of $in_\prec(I_A)$ if and only if (u, τ) is a standard pair for some $u \in \mathbb{N}^n$,*

2. *The multiplicity of* p_τ *as an associated prime is the number of* $u \in \mathbb{N}^n$ *such that* (u, τ) *is a standard pair, and*

3. *the arithmetic degree of* $in_\prec(I_A)$ *is the total number of standard pairs* (u, τ) *with* $u \in \mathbb{N}^n$ *and* $\tau \subset \{1, 2, \ldots, n\}$.

We have the following application of Theorem 1.1.15.

Theorem 3.5.6. *(Theorem 1 of [TW03]) Given* $A \in \mathbb{Z}^{m\times n}$, $c \in \mathbb{Z}^n$, *and* $\tau \subset \{1, 2, \ldots, n\}$, *let*

$$S^\tau = \{u \in \mathbb{N}^n : \ (u, \tau) \text{ is a standard pair}\},$$

and define the generating function

$$f(S^\tau; \mathbf{x}) = \sum_{u\in S^\tau} \mathbf{x}^u.$$

Then for fixed n, *there exists a polynomial time algorithm which, given* A, c, *and* τ *as above, computes* $f(S^\tau; \mathbf{x})$ *as a short rational generating function. Furthermore, the following are computable in polynomial time:*

1. *for each* $\tau \subset \{1, 2, \ldots, n\}$, *the multiplicity of* $p_\tau = \langle x_j : \ j \notin \tau\rangle$ *as an associated prime of* $in_\prec(I_A)$ *and*

2. *the arithmetic degree of* $in_\prec(I_A)$.

Proof. Given A, c, and τ, let $\Lambda = \{x \in \mathbb{Z}^n : \ Ax = 0\}$, let $r = \dim \Lambda$, and let $B \in \mathbb{Z}^{n\times r}$ be any matrix whose columns generate the lattice Λ. For $u \in \mathbb{N}^n$, let

$$Q_u = \{z \in \mathbb{R}^r : \ Bz \le u, (-cB) \cdot z \le 0\}.$$

Then Q_u is almost the image of the polytope $\{x \in \mathbb{R}^n : \ Ax = Au, x \ge 0\}$ under an affine transformation which bijectively maps $\{x \in \mathbb{Z}^n : \ Ax = Au\}$ to $\mathbb{Z}^r$, except that a constraint involving the objective function, c, has been added.

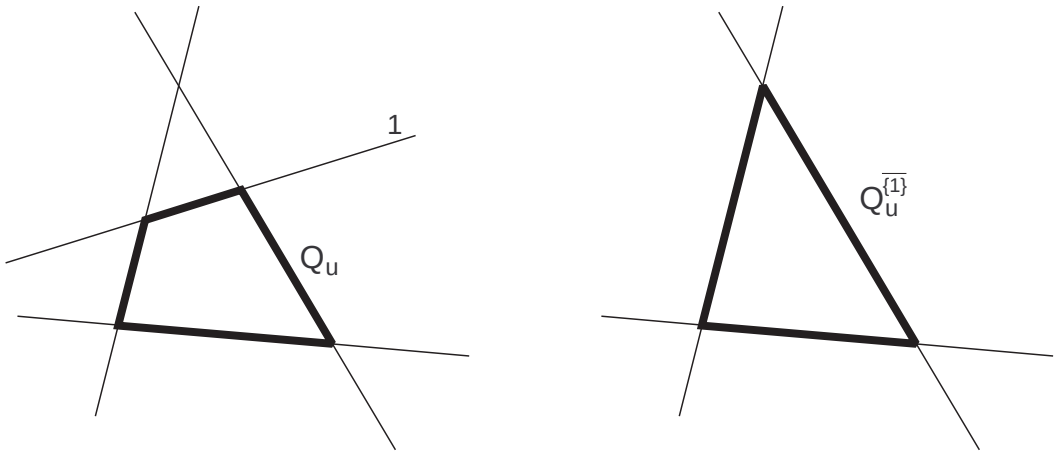


Figure 3.5.7: An example of (a) Q_u and (b) $Q_u^{\bar{\tau}}$

Let $Q_u^{\bar{\tau}}$ be the polyhedron

$$\{z \in \mathbb{R}^r : \ B^{\bar{\tau}} z \leq \pi_\tau(u), (-cB) \cdot z \leq 0\},$$

where $B^{\bar{\tau}}$ is the matrix obtained from B by deleting the rows indexed by τ, and $\pi_\tau : \mathbb{R}^n \to \mathbb{R}^{|\bar{\tau}|}$ is the projection that kills the coordinates indexed by τ. Then $Q_u^{\bar{\tau}}$ is the relaxation of Q_u obtained by removing the inequalities indexed by τ, see Figure 3.5.7 for an example. We will use the following fact.

Theorem 3.5.8. *(from Theorem 3.11 of [Tho03]) Let $\tau \subset \{1, 2, \ldots, n\}$ and $u \in \mathbb{N}^n$ be given. Then (u, τ) is a standard pair if and only if both*

1. *$Q_u^{\bar{\tau}} \cap \mathbb{Z}^r = \{0\}$ and*
2. *$Q_u^{\overline{\tau \cup \{i\}}}$ (that is, $Q_u^{\bar{\tau}}$ with one additional constraint removed) contains a non-zero lattice point, for all $i \notin \tau$.*

Note that if $Q_u^{\bar{\tau}}$ is unbounded for a given τ, then for no u is (u, τ) a standard pair, so we may assume that $Q_u^{\bar{\tau}}$ is a polytope.

We also need a bound $M \in \mathbb{R}_+$ such that $\log M$ is polynomial in the input size of A and c and such that if (u, τ) is a standard pair then $\|u\|_\infty \leq M$. This follows from Theorem 4.8 of [Tho03].

Let $P_u^{\bar{\tau}}$ be the set $Q_u^{\bar{\tau}} \backslash \{0\}$. Then by Theorem 3.5.8, we have the following corollary.

Corollary 3.5.9. *(u, τ) is a standard pair if and only if the following hold:*

1. $0 \in Q_u^{\bar{\tau}}$,
2. $P_u^{\bar{\tau}} \cap \mathbb{Z}^r = \emptyset$, *and*
3. $P_u^{\overline{\tau \cup \{i\}}} \cap \mathbb{Z}^r \neq \emptyset$ *for* $i \notin \tau$.

Let $P^\tau \subset \mathbb{R}^n \times \mathbb{R}^r$ be the set

$$\{(u, z) \in \mathbb{R}^n \times \mathbb{R}^r : \ 0 \leq u_i \leq M \text{ and } z \in P_u^{\bar{\tau}}\}.$$

P^τ is almost a polytope: it is bounded and defined by linear inequalities, except it is missing a piece

$$\{(u, 0) : \ 0 \leq u_i \leq M\}$$

from the boundary. The proof of Theorem 1.1.15 will still work for P^τ: the crucial points are that we can compute $f(P^\tau \cap (\mathbb{Z}^n \times \mathbb{Z}^r); \mathbf{x})$ in polynomial time and that Theorem 2.2.7 still applies since the missing piece is on the boundary.

Let $R^\tau = P^\tau \cap (\mathbb{Z}^n \times \mathbb{Z}^r)$, and let $\rho : \mathbb{R}^n \oplus \mathbb{R}^r \to \mathbb{R}^n$ be the projection $(u, z) \mapsto u$. Then

$$\rho(R^\tau) = \{u \in \mathbb{Z}^n : \ 0 \leq u_i \leq M \text{ and } P_u^{\bar{\tau}} \cap \mathbb{Z}^r \neq \emptyset\}.$$

Let

$$U^\tau = \{u \in \mathbb{Z}^n : \ 0 \leq u_i \leq M \text{ and } 0 \in Q_u^{\bar{\tau}}\}.$$

Then, by Corollary 3.5.9 we have

$$S^\tau = \Big[U^\tau \setminus \rho(R^\tau)\Big] \cap \Big[\bigcap_{i \notin \tau} \rho(R^{\tau \cup \{i\}})\Big].$$

By Theorem 1.2.3, since U^τ consists of the integer points in a polyhedron, we can compute (for fixed n) $f(U^\tau; \mathbf{x})$ in polynomial time, in the desired form. By Theorem 1.1.15, since R^τ consists of the integer points in a polytope, we can compute $f(\rho(R^\tau); \mathbf{x})$ in polynomial time, for all $\tau \subset \{, 2 \ldots, n\}$. By Theorem 1.2.10, since S^τ is a boolean combination of U^τ, $\rho(R^\tau)$, and $\rho(R^{\tau \cup \{i\}})$, and since we can compute $f(U^\tau; \mathbf{x})$, $f(\rho(R^\tau); \mathbf{x})$, and $f(\rho(R^{\tau \cup \{i\}}); \mathbf{x})$, we can compute $f(S^\tau; \mathbf{x})$ in polynomial time, as desired.

Furthermore, using Theorem 1.2.8, we can compute $f(S^\tau; 1)$, which is the number of standard pairs (u, τ) for a given τ, that is, we can compute the multiplicity of $p_\tau = \langle x_j : \ j \notin \tau \rangle$ as an associated prime of $\text{in}_\prec(I_A)$ (See Proposition 3.5.5). Summing this number over all $\tau \subset \{1, 2, \ldots, n\}$, we get the arithmetic degree of $\text{in}_\prec(I_A)$. $\square$

In addition, these algebraic ideas, combined with Theorem 1.1.15, can give us some information about the integer programming problems $IP_{A,c}(b)$. For the integer programming problem

$$IP_{A,c}(b) = \min\langle c, u \rangle : \ u \in \mathbb{N}^n \text{ and } Au = b,$$

we also have a linear relaxation

$$LP_{A,c}(b) = \min\langle c, u \rangle : \ u \in \mathbb{R}^n_{\geq 0} \text{ and } Au = b.$$

We know that $LP_{A,c}(b) \leq IP_{A,c}(b)$, and we would often like to know by how much they may differ (this difference is called the integer programming gap). Let

$$\text{gap}(A, c) = \max\big(IP_{A,c}(b) - LP_{A,c}(b)\big) \text{ over all } b \in \mathbb{N}^m.$$

Then we have the following.

Theorem 3.5.10. *(Theorem 1.2 of [HS04]) For fixed n, there is a polynomial time algorithm which, given $A \in \mathbb{Z}^{m\times n}$ and $c \in \mathbb{Z}^n$, computes gap(A, c).*

Sketch of proof: As we showed in the proof of Theorem 3.5.4, we may compute the generating function

$$o(\mathbf{x}) = \sum_{u\in\mathcal{O}} \mathbf{x}^u,$$

which is the generating function for the u which are optimal in $IP_{A,\prec}(Au)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}^m$ be the columns of A, let $c = (c_1, c_2, \ldots, c_n)$, and let $\mathbb{N}A = \{Au : u \in \mathbb{N}^n\}$. Note that for $b \notin \mathbb{N}A$, the integer programming problem has no solution (the feasible region is empty). Define

$$H_{IP}(\mathbf{y}, z) = o\big(\mathbf{y}^{\alpha_1} z^{c_1}, \mathbf{y}^{\alpha_2} z^{c_2}, \ldots, \mathbf{y}^{\alpha_n} z^{c_n}\big),$$

where $\mathbf{y} \in \mathbb{C}^m$. That is

$$H_{IP}(\mathbf{y}, z) = \sum_{b\in\mathbb{N}A} \mathbf{y}^b z^{IP_{A,c}(b)}.$$

We would also like to find

$$H_{LP}(\mathbf{y}, z) = \sum_{b\in\mathbb{N}A} \mathbf{y}^b z^{LP_{A,c}(b)}.$$

This is not too difficult, because $LP_{A,c}(b)$ is a piecewise linear function of b, and the pieces on which it is linear are polyhedral (we will need to use Theorem 1.2.3).

Next, we must use these two to get the generating function

$$G(\mathbf{y}, z) = \sum_{b\in\mathbb{N}A} \mathbf{y}^b z^{IP_{A,c}(b) - LP_{A,c}(b)}.$$

To compute $G(\mathbf{y}, z)$, we must use a variation of Lemma 1.2.11.

Finally, we notice that gap(A, c) is the degree of $G(\mathbf{y}, z)$ as a polynomial in z. Starting with a known upper bound for gap(A, c), we may find the degree using a binary search, exactly as we did to compute the Frobenius number in the proof of Theorem 1.1.5 (see Section 3.1). □

CHAPTER IV

The Neighborhood Complex and Generating Functions

In this chapter, we present an alternative approach for computing $f\big(T(P\cap\mathbb{Z}^d);\mathbf{x}\big)$. The previous method (see Chapter II) is probably not practical to implement. For example, several of the tools used, such as Theorem 1.2.10 (finding generating functions for boolean combinations of sets) or Lemma 2.3.4 (partitioning the image space into pieces based on flat directions), rapidly increase the complexity of the rational generating function, especially if repeatedly applied. On the other hand, the algorithm for finding the generating function for integer points in a polyhedron has proven practical: a version of it has been implemented [DLHTY04] as LattE. Extending LattE to find generating functions for the *projections* of integer points in polytopes seems to require some new mathematical ideas.

