Algorithmic Solution of Linear Diophantine Systems

Zafeirakis Zafeirakopoulos

Marshall Plan Scholarship - Final Report

Contents

Chapter 1

Geometry

1.1 Polyhedra and Polytopes

One of the earliest recorded uses of geometry as a counting tool is the notion of figurate numbers [1]. Ancient Greeks used pebbles (χαλίκι, where the word calculus comes from), in order to do arithmetic. For example, an arrangement of pebbles as in Figure **??** would be used to calculate triangular numbers. In general figurate numbers were popular in ancient times. Unfortunately today we mostly care about squares and for some odd cases (like pentagonal numbers in Euler's celebrated theorem). Among the mathematicians that were interested in figurate numbers was, of course, Diophantus. After an interesting turn of events, one of the most prominent methods for the solution of linear Diophantine systems relies on generalizing figurate numbers. We follow [4] which provides a complete presentation of the topic.

Given a polytope in $\mathbb{R}^d$ we are interested in computing the lattice points in the polytope. To make this sentence clear we first provide some definitions and terminology from polyhedral geometry. Throughout this section, we fix d to be the dimension of the ambient space $\mathbb{R}^d$.

Most of the theory presented here is valid for arbitrary lattices, but for simplicity we will always use the standard lattice $\mathbb{Z}^d$, except if another lattice is explicitly mentioned.

Our main goal is to investigate linear systems of equations/inequalities. An inequality in d variables $x_1, x_2, \ldots, x_d$ defines a halfspace in the Euclidean space $\mathbb{R}^d$.

Definition 1.1.1 (Linear Half Space)**.** A linear half space of $\mathbb{R}^d$ is a subset of $\mathbb{R}^d$ of the form $\mathcal{H}_{w,b} = \{v : v \cdot w \geq b\}$ for some $0 \neq w \in \mathbb{R}^d$ and $b \in \mathbb{R}$.

Given the inequality $\displaystyle\sum_{i=1}^{d} a_i x_i \geq b$, we have have the corresponding halfspace $\mathcal{H}_{a,b}$.

Similarly, we have the definition of a hyperplane

Definition 1.1.2 ((Affine) Hyperplane)**.** A hyperplane in $\mathbb{R}^d$ is a subspace of codimension 1. Like before we have $H_{w,b} = \{v : v \cdot w = b\}$ for some $0 \neq w \in \mathbb{R}^n$ and $b \in \mathbb{R}$.

[1] polygonal numbers in Greek

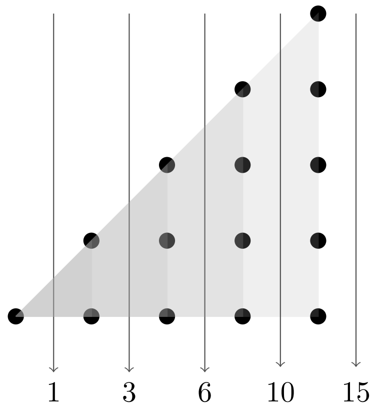


Figure 1.1: The first five triangular numbers.

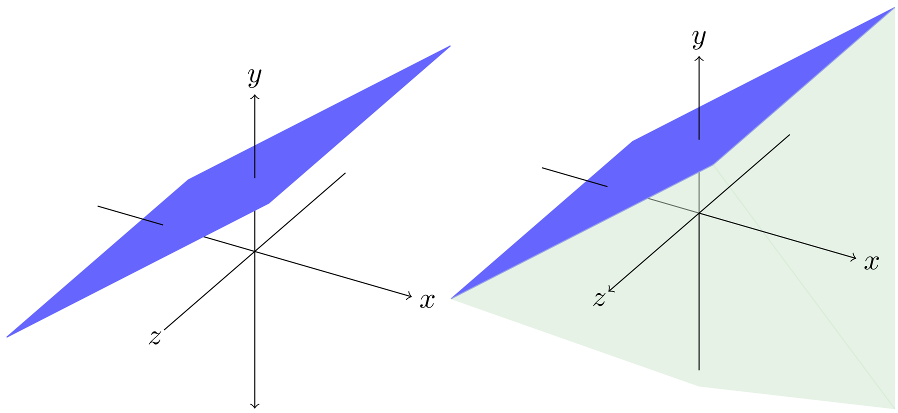


Figure 1.2: A hyperplane and a halfspace it defines.

We note that a hyperplane divides the Euclidean space in two half-spaces.

Since we want to deal with systems of inequalities, the next step is to consider intersections of halfspaces. This leads to the definition of

Definition 1.1.3 (Polyhedron)**.** A polyhedron is the intesection of finitely many linear halfspaces in $\mathbb{R}^n$.

More precisely, if $A \in \mathbb{Z}^{m \times n}$ and $b \in \mathbb{Z}^m$, then the polyhedron $\mathcal{P}_{A,b}$ is the subset of $\mathbb{R}^n$ defined as $\{x \in \mathbb{R}^n : A \cdot x \geq b\}$.

We note that the restriction for finite intersections is naturally met in our setting, since the number of inequalities in the system is always minite.

Although we will mostly deal with polyhedra, a very important object, especially when it comes to lattice point enumeration, is the polytope.

Definition 1.1.4 (Polytope)**.** A bounded polyhedron is called a polytope.

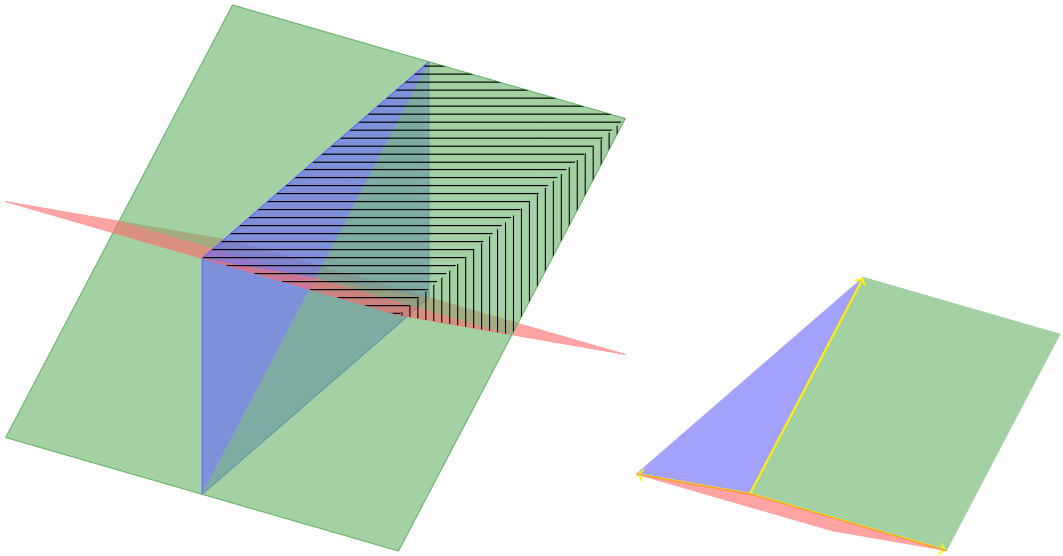


Figure 1.3: A polyhedron

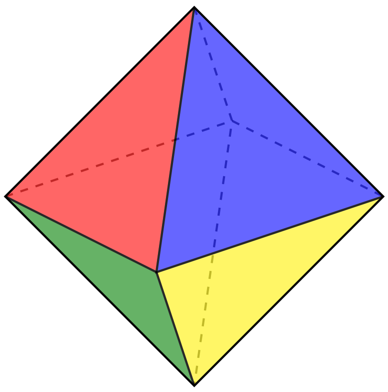


Figure 1.4: A polytope

A second equivalent definition is the following:

Definition 1.1.5 (Polytope)**.** A polytope is the convex hull of finitely many points in $\mathbb{R}^n$.

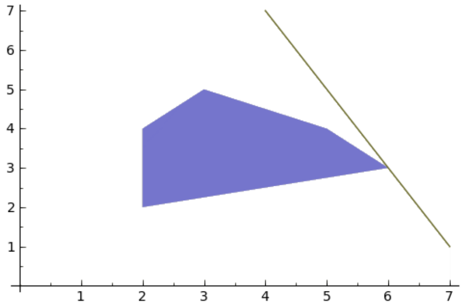
Polyhedra and polytopes are geometric objects with "flat" sides. The definitions of supporting hyperplanes and faces makes this more formal and provide some useful terminology.

Definition 1.1.6 (Supporting Hyperplane)**.** A hyperplane H is said to support a set S in $\mathbb{R}^d$ if:

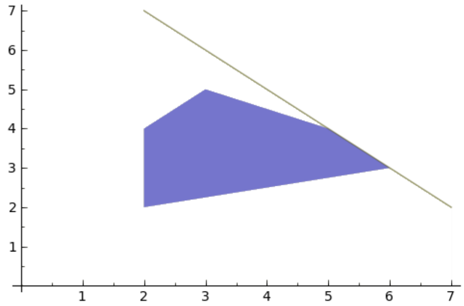
- S is contained in one of the two closed half-spaces determined by H.

- $\exists x \in S$ such that $x \in H$.

In other word, a supporting hyperplane H for the polyhedron P is a linear hyperplane that intesects P and leaves P entirely in one side. We note that in the definition of hyperplane we assumed that the codimension is 1, which is not a necessary condition for the supporting hyperplanes of non full dimensional polyhedra.



(a) Supporting hyperplane intersecting a vertex.



(b) Supporting hyperplane intersecting a facet.

Figure 1.5

Definition 1.1.7 (Face, ray and facet)**.** Let P be a polyhedron in $\mathbb{R}^d$.

A face F of P is the intersection of P with a supporting hyperplane S.

The dimension of a face F is the dimension of the affine subspace spanned by F.

A face of dimension d is called a d-face.

In particular a 0-face is called vertex and a $(d-1)$-face is called facet.

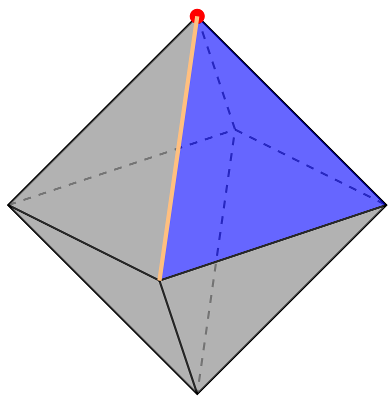


Figure 1.6: A facet, a 1-face and a vertex of a 3-polytope

Simplices are polytopes of very simple structure and are used as building blocks in polyhedral geometry. We first define the standard simplex in dimension d.

Definition 1.1.8 (Standard Simplex)**.** The standard d-simplex is the subset of $\mathbb{R}^d$ defined by

$$\Delta^d = \left\{ (x_1, x_2 \ldots, x_d) \in \mathbb{R}^{d+1} | \sum_{i=1}^{d} x_i \leq 1 \text{ and } x_i \geq 0 \ \forall i \right\}$$

Equivalently, The standard d-simplex Δ^d is the convex hull of the $d+1$ points:

$$e_0 = (0,0,0,\ldots,0), e_1 = (1,0,0,\ldots,0), e_2 = (0,1,0,\ldots,0), \vdots e_d = (0,0,0\ldots,1).$$

In general a simplex is defines as follows.

Definition 1.1.9 (Simplex)**.** The d-simplex defined by the vertices $v_0, v_1, \ldots, v_d$ is the subset of $\mathbb{R}^d$ obtained by mapping the standard d-simplex by

$$(t_0, \ldots, t_d) \mapsto \sum_{i=0}^{d} t_i v_i$$

In other words, a d-simplex is the convex hull of $d+1$ points (in generic position, linearly independent) in $\mathbb{R}^d$.

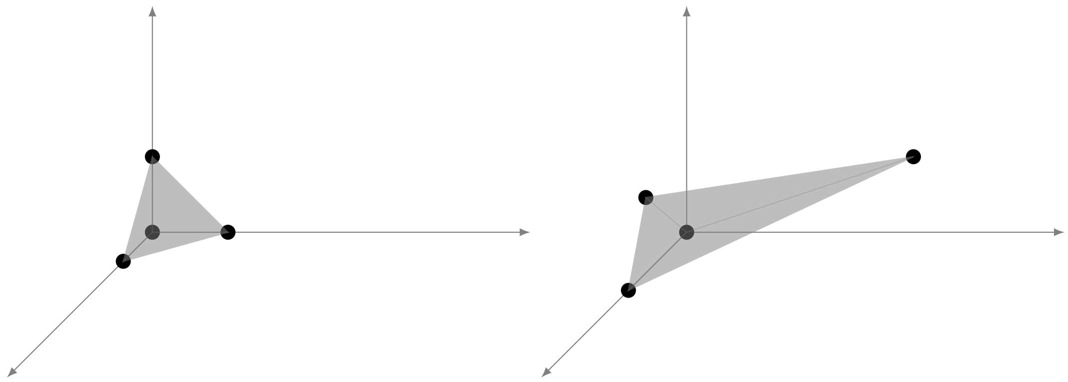


Figure 1.7: The standard 3-simplex and the simplex defined by $(3,1,0), (1,2,4), (0,0,2)$ and the origin

1.2 Cones

Although the solution set of a linear Diophantine system is in general a polyhedron, we will mostly work with polyhedral cones. Cones are polyhedra of a special type. A (polyhedral) cone in $\mathbb{R}^d$ is the intersection of finitely many halfspaces in $\mathbb{R}^d$, whose bounding hyperplanes contain the origin. We choose the following definition that allows more flexibility:

Definition 1.2.1 ((Polyhedral) Cone)**.** Given $a_1, a_2, \ldots, a_k, q \in \mathbb{R}^d$ and an index set $I \subseteq [k]$, we define the cone generated by $a_1, a_2, \ldots, a_k$ at q as

$$\mathcal{C}^I_{\mathbb{R}}(a_1, a_2, \ldots, a_k; q) = \{x \in \mathbb{R}^d : x = q + \sum_{i=1}^{k} \ell_i a_i, \ell_i \geq 0, \ell_i \in \mathbb{R}, \ell_j > 0 \text{ for } j \in I\}$$

If $I = [k]$ then the cone is called open. If $\emptyset \neq I \subset [k]$ then the cone is called half-open. If $I = \emptyset$ then the superscript will be omitted.

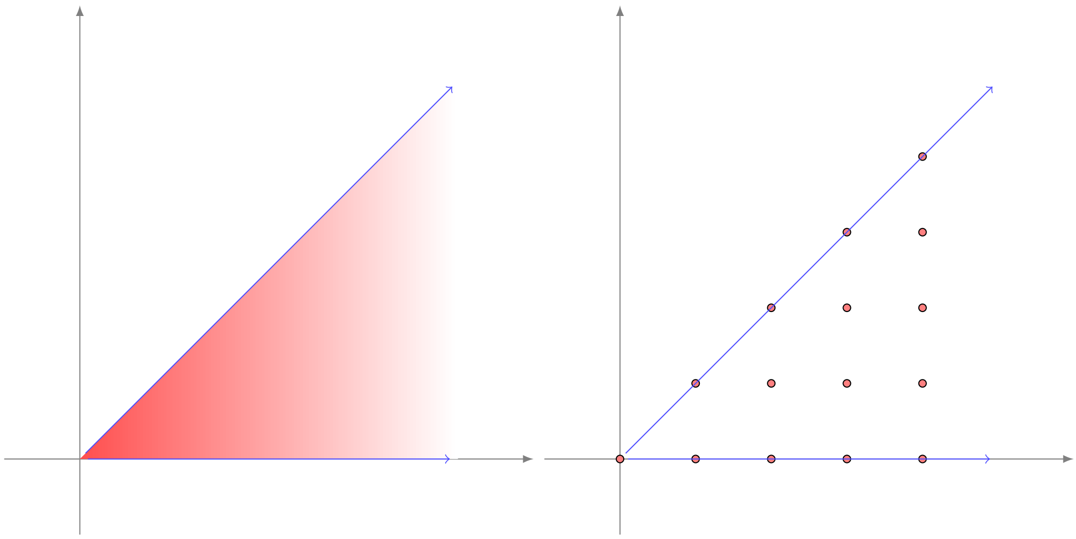


Figure 1.8: The cone generated by $(5, 0)$ and $(5, 5)$ and its lattice points

An object encoding all the information contained in a cone is the fundamental parallelepiped of the cone.

Definition 1.2.2 (Fundamental Parallelepiped)**.** Given a cone $C = \mathcal{C}_{\mathbb{R}}(a_1, a_2, \ldots, a_d; q) \in \mathbb{R}^d$, we define its fundamental parallelepiped as

$$\Pi^{\mathbb{R}}(C) = \left\{ \sum_{i=1}^{d} k_i a_i | k_i \in [0, 1) \right\}$$

and

$$\Pi^{\mathbb{Z}}(C) = \Pi^{\mathbb{R}}(C) \cap \mathbb{Z}^d$$

It is easy to see that a cone is spanned by copies of its fundamental parallelepiped.

Among cones there are two special types that have a central role in polyhedral geometry. These are simplicial and unimodular cones.

Definition 1.2.3 (Simplicial Cone)**.** A cone in $\mathbb{R}^d$ is called simplicial if it is generated by linearly independent vectors in $\mathbb{R}^d$.

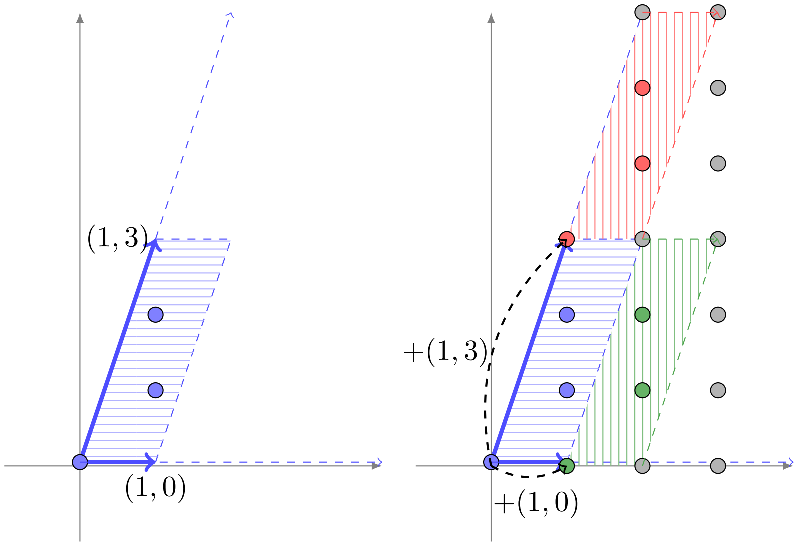


Figure 1.9: The fundamental parallelepiped of the cone generated by $(1, 0)$ and $(1, 3)$.

Although usually the definition asserts d linearly independent generators, we do not enforce this restriction. The reason is that often our cones, and polyhedra in general, will not be full dimensional.

Definition 1.2.4 (Unimodular Cone)**.** A cone C is called unimodular iff $\Pi(C) = \{0\}$.

Lemma 1.2.1. *Let $C = \mathcal{C}_{\mathbb{R}}(r_1, r_2, \ldots, r_n)$ in R^m. If the matrix $G = \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{bmatrix}$ contains a unimodular maximal minor, then C is unimodular.*

Proof. Let I be an index set such that $[G_i]_{i \in I}$ is unimodular and $|I| = n$, where G_i is the i-th column of G. Wlog rearrange the coordinate system such that I are the first n coordinates. Let C_n be the (orthogonal) projection of C into R^n. Then C_n is unimodular. Since projection maps lattice points to lattice points, the only way that C is not unimodular is that $\Pi(C)$ contains lattice points that all project to the origin. In that case, there would be a generator of the form $(0, 0, \ldots, 0, v_{n+1}, v_{n+2}, \ldots, v_m)$. Which contradicts the assumption that $[G_i]_{i \in I}$ is unimodular. □

Proposition 1.2.2. *A pointed convex polyhedral cone is the convex hull of its (finitely many) extreme rays.*

Definition 1.2.5. If the set of generators of the cone C is $\{v_1, v_2, \ldots, v_k\}$ then C is the conic hull of $\{v_1, v_2, \ldots, v_k\}$ and we denote it by $C = \text{co}(\{v_1, v_2, \ldots, v_k\})$

An important tool in polyhedral geometry is the triangulation. A polyhedral object with complicated geometry can be decomposed into simpler ones. The bulding block is the simplex. Since we are interested mostly in cones, we present the definition for the triangulation of a cone.

Definition 1.2.6 (Triangulation of a cone)**.** A triangulation of a cone C is a finite collection of simplicial cones $\Gamma = \{C_1, C_2, \ldots, C_t\}$ such that:

- $\cup C_i = C$,
- If $C\prime \in \Gamma$ then every face of $C\prime$ is in Γ.
- $C_i \cap C_j$ is a common face of C_i and C_j.

The following proposition says that we can triangulate a cone without introducing new rays.

Proposition 1.2.3. *A pointed convex polyhedral cone C admits a triangulation Γ, whose 1-dimensional cones are the extreme rays of C.*

Chapter 2

Semigroups

We start by fixing notation for different representations of subsets of $\mathbb{Z}^n$. Then we add some structure on these subsets. The next step is to investigate the space where the generating functions for such set live. Last we discuss how to change representation.

Some of the basic algebraic structures we need as underlying sets are

$\mathbb{C}$ The field of complex numbers

$\mathbb{Z}$ The ring of integer numbers

$\mathbb{N}$ The monoid of natural numbers

$\mathbb{P}$ The semigroup of positive integers

2.1 Representation

The main object of study in this thesis are subsets of $\mathbb{Z}^n$ and in particular subsets of $\mathbb{N}^n$. We will use four representations for a subset of $\mathbb{Z}^n$. The first one is as a set of points in $\mathbb{Z}^n$. The second one is the generating function of the set as a formal sum. The third representation is the rational form of the generating function. The fourth representation is as a geometric object living in some Euclidean space $\mathbb{R}^d$.

As a trivial example consider $[0, \infty) \cap \mathbb{Z}$:

1. $[0, \infty) \cap \mathbb{Z}$
2. $\sum_{x=0}^{\infty} z^x$
3. $\frac{1}{1-x}$
4. 

It is essential to fix notation in order to make clear which representation we consider each time. In some cases it is even important for correctness. When discussing geometry we will denote by $x1, x_2, \ldots, x_d$ the coordinates of $\mathbb{R}^d$. The corresponding variables in generating functions will be $z_1, z_2, \ldots, z_d$.

We will use the following conventions: Let S be a subset of $\mathbb{Z}^n$. The full generating function of a set S is denoted by $\Phi_S(z) = \sum_{s \in S} z^s$ (using multi-index notation) Its rational form is denoted by $\rho_S(z)$.

For the geometric representation we note that we do not assume our objects to be full dimensional by considering the ambient space to be their affine span.

2.2 Semigroups

Definition 2.2.1 (Semigroup)**.** A semigroup is a set S together with binary operation $\cdot$, such that

- For all $a, b \in S$ we have $a \cdot b \in S$.
- For all $a, b, c \in S$, we have $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

We note that our semigroups, as well as all other algebraic structures we use, are commutative. Moreover usually the semigroup operation will be called addition and will be denoted by $+$.

Considering a homogeneous system of Diophantine equations, the solution set has a semigroup structure. In particular it is a subsemigroup of the semigroup $\mathbb{N}^d$. These sets were the focus of Gordan and Hilbert in the context of invariant theory.

The following theorem shows the connection between cones and semigroups.

Theorem 2.2.1 (Gordan's Lemma, [9])**.** *If $C \subset \mathbb{R}^d$ is a rational cone, then $C \cap A$ is an affine semigroup for any subgroup A of $\mathbb{Z}^d$.*

All semigroups under consideration in what follows are affine and they are defined as

Definition 2.2.2 (Affine semigroup)**.** A semigroup that is isomorphic to a subsemigroup of $\mathbb{Z}^d$ for some d is called affine.

In particular, Gordan gave a procedure to compute a minimal generating set of an affine semigroup, while Hilbert proved that such a minimal generating set always exists and is finite. In fact, Hilbert's theorem is more general but the case we are interested in is covered (and is explicit in the last page of his paper).

Definition 2.2.3. An affine semigroup A is called pointed if its only unit is 0, where a unit is an element $a \in A$ such that its additive inverse $-a$ is in A.

In what follows we omit the characterization affine, since all of our semigroups are affine (except if the contrary is explicitly stated).

Let's see some semigroups that are relevant for our purposes.

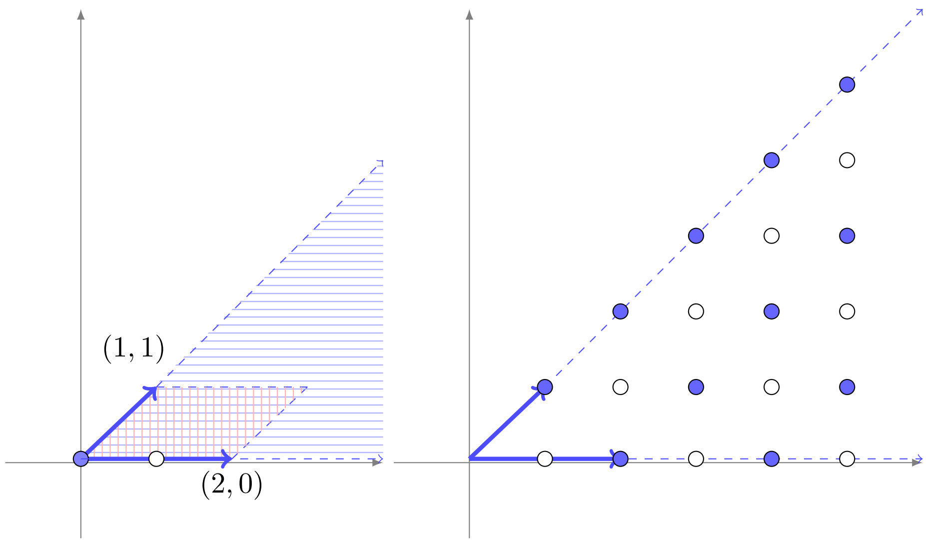


Figure 2.1: The affine semigroup S.