This chapter will examine one possible approach, involving neighborhood complexes (see Section 1.3 for definitions). In Section 4.1, we introduce this approach through an example. In Section 4.2, we state the result (Theorem 4.2.1). In Section 4.3, we examine some Euler characteristic calculations needed for the proof. In Section 4.4, we prove Theorem 4.2.1. In Section 4.5, we give some examples. Finally, in Section 4.6, we examine the non-generic case.

4.1 Introduction and Example

This new approach to generating functions will rely heavily on neighborhood complexes (see Section 1.3 for definitions). This method has its benefits, though it is not known (yet) how to use it to make a polynomial time algorithm. When the dimension of the kernel of T is at most 2, however, it does yield a polynomial time algorithm, one that would be much quicker than the original algorithm, in practice. In fact, it gives the "right" answer for the Frobenius problem with 3 generators:

$$f(S;x) = \frac{1 - x^{p_1} - x^{p_2} - x^{p_3} + x^{p_4} + x^{p_5}}{(1-x^{a_1})(1-x^{a_2})(1-x^{a_3})},$$

where p_i are quickly computable from the generators a_1, a_2, a_3.

This approach produces a new structural result (Theorem 4.2.1), and it also has the benefit of not needing heavy-handed tools such as Theorem 1.2.10 or Lemma 2.3.4. If the neighborhood complex in higher dimensions were to have the structural properties which L. Lovász conjectured it does (see Section 1.3 and [Lov89]), then this approach would provide a polynomial time algorithm which is much quicker than the original. Other structure (for example, a better way to compute the generating functions of neighbors) might also provide a more practical algorithm for Theorem 1.1.15.

This approach generalizes work of H. Scarf and K. Woods [SW03]. They consider $P = \{x \in \mathbb{R}^d : \ x_i \geq 0\}$, so that $T(P \cap \mathbb{Z}^d)$ is the additive semigroup generated by $T(e_1), T(e_2), \ldots, T(e_d)$ (where $e_1, e_2, \ldots, e_d$ is the standard basis of $\mathbb{R}^d$). See, for example, Corollary 4.5.4.

We first illustrate this approach with an example.

Example 4.1.1. Let $P = \big\{(x,y) \in \mathbb{R}^2 : \ x, y \geq 0\big\}$, let $T(x,y) = 2x + 5y$, and let $S = T(P \cap \mathbb{Z}^2)$. S is the Frobenius semigroup with two generators, 2 and 5.

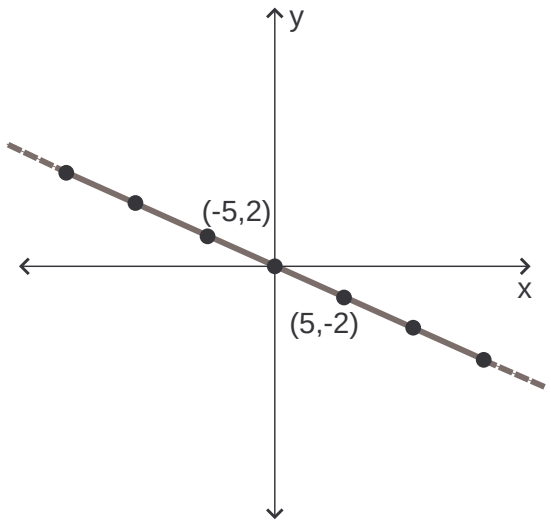


Figure 4.1.2: Neighborhood complex, C, for $T(x, y) = 2x + 5y$

We define a certain neighborhood complex, C, whose vertices are on the lattice $\{(x, y) \in \mathbb{Z}^2 : \ T(x, y) = 0\}$ (normally, we define the neighborhood complex on some $\mathbb{Z}^r$, but, in this case, it is more intuitive to define C on this lattice). This complex C will have vertices $(5k, -2k)$ and edges $\{(5k, -2k), (5(k + 1), -2(k + 1))\}$, where $k \in \mathbb{Z}$ (see Figure 4.1.2).

Given $a \in \mathbb{Z}$, this induces a complex on the integer points in $T^{-1}(a) \cap P$, as follows. First translate C by some vector $v_a \in \mathbb{Z}^2$ with $T(v_a) = a$, so that $C + v_a$ lies in the hyperplane $\{(x, y) \in \mathbb{R}^2 : \ T(x, y) = a\}$ (it doesn't matter what vector v_a we choose, since C is lattice invariant). Then let

$$C_a = \{(x, y) \in C + v_a : \ x, y \geq 0\},$$

the intersection of $C + v_a$ with the polyhedron P. Each C_a is a simplicial complex with vertices the integer points in $T^{-1}(a) \cap P$. Figure 4.1.3 illustrates these C_a in our example. The complex C_{17}, for example, consists of two vertices (in black) and one edge (in dark gray).

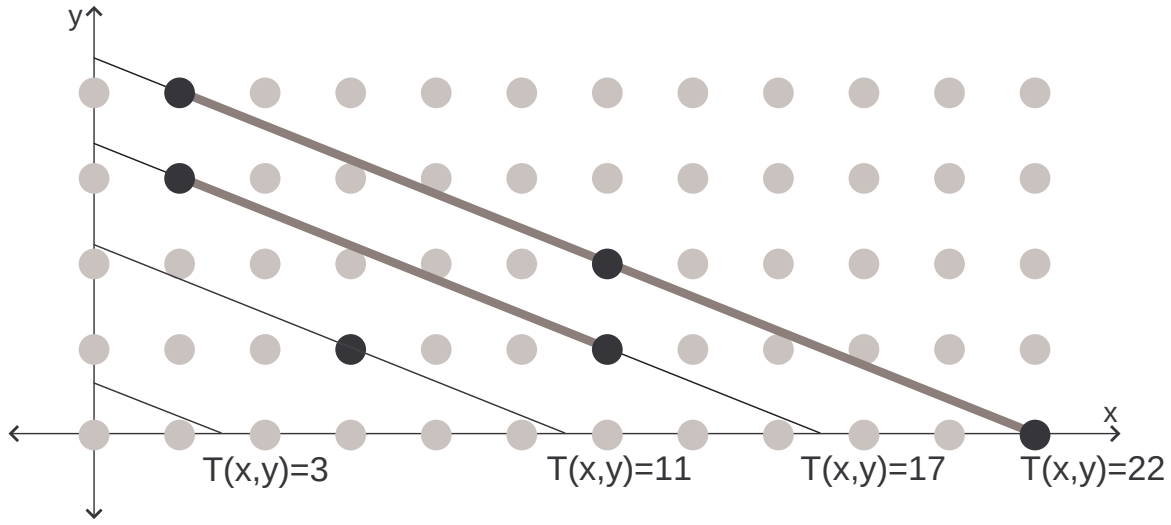


Figure 4.1.3: The complexes C_a

In Figure 4.1.3, we see that, for any $a \in \mathbb{Z}$,

$$\#\text{ of vertices in } C_a - \ \#\text{ of edges in } C_a = \begin{cases} 1, \text{ if } a \in T(P \cap \mathbb{Z}^d) \\ 0, \text{ otherwise} \end{cases}. \tag{4.1.4}$$

This can be viewed as an Euler characteristic calculation, and it relies on the fact that if C_a is nonempty then it is contractible.

We can compute the generating function

$$g(z) = \sum_{a \in \mathbb{Z}} (\ \#\text{ of vertices in } C_a) \cdot z^a.$$

Indeed

$$g(z) = (1 + z^2 + z^4 + \cdots)(1 + z^5 + z^{10} + \cdots) = \frac{1}{(1 - z^2)(1 - z^5)}.$$

For example, the integer point $(3, 1)$ satisfies $T(3, 1) = 11$, and it corresponds to the $(z^2)^3(z^5)^1 = z^{11}$ term in the expansion of $g(z)$.

If we could compute

$$h(z) = \sum_{a \in \mathbb{Z}} (\ \#\text{ of edges in } C_a) \cdot z^a,$$

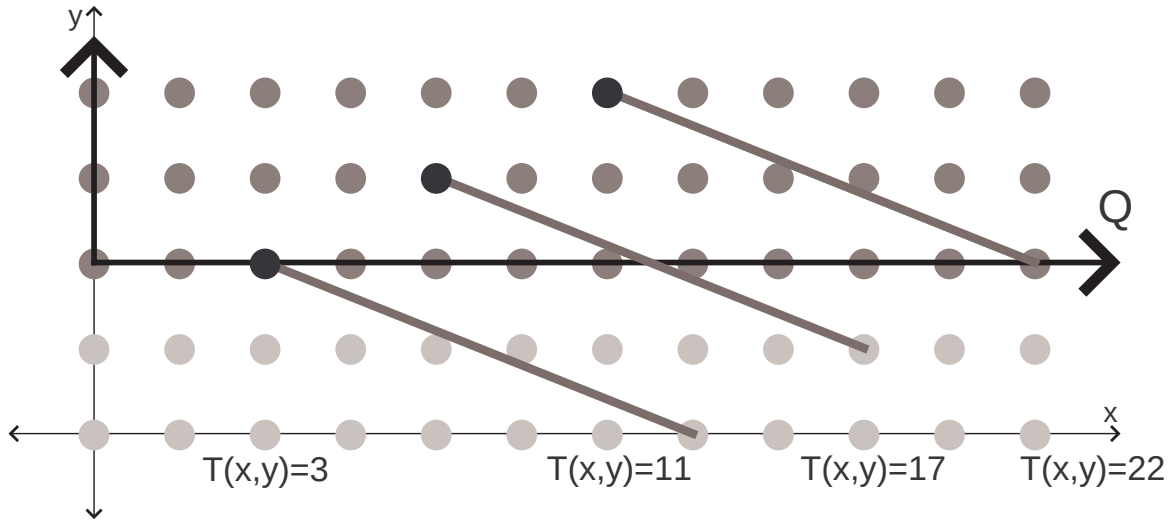


Figure 4.1.5: Bijection between integer points in Q and edges in the C_a

then, by (4.1.4), we would have

$$f\big(T(P\cap\mathbb{Z}^2);z\big)=g(z)-h(z).$$

Let $v=(5,-2)$ be the vector such that the edges of C_a are $\{c,c+v\}$. Let

$$\begin{aligned}Q&=\big\{(x,y)\in\mathbb{R}^2:\ (x,y)\in P \text{ and } (x,y)+v\in P\big\}\\&=\big\{(x,y)\in\mathbb{R}^2:\ x\geq 0 \text{ and } y\geq 2\big\}.\end{aligned}$$

Then, for any $a\in\mathbb{Z}$, there is a bijection between integer points $c\in T^{-1}(a)\cap Q$ and edges $\{c,c+v\}\in C_a$. For example, in Figure 4.1.5, the bijection maps the three black points to the three dark gray edges. We can easily calculate

$$h(z)=\frac{z^{10}}{(1-z^2)(1-z^5)},$$

and so

$$f\big(T(P\cap\mathbb{Z}^2);z\big)=g(z)-h(z)=\frac{1-z^{10}}{(1-z^2)(1-z^5)},$$

which is easy to see directly (see Section 1.1).

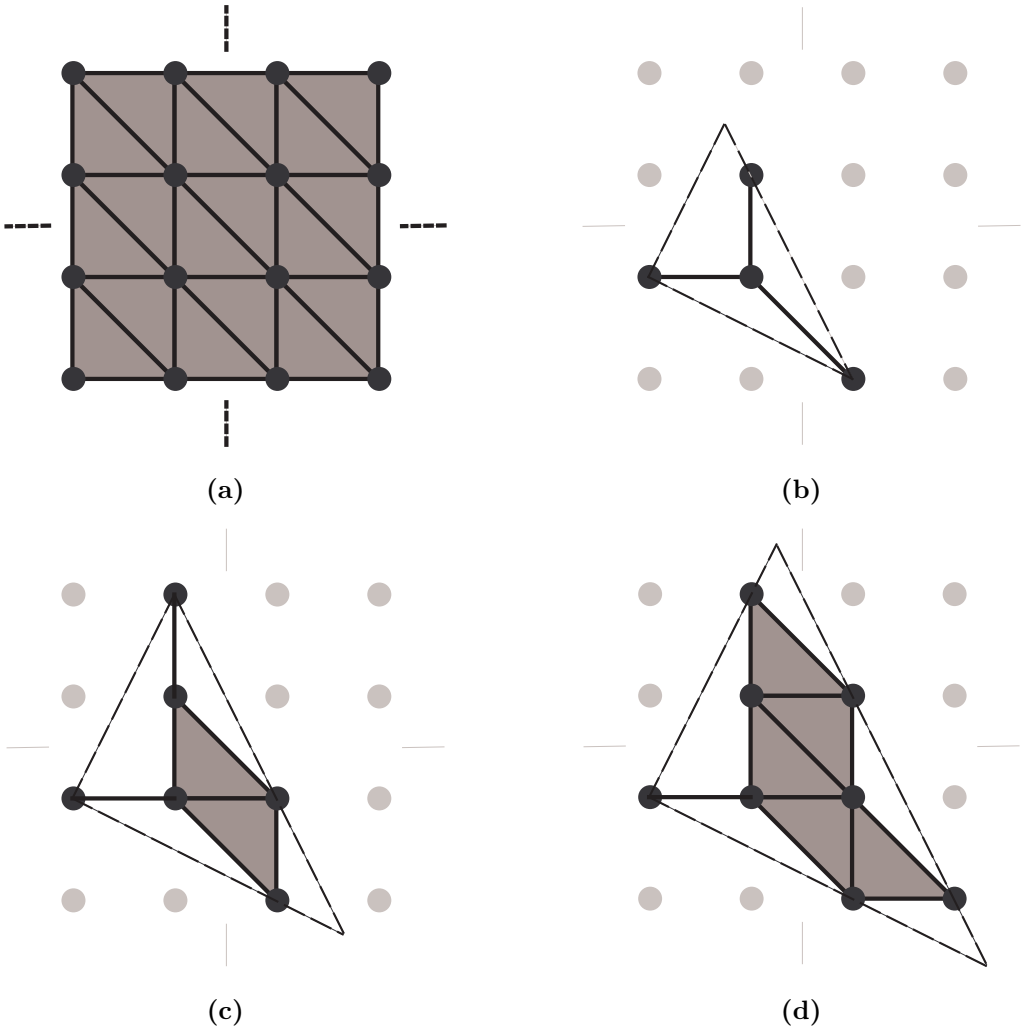


Figure 4.1.6: Example 4.1.7, $T(x, y, z) = 3x + 4y + 5z$, (a) C, (b) C_{15}, (c) C_{20}, (d) C_{25}

In the next section, we will examine this method for general P and T. In this general case, we will have to do a more complicated Euler characteristic count, but the idea still works.

Example 4.1.7. Let $P = \mathbb{R}^3_{\geq 0}$, and let $T : \mathbb{R}^3 \to \mathbb{R}$ be defined by $T(x, y, z) = 3x + 4y + 5z$. Then $\dim(\ker(T)) = 2$, and so C is 2-dimensional. If we transform C and C_a to have vertices in $\mathbb{Z}^2$, then Figure 4.1.6(a) shows C and Figures 4.1.6(b)-(d) show C_{15}, C_{20}, and C_{25}, respectively (the dotted lines are $T^{-1}(a) \cap P$). Note that each C_a is contractible and has Euler characteristic one.

We will be more explicit in the next section, where we state Theorem 4.2.1.

4.2 The General Case

Let $P \subset \mathbb{R}^d$ be a polyhedron which contains no straight lines, and let $T : \mathbb{R}^d \to \mathbb{R}^k$ be such that $T(\mathbb{Z}^d) \subset \mathbb{Z}^k$ and such that $T^{-1}(y) \cap P$ is bounded, for all $y \in \mathbb{R}^k$.

Suppose P is defined by

$$P = \left\{ x \in \mathbb{R}^d : \ Ax \leq b \right\},$$

where A is an $n \times d$ integer matrix and $b \in \mathbb{Z}^n$. Define a $d \times r$ matrix B, where $r = \dim(\ker(T))$, whose columns form a basis for the lattice $\ker(T) \cap \mathbb{Z}^d$. We may do this in polynomial time, as follows.

As in the proof of Lemma 2.3.1, if M is the $k \times d$ matrix representing T, then decompose

$$M = M'C,$$

where M' is a $k \times d$ lower triangular matrix and C is a $d \times d$ unimodular matrix. Then $r = \dim(\ker(T))$ is the number of zero columns of M, and we may take B to be the last r columns of C^{-1}.

As a linear transformation, $B : \mathbb{R}^r \to \mathbb{R}^d$ bijectively maps $\mathbb{Z}^r$ to $\ker(T) \cap \mathbb{Z}^d$. Define

$$A' = AB,$$

an $n \times r$ matrix.

Now let $C = C(A')$ be the neighborhood complex defined on $\mathbb{Z}^r$ by the matrix A'. Recall that if A' is not generic, then we must choose a proper perturbation φ in order to define C (see Section 1.3). The complex C is invariant under translation by $\mathbb{Z}^r$. Let $\bar{C}$ be a set of distinct representatives of C modulo $\mathbb{Z}^r$.

In Section 4.4, we will prove the following theorem, which says that we may write $f(S;\mathbf{z})$ as a sum of simpler generating functions, using $\bar{C}$.

Theorem 4.2.1. *Given $T:\mathbb{R}^d\to\mathbb{R}^k$ and $P=\{x\in\mathbb{R}^d:\ Ax\le b\}$, define A', $C=C(A')$, and $\bar{C}$ as above. For $s=\{h^0,h^1,\dots,h^l\}\in\bar{C}$, let $b_s=b-\max(A'h^0,A'h^1,\dots,A'h^l)$, where the maximum is taken coordinate-wise, and let*

$$Q_s=\{x\in\mathbb{R}^d:\ Ax\le b_s\}.$$

Then

$$f\big(T(P\cap\mathbb{Z}^d);\mathbf{z}\big)=\sum_{s\in\bar{C}}(-1)^{\dim s}f\big(Q_s\cap\mathbb{Z}^d;\mathbf{z}^{f_1},\mathbf{z}^{f_2},\dots,\mathbf{z}^{f_d}\big),$$

where $f_i=T(e_i)$ and $e_1,e_2,\dots,e_d$ is the standard basis of $\mathbb{R}^d$.

Note that the generating functions $f(Q_s\cap\mathbb{Z}^d;\mathbf{x})$ can be computed using Theorem 1.2.3, and the substitution of $\mathbf{z}^{f_i}$ for x_i can be accomplished using Theorem 1.2.8.

Example 4.2.2. Let us apply Theorem 4.2.1 to Example 4.1.1. Let $A=\left[\begin{smallmatrix}-1&0\\0&-1\end{smallmatrix}\right]$ and $b=\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]$, so that

$$P=\big\{(x_1,x_2)\in\mathbb{R}^2:\ x_1,x_2\ge 0\big\}=\big\{x\in\mathbb{R}^2:\ Ax\le b\big\}.$$

We could choose $B=\left[\begin{smallmatrix}5\\-2\end{smallmatrix}\right]$, and so $A'=AB=\left[\begin{smallmatrix}-5\\2\end{smallmatrix}\right]$. C is a simplicial complex on $\mathbb{Z}$, and we may choose $\bar{C}$ to be the vertex $\{0\}$ and the edge $\{0,1\}$ (note that the edge $\{0,1\}\subset\mathbb{Z}$ corresponds to $\{B\cdot[0],B\cdot[1]\}=\big\{0,(5,-2)\big\}\subset(\ker T\cap\mathbb{Z}^2)$, which is an edge of the complex as defined in Example 4.1.1). Then

$$b_{\{0\}}=\left[\begin{smallmatrix}0\\0\end{smallmatrix}\right]\text{ and }b_{\{0,1\}}=\left[\begin{smallmatrix}0\\-2\end{smallmatrix}\right].$$

Therefore

$$Q_{\{0\}}=P\text{ and }Q_{\{0,1\}}=\big\{(x,y)\in\mathbb{R}^2:\ x\ge 0\text{ and }y\ge 2\big\}=Q,$$

where Q is as defined in the previous section. Then

$$f(Q_{\{0\}}; x, y) = \frac{1}{(1-x)(1-y)} \text{ and } f(Q_{\{0,1\}}; x, y) = \frac{y^2}{(1-x)(1-y)}.$$

Applying Theorem 4.2.1,

$$f(S; \mathbf{z}) = f(Q_{\{0\}}; z^2, z^5) - f(Q_{\{0,1\}}; z^2, z^5) = \frac{1-z^{10}}{(1-z^2)(1-z^5)},$$

just as we calculated in the previous section.

4.3 The Euler Characteristic

To prove Theorem 4.2.1, we will do Euler characteristic calculations on certain subcomplexes of C. For $a \in \mathbb{R}^k$, choose an affine transformation, bijectively mapping $T^{-1}(a) \cap \mathbb{Z}^d$ to $\mathbb{Z}^r$, which takes $T^{-1}(a) \cap P$ to

$$P_a := \big\{ y \in \mathbb{R}^r : \ A'y \leq b_a \big\},$$

where b_a is an affine image of a. Given $a \in \mathbb{R}^k$, define

$$C_a = \big\{ \{h^0, h^1, \ldots, h^l\} \in C : \ h^i \in P_a \text{ for all } i \big\}.$$

This is the subcomplex of C which is its restriction to P_a. In this section, we will prove the following theorem.

Theorem 4.3.1. *Given C_a as above*

$$\chi(C_a) = \begin{cases} 1, & \text{if } a \in T(P \cap \mathbb{Z}^d) \\ 0, & \text{otherwise} \end{cases},$$

where $\chi(C_a) = \sum_{s \in C_a} (-1)^{\dim s}$.

We will prove this theorem by giving a geometric realization of the C_a and then using properties of this realization to compute the Euler characteristic. For purposes

of exposition, we will present lemmas in a different order from how they are proved. The structure of the proof of Theorem 4.3.1 is: Lemma 4.3.8 and Lemma 4.3.7 imply Lemma 4.3.3, and then Lemma 4.3.2 and Lemma 4.3.3 imply Theorem 4.3.1.

We first examine another simplicial complex. Let $X = \{x^1, x^2, \ldots, x^m\}$ be a finite subset of $\mathbb{R}^n$. We say that X is *generic* if there is no $x, y \in X$ $(x \neq y)$ with $(A'x)_i = (A'y)_i$ for some i. (A less strict version of this definition would work if we wanted). We will deal with the non-generic case in Section 4.6. For now we assume, for the sake of clarity, that X is generic. Recall that, for $b' \in \mathbb{R}^n$,

$$K_{b'} = K_{b'}(A') := \{x \in \mathbb{R}^r : \ A'x \leq b'\}.$$

Define the simplicial complex $S(X)$ on the vertices X to be the $s \subset X$ for which there exists a $b' \in \mathbb{R}^n$ such that $s \subset K_{b'}$ but $X \cap \operatorname{int}(K_{b'}) = \emptyset$ (compare this to the definition of the neighborhood complex in Section 1.3).

Lemma 4.3.2. *If $X = P_a \cap \mathbb{Z}^r$, then $C_a = S(X)$.*

Proof. Suppose $s = \{h^0, h^1, \ldots, h^l\} \in C_a$. Then there exists a $b' \in \mathbb{R}^n$ such that $s \subset K_{b'}$ but $\mathbb{Z}^r \cap \operatorname{int}(K_{b'}) = \emptyset$. Since $X \subset \mathbb{Z}^r$, $X \cap \operatorname{int}(K_{b'}) = \emptyset$ and $s \in S(X)$.

Conversely, suppose $s = \{h^0, h^1, \ldots, h^l\} \in S(X)$. Then there exists a $b' \in \mathbb{R}^n$ such that $s \subset K_{b'}$ but $X \cap \operatorname{int}(K_{b'}) = \emptyset$. We may choose b' such that $K_{b'} \subset P_s$, since $X \subset P_a$ and P_a is itself K_{b_a}. But then

$$\mathbb{Z}^r \cap \operatorname{int}(K_{b'}) = \mathbb{Z}^r \cap P_a \cap \operatorname{int}(K_{b'}) = X \cap \operatorname{int}(K_{b'}) = \emptyset,$$

and so $s \in C_a$. □

Theorem 4.3.1 follows from Lemma 4.3.2 and the following lemma.

Lemma 4.3.3. *If $X = \{x^1, x^2, \cdots, x^m\}$, for some $m \geq 1$, and $S(X)$ is defined as above, then $\chi\big(S(X)\big) = 1$.*

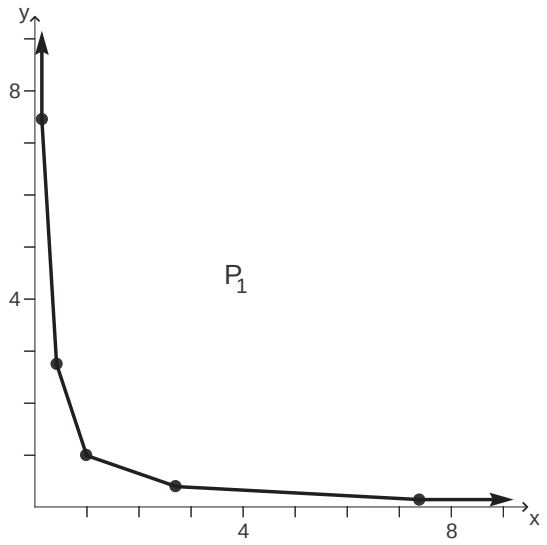


Figure 4.3.4: Example 4.3.6, P_1, with $X = \{-2, -1, 0, 1, 2\}$

4.3.5 Geometric realization of $S(X)$ and C

To prove this lemma, we follow the method of [BSS98] and construct a polyhedron P_t from the points $x^1, x^2, \ldots, x^m$, as follows. Given $t \geq 0$, define $E_t : \mathbb{R}^r \to \mathbb{R}^n$ by

$$E_t(x) = \mathbf{e}^{t(A'x)} = (e^{t\langle a'_1, x\rangle}, e^{t\langle a'_2, x\rangle}, \ldots, e^{t\langle a'_n, x\rangle}),$$

where a'_i is the ith row of A'. Now we define

$$P_t = \mathbb{R}^n_{\geq 0} + \operatorname{conv}\left\{E_t(x^1), E_t(x^2), \ldots, E_t(x^m)\right\},$$

where $X = \{x^1, x^2, \ldots, x^m\}$ and "conv" means the convex hull.