Example 2.2.1. Let S be the semigroup generated by $(1,1)$ and $(2,0)$ (a semigroup of $\mathbb{N}^2$). In the first figure we see the cone generated by $(1,1)$ and $(2,0)$ in $\mathbb{R}^2$ and its fundamental parallelepiped. In the second figure we see the semigroup generated (the filled points).

Example 2.2.2. Let C be the cone generated by $(1,4)$ and $(2,1)$ in $\mathbb{R}^2$. We define S to be the semigroup obtained as the intersection $C \cap \mathbb{Z}^2$. In the first figure is the cone C, in the second figure we see the semigroup S.

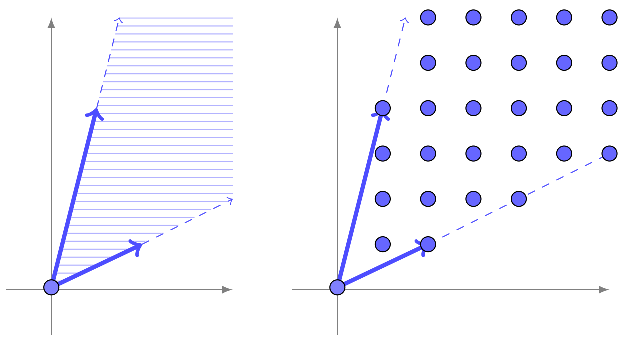


Figure 2.2: The cone and the semigroup generated by $(1,4)$ and $(2,1)$.

It is easy to observe that following the procedure of the second example, we obtain a semigroup that is not the semigroup generated by the generators of the cone. In particular, there are elements of the semigroup that are not positive linear combinations of the generators, such as the points $(1,1)$ and $(2,3)$.

We extend the definition of a polyhedral cone and introduce notation to make this distinction clear.

Definition 2.2.4. Given $a_1, a_2, \ldots, a_k, q \in \mathbb{R}^d$ and an index set $I \subseteq [k]$, we define:

- the (real) cone generated by $a_1, a_2, \ldots, a_k$ at q as

$$\mathcal{C}^I_{\mathbb{R}}(a_1, a_2, \ldots, a_k; q) = \{x \in \mathbb{R}^d : x = q + \sum_{i=1}^{k} \ell_i a_i, \ell_i \geq 0, \ell_i \in \mathbb{R}, \ell_j > 0 \text{ for } j \in I\}$$

- the semigroup cone generated by $a_1, a_2, \ldots, a_k$ at q as

$$\mathcal{C}^I_{\mathbb{N}}(a_1, a_2, \ldots, a_k; q) = \{x \in \mathbb{R}^d : x = q + \sum_{i=1}^{k} \ell_i a_i, \ell_i \in \mathbb{N}, \ell_j > 0 \text{ for } j \in I\}$$

- the conic semigroup generated by $a_1, a_2, \ldots, a_k$ at q as

$$\mathcal{C}^I_{\mathbb{Z}}(a_1, a_2, \ldots, a_k; q) = \mathcal{C}^I_{\mathbb{R}}(a_1, a_2, \ldots, a_k; q) \cap \mathbb{Z}^d$$

As before, if $I = [k]$ then the cone is called open and if $\emptyset \neq I \subset [k]$ then the cone is called half-open.

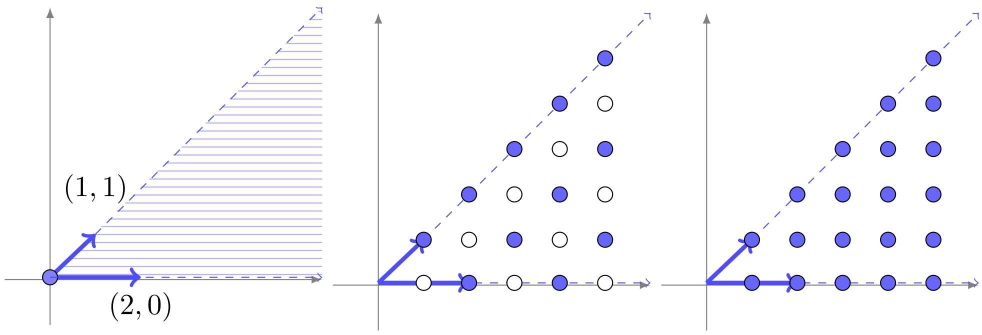


Figure 2.3: $\mathcal{C}_{\mathbb{R}}(a_1, a_2)$, $\mathcal{C}_{\mathbb{N}}(a_1, a_2)$ and $\mathcal{C}_{\mathbb{Z}}(a_1, a_2)$ for $a_1 = (1, 1)$, $a_2 = (2, 0)$.

Then $\mathcal{C}^I_{\mathbb{R}}(a_1, a_2, \ldots, a_k; q)$ is the cone generated by $a_1, a_2, \ldots, a_k$ and translated at q, $\mathcal{C}^I_{\mathbb{N}}(a_1, a_2, \ldots, a_k; q)$ is the the semigroup generated by $a_1, a_2, \ldots, a_k$ at q (as in Example 2.2.1) and $\mathcal{C}^I_{\mathbb{Z}}(a_1, a_2, \ldots, a_k; q)$ is the semigroup obtained as the intersection of $\mathcal{C}^I_{\mathbb{R}}(a_1, a_2, \ldots, a_k; q)$ with $\mathbb{Z}^d$ (as in Example 2.2.2).

We note that $\mathcal{C}^I_{\mathbb{N}}(a_1, a_2, \ldots, a_n; q) \oplus \Pi^I \left(\mathcal{C}^I_{\mathbb{N}}(a_1, a_2, \ldots, a_n; q)\right) = \mathcal{C}^I_{\mathbb{Z}}(a_1, a_2, \ldots, a_n; q)$.

Due to the nature of linear Diophantine systems, the semigroup we are interested in is $\mathcal{C}^I_{\mathbb{Z}}(a_1, a_2, \ldots, a_k)$. Thus, it is important to have a suitable notion of a basis for the semigroup (since the generators are not necessarily enough).

2.3 Hilbert Basis

The Hilbert basis is the unique minimal generating set of an conic semigroup, in the sense that it does generate the semigroup but no subset of the Hilbert basis does.

Definition 2.3.1 (Hilbert basis for cones)**.** A set of vectors $\{h_1, h_2, \ldots, h_n\}$ is a Hilbert basis of $C = \mathcal{C}_{\mathbb{R}}(h_1, h_2, \ldots, h_n) \subset \mathbb{R}^d$ if $\mathcal{C}_{\mathbb{Z}}(h_1, h_2, \ldots, h_n) = \mathcal{C}_{\mathbb{N}}(h_1, h_2, \ldots, h_n)$ and for all $i \in [n]$ we have that $h_i \notin \mathcal{C}_{\mathbb{N}}(h_1, h_2, \ldots, h_{i-1}, h_{i+1}, \ldots, h_n)$.

Let $\mathcal{HB}(C)$ denote the Hilbert basis of the cone C. We illustrate the definition by examples.

Example 2.3.1. Let $C = \mathcal{C}_{\mathbb{R}}((1,4),(2,1)) \subset \mathbb{R}^2$. Then $\mathcal{HB}(C)$ is the minimal generating set of $\mathcal{C}_{\mathbb{Z}}((1,4),(2,1))$.

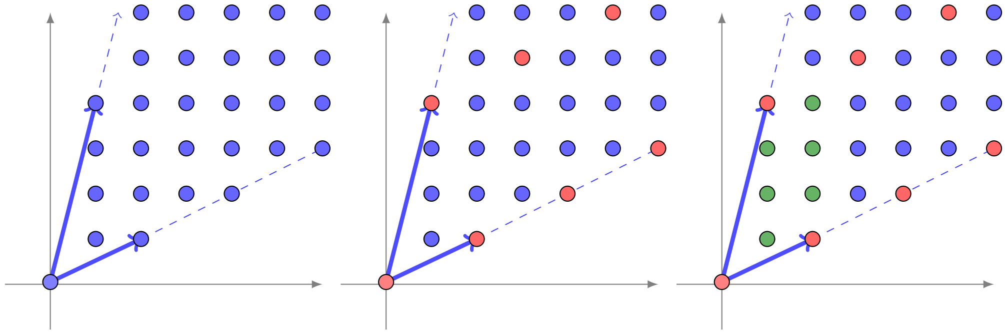


Figure 2.4: The conic semigroup generated by $(1,4)$ and $(2,1)$. The red points are combinations of the generators and the green points are the lattice points in the fundamental parallelepiped except for the origin.

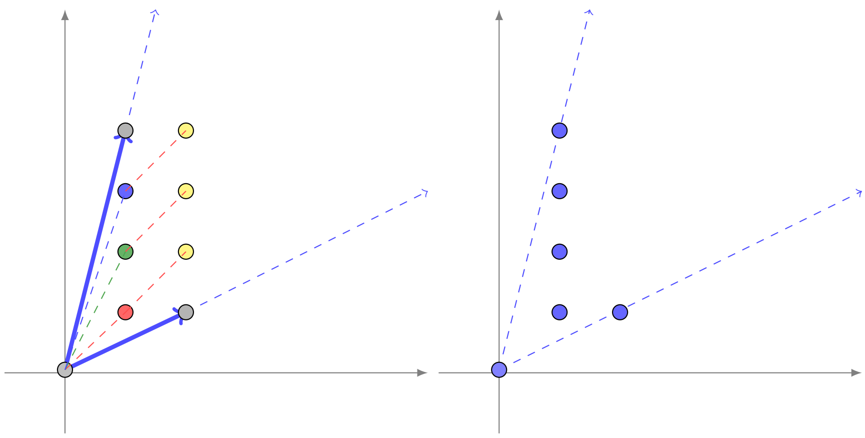


Figure 2.5: If $(1,1),(1,2),(1,3) \in \mathcal{HB}(C)$ then $(2,2),(2,4),(2,4) \notin \mathcal{HB}(C)$.

Since the lattice points of the fundamental parallelepiped are by definition not reachable by combinations of the generators, we definitely need to add some elements in the

Hilbert basis. But not all of them as exhibited in Figure 2.5.

Example 2.3.2. Let C_4 denote the set of all real solutions to the lecture hall inequalities, i.e.

$$C_4 = \left\{ \lambda \in \mathbb{R}^4 : 0 \leq \frac{\lambda_1}{s_1} \leq \frac{\lambda_2}{s_2} \leq \frac{\lambda_3}{s_3} \leq \frac{\lambda_4}{s_4} \right\}$$

Note that C_4 is a cone. The Hilbert basis of C_4 is given by the columns of

$$\begin{array}{c|c|cc|cccc|}
1 & 2 & 3 & 3 & 4 & 4 & 4 & 4 \\
0 & 1 & 2 & 2 & 3 & 3 & 3 & 3 \\
0 & 0 & 0 & 1 & 0 & 1 & 2 & 2 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}$$

Note. The minimality of the Hilbert basis is interpreted differently by different author in various contexts. Here we consider minimality with respect to inclusion. On the other hand, given a grading or ordering, one can request that the elements in the basis are minimal with respect to that grading.

2.3.1 Syzygies

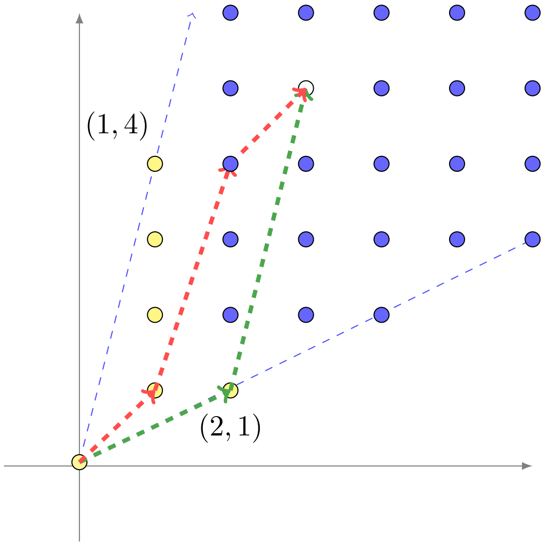


Figure 2.6: The syzygy $(1,1) + (1,3) + (1,1) = (1,4) + (2,1)$

Since a Hilbert basis is the set of generators with some extra elements, there is no guarantee anymore that each element of the semigroup has a unique representation as a combination of Hilbert basis elements. A relation between Hilbert basis elements is called a syzygy. Continuing the previous example, we observe such a situation in Figure 2.6

Syzygies are important because they encode the elements of the semigroup that will be counted more than once if we count the number of points generated by the Hilbert basis elements.

Chapter 3

Generating Functions

One of the most importnat tools in combinatorics and number theory, when dealing with infinite sequences, is that of generating functions. The hope is that the generating function, although encoding full information of an infinite object, has a short (or at least finite) representation.