Example 4.3.6. Let $X = \{-2, -1, 0, 1, 2\}$. Then Figure 4.3.4 illustrates P_1.

The polyhedron P_t has the following useful property.

Lemma 4.3.7. *There exists a sufficiently large t such that, if $s \subset X$ with $s = \left\{h^0, h^1, \ldots, h^l\right\}$, then $s \in S(X)$ if and only if $\operatorname{conv}\left\{E_t(h^0), E_t(h^1), \ldots, E_t(h^l)\right\}$ is a face of P_t.*

Proof. Theorem 2 of [BSS98] proves this fact for $X = \mathbb{Z}^r$, and that proof also works here (in fact, their proof is more difficult, because they must deal with an infinite X). The contents of this lemma are also proved in [BS98] using matroid theory. $\square$

In Example 4.3.6 (see Figure 4.3.4), this lemma tells us that $S(X)$ has vertices $-2, -1, 0, 1, 2$, and edges $\{-2, -1\}, \{-1, 0\}, \{0, 1\}, \{1, 2\}$, as we would expect. In general, Lemma 4.3.7 gives a geometric realization of $S(X)$ in $\mathbb{R}^n$. In fact, as shown in Theorem 2 of [BSS98], if we take X to be the (infinite) set $\mathbb{Z}^r$, this gives a geometric realization of C.

Now pick a sufficiently large t such that Lemma 4.3.7 holds. Then the simplices in $S(X)$ are exactly the bounded faces of P_t. Then Lemma 4.3.3 (and hence Theorem 4.3.1) follows from the following lemma.

Lemma 4.3.8. *Let Q be an unbounded polyhedron in $\mathbb{R}^n$. Let $\mathcal{F}$ be the collection of bounded faces of Q. Then*

$$\chi(\mathcal{F}) = \sum_{F \in \mathcal{F}} (-1)^{\dim(F)} = 1.$$

Proof. Choose a half-space H_+ such that H_+ contains all of the bounded faces of Q in its interior and such that $Q' = Q \cap H_+$ is bounded. Let $\mathcal{F}'$ be the collection of faces of Q'. We know

$$\sum_{F' \in \mathcal{F}'} (-1)^{\dim(F')} = 1 + (-1)^{n-1}.$$

This is the Euler-Poincaré formula, and it can be seen combinatorially (see, for example, Corollary VI.3.2 of [Bar02]), or it can be seen from the fact that the complex $\mathcal{F}'$ is homeomorphic to an $n-1$ sphere (and then applying standard facts from the homology of CW-complexes, see, for example, Theorem IX.4.4 of [Mas91]). Let H be the hyperplane which is the boundary of H_+. The faces of Q' fall into 4 categories:

1. $\mathcal{F}$, the bounded faces of Q,

2. The face $Q \cap H$,

3. $F \cap H_+$, where F is an unbounded face of Q, and

4. $F \cap H$, where F is an unbounded face of Q.

There is a bijective correspondence between the last two categories, mapping a face F from category 3 of dimension k to $F \cap H$, a face from category 4 of dimension $k-1$. Therefore, in $\sum_{F' \in \mathcal{F}'} (-1)^{\dim(F')}$, these two categories will exactly cancel each other, and so we have

$$1 + (-1)^{n-1} = \sum_{F' \in \mathcal{F}'} (-1)^{\dim(F')} = \Big[\sum_{F \in \mathcal{F}} (-1)^{\dim(F)} \Big] + (-1)^{n-1} + 0.$$

The lemma follows. □

4.4 Proof of Theorem 4.2.1

Now we turn to proving Theorem 4.2.1. Given $s \in \bar{C}$ define the generating function

$$g_s(\mathbf{z}) = \sum_{a \in \mathbb{Z}^k} c_a \mathbf{z}^a,$$

where c_a is the number of $s + \lambda$, as λ varies over $\mathbb{Z}^r$, which are contained in C_a, that is, $c_a = |(s + \mathbb{Z}^r) \cap C_a|$. Note that C is the disjoint union

$$\bigcup_{s \in \bar{C}} (s + \mathbb{Z}^r).$$

Then Theorem 4.3.1 tells us that

$$f(S;\mathbf{x}) = \sum_{a \in T(P \cap \mathbb{Z}^d)} \mathbf{z}^a = \sum_{s \in \bar{C}} (-1)^{\dim s} g_s(\mathbf{z}).$$

Recall that B is the matrix whose columns form a basis for the lattice $\ker T \cap \mathbb{Z}^d$, and so B as a linear transformation bijectively maps $\mathbb{Z}^r$ to $\ker T \cap \mathbb{Z}^d$. Given $s = \{h^0, h^1, \ldots, h^l\} \in \bar{C}$, let

$$Q_s = \left\{ x \in \mathbb{R}^d : \ x + Bh^i \in P \text{ for all } i \right\}.$$

For any $a \in \mathbb{Z}^k$, there is a bijection between integer points λ in $Q_s \cap T^{-1}(a)$ and simplices $s + \lambda$ in C_a. If $P = \{x \in \mathbb{R}^d : \ Ax \leq b\}$, then

$$\begin{aligned} Q_s &= \{x \in \mathbb{R}^d : \ A(x + Bh^i) \leq b \text{ for all } i\} \\ &= \{x \in \mathbb{R}^d : \ Ax \leq b - A'h^i \text{ for all } i\} \\ &= \{x \in \mathbb{R}^d : \ Ax \leq b_s\}, \end{aligned}$$

where

$$b_s = b - \max\left(A'h^0, A'h^1, \ldots, A'h^l\right).$$

If $c = (c_1, c_2, \ldots, c_d) \in Q_s \cap \mathbb{Z}^d$, we want it to contribute $\mathbf{z}^{T(c)}$ to

$$g_s(\mathbf{z}) = \sum_{a \in \mathbb{Z}^k} c_a \mathbf{z}^a.$$

This is accomplished by substituting $x_i = \mathbf{z}^{f_i}$ into $f(Q_s \cap \mathbb{Z}^d; \mathbf{x})$, where $f_i = T(e_i)$, because $x_1^{c_1} x_2^{c_2} \cdots x_d^{c_d}$ becomes $\mathbf{z}^{c_1 f_1 + c_2 f_2 + \cdots + c_d f_d} = \mathbf{z}^{T(c)}$. Therefore

$$f(Q_s \cap \mathbb{Z}^d; \mathbf{z}^{f_1}, \mathbf{z}^{f_2}, \ldots, \mathbf{z}^{f_d}) = g_s(\mathbf{z}),$$

and the theorem is proved.

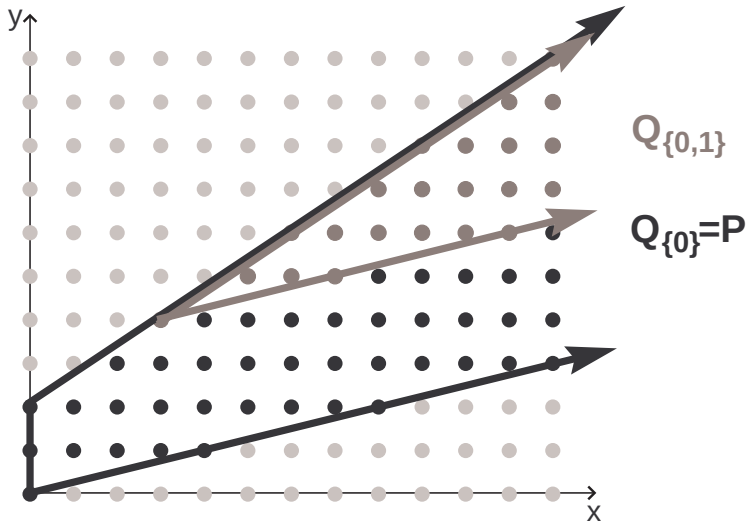


Figure 4.5.1: $Q_{\{0\}} = P$ and $Q_{\{0,1\}}$ in Example 4.5.2

4.5 Examples

Note that we may use Theorems 1.2.3 and 1.2.8 to calculate $f(Q_s \cap \mathbb{Z}^d; \mathbf{z}^{f_1}, \mathbf{z}^{f_2}, \ldots, \mathbf{z}^{f_d})$ in polynomial time. In some cases, this works out well. In general though, the problem is that $\bar{C}$ may have exponentially many simplices.

Here we present some examples of Theorem 4.2.1. In particular, if we take $P = \mathbb{R}^d_{\geq 0}$, so that $T(P \cap \mathbb{Z}^d)$ is the affine semigroup (that is, additive semigroup with zero in $\mathbb{R}^k$) generated by $T(e_1), T(e_2), \ldots, T(e_d)$, then we recover Corollary 4.5.4, which originally appeared in [SW03].

Example 4.5.2. Let

$$A = \begin{bmatrix} -1 & 0 \\ 1 & -4 \\ -2 & 3 \end{bmatrix} \text{ and } b = \begin{bmatrix} 0 \\ 0 \\ 6 \end{bmatrix},$$

and let $P = \{x \in \mathbb{R}^2 : \ Ax \leq b\}$, as pictured in Figure 4.5.1. Let $T : \mathbb{R}^2 \to \mathbb{R}$ be defined by $T(x, y) = 2x + 5y$. Then $\ker(T) \cap \mathbb{Z}^2$ is generated by $(5, -2)$, so we may take

$$B = \begin{bmatrix} 5 \\ -2 \end{bmatrix} \text{ and } A' = AB = \begin{bmatrix} -5 \\ 13 \\ -16 \end{bmatrix}.$$

We may take $\bar{C}$ to be the vertex $\{0\}$ and the edge $\{0,1\}$. Then, as in Theorem 4.2.1, we have

$$b_{\{0\}} = b - \max\{A'[0]\} = b \text{ and } b_{\{0,1\}} = b - \max\{A'[0], A'[1]\} = \begin{bmatrix} 0 \\ -13 \\ 6 \end{bmatrix},$$

and $P = Q_{\{0\}}$ and $Q_{\{0,1\}}$ are as pictured in 4.5.1. We may compute (using LattE [DLHTY04] or by hand)

$$f(Q_{\{0\}} \cap \mathbb{Z}^2; x, y) = \frac{1 + xy + x^2y + x^3y}{(1-y)(1-x^4y)} - \frac{y^3 + xy^3 + x^2y^4}{(1-y)(1-x^3y^2)}$$

and

$$f(Q_{\{0,1\}} \cap \mathbb{Z}^2; x, y) = \frac{x^3y^4 + x^5y^5 + x^6y^5 + x^7y^6 + x^8y^6}{(1-x^4y)(1-x^3y^2)}.$$

Then, by Theorem 4.2.1,

$$\begin{aligned} f\big(T(P \cap \mathbb{Z}^2); t\big) &= f(Q_{\{0\}} \cap \mathbb{Z}^2; t^2, t^5) - f(Q_{\{0,1\}} \cap \mathbb{Z}^2; t^2, t^5) \\ &= \frac{1 + t^7 + t^9 + t^{11}}{(1-t^5)(1-t^{13})} - \frac{t^{15} + t^{17} + t^{24}}{(1-t^5)(1-t^{16})} - \frac{t^{26} + t^{35} + t^{37} + t^{44} + t^{46}}{(1-t^{13})(1-t^{16})}. \end{aligned}$$

4.5.3 Affine Semigroups

Now we apply Theorem 4.2.1 to affine semigroups.

Corollary 4.5.4. *Given $m_1, m_2, \ldots, m_d \in \mathbb{Z}^k$, let $S \subset \mathbb{Z}^k$ be the affine semigroup they generate. Let M be the $k \times d$ matrix whose columns are m_i, let $\Lambda = \{\lambda \in \mathbb{Z}^d : \langle m_i, \lambda \rangle = 0$ for all $i\}$, and let $r = \dim \Lambda$. Let A' be a $d \times r$ matrix whose columns are a basis for Λ. Define the neighborhood complex $C = C(A')$ on $\mathbb{Z}^r$ as above, and let $\bar{C}$ be a set of distinct representatives of C modulo $\mathbb{Z}^r$. Then*

$$f(S; \mathbf{z}) = \frac{\sum_{s \in \bar{C}} (-1)^{\dim s} \mathbf{z}^{M \cdot \max(A's)}}{(1 - \mathbf{z}^{m_1})(1 - \mathbf{z}^{m_2}) \cdots (1 - \mathbf{z}^{m_d})},$$

where $\max(A's)$ *is the coordinate-wise maximum of $A'h^0, A'h^1, \ldots, A'h^l$ when $s = \{h^0, h^1, \ldots, h^l\}$.*

Proof. Note that $S = T(P \cap \mathbb{Z}^d)$, where $P = \{x \in \mathbb{R}^d : \ x_i \geq 0\}$ and $T : \mathbb{R}^d \to \mathbb{R}^k$ is given by the matrix M. Let A be the negative $d \times d$ identity matrix, and let $b = 0 \in \mathbb{R}^d$, so that $P = \{x \in \mathbb{R}^d : \ Ax \leq b\}$. Let $B = -A'$, so that the columns of B also form a basis for $\Lambda = \ker(T) \cap \mathbb{Z}^d$. Then we have that $A' = AB$, as required for Theorem 4.2.1. For $s \in \bar{C}$, let $b_s = b - \max(A's) = -\max(A's)$, and let

$$Q_s = \{x \in \mathbb{R}^d : \ Ax \leq b_s\} = \{x \in \mathbb{R}^d : \ x \geq \max(A's)\}.$$

Then

$$f(Q_s \cap \mathbb{Z}^d; \mathbf{z}) = \frac{\mathbf{x}^{\max(A's)}}{(1-x_1)(1-x_2)\cdots(1-x_d)}.$$

Therefore, by Theorem 4.2.1,

$$\begin{aligned} f(S; \mathbf{x}) &= \sum_{s \in \bar{C}} (-1)^{\dim s} f\big(Q_s \cap \mathbb{Z}^d; \mathbf{z}^{m_1}, \mathbf{z}^{m_2}, \ldots, \mathbf{z}^{m_d}\big) \\ &= \frac{\sum_{s \in \bar{C}} (-1)^{\dim s} \mathbf{z}^{M \cdot \max(A's)}}{(1-\mathbf{z}^{m_1})(1-\mathbf{z}^{m_2})\cdots(1-\mathbf{z}^{m_d})}, \end{aligned}$$

as desired. □

This corollary originally appeared in [SW03]. We note that Corollary 4.5.4 also follows from algebraic results in [BS98]. Here we have proved it geometrically. Now we examine Corollary 4.5.4 for some specific d and k.

Suppose $k = 1$. If $m_1, m_2, \ldots, m_d$ are positive integers whose greatest common divisor is one, then S is the Frobenius semigroup. H. Scarf and D. Shallcross [SS93] have related the Frobenius number itself to the neighborhood complex. They show (using slightly different terminology) that, if

$$N = \max\{M \cdot \max(A's) : \ s \text{ is in the neighborhood complex, } C\},$$

then the Frobenius number is

$$N - (m_1 + m_2 + \cdots + m_n).$$

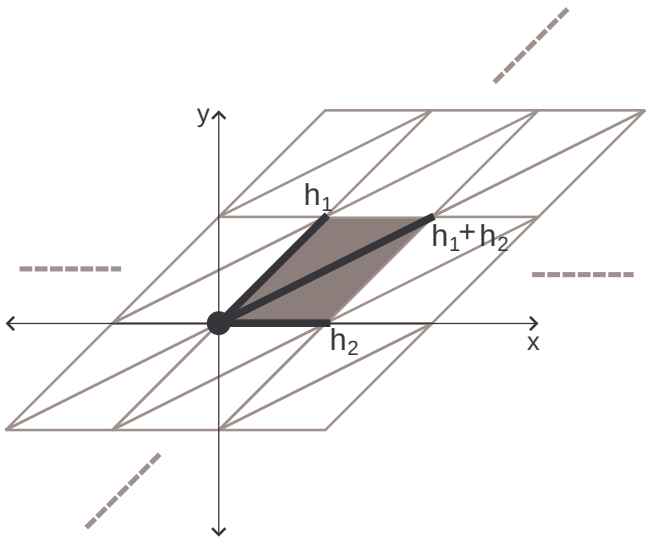


Figure 4.5.5: $\bar{C}$ for $k = 1, d = 3$ in Example 4.5.7

Note that, in the terminology of this dissertation, N is the largest exponent in the numerator of $f(S; \mathbf{z})$ in the form from Corollary 4.5.4.

Example 4.5.6. Corollary 4.5.4, with $k = 1, d = 2$. Then

$$f(z) = \frac{1 - z^{\mathrm{lcm}(m_1, m_2)}}{(1 - z^{m_1})(1 - z^{m_2})}.$$

In this case, we may choose $\bar{C} \subset \mathbb{Z}$ to consist of the vertex $\{0\}$ and the edge $\{0, 1\}$. This formula can easily be verified directly.

Example 4.5.7. Corollary 4.5.4, with $k = 1, d = 3$. Then

$$f(z) = \frac{1 - x^{p_1} - x^{p_2} - x^{p_3} + x^{p_4} + x^{p_5}}{(1 - z^{m_1})(1 - z^{m_2})(1 - z^{m_3})},$$

where $p_1, p_2, \ldots, p_5 \in \mathbb{Z}_+$ are quickly computable from m_1, m_2, m_3.

In this case, $\bar{C}$ consists of one vertex, three edges, and two triangles (see Section 1.3 and [Sca81]). More specifically, for some $h^1, h^2 \in \mathbb{Z}^2$, we may take $\bar{C}$ to be the set with vertex $\{0\}$; edges $\{0, h^1\}$, $\{0, h^2\}$, and $\{0, h^1 + h^2\}$; and triangles $\{0, h^1, h^1 + h^2\}$

and $\{0, h^2, h^1+h^2\}$ (see Figure 4.5.5). This formula was previously shown in [Den03], and also follows from [Her70] and [BS98], but their proofs use algebraic methods.

Here is a specific example:

Example 4.5.8. Corollary 4.5.4, with $m_1 = 11$, $m_2 = 17$, and $m_3 = 23$. Then

$$f(z) = \frac{1 - z^{34} - z^{138} - z^{132} + z^{155} + z^{149}}{(1 - z^{11})(1 - z^{17})(1 - z^{23})}.$$

In this case, if we choose $A' = \begin{bmatrix} 1 & 11 \\ -2 & 1 \\ 1 & -6 \end{bmatrix}$, then we may take $h^1 = (1, 0)$ and $h^2 = (0, 1)$.

Unfortunately, for $k = 1, d \geq 4$, the number of simplices in $\bar{C}$ may be very large, so no formula is quite so nice. Now we examine Corollary 4.5.4 for arbitrary k.

Example 4.5.9. Corollary 4.5.4, with $d = k + 1$. If the $\mathbb{R}$-span of the m_i is all of $\mathbb{R}^k$, then

$$f(\mathbf{z}) = \frac{1 - \mathbf{z}^m}{\prod_{i=1}^{d}(1 - \mathbf{z}^{m_i})},$$

where $m = M \cdot \max\{0, \lambda\}$ and λ is the generator of the 1-dimensional lattice $\Lambda = \{\lambda \in \mathbb{Z}^d : \ \langle m_i, \lambda \rangle = 0, \text{ for all } i\}$.

As in the special case $k = 1, d = 2$, $\bar{C}$ consists solely of one vertex and one edge. This formula can also easily be verified directly.

Example 4.5.10. Corollary 4.5.4, with $d = k + 2$. If the $\mathbb{R}$-span of the m_i is all of $\mathbb{R}^k$, then

$$f(\mathbf{z}) = \sum_j \frac{\mathbf{z}^{p_j}}{(1 - \mathbf{z}^{q_j}) \prod_i (1 - \mathbf{z}^{m_i})} + \sum_l \frac{\mathbf{z}^{p'_l}}{\prod_i (1 - \mathbf{z}^{m_i})},$$

where $p_j, q_j, p'_l \in \mathbb{Z}^k$. The number of terms in the sums is bounded by $C \cdot (dk + \sum \log_2 A'_{ij})$, for some constant C.

In other words, we can write $f(S; \mathbf{z})$ using relatively "few" terms. This is not immediately obvious, because the number of simplices in $\bar{C}$ may be much larger

than $C \cdot (dk + \sum \log_2 A'_{ij})$, exponentially larger, in fact. In [Sca81], however, H. Scarf shows that $\bar{C}$ has a nice structure, which we will exploit. In particular, we may represent the edges of $\bar{C}$ by $\{0, h_{ij}\}$, for $i \in I$ and $0 \leq j \leq N_i$, where $h_{i0}, h_{i1}, \ldots, h_{iN_i}$ lie on an interval, that is,

$$h_{ij} = c_i + jd_i,$$

for some $c_i, d_i \in \mathbb{Z}^2$. The number of such intervals, $|I|$, is bounded by $C_1 \cdot (dk + \sum \log_2 A'_{ij})$, where C_1 is a constant. The triangles and 3-simplices also lie on intervals (and there are no higher dimensional simplices, by Proposition 1.3.12). For example, the 3-simplices are

$$\{0, d_i, c_i + (j-1)d_i, c_i + jd_i\},$$

for $i \in I$ and $1 \leq j \leq N_i$. The exponents in the numerator of $f(S; \mathbf{z})$, which are $M \cdot \max(A's)$ for $s \in \bar{C}$, will also lie on intervals $\alpha_k + j\beta_k$, for $k \in K$, $0 \leq j \leq N_k$, and $\alpha_k, \beta_k \in \mathbb{Z}^2$, and we may write

$$\sum_{j=0}^{N_k} \mathbf{z}^{\alpha_k + j\beta_k} \text{ as } \frac{\mathbf{z}^{\alpha_k} - \mathbf{z}^{\alpha_k + (N_k+1)\beta_k}}{1 - \mathbf{z}^{\beta_k}}.$$

Doing this gives us a short formula for $f(\mathbf{z})$.

Here is a specific example:

Example 4.5.11. Corollary 4.5.4, with $a_1 = (2, 0)$, $a_2 = (0, 3)$, $a_3 = (3, 8)$, and $a_4 = (5, 2)$. Then

$$\begin{aligned} f(S; z, w) = &\frac{-(z^{20}w^{42} - z^{32}w^6) + (z^{23}w^{50} - z^{35}w^{14})}{(1 - z^2w^{-6})(1 - z^2)(1 - w^3)(1 - z^3w^8)(1 - z^5w^2)} \\ &+ \frac{(z^{22}w^{42} - z^{32}w^{12}) - (z^{25}w^{50} - z^{35}w^{20})}{(1 - z^2w^{-6})(1 - z^2)(1 - w^3)(1 - z^3w^8)(1 - z^5w^2)} \\ &+ \frac{1 - z^5w^8 - z^{18}w^{48} + z^{20}w^{48}}{(1 - z^2)(1 - w^3)(1 - z^3w^8)(1 - z^5w^2)}. \end{aligned}$$

In this example, if we choose $A' = \begin{bmatrix} 1 & 10 \\ -2 & 14 \\ 1 & -5 \\ -1 & -1 \end{bmatrix}$ then $\bar{C}$ has one vertex, and it has eight edges on two intervals, represented by $\{0, h_{ij}\}$, where $h_{10} = (1, 0)$ and

$$h_{2j} = (j - 1, 1), \text{ for } j = 0, \ldots, 6.$$

In all, $\bar{C}$ has twelve triangles and five 3-simplices.

Unfortunately, for general d and k, the neighborhood complex has no known structure as nice as in the $d = k + 2$ case. See the discussion at the beginning of this chapter and in Section 1.3.

4.6 The Non-generic Case

Since we are mostly concerned with A' which are integer matrices, A' and $X = P_a \cap \mathbb{Z}^r$ will often not be generic. In this case, we define $C(A')$ as in the discussion of non-genericity in Section 1.3. In particular, given a proper perturbation $\varphi : \mathbb{Z}^n \to \mathbb{R}^n$, we define the neighborhood complex, C, on the vertices $\mathbb{Z}^r$, by saying $s = \{h^0, h^1, \ldots, h^l\} \subset \mathbb{Z}^r$ is in C if and only if for no $x \in \mathbb{Z}^r$ is

$$\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big).$$

Then we may again define C_a by

$$C_a = \big\{\{h^0, h^1, \ldots, h^l\} \in C : \ h^i \in P_a \text{ for all } i\big\}.$$

Using φ, we may also define $S(X)$ by saying $s = \{h^0, h^1, \ldots, h^l\} \subset X$ is in $S(X)$ if and only if for no $x \in X$ is

$$\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big).$$

First we prove a non-generic version of Lemma 4.3.2.

Lemma 4.6.1. *If a proper perturbation, φ, and $a \in \mathbb{R}^k$ are given, let $X = P_a \cap \mathbb{Z}^r$, and let C_a and $S(X)$ be defined as above. Then $C_a = S(X)$.*

Proof. Suppose $s = \{h^0, h^1, \ldots, h^l\} \in C_a$. Then $h^0, \ldots, h^l \in P_a$ and for no $x \in \mathbb{Z}^r$ is

$$\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big).$$

Therefore for no $x \in X$ is $\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big)$ (since $X \subset \mathbb{Z}^r$), and so $s \in S(X)$.