3.1 Univariate Generating Functions

We start by univariate (ordinary) generating functions. For a detailed introduction see [7**?**]. Given a set $S \subseteq \mathbb{Z}$, we define the generating function $\Phi_S(z)$ as

$$\Phi_S(z) = \sum_{s \in S} z^s$$

A better way to describe a countable set though, is though a function $f : \mathbb{N} \mapsto S \cup \{0\}$. This leads to the

Definition 3.1.1 (Univariate Generating Function)**.** Let $S \subseteq \mathbb{Z}$. Given a function $f : \mathbb{N} \mapsto S \cup \{0\}$, we define the generating function $\Phi_f(z)$ as

$$\Phi_f(z) = \sum_{n \in \mathbb{N}} f(n) z^n$$

When instead of a function f we use the name of a set S, we mean that the function is the characteristic function

$$f_S(x) = \begin{cases} 1 & : x \in S \\ 0 & : x \notin S \end{cases}$$

The first example is of course the geometric series. Let $S = \mathbb{N}$ and then

$$\Phi_{\mathbb{N}}(z) = \sum_{i \in \mathbb{N}} f(i) z^i = \sum_{i \in \mathbb{N}} z^i = \frac{1}{(1-z)}$$

Although it is easy to agree that the equations are "valid", there are different ways to interpret the last one, such as MacLaurin expansion or the multiplicative inverse of $1 - z$ as a formal power series. Such questions will be our focus later.

Already from this example, we see that it is possible (and sometimes useful) to think of our sets as sequences. In the previous example we considered the sequence $(1, 1, \ldots)$.

A slight variation is the sequence $(1, 0, 1, 0, 1 \ldots)$. Namely, we just introduce a gap pattern, omitting the odd numbers. Then we have

$$\Phi_{2\mathbb{N}}(z) = \sum_{i \in 2\mathbb{N}} z^i = \sum_{i \in \mathbb{N}} z^{2i} = \frac{1}{(1 - z^2)}$$

Although these two examples look too simple, it is their multivariate versions that cover the majority of the cases we are interested in.

A slightly more interesting example would be that of triangular numbers $(1, 3, 6, 10, 15, 21, \ldots)$. The n-th term is the binomial coefficient $\binom{n+2}{2}$. We have that

$$\sum_{n=0}^{\infty} \binom{n+2}{2} z^n = \frac{1}{(1 - z)^3}$$

3.1.1 Rational Univariate Generating Functions

One of the main reasons for using generating functions is the hope that one can encode them as rational functions, which provides a compact representation.

Definition 3.1.2 (Rational Generating Function)**.** Let

$$\rho(x) = \sum_{n \geq 0} f(n) x^n$$

such that there exist $P(x), Q(x) \in \mathbb{C}[x]$, with $Q(0) \neq 0$ and $F(x) = P(x)Q(x)^{-1}$.

Theorem 3.1.1 (Fundamental Property[**?**])**.** *Let $d \in \mathbb{N}^*$ and $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$, with $\alpha_d \neq 0$ and $f : \mathbb{N} \to \mathbb{C}$. The following are equivalent:*

1. $\displaystyle\sum_{n \geq 0} f(n) x^n = \frac{P(x)}{Q(x)}$ *where* $Q(x) = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_d x^d$ *and* $P(x) \in \mathbb{C}[x]$ *with* $\deg(P(x)) < d$.

2. *For all $n \in \mathbb{N}$,*

$$f(n + d) + \alpha_1 f(n + d - 1) + \alpha_2 f(n + d - 2) + \ldots + \alpha_d f(n) = 0 \qquad (3.1)$$

3. *For all $n \in \mathbb{N}$, $f(n) = \sum_{i=1}^{k} P_i(n) \gamma_i^n$, where $\prod_{i=1}^{k} (1 - \gamma_i x)^{d_i} = 1 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_d x^d$, the γ_i's are distinct and $P_i(x)$ is a polynomial in n with $\deg(P_i(x)) < d_i$.*

Proposition 3.1.2. *Let $d \in \mathbb{N}$ and $\alpha_1, \alpha_2, \ldots, \alpha_d \in \mathbb{C}$, with $\alpha_d \neq 0$.*
Suppose $f : \mathbb{Z} \to \mathbb{C}$ satisfies the reccurence

$$f(n+d) + \alpha_1 f(n+d-1) + \alpha_2 f(n+d-2) + \ldots + \alpha_d f(n) = 0 \tag{3.2}$$

for all $n \in \mathbb{Z}$
Then $F(x) = \sum_{n \geq 0} f(n)x^n$ and $-F(\frac{1}{x}) = \sum_{n \geq 1} f(-n)x^n$ are rational functions.

Proof. Let $F(x) = \dfrac{P(x)}{Q(x)}$, where $Q(x) = 1+\alpha_1 x+\alpha_2 x^2+\ldots+\alpha_d x^d$. Moreover, let $\mathcal{L}$ be the vector space of Laurent series over $\mathbb{C}$. The map $\mathcal{L} \xrightarrow{Q} \mathcal{L}$ defined as multiplication by Q is a linear transformation. By hypothesis, we have that $Q(x)\sum_{n \geq 0} f(n)x^n = 0$. By linearity we have that $Q(x)\sum_{n \geq 1} f(-n)x^{-n} = -Q(x)\sum_{n \geq 0} f(n)x^n = -P(x)$. By substituting x by $\frac{1}{x}$ we get $\sum_{n \geq 1} f(-n)x^n = -\dfrac{P(x)}{Q(x)} = -F\left(\dfrac{1}{x}\right)$.

Proposition 3.1.3 (Closure properties)**.** *Let $F(x)$ and $G(x)$ be rational power series in $\mathbb{C}[[x]]$. Then the following are true:*

- *$aF(x) + bG(x) \in \mathbb{C}[[x]]$ for $a, b \in \mathbb{C}$*
- *If $\dfrac{F(x)}{G(x)} \in \mathbb{C}[[x]]$, then $\dfrac{F(x)}{G(x)}$ is rational.*
- *$F(x) * G(x)$ is rational powerseries. (Hadamard product)*

Definition 3.1.3 (quasipolynomial[1])**.** is a function $\mathbb{N} \to \mathbb{C}$ of the form $f(n) = \sum_{i=0}^{d} c_i(n)n^i$, where each $c_i(n)$ is a periodic function with integer period and $c_d(n)$ is not identically zero.

Proposition 3.1.4 (Characterization of quasipolynomial)**.** *f is a quasipolynomial if there exists an integer $N > 0$ (the common period of the $c_i(n)$) and polynomials $f_0, f_1, \ldots, f_{N-1}$ such that $f(n) \equiv f_i(n)$ if $n \equiv i(modN)$*

3.2 Multivariate Generating Functions

Although univariate generating functions are very useful in many domains of mathematics, for our purposes multivariate ones are essential.

[1] pseudopolynomial, polynomial on redidue classes

Definition 3.2.1 (Generating Function)**.** Given a set $S \subset \mathbb{Z}^d$, we define the generating function

$$\sigma_S = \sum_{\mathbf{s} \in S} \mathbf{z}^{\mathbf{s}}$$

All the generating functions we will encounter in later chapters are generating functions with $0-1$ coefficients. In other words they represent a set $S \subseteq \mathbb{Z}^d$ as

$$\Phi_{f_S}(\mathbf{z}) = \sum_{\mathbf{i} \in \mathbb{Z}^d} f_S(\mathbf{i}) \mathbf{z}^{\mathbf{i}}$$

for

$$f_S(x) = \begin{cases} 1 & : x \in S \\ 0 & : x \notin S \end{cases}$$

3.3 Generating Functions of Semigroups

3.3.1 Semigroup Cone

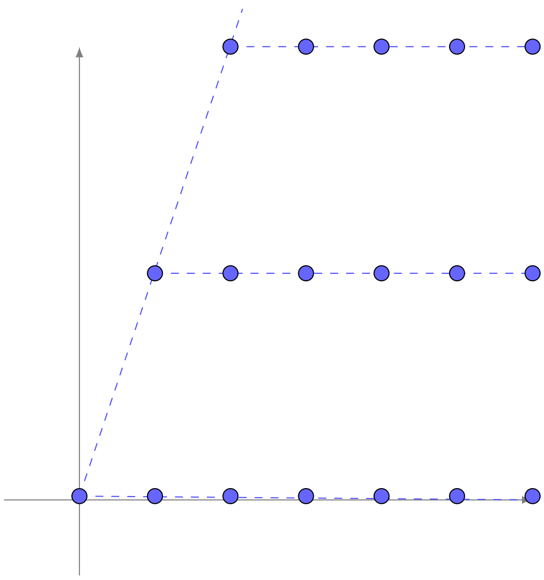


Figure 3.1: $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0)\right)$

We first compute the generating function of a semigroup cone $S = \mathcal{C}_{\mathbb{N}}\left((1,3),(1,0)\right)$ of Figure 3.1 .

The generating function as a formal power series is

$$\Phi_S(\mathbf{z}) = \sum_{\mathbf{i} \in \{k(1,3)+\ell(1,0) \mid k,\ell \in \mathbb{N}\}} \mathbf{z}^{\mathbf{i}} = \sum_{k,\ell \in \mathbb{N}} \mathbf{z}^{k(1,3)+\ell(1,0)} = \left(\sum_{k \in \mathbb{N}} \mathbf{z}^{k(1,3)}\right)\left(\sum_{\ell \in \mathbb{N}} \mathbf{z}^{\ell(1,0)}\right)$$

Thus by the geometric series expansion formula we have

$$\rho_S(\mathbf{z}) = \left(\frac{1}{1-\mathbf{z}^{(1,3)}}\right)\left(\frac{1}{1-\mathbf{z}^{(1,0)}}\right) = \frac{1}{\left(1-z_1z_2^3\right)\left(1-z_1\right)}$$

In general it is easy to see that for a semigroup cone $S = \mathcal{C}_{\mathbb{Z}}\left(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}\right)$ we have

$$\rho_S(\mathbf{z}) = \frac{1}{\left(1-\mathbf{z}^{\mathbf{a_1}}\right)\left(1-\mathbf{z}^{\mathbf{a_2}}\right)\cdots\left(1-\mathbf{z}^{\mathbf{a_n}}\right)}$$

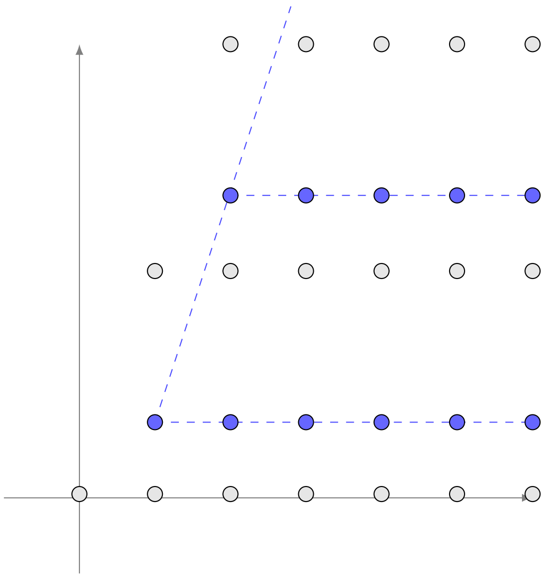


Figure 3.2: $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0);(1,1)\right)$

Observe (Figure 3.2) that if we translate the semigroup to a lattice point, then the structure does not change at all. There is a bijection between $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0)\right)$ and $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0);(1,1)\right)$, given by $f(s) = s+(1,1)$. Translating this to generating function we have that

$$\begin{aligned}
\Phi_{\mathcal{C}_{\mathbb{N}}((1,3),(1,0);(1,1))}(\mathbf{z}) &= \sum_{\mathbf{i}\in\{k(1,3)+\ell(1,0)+(1,1)\mid k,\ell\in\mathbb{N}\}} \mathbf{z}^{\mathbf{i}} \\
&= \sum_{k,\ell\in\mathbb{N}} \mathbf{z}^{k(1,3)+\ell(1,0)+(1,1)} \\
&= \mathbf{z}^{(1,1)}\left(\sum_{k\in\mathbb{N}} \mathbf{z}^{k(1,3)}\right)\left(\sum_{\ell\in\mathbb{N}} \mathbf{z}^{\ell(1,0)}\right)
\end{aligned}$$

Now it should be clear that the rational generating function for $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0);(1,1)\right)$ is

$$\rho_{\mathcal{C}_{\mathbb{N}}((1,3),(1,0);(1,1))}(\mathbf{z}) = \mathbf{z}^{(1,1)} \left(\frac{1}{1-\mathbf{z}^{(1,3)}}\right)\left(\frac{1}{1-\mathbf{z}^{(1,0)}}\right) = \frac{\mathbf{z}^{(1,1)}}{\left(1-z_1 z_2^3\right)(1-z_1)}$$

In general for a semigroup cone $S = \mathcal{C}_{\mathbb{Z}}\left(\mathbf{a_1}, \mathbf{a_2}, \ldots, \mathbf{a_n}; \mathbf{q}\right)$ we have

$$\rho_S(\mathbf{z}) = \frac{\mathbf{z^q}}{\left(1-\mathbf{z^{a_1}}\right)\left(1-\mathbf{z^{a_2}}\right)\cdots\left(1-\mathbf{z^{a_n}}\right)}$$

3.3.2 Conic Semigroup

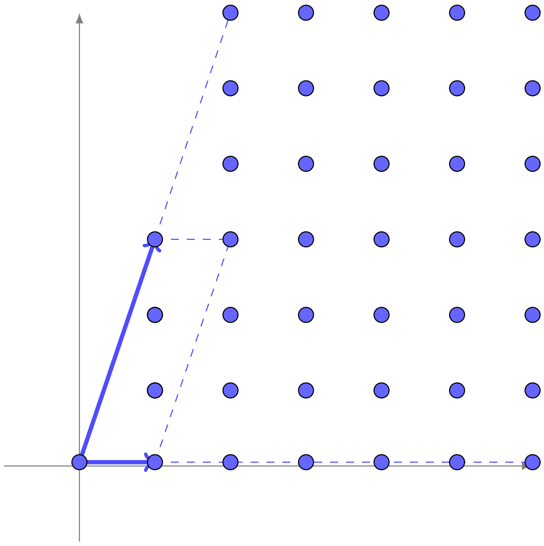


Figure 3.3: $\mathcal{C}_{\mathbb{Z}}\left((1,3),(1,0)\right)$.