Conversely, suppose $s \in S(X)$, with $s = \{h^0, h^1, \ldots, h^l\}$. Then $h^0, \ldots, h^l \in P_a$ and for no $x \in X$ is $\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big)$. Since $P_a = \{y \in \mathbb{R}^r : A'y \leq b_a\}$, and $h^j \in P_a$ for all j, we have that

$$[A'h^j]_i \leq [b_a]_i$$

for all i, j. Suppose (seeking a contradiction) that

$$\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big)$$

for some $x \in \mathbb{Z}^r$. Then for each i there is a j such that

$$[\varphi(A'x)]_i < [\varphi(A'h^j)]_i.$$

Therefore, for that i and j, $[A'x]_i \leq [A'h^j]_i \leq [b_a]_i$, by Property 2 of proper perturbations. But then we must have that $x \in P_a$, contradicting that for no $x \in X = P_a \cap \mathbb{Z}^r$ is $\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big)$. Therefore, for no $x \in \mathbb{Z}^r$ is $\varphi(A'x) < \max\big(\varphi(A'h^0), \varphi(A'h^1), \ldots, \varphi(A'h^l)\big)$, and so $s \in C_a$. □

The rest of the proof of Theorem 4.2.1 remains the same, except that we examine the polyhedron

$$P_t = \mathbb{R}^n_{\geq 0} + \operatorname{conv}\big\{\mathbf{e}^{t\varphi(A'x^1)}, \mathbf{e}^{t\varphi(A'x^2)}, \mathbf{e}^{t\varphi(A'x^m)}\big\},$$

where $X = \{x^1, x^2, \ldots, x^m\}$ and t is taken sufficiently large.

CHAPTER V

Presburger Arithmetic

In Presburger arithmetic, we try to answer yes-or-no questions about integers. In writing these questions, we are allowed to use addition, multiplication by integer constants, comparison ($\leq$), boolean operations (and, or, not), and quantifiers ($\forall$ and $\exists$). For example, we might want to decide whether the following statement is true or false:

$$\exists x \forall y : \ (5x + 3y \leq 7) \text{ or } (2x - y \leq 10 \text{ and } -5x - 3y \leq -5), \text{ with } x, y \in \mathbb{N}.$$

In general, Presburger sentences are of the form

$$Q_1 x_1 Q_2 x_2 \cdots Q_d x_d : \ F(x_1, x_2, \ldots, x_d), x_i \in \mathbb{N},$$

where the Q_i represent quantifiers (either $\exists$ or $\forall$), and F is a quantifier-free formula consisting of linear inequalities and boolean operations (there is no loss of generality here in restricting our attention to $\mathbb{N} = \{0, 1, 2, \ldots\}$ instead of all of $\mathbb{Z}$).

Presburger arithmetic is intimately related to the subject of rational generating functions. We say that a set $S \subset \mathbb{N}^l$ is *definable in Presburger arithmetic* if, for some d, there exist quantifiers $Q_1, Q_2, \ldots, Q_d$ (each either $\exists$ or $\forall$) and a quantifier-free formula $F(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_l)$ consisting of linear inequalities and boolean

operations, such that

$$S = \left\{ y \in \mathbb{N}^l \;\middle|\; Q_1 x_1 Q_2 x_2 \cdots Q_d x_d : \; F(x, y), x_i \in \mathbb{N} \right\}.$$

In Section 5.1, we will prove that the sentences which are definable in Presburger arithmetic are exactly the sentences which can be encoded as rational generating functions.

In Section 5.2, we will examine Presburger arithmetic from a complexity point of view. In Section 5.3, we examine the connection between Presburger arithmetic and rational generating functions, again from a complexity point of view.

5.1 Presburger Arithmetic and Rational Generating Functions

In this section, we prove the following theorem.

Theorem 5.1.1. *A set $S \subset \mathbb{N}^l$ is definable in Presburger arithmetic if and only if $f(S; \mathbf{x})$ can be written as a rational generating function of the form*

$$\sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}})(1 - \mathbf{x}^{a_{i2}}) \cdots (1 - \mathbf{x}^{a_{ik_i}})},$$

where $\alpha_i \in \mathbb{Q}$, $p_i, a_{ij} \in \mathbb{Z}^l$, and $a_{ij} \neq 0$.

Let $S \subset \mathbb{N}^l$ be given.

To prove the forward implication, suppose S is definable in Presburger arithmetic. We must show how to write $f(S; \mathbf{x})$ as a rational generating function.

5.1.2 Quantifier elimination

The tool we employ is *quantifier elimination* (see [Opp78] for a nice exposition). Using quantifier elimination, we may write

$$S = \left\{ y \in \mathbb{N}^l \;\middle|\; F(y) \right\},$$

where $F(y)$ is a quantifier-free formula consisting of linear inequalities, boolean operations, and statements of the form

$$a_1y_1 + a_2y_2 + \cdots + a_ly_l \equiv c \,(\mathrm{mod}\ d),$$

where $a_i, c, d \in \mathbb{Z}$. Note that the elements of $\mathbb{Z}^l$ which satisfy such a congruence equation form an affine translate of a sublattice of $\mathbb{Z}^l$. Therefore, using this form, we may then write S as a disjoint union

$$S = \bigcup_{i=1}^{n} \mathrm{int}(P_i) \cap (\lambda_i + \Lambda_i),$$

where, for $1 \leq i \leq n$, $P_i \subset \mathbb{R}^l$ is a polyhedron, Λ_i is a sublattice of $\mathbb{Z}^l$, λ_i is in $\mathbb{N}^l$, and $\mathrm{int}(P_i)$ is the relative interior of P_i (in general, some of the polyhedra in this disjoint union will not be full-dimensional). We know we can write $f(S_i; \mathbf{y})$ as a rational generating function, where $S_i = \mathrm{int}(P_i) \cap (\lambda_i + \Lambda_i)$ (in fact Theorem 1.2.3, Theorem 1.2.10, and Lemma 2.3.6 give a way to compute this quickly), and so

$$f(S; \mathbf{x}) = \sum_i f(S_i; \mathbf{x})$$

can be written as a rational generating function.

Conversely, suppose we have that $f(S; \mathbf{x})$ can be written as a rational generating function. We must show how to define S in Presburger arithmetic. First we need a few definitions.

5.1.3 Quasi-polynomials

We say that a function $g : \mathbb{Z}^l \to \mathbb{R}$ is a *quasi-polynomial* if there is a full-dimensional sublattice Λ of $\mathbb{Z}^l$ and there are polynomials $p_{\bar{\lambda}}(y_1, \ldots, y_l)$, one for each $\bar{\lambda} \in \mathbb{Z}^l/\Lambda$, such that

$$g(y) = p_{\bar{\lambda}}(y), \text{ for } \bar{y} = \bar{\lambda}.$$

We say that a function $g : \mathbb{Z}^l \to \mathbb{R}$ is a *quasi-polynomial on polyhedral pieces* if there is a finite partition $\bigcup_i \text{int}(P_i)$ of $\mathbb{R}^l$ with P_i polyhedra and there are quasi-polynomials g_i such that

$$g(y) = g_i(y) \text{ for } y \in \text{int}(P_i).$$

We need the following lemma.

Lemma 5.1.4. *Let*

$$h(\mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{p_i}}{(1 - \mathbf{x}^{a_{i1}})(1 - \mathbf{x}^{a_{i2}}) \cdots (1 - \mathbf{x}^{a_{ik_i}})}$$

be a rational function, where $\mathbf{x} \in \mathbb{C}^l$, $\alpha_i \in \mathbb{Q}$, $p_i, a_{ij} \in \mathbb{Z}^l$, *and* $a_{ij} \neq 0$ *for all* i, j, *and let*

$$\sum_{m \in \mathbb{Z}^l} c_m \mathbf{x}^m$$

be a Laurent series expansion of $h(\mathbf{x})$ *convergent on some neighborhood in* $\mathbb{C}^l$. *Then* c_m, *as a function of* m, *is a quasi-polynomial on polyhedral pieces.*

Proof. It suffices to prove this for rational functions of the form

$$h(\mathbf{x}) = \frac{\mathbf{x}^p}{(1 - \mathbf{x}^{a_1})(1 - x^{a_2}) \cdots (1 - x^{a_k})},$$

where $p, a_i \in \mathbb{Z}^l$, because the property of being a quasi-polynomial on polyhedral pieces is preserved under summation. Furthermore, we may take $p = 0$, because multiplying by $\mathbf{x}^p$ only shifts the function c_m. Let

$$\sum_{m \in \mathbb{Z}^l} c_m \mathbf{x}^m$$

be the Laurent series expansion of $h(\mathbf{x})$ convergent on the neighborhood of some point $(e^{r_1}, e^{r_2}, \ldots, e^{r_l})$, and let $r = (r_1, r_2, \ldots, r_l)$. As in the proof of Theorem 1.2.10, we may assume that $\langle r, a_i \rangle < 0$ for all i; otherwise, use the fact that

$$\frac{1}{1 - x^{a_i}} = -\frac{x^{-a_i}}{1 - x^{-a_i}}$$

to transform the fraction so that it does hold.

Then

$$\sum_{m\in\mathbb{Z}^l} c_m \mathbf{x}^m = \sum_{\lambda_1,\ldots,\lambda_k\in\mathbb{N}} \mathbf{x}^{\lambda_1 a_1+\lambda_2 a_2+\cdots+\lambda_k a_k}$$

as Laurent series, and so

$$c_m = \#\big\{\lambda_1,\lambda_2,\ldots,\lambda_k\in\mathbb{N}:\ m=\lambda_1 a_1+\lambda_2 a_2+\cdots+\lambda_k a_k\big\}.$$

In this form, c_m, as a function of m, is the *vector partition function*, and it is known to be a quasi-polynomial on polyhedral pieces, see, for example Theorem 1 of [Stu95].

□

We use this lemma as follows. We know that our rational function $f(S;\mathbf{x})$ is actually a generating function, meaning that for some Laurent series expansion $\sum_{m\in\mathbb{Z}^l} c_m\mathbf{x}^m$ of f, the coefficients c_m are all either 1 or 0. Let $\bigcup_{i=1}^n \operatorname{int}(P_i)$ be a partition of $\mathbb{R}^l$ with P_i polyhedra, let Λ_i be full-dimensional sublattices of $\mathbb{Z}^l$, and let $p_{i,\bar\lambda}$ be polynomials (for $\bar\lambda\in\mathbb{Z}^l/\Lambda_i$), such that

$$c_m = p_{i,\bar\lambda}(m) \text{ for } m\in\operatorname{int}(P_i)\cap(\lambda+\Lambda_i),$$

as guaranteed by the lemma. It suffices to show that $S\cap\operatorname{int}(P_i)\cap(\lambda+\Lambda_i)$ can be defined in Presburger arithmetic for each i and each $\bar\lambda\in\mathbb{Z}^l/\Lambda_i$, because S is the union of these pieces.

Let a particular i and $\bar\lambda\in\mathbb{Z}^l/\Lambda_i$ be given.

If P_i is bounded, then $S\cap\operatorname{int}(P_i)\cap(\lambda+\Lambda_i)$ is finite and so can easily be defined in Presburger arithmetic.

If P_i is unbounded, let K be the cone

$$K=\{y\in\mathbb{R}^l:\ y+P_i\subset P_i\}.$$

Then K is the largest cone such that $x + K \subset P_i$ for all $x \in P_i$, and is often called the *recession cone* or *characteristic cone* of P (see Section 8.2 of [Sch86]).

If $\dim K = \dim P_i$, then, since $p_{i,\bar{\lambda}}(m) = c_m$ is 0 or 1 (for $m \in \text{int}(P_i) \cap (\lambda + \Lambda_i)$), $p_{i,\bar{\lambda}}$ must be a constant function on $\text{int}(P_i) \cap (\lambda + \Lambda_i)$. In this case, if $p_{i,\bar{\lambda}} \equiv 1$, then

$$S \cap \text{int}(P_i) \cap (\lambda + \Lambda_i) = \text{int}(P_i) \cap (\lambda + \Lambda_i)$$

can be defined in Presburger arithmetic, and if $p_{i,\bar{\lambda}} \equiv 0$, then

$$S \cap \text{int}(P_i) \cap (\lambda + \Lambda_i) = \emptyset$$

can also be defined in Presburger arithmetic.

If $\dim K < \dim P_i$, then $p_{i,\bar{\lambda}}(m)$ need not be constant on $\text{int}(P_i) \cap (\lambda + \Lambda_i)$. For example, if

$$P_i = \big\{(x, y) \in \mathbb{R}^2 : \ x \geq 0 \text{ and } -.5 \leq y \leq 1.5\big\},$$

then

$$K = \big\{(x, 0) : \ x \geq 0\big\},$$

and the polynomial $p(x, y) = y$ is 1 for $y = 1$ and 0 for $y = 0$. However, we can partition $\text{int}(P_i) \cap (\lambda + \Lambda_i)$ into a finite number of pieces, Q_j, of the form

$$Q_j = (v_j + K) \cap (\lambda + \Lambda_i),$$

for some v_j, and on each of these pieces $p_{i,\bar{\lambda}}(m)$ will be constant. We then proceed as in the previous case, where $\dim K = \dim P_i$. The proof follows.

5.2 Complexity and Presburger Arithmetic

In this section, we will discuss algorithms for deciding whether statements in Presurger arithmetic are true or false. In general, there is no good algorithm, but we

will examine various subclasses of this problem (for example, when the number of quantifiers is fixed), and we will be looking for subclasses for which there is a quick (that is, polynomial time) algorithm to decide whether statements are true or false.

Note that another reasonable class of problems to study would be sentences where we are also allowed multiplication of variables, for example

$$\exists x \exists y : \ x^2 + 2y^2 \leq 4 \text{ and } x^2 - 4x + y^2 - 4y + xy \leq -5, \text{ with } x, y \in \mathbb{N}.$$

In general, however, these problems are very hard. In fact, there is a certain multivariate polynomial $p(x_0, x_1, \ldots, x_d)$ such that the class of problems

Given $a \in \mathbb{N}$, decide whether

$$\exists x_1, \exists x_2, \ldots, \exists x_d : \ p(a, x_1, x_2, \ldots, x_d) = 0, \text{ with } x_i \in \mathbb{N}$$

is undecidable. This is a consequence of the DPRM-theorem (after Davis, Putnam, Robinson, and Matiyasevich, see, for example, [Dav73]), which solves Hilbert's 10th problem in the negative. Hilbert asked [Hil00] for an algorithm that, given a multivariate polynomial p, would decide whether p has any integer roots.

The Presburger arithmetic problem, at least, is decidable, as originally proved [Pre91] by Presburger in 1929. Since then, better algorithms have been found. For example, D. Oppen gave an algorithm [Opp78], based on work of D. Cooper [Coo72], with running time $2^{2^{2^{c\phi}}}$, where ϕ is the input size of the problem and c is a constant. Nevertheless, lower bounds on the running time exist [FR74], which say any algorithm that solves all Presburger arithmetic problems will sometimes take at least $2^{2^{c'\phi}}$ steps, where c' is a constant.

A natural subclass to look at in order to find quick algorithms is the class where the number of quantifiers is fixed, but the number of boolean operations, linear inequalities, and the coefficients of the linear inequalities are all allowed to vary.

With the number of quantifiers fixed, we are able to use integer programming ideas to solve some of these problems.

5.2.1 Presburger arithmetic and integer programming

For example, suppose we have a problem

$$Q_1 x_1 Q_2 x_2 \cdots Q_d x_d : \ F(x_1, x_2, \ldots, x_d), x_i \in \mathbb{N},$$

where the Q_i represent quantifiers (either $\exists$ or $\forall$), and F is a quantifier-free formula consisting of linear inequalities and boolean operations. We would like to convert F into disjunctive normal form in polynomial time, that is, into the form

$$(p_{11} \text{ and } \cdots \text{ and } p_{1,n_1}) \text{ or } \cdots \text{ or } (p_{m1} \text{ and } \cdots \text{ and } p_{m,n_m}),$$

where p_{ij} are (possibly strict) linear inequalities. In this form, the problem would have a nice geometric interpretation, because F could be written as

$$x \in \bigcup_{j=1}^{n} \operatorname{int}(P_j),$$

where P_j are polyhedra.

To convert into disjunctive normal form is, in general, a hard problem. For example, if A_{ij} are boolean functions, for $1 \leq i \leq n$ and $j \in \{1, 2\}$ (and we don't know anything special about the A_{ij}, such as their being linear inequalities), then the disjunctive normal form for

$$(A_{11} \text{ or } A_{12}) \text{ and } (A_{21} \text{ or } A_{22}) \text{ and } \cdots \text{ and } (A_{n1} \text{ or } A_{n2}) = \bigwedge_{i=1}^{n} (A_{i1} \vee A_{i2})$$

is

$$\bigvee_{\psi:[n]\to\{1,2\}} \left(\bigwedge_{i=1}^{n} A_{i\psi(i)} \right),$$

where $\vee$ is the disjunction "or" and $\wedge$ is the conjunction "and." The number of atoms needed changes from $2n$ in the conjunctive normal form to $n2^n$ in the disjunctive normal form.

Nevertheless, if the atoms A_i are linear inequalities, and the number of quantifiers is fixed, we may use geometry to help us put F into disjunctive normal form quickly.

Proposition 5.2.2. *Fix d. There is a polynomial time algorithm which, given a quantifier-free formula $F(x_1, x_2, \ldots, x_d)$ consisting of linear inequalities and boolean operations, converts F into disjunctive normal form.*

Proof. The inequalities appearing in F cut $\mathbb{R}^d$ into many polyhedral pieces. It might appear at first glace that the number of such pieces could be 2^N, where N is the total number of inequalities in F. Nevertheless, as discussed in Section 3.3, the number of pieces is bounded by

$$\Phi(d, N) = \binom{N}{0} + \binom{N}{1} + \cdots + \binom{N}{d}.$$

See Section 6.1 of [Mat02] for a proof. We have that $\Phi(d, N)$ is a polynomial in N of degree at most d (where d is fixed), and the description of each piece may be found in polynomial time. Within each piece, F is either always true or always false. Then the disjunctive normal form is simply $\bigvee_P \{x \in P\}$, where the disjunction is taken over all polyhedral pieces P such that F is true. $\square$

Converting F into disjunctive normal form allows us to use integer programming methods to solve these problems. For example, if the fixed number of quantifiers are all $\exists$, then we have

$$\exists x_1 \exists x_2 \cdots \exists x_d : \ x \in \bigcup_j \operatorname{int}(P_j), x_i \in \mathbb{N},$$

where P_j are polyhedra. Now we may use Lenstra's algorithm for integer programming [Len83] to solve this problem in polynomial time, by checking each $\text{int}(P_i)$ one at a time to see if it contains an integer point. If the quantifiers are not all $\exists$, however, we cannot expect a polynomial time algorithm, as the following theorem (see [Sch97]) shows.

Theorem 5.2.3. *(from [Sch97]) The problem of deciding whether sentences of the form*

$$\exists x_1 \forall x_2 : \ F(x_1, x_2), x_i \in \mathbb{N},$$

where F is a quantifier-free formula consisting of linear inequalities and boolean operations, are true or false is NP-complete.

The next possibility is to examine the class of problems where the number of quantifiers and the number of linear inequalities and boolean operations are all fixed, but the coefficients of the linear inequalities are allowed to vary. In this case, R. Kannan showed [Kan90] that sentences of the form

$$\exists x_1 \cdots \exists x_k \forall x_{k+1} \cdots \forall x_d : \ F(x_1, x_2, \ldots, x_d), x_i \in \mathbb{N}$$

can be decided in polynomial time. He used integer programming methods similar to Lemma 2.3.4, together with Lenstra's algorithm for integer programming in fixed dimension. For sentences with more quantifier alternation (alternation between $\exists$ and $\forall$), no polynomial time algorithm is known.

5.3 Complexity, Presburger Arithmetic, and Rational Generating Functions

Theorem 5.1.1 shows that the sentences which are definable in Presburger arithmetic are exactly the sentences which can be encoded as rational generating func-

tions. Here we will discuss complexity issues related to this correspondence. In particular, given a set defined by a Presburger sentence, can we find a rational generating function for it quickly?

From the discussion in the last section, it is certainly true that we will have to fix the number of variables in the sentence to have any hope of finding a quick algorithm. The following proposition says that if we fix the number of variables and if the Presburger sentence has no quantifiers, then we can find a rational generating function in polynomial time.

Proposition 5.3.1. *Fix l. There is a polynomial time algorithm which, given a quantifier-free formula $F(y_1, y_2, \ldots, y_l)$ consisting of boolean combinations of linear inequalities, computes $f(S; \mathbf{y})$, where*

$$S = \left\{ y \in \mathbb{N}^l \;\middle|\; F(y) \right\}.$$

Proof. First use Proposition 5.2.2 to convert $F(y)$ to disjunctive normal form. In particular, we see from the proof of Proposition 5.2.2 that we can find polyhedra $P_i \subset \mathbb{R}^l$, whose relative interiors $\mathrm{int}(P_i)$ are disjoint, such that

$$F(y) \text{ if and only if } y \in \bigcup_i \mathrm{int}(P_i).$$

Then if $S_i = \mathrm{int}(P_i) \cap \mathbb{N}^l$, we can find $f(S_i; \mathbf{y})$ in polynomial time using Theorem 1.2.3 and Lemma 2.3.6, and

$$f(S; \mathbf{y}) = \sum_i f(S_i; \mathbf{y}).$$

□

In general, however, the problem of finding a rational generating function for a set defined by a Presburger formula becomes hard if even one quantifier is allowed.

Proposition 5.3.2. *The following class of problems is NP-hard: Given a quantifier-free formula $F(x, y)$ consisting of boolean combinations of linear inequalities, compute $f(S; y)$, where*

$$S = \left\{ y \in \mathbb{N} \;\middle|\; \forall x : \; F(x, y), x \in \mathbb{N} \right\}.$$

Proof. As usual for these sorts of proofs, we give a polynomial time reduction of a known NP-complete problem to this problem. Here we use Theorem 5.2.3, which states that the problem of deciding whether sentences of the form

$$\exists x_1 \forall x_2 : \; F(x_1, x_2), x_i \in \mathbb{N},$$

where F is a quantifier-free formula consisting of linear inequalities and boolean operations, are true or false is NP-complete. Indeed, suppose we know $f(S; y)$ as a rational function, where

$$S = \left\{ y \in \mathbb{N} \;\middle|\; \forall x : \; F(x, y), x \in \mathbb{N} \right\}.$$

Then the sentence

$$\exists x \forall y : \; F(x, y), x_i \in \mathbb{N},$$

is true if and only if $f(S; y)$ is nonzero, which we can decide in polynomial time by performing the substitution $y = 1$, using Theorem 1.2.8 (if the set S is infinite, we cannot apply this theorem, but we could have checked that in advance, in polynomial time). □

We note that this proposition also shows that the following problem is NP-hard: given a rational generating function $f(\hat{S}; x, y)$, find $f(\pi(\hat{S}); y)$ where $\pi : \mathbb{R}^2 \to \mathbb{R}$ is defined by $\pi(x, y) = y$. Indeed, given a quantifier-free formula $F(x, y)$ consisting of boolean combinations of linear inequalities, we can compute in polynomial time

$f(\hat{S}; x, y)$, where

$$\hat{S} = \{(x, y) \in \mathbb{N}^2 : \ F(x, y)\},$$

using Proposition 5.3.1. But then $\pi(\hat{S}) = S$, where S is defined as in the statement of Proposition 5.3.2, and finding $f(S; y)$ is NP-hard. In contrast, given rational generating functions $f(S_1; \mathbf{x}), \ldots, f(S_n; \mathbf{x})$, where $S_i \subset \mathbb{N}^l$, we can use Theorem 1.2.10 to find $f(S; \mathbf{x})$ in polynomial time (for fixed l and n), where S is a boolean combination of the S_i.

As we did in the previous section, we might then turn to the class of problems where not only the number of variables, but also the number of linear inequalities in the formula is fixed, but the coefficients of the linear inequalities are allowed to vary. We have the following corollary to Theorem 1.1.15.

Corollary 5.3.3. *Fix l, d, and n. There is a polynomial time algorithm which, given a quantifier-free formula $F(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_l)$ consisting of boolean combinations of at most n linear inequalities, computes $f(S; \mathbf{y})$, where*

$$S = \left\{ y \in \mathbb{N}^l \ \middle| \ \exists x_1 \exists x_2 \cdots \exists x_d : \ F(x, y), x_i \in \mathbb{N} \right\}.$$

Proof. First convert F into disjunctive normal form, $(x, y) \in \bigcup_{j=1}^{N} \operatorname{int}(P_j)$, where P_j are polyhedra. Since n, l, and d are fixed, N is fixed. For each P_j, let

$$S_j = \left\{ y \in \mathbb{N}^l \ \middle| \ \exists x_1 \exists x_2 \cdots \exists x_d : \ (x, y) \in \operatorname{int}(P_j), x_i \in \mathbb{N} \right\},$$

so that $S = \bigcup_j S_j$. We would like to compute each $f(S_j; \mathbf{y})$ in polynomial time, and then we can compute $f(S; \mathbf{y})$ using Theorem 1.2.10. Let j be fixed. Note that $\operatorname{int}(P_j) \cap \mathbb{N}^{d+l} = P \cap \mathbb{N}^{d+l}$ for some polyhedron P (for example, if $P_j = \{x \in \mathbb{R}^{d+l} : Ax \leq b\}$ is full-dimensional, then we may take $P = \{x \in \mathbb{R}^{d+l} : \ Ax \leq b - 1\}$, where $b - 1 = (b_1 - 1, \ldots, b_m - 1)$). As often occurred in Chapter III, we would like to

apply Theorem 1.1.15, since $S_j = T(P \cap \mathbb{N}^{d+l})$ where $T : \mathbb{R}^d \oplus \mathbb{R}^l \to \mathbb{R}^l$ is given by $T(x, y) = y$, but we cannot apply it directly, since P may be unbounded.