There are two ways to construct the generating function for a conic semigroup. Let's consider the conic semigroup $S = \mathcal{C}_{\mathbb{Z}}\left((1,3),(1,0)\right)$ of Figure 3.3, and compute its generating function

$$\Phi_S = \sum_{s \in S} \mathbf{z}^s$$

We observe in Figure 3.4 that S can be partitioned in three sets. The blue points are reachable starting form the origin and using only the cone generators. The red points are reachable by using only the cone generators if we start from the point $(1,1)$. And similarly for the green ones if we start from $(1,2)$.

We observe that we have a partitioning of $\mathcal{C}_{\mathbb{Z}}\left((1,3),(1,0)\right)$ to $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0)\right)$, $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0);(1,1)\right)$ and $\mathcal{C}_{\mathbb{N}}\left((1,3),(1,0);(1,2)\right)$.

The generating function of the semigroup generated by $\{h_1, h_2, \ldots, h_n\}$ is given by $\frac{p(z)}{\prod_{i=1}^{n}(1-z^{h_i})}$ where $p(z)$ is a Laurent polynomial. The role of $p(z)$ is to encode the syzygies among the Hilbert basis elements h_i.

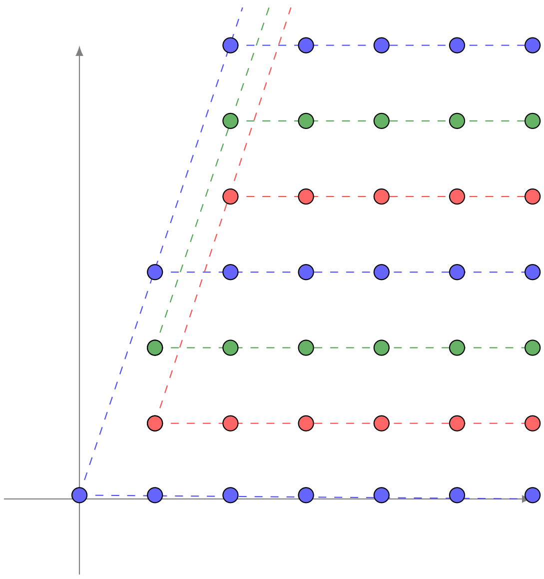


Figure 3.4: The conic semigroup separated in three subsets.

Chapter 4

Partition Analysis

Partition Analysis is a general methodology for the treatment of linear Diophantine systems. There are different algorithmic (or non algorithmic) realizations of the general idea. The methodology is commonly attributed to MacMahon[8], since he was the first to apply it in a way very similar to the one used today. That is, using Partition Analysis for the solution of combinatorial problems subject to linear Diophantine systems.

Nevertheless, it is important to note that Elliott[6] introduced the basics of the methodology and used it to solve linear homogeneous Diophantine equations. In particular, Elliott's method is of interest because it is algorithmic. Elliott himself, although lacking modern terminology, is arguing on the termination of the procedure.

MacMahon in Combinatory Analysis [8] exhibited how to use such a method in order to solve interesting combinatorial problems. Due to various historical reasons, including the lack of interest for computational procedures in mathematics for most of the 20th century, MacMahon's method did not become mainstream among mathematicians. Towards the end of the last century the method was revived [**?**] and with the turn of the century Andrews, Paule and Riese[1] gave a completely algorithmic version of Partition Analysis, named Omega after the Omega operator introduced by MacMahon. Partition Analysis powered by Symbolic Computation is a method that can algorithmically treat combinatorial problems, subject to linear Diophantine systems.

For this section, we restrict to the following (non-parametric) problem:

Problem 4.0.1. Given $A \in M^{m\times n}(\mathbb{Z})$ and $b \in \mathbb{Z}^m$ compute $g_{A,b} = \displaystyle\sum_{x\in\mathbb{N}^n, Ax\geq b} z^x$.

Exhibiting the method we will follow the historical timeline starting from Elliott and arriving to Omega2.

4.1 MacMahon's Partition Analysis

MacMahon was interested in solving systems of linear Diophantine inequalities. We start by the case of one inequality first.

Problem 4.1.1 (Homogeneous Inequality)**.** Let $A \in \mathbb{Z}^n$ and $b \in \mathbb{Z}$. Find all $x \in \mathbb{N}^n$ satisfying $Ax \geq b$.

The generating function of the solution set is

$$g_{Ax\geq 0}(z) = \sum_{Ax\geq 0} z^x$$

Partition Analysis suggest the introduction of an extra variable λ to encode the inequality $Ax \geq 0$. This would transform the generating function to

$$\sum_{x\in\mathbb{N}^n, Ax\geq 0} \lambda^{Ax} z^x$$

The λ variable is introduced to encode the inequalities, but the solutions we are searching for live in one dimension less. The λ dimension is used to control that after the decomposition we can filter out the solutions involving negative exponents.

In the same way, Partition Analysis can be used to treat systems of inequalities as well as inhomogeneous problems.

Following this principle, MacMahon introduced the concept of the crude generating function. But before that, we define the λ-generating function as an intermediate step, both in order to increase clarity in this section and because it is essential when discussing geometry later.

Definition 4.1.1 (λ Generating Function)**.** Given $A \in M^{m\times n}(\mathbb{Z})$ and $b \in \mathbb{Z}^m$ we define the λ generating function as

$$\Phi^\lambda_{A,b} = \sum_{x\in\mathbb{N}^n} z^x \prod_{i=1}^{m} \lambda_i^{A_i x - b_i}$$

Based on the geometric series expansion formula

$$(1-z)^{-1} = \sum_{x\geq 0} z^x$$

we can transform the series into a rational function. The rational form of $\Phi^\lambda_{A,b}$ is denoted by $\rho^\lambda_{A,b}$ and it has the form

$$\rho^\lambda_{A,b} = \lambda^{-b} \prod_{i=1}^{n} \frac{1}{\left(1 - z_i \lambda^{(A^T)_i}\right)}$$

The λ generating function is the main object of study in this thesis.

Let's see three examples. The first two are homogeneous thus the numerator is 1.

Example 4.1.1 (Homogeneous Inequality)**.** Let $A = [\ 3 \quad -1\ ]$ and $b = 0$.

Then

$$\Phi^{\lambda}_{A,b}(z_1, z_2) = \sum_{x_1, x_2 \in \mathbb{N}} \lambda^{3x_1 - x_2} z_1^{x_1} z_2^{x_2}$$

and

$$\rho^{\lambda}_{A,b} = \frac{1}{(1 - z_1 \lambda^3)(1 - z_2 \lambda^{-1})}$$

Example 4.1.2 (Homogeneous System)**.** Let $A = \begin{bmatrix} 3 & -1 \\ 4 & -3 \end{bmatrix}$ and $b = 0$. Then

$$\Phi^{\lambda}_{A,b}(z_1, z_2) = \sum_{x_1, x_2 \in \mathbb{N}} \lambda_1^{3x_1 - x_2} \lambda_2^{4x_1 - 3x_2} z_1^{x_1} z_2^{x_2}$$

and

$$\rho^{\lambda}_{A,b} = \frac{1}{(1 - z_1 \lambda_1^3 \lambda_2^4)(1 - z_2 \lambda_1^{-1} \lambda_2^{-3})}$$

Example 4.1.3 (Inhomogeneous System)**.** Let $A = \begin{bmatrix} 3 & -1 \\ 4 & -3 \end{bmatrix}$ and $b = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$. Then

$$\Phi^{\lambda}_{A,b}(z_1, z_2) = \sum_{x_1, x_2 \in \mathbb{N}} \lambda_1^{3x_1 - x_2 - 1} \lambda_2^{4x_1 - 3x_2 - 2} z_1^{x_1} z_2^{x_2}$$

and

$$\rho^{\lambda}_{A,b} = \frac{\lambda_1^{-1} \lambda_2^{-2}}{(1 - z_1 \lambda_1^3 \lambda_2^4)(1 - z_2 \lambda_1^{-1} \lambda_2^{-3})}$$

The $\Omega_{\geq}$ operator MacMahon introduced (see [8]) the $\Omega_{\geq}$ operator for the solution of linear Diophantine systems. We take the definition from [1]:

Definition 4.1.2. The $\Omega_{\geq}$ operator is defined on functions with absolutely convergent multisum expansions

$$\sum_{s_1=-\infty}^{\infty} \sum_{s_2=-\infty}^{\infty} \cdots \sum_{s_r=-\infty}^{\infty} A_{s_1, s_2, \ldots, s_r} \lambda_1^{s_1} \lambda_2^{s_2} \cdots \lambda_r^{s_r} \tag{4.1}$$

in an open neighborhood of the complex circles $|\lambda_i| = 1$. The action of $\Omega_{\geq}$ is given by

$$\Omega_{\geq} \sum_{s_1=-\infty}^{\infty} \sum_{s_2=-\infty}^{\infty} \cdots \sum_{s_r=-\infty}^{\infty} A_{s_1, s_2, \ldots, s_r} \lambda_1^{s_1} \lambda_2^{s_2} \cdots \lambda_r^{s_r} := \sum_{s_1=0}^{\infty} \sum_{s_2=0}^{\infty} \cdots \sum_{s_r=0}^{\infty} A_{s_1, s_2, \ldots, s_r} \tag{4.2}$$

Note. Although the definition is concerned with convergence issues, in what follows we will use $\Omega_{\geq}$ acting on purely formal objects. Nevertheless, the convergence properties will be important in their connection to the geometric understanding.

Having defined the $\Omega_{\geq}$ operator, we can define the Crude Generating Function. This is the form of the generating function for the solution set of a linear Diophantine system that MacMahon introduced based on Elliott's method and the $\Omega_{\geq}$ operator.

Definition 4.1.3 (Crude Generating Function)**.** Given $A \in M^{m\times n}(\mathbb{Z})$ and $b \in \mathbb{Z}^m$ we define the crude generating function as

$$\Phi^{\Omega}_{A,b} := \Omega_{\geq} \sum_{x\in\mathbb{N}^n} z^x \prod_{i=1}^{m} \lambda_i^{A_i x - b_i}$$

We stress the fact that the assignment is meant formally, since it is easy to see that

$$\Omega_{\geq} \Phi^{\lambda}_{A,b}(z;\lambda) = g_{A,b}(z)$$

as well as

$$\Phi^{\Omega}_{A,b}(z;\lambda) = \sum_{x\in\mathbb{N}^n, Ax\geq b} z^x = g_{A,b}(z)$$

This means that $\Omega_{\geq} \sum_{x\in\mathbb{N}^n} z^x \prod_{i=1}^{m} \lambda_i^{A_i x - b_i}$ is the answer to the problem of solving linear Diophantine system. Thus, it is expected that the computation of the action of the $\Omega_{\geq}$ operator is not computationally easy.

In order to compute the action of $\Omega_{\geq}$ on such a crude generating function, we have 3 algorithmic alternatives. These are Elliott's Algorithm[6], Omega1[1] and Omega2[2]. Nevertheless, we start by presenting part of MacMahon's ad hoc rules for computing $\Omega_{\geq}$, which cannot solve all possible inputs but were powerful enough for him to attack many interesting combinatorial problems.

4.2 Elliott

The problem Elliott considers is to find all non-negative solutions to the equation

$$\sum_{i=1}^{m} a_i x_i - \sum_{i=m+1}^{m+n} b_i x_i = 0 \qquad \text{for } a_i, b_i \in \mathbb{N} \tag{4.3}$$

In other words, we consider one homogeneous equation.

Note. It is hard to resist noting that Elliott himself (as well as subsequent authors) expressed the equation in the form that Diophantus would prefer. Without using negative coefficients.