We will use Proposition 3.2.3, which says that we may find $T'(\mathbb{N}^r)$ in polynomial time, for fixed r, where $T' : \mathbb{R}^r \to \mathbb{R}^k$ is a linear transformation with $T'(\mathbb{Z}^r) \subset \mathbb{Z}^k$. Suppose $P = \{x \in \mathbb{R}^{d+l}_{\geq 0} : \ Ax \leq b\}$, for some $m \times (d+l)$ integer matrix A and some $b \in \mathbb{Z}^m$. Then the map $\varphi : \mathbb{R}^{d+l} \to \mathbb{R}^{d+l} \oplus \mathbb{R}^m$ given by

$$\varphi(x) = (x, b - Ax)$$

maps P to

$$Q := \big\{(x, z) \in \mathbb{R}^{d+l}_{\geq 0} \times \mathbb{R}^m_{\geq 0} : \ Ax + z = b\big\},$$

and bijectively maps $P \cap \mathbb{N}^{d+l}$ onto $Q \cap \mathbb{N}^{d+l+m}$. Let $T' : \mathbb{R}^{d+l} \oplus \mathbb{R}^m \to \mathbb{R}^l \oplus \mathbb{R}^m$ be given by

$$T'(x, z) = (T(x), Ax + z).$$

Then we may find $f\big(T'(\mathbb{N}^{d+l} \times \mathbb{N}^m); \mathbf{y}, \mathbf{z}\big)$ in polynomial time using Proposition 3.2.3, and then $f(T(P \cap \mathbb{N}^{d+l}); \mathbf{y})$ is the coefficient (in $\mathbb{C}[\mathbf{y}]$) of $\mathbf{z}^b$. We may compute $f(T(P \cap \mathbb{N}^{d+l}); \mathbf{y})$ by first taking the Hadamard product of $f\big(T'(\mathbb{N}^{d+l} \times \mathbb{N}^m); \mathbf{y}, \mathbf{z}\big)$ and

$$\mathbf{z}^b \prod_{i=1}^{l} \frac{1}{1 - y_i},$$

using Lemma 1.2.11, and then specializing at $\mathbf{z} = (1, 1, \ldots, 1)$, using Theorem 1.2.8.

□

This corollary also holds if all of the quantifiers are $\forall$, because

$$\Big\{y \in \mathbb{N}^l \ \Big| \ \forall x_1 \forall x_2 \cdots \forall x_d : \ F(x, y), x_i \in \mathbb{N}\Big\}$$
$$= \mathbb{N}^l \setminus \Big\{y \in \mathbb{N}^l \ \Big| \ \exists x_1 \exists x_2 \cdots \exists x_d : \ \neg F(x, y), x_i \in \mathbb{N}\Big\}.$$

A natural question, then, is whether we can extend this to cases where the quantifiers are not all the same. It might also be true that answering these questions about generating functions would help us with the original decision problem. We close with the following conjecture.

Conjecture 5.3.4. *Fix l, d, and n. There is a polynomial time algorithm which, given a quantifier-free formula $F(x_1, x_2, \ldots, x_d, y_1, y_2, \ldots, y_l)$ consisting of boolean combinations of at most n linear inequalities, and given quantifiers $Q_1, Q_2, \ldots, Q_d$ (each either $\exists$ or $\forall$), computes $f(S; \mathbf{y})$, where*

$$S = \left\{ y \in \mathbb{N}^l \;\middle|\; Q_1 x_1 Q_2 x_2 \cdots Q_d x_d : \; F(x, y), x_i \in \mathbb{N} \right\}.$$

In particular, there is a polynomial time algorithm which, given a quantifier-free formula $G(x_1, x_2, \ldots, x_d)$ consisting of boolean combinations of at most n linear inequalities, and given quantifiers $Q_1, Q_2, \ldots, Q_d$ (each either $\exists$ or $\forall$), decides whether

$$Q_1 x_1 Q_2 x_2 \cdots Q_d x_d : \; G(x), x_i \in \mathbb{N}.$$

BIBLIOGRAPHY

BIBLIOGRAPHY

[Bar94] Alexander Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. Oper. Res.*, 19(4):769–779, 1994.

[Bar02] Alexander Barvinok. *A Course in Convexity*, volume 54 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2002.

[Bel77] David Bell. A theorem concerning the integer lattice. *Studies in Appl. Math.*, 56(2):187–188, 1976/77.

[BLPS99] Wojciech Banaszczyk, Alexander Litvak, Alain Pajor, and Stanislaw Szarek. The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces. *Math. Oper. Res.*, 24(3):728–750, 1999.

[BP99] Alexander Barvinok and James Pommersheim. An algorithmic theory of lattice points in polyhedra. In *New Perspectives in Algebraic Combinatorics (Berkeley, CA, 1996–97)*, volume 38 of *Math. Sci. Res. Inst. Publ.*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.

[Bri88] Michel Brion. Points entiers dans les polyèdres convexes. *Ann. Sci. École Norm. Sup. (4)*, 21(4):653–663, 1988.

[BS98] Dave Bayer and Bernd Sturmfels. Cellular resolutions of monomial modules. *J. Reine Angew. Math.*, 502:123–140, 1998.

[BSS98] Imre Bárány, Herbert Scarf, and David Shallcross. The topological structure of maximal lattice free convex bodies: the general case. *Math. Programming*, 80(1, Ser. A):1–15, 1998.

[BW03] Alexander Barvinok and Kevin Woods. Short rational generating functions for lattice point problems. *J. Amer. Math. Soc.*, 16(4):957–979 (electronic), 2003.

[CGST86] William Cook, Albertus Gerards, Alexander Schrijver, and Éva Tardos. Sensitivity theorems in integer linear programming. *Math. Programming*, 34(3):251–264, 1986.

[Coo72] D.C. Cooper. Theorem proving in arithmetic without multiplication. *Machine Intelligence*, 7:91–99, 1972.

[Dav73] Martin Davis. Hilbert's tenth problem is unsolvable. *Amer. Math. Monthly*, 80:233–269, 1973.

[Den03] Graham Denham. Short generating functions for some semigroup algebras. *Electron. J. Combin.*, 10:Research Paper 36, 7 pp. (electronic), 2003.

[DLHH+04] Jesus De Loera, David Haws, Raymond Hemmecke, Peter Huggins, Bernd Sturmfels, and Ruriko Yoshida. Short rational functions for toric algebra. to appear in *Journal of Symbolic Computation*, 2004.

[DLHTY04] Jesus De Loera, Raymond Hemmecke, Jeremy Tauzer, and Ruriko Yoshida. Effective lattice point counting in rational convex polytopes. to appear in *Journal of Symbolic Computation*, http://www.math.ucdavis.edu/∼latte, 2004.

[Doi73] Jean-Paul Doignon. Convexity in cristallographical lattices. *J. Geometry*, 3:71–85, 1973.

[EG72] Paul Erdős and Ronald Graham. On a linear diophantine problem of Frobenius. *Acta Arith.*, 21:399–408, 1972.

[Eis95] David Eisenbud. *Commutative Algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Ewa96] Günter Ewald. *Combinatorial Convexity and Algebraic Geometry*, volume 168 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1996.

[FR74] Michael Fischer and Michael Rabin. Super-exponential complexity of Presburger arithmetic. In *Complexity of computation (Proc. SIAM-AMS Sympos., New York, 1973)*, pages 27–41. SIAM–AMS Proc., Vol. VII. Amer. Math. Soc., Providence, R.I., 1974.

[Ful93] William Fulton. *Introduction to Toric Varieties*, volume 131 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1993.

[Her70] Jürgen Herzog. Generators and relations of abelian semigroups and semigroup rings. *Manuscripta Math.*, 3:175–193, 1970.

[Hil00] David Hilbert. Mathematical problems. *Bull. Amer. Math. Soc. (N.S.)*, 37(4):407–436 (electronic), 2000. Reprinted from Bull. Amer. Math. Soc. **8** (1902), 437–479.

[HS04] Serkan Hoşten and Bernd Sturmfels. Computing the integer programming gap. to appear in *Combinatorics*, 2004.

[HT99] Serkan Hoşten and Rekha Thomas. The associated primes of initial ideals of lattice ideals. *Math. Res. Lett.*, 6(1):83–97, 1999.

[Kan90] Ravi Kannan. Test sets for integer programs, ∀∃ sentences. In *Polyhedral combinatorics (Morristown, NJ, 1989)*, volume 1 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 39–47. Amer. Math. Soc., Providence, RI, 1990.

[Kan92] Ravi Kannan. Lattice translates of a polytope and the Frobenius problem. *Combinatorica*, 12(2):161–177, 1992.

[KLS90] Ravi Kannan, László Lovász, and Herbert Scarf. The shapes of polyhedra. *Math. Oper. Res.*, 15(2):364–380, 1990.

[Len83] Hendrik Lenstra, Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983.

[Lov89] László Lovász. Geometry of Numbers and Integer Programming. In *Mathematical programming (Tokyo, 1988)*, volume 6 of *Math. Appl. (Japanese Ser.)*, pages 177–201. SCIPRESS, Tokyo, 1989.

[Mas91] William Massey. *A Basic Course in Algebraic Topology*, volume 127 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.

[Mat02] Jiří Matoušek. *Lectures on Discrete Geometry*, volume 212 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[Opp78] Derek Oppen. A superexponential upper bound on the complexity of Presburger arithmetic. *J. Comput. System Sci.*, 16(3):323–332, 1978.

[Pap94] Christos Papadimitriou. *Computational Complexity*. Addison-Wesley Publishing Company, Reading, MA, 1994.

[Pre91] Mojżesz Presburger. On the completeness of a certain system of arithmetic of whole numbers in which addition occurs as the only operation. *Hist. Philos. Logic*, 12(2):225–233, 1991. Translated from the German and with commentaries by Dale Jacquette.

[RA96] Jorge Ramírez-Alfonsín. Complexity of the Frobenius problem. *Combinatorica*, 16(1):143–147, 1996.

[Sca77] Herbert Scarf. An observation on the structure of production sets with indivisibilities. *Proc. Nat. Acad. Sci. U.S.A.*, 74(9):3637–3641, 1977.

[Sca81] Herbert Scarf. Production sets with indivisibilities. II. The case of two activities. *Econometrica*, 49(2):395–423, 1981.

[Sca97] Herbert Scarf. Test sets for integer programs. *Math. Programming*, 79(1-3, Ser. B):355–368, 1997.

[Sch86] Alexander Schrijver. *Theory of Linear and Integer Programming*. Wiley-Interscience Series in Discrete Mathematics. John Wiley & Sons Ltd., Chichester, 1986.

[Sch97] Uwe Schöning. Complexity of Presburger arithmetic with fixed quantifier dimension. *Theory Comput. Syst.*, 30(4):423–428, 1997.

[Sha92] David Shallcross. Neighbors of the origin for four by three matrices. *Math. Oper. Res.*, 17(3):608–614, 1992.

[SS93] Herbert Scarf and David Shallcross. The Frobenius problem and maximal lattice free bodies. *Math. Oper. Res.*, 18(3):511–515, 1993.

[Stu95] Bernd Sturmfels. On vector partition functions. *J. Combin. Theory Ser. A*, 72(2):302–309, 1995.

[Stu96] Bernd Sturmfels. *Gröbner Bases and Convex Polytopes*, volume 8 of *University Lecture Series*. American Mathematical Society, Providence, RI, 1996.

[SW86] László Székely and Nicholas Wormald. Generating functions for the Frobenius problem with 2 and 3 generators. *Math. Chronicle*, 15:49–57, 1986.

[SW03] Herbert Scarf and Kevin Woods. Neighborhood complexes, generating functions, and semigroups. preprint, 2003.

[Tho95] Rekha Thomas. A geometric Buchberger algorithm for integer programming. *Math. Oper. Res.*, 20(4):864–884, 1995.

[Tho03] Rekha Thomas. The structure of group relaxations. to appear in Handbook of Discrete Optimization (eds: K. Aardal, G. Nemhauser, R. Weismantel), 2003.

[TW03] Rekha Thomas and Kevin Woods. Generating functions for standard pairs. manuscript, 2003.

ABSTRACT

Rational Generating Functions and Lattice Point Sets

by

Kevin M. Woods

Chair: Alexander Barvinok

We prove that, for any fixed d, there is a polynomial time algorithm for computing the generating function of any projection of the set of integer points in a d-dimensional polytope. This implies that many interesting sets of integer points can be encoded as short rational generating functions, such as the Frobenius semigroup of all nonnegative integer combinations of given positive integers, affine semigroups, neighbors and the neighborhood complex (also known as the Scarf complex or complex of maximal lattice-free bodies), Hilbert bases, and sets from algebraic integer programming. We also show how to use the generating functions to solve computational problems (such as finding the cardinality of the set or finding its maximum element) in polynomial time. We may also use this theorem to compute, as a short rational function, the Hilbert series of rings generated by monomials. We examine the connection between generating functions and the neighborhood complex, and we consider possibilities for improving the algorithm for the main theorem. Finally, we examine the relationship between rational generating functions and the complexity of Presburger arithmetic.