4.2.1 The method

Elliott outlines his method[6]:

> The principle is that in the infinite expansion which is the formal product of the infinite expansions
> $1 + \xi_1 u^{a_1} + \xi_1 u^{2a_1} + \ldots$
> $1 + \xi_2 u^{a_2} + \xi_2 u^{2a_2} + \ldots$
> $\vdots$
> $1 + \xi_m u^{a_m} + \xi_m u^{2a_m} + \ldots$
> $1 + \xi_{m+1} u^{-b_{m+1}} + \xi_{m+1} u^{-2b_{m+1}} + \ldots$
> $1 + \xi_{m+2} u^{-b_{m+2}} + \xi_{m+2} u^{-2b_{m+2}} + \ldots$
> $\vdots$
> $1 + \xi_{m+n} u^{-b_{m+n}} + \xi_{m+n} u^{-2b_{m+n}} + \ldots$
>
> the terms free from u are of the form $\xi_1^{x_1}\xi_2^{x_2}\cdots\xi_m^{x_m}\xi_{m+1}^{x_{m+1}}\xi_{m+2}^{x_{m+2}}\cdots\xi_{m+n}^{x_{m+n}}$ with 1 for numerical coefficient, where $x_1, x_2, \ldots, x_m, x_{m+1}, \ldots, x_{m+n}$ are a set of positive integers (zero included), which satisfy our diophantine equation 4.3, and that there is just one such term for each set of solutions.
>
> In other words, the generating function for determining the sets of solutions, each once, of 4.3, as sets of exponents of the ξ_i's in its several terms, is the expression for the part which is free from u of the expansion of
>
> $$\frac{1}{(1-\xi_1 u^{a_1})(1-\xi_u 2^{a_2})\cdots(1-\xi_m u^{a_m})(1-\xi_{m+1} u^{a_{m+1}})\cdots(1-\xi_{m+n} u^{a_{m+n}})} \quad (4.4)$$
>
> in the positive powers of the ξ_i's.
>
> The problem is, in any case, to extract from 4.4, and to examine, this generating function. The extraction may be effected by a finite number of easy steps as follows.

The principle presented here by Elliott is the basis of Partition Analysis. That is, introducing an extra variable, denoted by u in Elliott, that is denoted by λ in modern Partition Analysis. In the following sections, we will see that this principle can be generalized by introducing one λ variable for each equation/inequality in a linear Diophantine system.

Before proceeding with presenting (in modern language) Elliott's Algorithm, it should be highlighted that Elliott explicitly says that he has an algorithm, even using almost modern terminology ("a finite succession of simple stages").

The method of Elliot is an algorithm that computes a Partial Fraction Decomposition of an expression

$$\frac{1}{\prod_i^k (1-q_i)}$$

where $q_i \in [z_1, z_2, \ldots, z_{m+n}, \lambda, \lambda^{-1}]$, into a sum of the form

$$\sum_i \frac{\pm 1}{\prod_j (1-p_{ij})}.$$

such that for each i either $p_{ij} \in [z_1, z_2, \ldots, z_{m+n}, \lambda]$ or $p_{ij} \in [z_1, z_2, \ldots, z_{m+n}, \lambda^{-1}]$ for all j. [1].

The algorithm is based on the fact

$$\frac{1}{(1 - z_1\lambda^s)(1 - \frac{z_2}{\lambda^t})} = \frac{1}{1 - z_1 z_2 \lambda^{s-t}} \left(\frac{1}{1 - z_1\lambda^s} + \frac{1}{1 - \frac{z_2}{\lambda^t}} - 1 \right)$$

which expanded gives:

$$\frac{1}{(1 - z_1\lambda^s)(1 - \frac{z_2}{\lambda^t})} = \frac{1}{(1 - z_1 z_2 \lambda^{s-t})(1 - z_1\lambda^s)} + \frac{1}{(1 - z_1 z_2 \lambda^{s-t})(1 - \frac{z_2}{\lambda^t})} - \frac{1}{(1 - z_1 z_2 \lambda^{s-t})}$$

Example 4.2.1. A very simple example, where applying once the identity we obtain the desired PFD is

$$\frac{1}{(1 - x\lambda)(1 - \frac{y}{\lambda})} = \frac{1}{(1 - xy)(1 - x\lambda)} + \frac{1}{(1 - xy)(1 - \frac{y}{\lambda})} - \frac{1}{(1 - xy)}$$

Each of the summands in $\displaystyle\sum_i \frac{\pm 1}{\prod_j (1 - p_{ij})}$ can be expanded using the geometric series expansion. It is easy to see that the summands contributing to the generating function for the solution of Equation 4.3, are exactly the ones where in their expansion λ does not appear. This happens only for the terms $\displaystyle\frac{\pm 1}{\prod_k (1 - p_k)}$, where all p_k are λ-free. Summing up only these terms we get the wanted generating function.

4.2.2 Elliott for Inequalities

In a very similar way, one can use Elliott's algorithm to solve inequalities (as mentioned in [2]). In particular, after obtaining the partial fraction decomposition $\displaystyle\sum_i \frac{\pm 1}{\prod_j (1 - p_{ij})}$, we observe that terms $\displaystyle\frac{\pm 1}{\prod_j (1 - p_{ij})}$ contributing to the generating function of the solution set of the homogeneous inequality

$$\sum_{i=1}^{m} a_i x_i - \sum_{i=m+1}^{m+n} b_i x_i \geq 0 \qquad \text{for } a_i, b_i \in \mathbb{N} \tag{4.5}$$

are exactly the ones that contain no negative exponents of λ in their p_{ij}'s. This is because of the separation to summands containing in their denominators products either only from $[z_1, z_2, \ldots, z_{m+n}, \lambda]$ or only from $[z_1, z_2, \ldots, z_{m+n}, \lambda^{-1}]$. Obviously, a summand containing only non-positive products in the denominator cannot have in its expansion a term with positive λ exponent.

Thus, summing up the terms where λ appears only in non-negative powers (including the λ-free terms) we get the wanted generating function for the solution of Inequality 4.5.

[1] We change from ξ and u to z and λ in order to conform with more modern notational conventions.

4.2.3 Elliott for Systems

It is important to note that Elliott's method relies on the fact that the numerators in all the expressions involved are equal to 1. Of course after bringing all the terms the algorithm returns under common denominator, there is no guarantee that the numerator will be 1. But for each term returned the condition is preserved. Thus it is possible to iteratively apply the algorithm to eliminate λ's in order to solve systems of equations or inequalities. We note that Elliott proves that the numerators will always be ± 1. No repetitions occur in the computed expression.

Example 4.2.2. The system of linear homogeneous inequalities $\{7a-b \geq 0, a-3b \geq 0\}$ can be solved by Elliot, resulting to $\frac{1}{(1-x)(1-x^3y)}$, if the inequality "$a-3b \geq 0$" is treated first. If the order is reversed then the intermediate expression $\frac{-1-\frac{xy^6}{\lambda^{17}}-\frac{xy^5}{\lambda^{14}}-\frac{xy^4}{\lambda^{11}}-\frac{xy^3}{\lambda^8}-\frac{xy^2}{\lambda^5}-\frac{xy}{\lambda^2}}{(1-x\lambda)(1-\frac{xy^7}{\lambda^{20}})}$ is violating the condition that numerators are equal to 1.

We observe that the second inequality "covers" the first one. Thus, choosing the right order, the intermediate expression $\frac{1}{(1-x\lambda^7)(1-x^3y\lambda^{20})}$ is behaving well.

We could still apply Elliott's method if we did not bring the intermediate expression under common denominator.

4.3 MacMahon

Here we present nine of the rules MacMahon (taken from [1]) used for the evaluation of the $\Omega_\geq$ operator. The proofs are usually easy, so we restrict to some observations.

Lemma 4.3.1 (MacMahon Rule 1)**.**

$$\Omega_\geq \frac{1}{(1-\lambda x)\left(1-\frac{y}{\lambda^s}\right)} = \frac{1}{(1-x)(1-x^s y)}$$

Lemma 4.3.2 (MacMahon Rule 2)**.**

$$\Omega_\geq \frac{1}{(1-\lambda^s x)\left(1-\frac{y}{\lambda}\right)} = \frac{1+xy\frac{1-y^{s-1}}{1-y}}{(1-x)(1-xy^s)}$$

Note. The first two rules are about evaluating $\Omega_\geq \frac{1}{(1-\lambda x)\left(1-\frac{y}{\lambda^s}\right)}$ and $\Omega_\geq \frac{1}{(1-\lambda^s x)\left(1-\frac{y}{\lambda}\right)}$. There is an apparent symmetry in the input, but elimination results in structurally different numerators, i.e. 1 versus $1+xy\frac{1-y^{s-1}}{1-y}$.

Lemma 4.3.3 (MacMahon Rule 3)**.**

$$\Omega_\geq \frac{1}{(1-\lambda x)\left(1-\frac{y}{\lambda}\right)\left(1-\frac{z}{\lambda}\right)} = \frac{1}{(1-x)(1-xy)(1-xz)}$$

Lemma 4.3.4 (MacMahon Rule 4).

$$\Omega_{\geq} \frac{1}{(1-\lambda x)(1-\lambda y)\left(1-\frac{z}{\lambda}\right)} = \frac{1-xyz}{(1-x)(1-y)(1-xz)(1-yz)}$$

Note. Although the rational function on which $\Omega_{\geq}$ acts has three factors in the denominator, the resulting rational generating function has four factors in the denominator.

Lemma 4.3.5 (MacMahon Rule 5).

$$\Omega_{\geq} \frac{1}{(1-\lambda x)(1-\lambda y)\left(1-\frac{z}{\lambda^2}\right)} = \frac{1+xyz-x^2yz-xy^2z}{(1-x)(1-y)(1-x^2z)(1-y^2z)}$$

Lemma 4.3.6 (MacMahon Rule 6).

$$\Omega_{\geq} \frac{1}{(1-\lambda^2 x)\left(1-\frac{y}{\lambda}\right)\left(1-\frac{z}{\lambda}\right)} = \frac{1+xy+xz+xyz}{(1-x)(1-xy^2)(1-xz^2)}$$

Lemma 4.3.7 (MacMahon Rule 7).

$$\Omega_{\geq} \frac{1}{(1-\lambda^2 x)(1-\lambda y)\left(1-\frac{z}{\lambda}\right)} = \frac{1+xz-xyz-xyz^2}{(1-x)(1-y)(1-yz)(1-xz^2)}$$

Lemma 4.3.8 (MacMahon Rule 8).

$$\Omega_{\geq} \frac{1}{(1-\lambda x)(1-\lambda y)(1-\lambda z)\left(1-\frac{w}{\lambda}\right)} = \frac{1-xyw-xzw-yzw+xyzw+xyzw^2}{(1-x)(1-y)(1-z)(1-xw)(1-yw)(1-zw)}$$

Lemma 4.3.9 (MacMahon Rule 9).

$$\Omega_{\geq} \frac{1}{(1-\lambda x)(1-\lambda y)\left(1-\frac{z}{\lambda}\right)\left(1-\frac{w}{\lambda}\right)} = \frac{1-xyz-xyw-xyzw+xy^2zw+x^2yzw}{(1-x)(1-y)(1-xz)(1-xw)(1-yz)(1-yw)}$$

Note. For the rules for which the resulting rational function has more factors in the denominator than what the original rational function, we observe that the numerator has terms with both positive and negative signs.

Although these rules are not comprehensive, in the sense that they cannot cover all cases needed to treat linear Diophantine system, they are useful and can solve certain combinatorial problems. In what follows we present algorithmic approaches that can attack any input of the linear Diophantine problem.

4.4 Andrews-Paule-Riese

4.4.1 Omega1

In [1], Andrews et al. present an algorithmic version of Partition Analysis combined with the power of Symbolic Computation. The main tool is the Fundamental Recurrence for the Omega operator. Iterative application of this recurrence is enough for computing the action of the Omega operator.

Lemma 4.4.1 (Theorem 2.1 in [1]).

$$\Omega_{\geq} \frac{\lambda^a}{(1-x_1\lambda)\cdots(1-x_n\lambda)(1-\frac{y_1}{\lambda})\cdots(1-\frac{y_m}{\lambda})} = \frac{P_{n,m,a}(x_1,x_2,\ldots,x_n;y_1,y_2,\ldots,y_m)}{\prod_{i=1}^n(1-x_i)\prod_{i=1}^n\prod_{j=1}^m(1-x_iy_j)} \tag{4.6}$$

where for $n>1$

$$P_{n,m,a}(x_1,x_2,\ldots,x_n;y_1,y_2,\ldots,y_m) = \frac{1}{x_n-x_{n-1}}\Bigg(x_n(1-x_{n-1})\prod_{j=1}^m(1-x_{n-1}y_j)P_{n-1,m,a}(x_1,x_2,\ldots,x_{n-2},x_n;y_1,y_2,\ldots,y_m) - x_{n-1}(1-x_n)\prod_{j=1}^m(1-x_ny_j)P_{n-1,m,a}(x_1,x_2,\ldots,x_{n-2},x_{n-1};y_1,y_2,\ldots,y_m)\Bigg)$$

and for $n=1$

$$P_{1,m,a}(x_1;y_1,y_2,\ldots,y_m) = \begin{cases} x_1^{-a} & \text{if } a\leq 0\\ x_1^{-a}+\prod_{j=1}^m(1-x_1y_j)\sum_{j=0}^a h_j(y_1,y_2,\ldots,y_m)(1-x_1^{j-a}) & \text{if } a>0\end{cases}$$

The base cases for the recurrence are when either all the terms have positive λ exponents or all the terms have negative λ exponents. For the two base cases we need to define the Complete Homogeneous Symmetric Polynomials and some notational sugar mostly to be used later.

Definition 4.4.1 (Complete Homogeneous Symmetric Polynomials, [2]). We define $h_i(z_1,z_2,\ldots,z_n)$ through the generating function

$$\sum_{i=0}^{\infty} h_i(z_1,z_2,\ldots,z_n)t^i = \frac{1}{(1-z_1t)(1-z_2t)\cdots(1-z_nt)}$$

Definition 4.4.2. We denote by $H_a(z_1,z_2,\ldots,z_n)$ the sum $\sum_{i=0}^{a} h_i(z_1,z_2,\ldots,z_n)$.

Lemma 4.4.2 (Lemma 2.1 in [1]). *For any integer* a,

$$\begin{aligned}\Omega_{\geq} \frac{\lambda^\alpha}{(1-x_1\lambda)(1-x_2\lambda)\ldots(1-x_n\lambda)} &= \Omega_{\geq}\sum_{j=0}^{\infty} h_j(x_1,x_2,\ldots,x_n)\lambda^{a+j}\\ &= \tfrac{1}{(1-x_1)(1-x_2)\ldots(1-x_n)} - H_{-a-1}(x_1,x_2,\ldots,x_n)\end{aligned}$$

Lemma 4.4.3 (Lemma 2.2 in [1]). *For any integer* a,

$$\begin{aligned}\Omega_{\geq} \frac{\lambda^\alpha}{(1-\frac{y_1}{\lambda})(1-\frac{y_2}{\lambda})\ldots(1-\frac{y_m}{\lambda})} &= \Omega_{\geq}\sum_{j=0}^{\infty} h_j(y_1,y_2,\ldots,y_m)\lambda^{a-j}\\ &= H_a(x_1,x_2,\ldots,x_n)\end{aligned}$$

The fundamental recurrence assumes that the exponents of λ are ±1. This is not a strong assumption since we can always employ the following decomposition.

Note (Roots of unity decomposition). The recurrence assumes that all powers of λ in the denominator are ± 1. As noted in [1], this can be achieved by the following transformations:

$$(1 - x\lambda^r) = \prod_{j=0}^{r-1} (1 - \rho^j x^{\frac{1}{r}} \lambda) \tag{4.7}$$

$$(1 - \frac{y}{\lambda^s}) = \prod_{j=0}^{s-1} (1 - \frac{\sigma^j y^{\frac{1}{s}}}{\lambda}) \tag{4.8}$$

where $\rho = e^{\frac{2\pi i}{r}}$ and $\sigma = e^{\frac{2\pi i}{s}}$.

The obvious drawback of this approach is that we introduce complex coefficients instead of ± 1. This motivates the need for a better recurrence, which the same authors provide in [2].

4.4.2 Omega2

In [2] the authors introduce an improved partial fraction decomposition method, given by the recurrence of Theorem 4.4.4

Theorem 4.4.4 (Generalized PFD [2]). *Let* $\alpha \geq \beta \geq 1$ *and* $\gcd(\alpha, \beta) = 1$. *Then*

$$\frac{1}{(1 - z_1 z_3^{\alpha})(1 - z_2 z_3^{\beta})} = \frac{1}{(z_2^{\alpha} - z_1^{\beta})} \left(\frac{\bar{P}(z_3)}{(1 - z_1 z_3^{\alpha})} + \frac{\bar{Q}(z_3)}{(1 - z_2 z_3^{\beta})} \right) \tag{4.9}$$

$$\text{where } \bar{P}(z_3) := \sum_{i=0}^{\alpha-1} \bar{a}_i z_3^i \text{ and } \bar{a}_i = \begin{cases} -z_1^{\beta} z_2^{\frac{i}{\beta}} & \text{, if } \beta | i \text{ or } i = 0 \\ -z_1^{rmd((\alpha^{-1} \mod \beta)i, \beta)} z_2^{rmd((\beta^{-1} \mod \alpha)i, \alpha)} & \text{, otherwise} \end{cases}$$

$$\text{while } \bar{Q}(z_3) := \sum_{i=0}^{\beta-1} \bar{b}_i z_3^i \text{ and } \bar{b}_i = \begin{cases} z_2^{\alpha} & \text{, if } i = 0 \\ z_1^{rmd((\alpha^{-1} \mod \beta)i, \beta)} z_2^{rmd((\beta^{-1} \mod \alpha)i, \alpha)} & \text{, otherwise} \end{cases}$$

Moreover, two new base cases are introduced. As before, we define some notation for homogeneous polynomials.

Definition 4.4.3 (Weighted Complete Homogeneous Symmetric Polynomials, [2]). We define $h_i(z_1, z_2, \ldots, z_n; \zeta_1, \zeta_2, \ldots, \zeta_n)$ through the generating function

$$\sum_{i=0}^{\infty} h_i(z_1, z_2, \ldots, z_n; \zeta_1, \zeta_2, \ldots, \zeta_n) t^i = \frac{1}{(1 - z_1 t^{\zeta_1})(1 - z_2 t^{\zeta_2}) \cdots (1 - z_n t^{\zeta_n})}$$

Definition 4.4.4. We denote by $H_a(z_1, z_2, \ldots, z_n; \zeta_1, \zeta_2, \ldots, \zeta_n)$ the sum

$$\sum_{i=0}^{a} h_i(z_1, z_2, \ldots, z_n; \zeta_1, \zeta_2, \ldots, \zeta_n)$$

Lemma 4.4.5 (Case $m = 0$, Section 2 in [2]). *For any integer a,*

$$\Omega_{\geq} \frac{\lambda^a}{(1-x_1\lambda^{j_1})(1-x_2\lambda^{j_2})\ldots(1-x_n\lambda^{j_n})} = \Omega_{\geq} \sum_{j=0}^{\infty} h_j(x_1, x_2, \ldots, x_n; j_1, j_2, \ldots, j_n)\lambda^{a+j}$$
$$= \frac{1}{(1-x_1)(1-x_2)\ldots(1-x_n)} - H_{-a-1}(x_1, x_2, \ldots, x_n; j_1, j_2, \ldots, j_n)$$

Lemma 4.4.6 (Case $n = 0$, Section 2 in [2]). *For any integer a,*

$$\Omega_{\geq} \frac{\lambda^a}{(1-\frac{y_1}{\lambda^{j_1}})(1-\frac{y_2}{\lambda^{j_2}})\ldots(1-\frac{y_m}{\lambda^{j_m}})} = \Omega_{\geq} \sum_{j=0}^{\infty} h_j(x_1, x_2, \ldots, x_n; j_1, j_2, \ldots, j_n)\lambda^{a-j}$$
$$= H_a(x_1, x_2, \ldots, x_n; j_1, j_2, \ldots, j_n)$$

Lemma 4.4.7 (Case $m = 1$, Section 2 in [2]). *For any integer $a > -k$,*

$$\Omega_{\geq} \frac{\lambda^a}{(1-x_1\lambda^{j_1})(1-x_2\lambda^{j_2})\ldots(1-x_n\lambda^{j_n})(1-y\lambda^{-k})}$$
$$= \frac{1}{(1-x_1)(1-x_2)\ldots(1-x_n)(1-y)} - \frac{\sum_{\tau_1,\tau_2,\ldots,\tau_n=0}^{k-1} \prod x_i^{\tau_i} y^{\left\lfloor \frac{\sum j_i\tau_i + a}{k} \right\rfloor + 1}}{(1-x_1^k y^{j_1})(1-x_2^k y^{j_2})\ldots(1-x_n^k y^{j_n})(1-y)}$$

Lemma 4.4.8 (Case $n = 1$, Section 2 in [2]). *For any integer $a > -k$,*

$$\Omega_{\geq} \frac{\lambda^a}{(1-x\lambda^{j})(1-y_1\lambda^{-k_1})(1-y_2\lambda^{-k_2})\ldots(1-y_m\lambda^{-k_m})} = \frac{\sum_{\tau_1,\tau_2,\ldots,\tau_n=0}^{j-1} \prod y_i^{\tau_i} x^{\left\lceil \frac{\sum k_i\tau_i - a}{j} \right\rceil}}{(1-x)(1-x^{k_1} y_1^{j})(1-x^{k_2} y_2^{j})\ldots(1-x^{k_m} y_m^{j})}$$

Chapter 5

Linear Diophantine Systems

Diophantus in Arithmetica dealt with the solution of equations. But in the time of Diophantus, a couple of things were essentially different than in modern mathematics:

- No notion of zero existed.
- Fractions were not treated as numbers (Diophantus was the first to do so).
- There was no notation for arithmetic.

Arithmetica consisted of 13 books, out of which only six survive and possibly another four through arab translations survive, dealing with the solution of 130 equations. On one hand his work is important because it is the oldest account we have for indefinite equations (equations with more than one solutions). More importantly though, Diophantus introduced a primitive notational system for (what later was called) algebra.

For our purposes, the essential part of his work is his view on what is the solution of an equation. He considered equations with positive rational coefficients whose solutions are positive rationals. Following this path, we consider a Diophantine problem to have integer coefficients and non-negative integer solutions.

In 1463 the German mathematician Regiomontanus wrote that "No one has yet translated from Greek into Latin the thirteen books of Diophantus, in which the very flower of the whole of arithmetic lies hidden", indicating that Arithmetica was recognized as an important source.

Although the most famous marginal note to be found in a copy of Arithmetica is by Fermat (his last theorem), there is another one which is very interesting. The Byzantine scholar Chortasmenos notes "Thy soul, Diophantus, be with Satan because of the difficulty of your problems" (funnily enough next to Fermat's last theorem).

This last comment, combined with the note that Diophantus did not have a general method (after solving the 100th problem, you still have no clue how to attack the 101st) is important for us. Of course, for non-linear Diophantine problems one cannot expect a general method due to the negative answer to Hilbert's 10th problem. But we present algorithmic solutions for linear Diophantine systems (developed last century) and examine their connections.

We first define what a linear Diophantine system is

Definition 5.0.5. Given $A \in \mathbb{Z}^{m\times n}$ and $b \in \mathbb{Z}[t_1, t_2, \ldots, t_k]^m$ find all $x \in \mathbb{N}^n$ satisfying $Ax\diamond b$. The triple $(A, b, \diamond)$ is called a linear Diophantine system.

As the name suggests we have a linear system of equations/inequalities (thus $\diamond \in \{\geq, =\}$). From linear algebra, the standard representation of linear systems is in matrix notation. Since we respect Diophantus viewpoint, our matrices will always be in $\mathbb{Z}^{m\times n}$. In addition, there is the restriction that the solutions are non-negative integers.

We note that the right hand side of the system is considered to live in $\mathbb{Z}[t_1, t_2, \ldots, t_k]^m$. This is essential for the understanding of a certain category of problems, but for most cases one can restrict to having constant right hand side, i.e. $b \in \mathbb{Z}^m$.

Given a linear Diophantine system, one can ask two questions:

- How many solutions are there?
- What are the solutions?

The first is called the Counting problem, while the second is the Listing problem. We are interested in solving these two problems in an efficient way. The listing of the solutions may be exponentially big in comparison to the input (or even infinite), thus we need a representation of the answer that encodes the solutions in an efficient way.

We resort to the use of generating functions for that reason. More precisely (using terminology that will be clear later), the solution to the Listing Problem is the full (or multivariate) generating function, while for the Counting problem is the counting generating function.

In the literature, depending on the motivation of each author, the problem specification is (sometimes silently) altered. In order to tackle the problem in an algorithmic way, we have to first resolve the specification issue. The formal definitions we use for the two problems we are interested in are

Definition 5.0.6 (Listing Linear Diophantine Problem)**.** Given a linear Diophantine system $(A, b, \diamond) \in \mathbb{Z}^{m\times n} \times \mathbb{Z}[t_1, t_2, \ldots, t_k]^m \times \{=, \geq\}$, denote by $S(t)$ the solution set of the system (depending on $t = (t_1, t_2, \ldots, t_k)$). Compute the generating function $\mathcal{L}_{A,b,\diamond}(z, t) = \sum_{s\in S(t)} z^s q^t$.

Definition 5.0.7 (Counting Linear Diophantine Problem)**.** Given a linear Diophantine system $(A, b, \diamond) \in \mathbb{Z}^{m\times n} \times \mathbb{Z}[t_1, t_2, \ldots, t_k]^m \times \{=, \geq\}$, denote by $S(t)$ the solution set of the system (depending on $t = (t_1, t_2, \ldots, t_k)$). Compute the generating function $\mathcal{C}_{A,b,\diamond}(t) = |S(t)|q^t$.

5.0.3 Parametric vs Non-Parametric

The answer to all the problems we are interested in is the generating function of some quantity. This implies that there is always (at least) one parameter involved, such as the z variables. The interesting set of parameters though is that of t-variables .

For the most of what follows we will consider the case where $t_1 = t_2 = \cdots = t_k = 0$. This corresponds to the case $b \in \mathbb{Z}^m$ and is the most studied case. A second case that is encountered mostly in combinatorial problems (such as magic squares) and Ehrhart theory (as the dilation parameter) is when $b \in [t]^m$ (the additive monoid generated by t). That means that b contains monomials in one variable t.

This distinction is better expressed by introducing some terminology. When referring to a parametric problem, we consider a problem where the choice of different parameter values changes essentially the structure of the problem. From a geometric point of view, this means that the parameter choice changes the geometry of the object at hand, in a way different than just dilating it.

For example, the problem (of symmetric 3×3 Latin squares)

$$\left(\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} r \\ r \\ r \end{pmatrix}, = \right)$$

is not considered a parametric problem, since the (positive integer) parameter r does not change the geometry of the problem (the right hand side has elements from $[r]$). In other words, we can consider the linear Diophantine system

$$\left(\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, = \right)$$

and then r is the dilation parameter (usually referred to as t in Ehrhart Theory).

On the other hand, the (vector partition function) problem

$$\left(\begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}, = \right)$$

is parametric, since the right hand side contains (honest) elements of $[b_1, b_2]$. The choice of b_1 and b_2 can change considerably the geometry of the problem.

5.0.4 Bounded vs Unbounded

A fundamental property of a problem is whether it is bounded or not, i.e. if the cardinality of $S(t)$ is finite. For counting problems, unbounded ones make no sense. For enumeration problems, both cases are interesting.

One can easily see that the counting problem can be reduced to the listing problem, since knowing the solutions provides enough knowledge about how many solutions there are. Nevertheless, it is not always trivial to count the number of elements of a given set. At least not computationally trivial.

Note. The case $x \in \mathbb{Z}^n$ is easier than $x \in \mathbb{N}^n$, since the solution set S forms a subgroup of $\mathbb{Z}^m$, the rank of which is equal to the nullity of A and we can express the generators of the subgroup explicitly.

On the other hand, in the case $x \in \mathbb{N}^n$, the solution set S forms a commutative monoid.

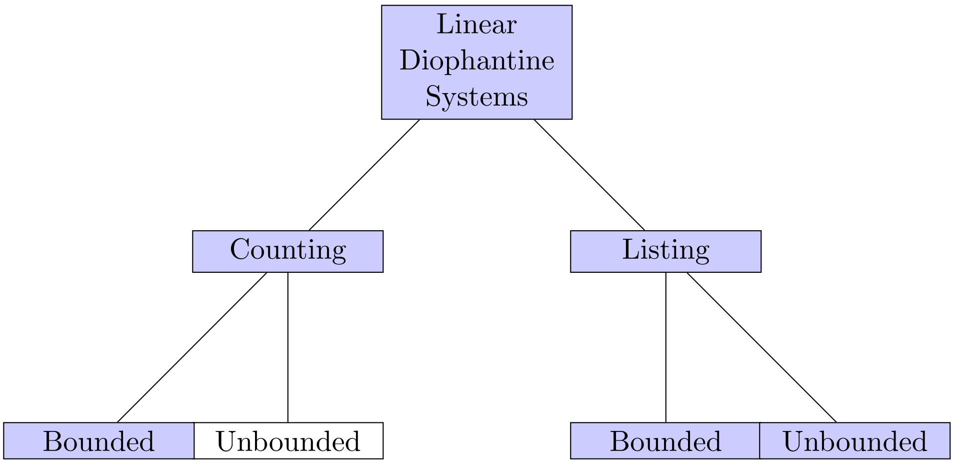


Figure 5.1: Linear Diophantine Problems

Chapter 6

Geometry of Partition Analysis

In what follows we examine how the Partition Analysis methods can be interpreted in the Polyhedral Geometry world. As we have seen, both methods rely on partial fraction decompositions. On the other hand, the rational functions appearing on Partition Analysis look very much like the rational generating functions of cones. These two observations lead naturally to an attempt to interpret the geometry of the two methods as cone decompositions.

6.1 The geometry of Elliott's Algorithm

Elliott's method relies on the partial fraction decomposition

$$\begin{aligned}\frac{1}{(1-x\lambda^{\alpha})(1-\frac{y}{\lambda^{\beta}})} &= \frac{1}{1-xy\lambda^{\alpha-\beta}}\left(\frac{1}{1-x\lambda^{\alpha}}+\frac{1}{1-\frac{y}{\lambda^{\beta}}}-1\right)\\ &= \frac{1}{(1-xy\lambda^{\alpha-\beta})(1-x\lambda^{\alpha})}+\frac{1}{(1-xy\lambda^{\alpha-\beta})(1-\frac{y}{\lambda^{\beta}})}-\frac{1}{(1-xy\lambda^{\alpha-\beta})}\end{aligned}$$

In order to translate this ratinal function identity to an identity about cones we first observe that

$$\frac{1}{(1-x\lambda^{\alpha})(1-\frac{y}{\lambda^{\beta}})}$$

is the generating function of the 2-dimensional cone C generated by $(1,0,\alpha)$ and $(1,0,-\beta)$. Lemma 1.2.1 guarantees that the numerator in the generating function of C is indeed 1.

The point $(1,1,\alpha-\beta)$ is in the interior of the cone C.

This means that the cones

$$A=\mathbb{R}_{+}\left((1,0,\alpha),(1,1,\alpha-\beta)\right)B=\mathbb{R}_{+}\left((1,0,-\beta),(1,1,\alpha-\beta)\right)$$

subdivide cone C. Their intersection is exactly the ray starting from the origin and passing through $(1,1,\alpha-\beta)$.

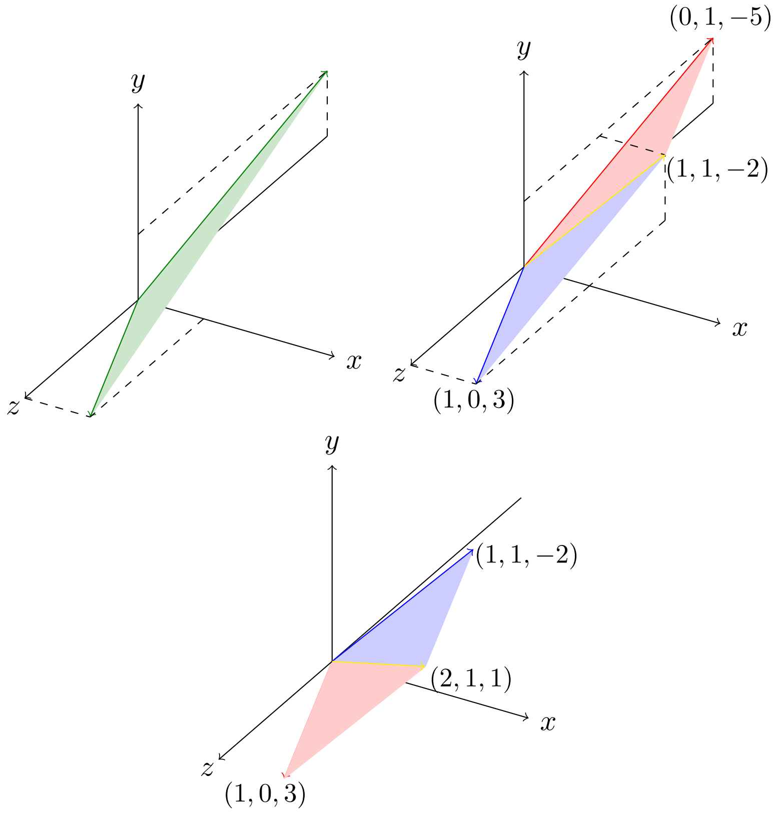


Figure 6.1: Two iterations of Elliott's algorithm.

By a simple inclusion-exclusion argument we have the signed decomposition $C = A + B - (A \cap B)$. This decomposition translated to the generating functions level is exactly the partial fraction decomposition employed by Elliott.

The Algorithm

It is easy to see that, after a finite number of steps, we end up with a sum of cones of three types:

1. the generators contain only zero λ-coordinate
2. the generators contain only non-negative (but not all zero) λ-coordinate
3. the generators contain only non-positive (but not all zero) λ-coordinate

Note that all the cones involved are unimodular according to Lemma 1.2.1

At this point we intersect each cone with the non-negative λ halfspace. This means that we discard the cones of the 3$^{\text{rd}}$ type. Then we (orthogonally) project wrt the λ-coordinate.

6.2 Geometry of Omega2

The main step in the algorithm is given by the theorem 4.4.4:

Theorem. *Let $\alpha \geq \beta \geq 1$ and* $\gcd(\alpha, \beta) = 1$*. Then*

$$\frac{1}{(1 - z_1 z_3^\alpha)(1 - z_2 z_3^\beta)} = \frac{1}{(z_2^\alpha - z_1^\beta)} \left(\frac{\bar{P}(z_3)}{(1 - z_1 z_3^\alpha)} + \frac{\bar{Q}(z_3)}{(1 - z_2 z_3^\beta)} \right) \tag{6.1}$$

where $\bar{P}(z_3) := \sum_{i=0}^{\alpha-1} \bar{a}_i z_3^i$ *and* $\bar{a}_i = \begin{cases} -z_1^\beta z_2^{\frac{i}{\beta}} & \text{, if } \beta | i \text{ or } i = 0 \\ -z_1^{rmd((\alpha^{-1} \mod \beta)i, \beta)} z_2^{rmd((\beta^{-1} \mod \alpha)i, \alpha)} & \text{, otherwise} \end{cases}$

while $\bar{Q}(z_3) := \sum_{i=0}^{\beta-1} \bar{b}_i z_3^i$ *and* $\bar{b}_i = \begin{cases} z_2^\alpha & \text{, if } i = 0 \\ z_1^{rmd((\alpha^{-1} \mod \beta)i, \beta)} z_2^{rmd((\beta^{-1} \mod \alpha)i, \alpha)} & \text{, otherwise} \end{cases}$

We first rewrite Equation 6.1, by pulling out $-z_1^\beta$ from the denominator of $\frac{1}{(z_2^\alpha - z_1^\beta)}$

$$\frac{1}{(1 - z_1 z_3^\alpha)(1 - z_2 z_3^\beta)} = \frac{-z_1^{-\beta} \bar{P}(z_3)}{(1 - z_1^{-\beta} z_2^\alpha)(1 - z_1 z_3^\alpha)} - \frac{z_1^{-\beta} \bar{Q}(z_3)}{(1 - z_1^{-\beta} z_2^\alpha)(1 - z_2 z_3^\beta)} \tag{6.2}$$

which motivates

Definition 6.2.1. We define $P_{\alpha,\beta}$ and $Q_{\alpha,\beta}$ as

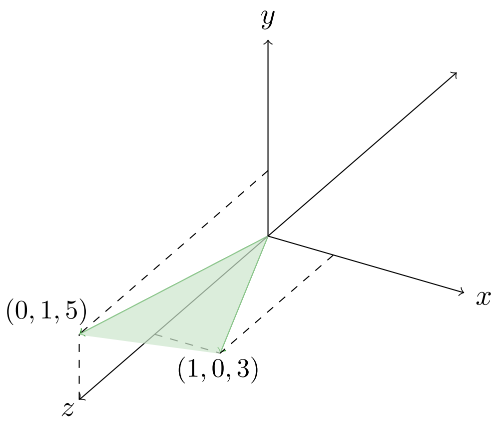
- $P_{\alpha,\beta} := -z_1^{-\beta} \bar{P}(z_3) = \sum_{i=0}^{\alpha-1} a_i z_3^i$

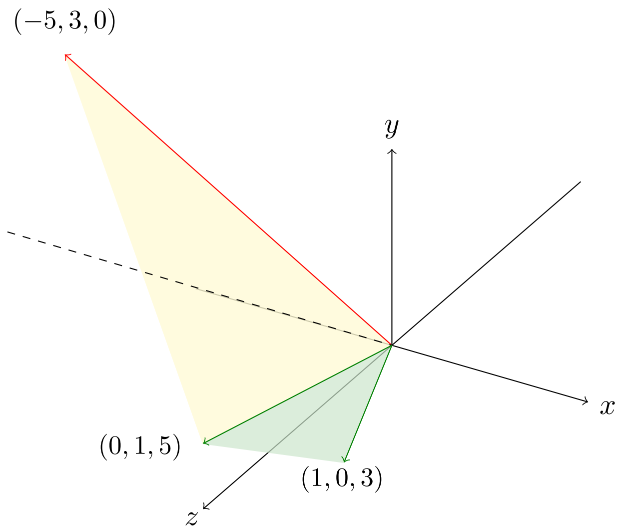
- $Q_{\alpha,\beta} := z_1^{-\beta}\bar{Q}(z_3) = \sum_{i=0}^{\beta-1} b_i z_3^i$

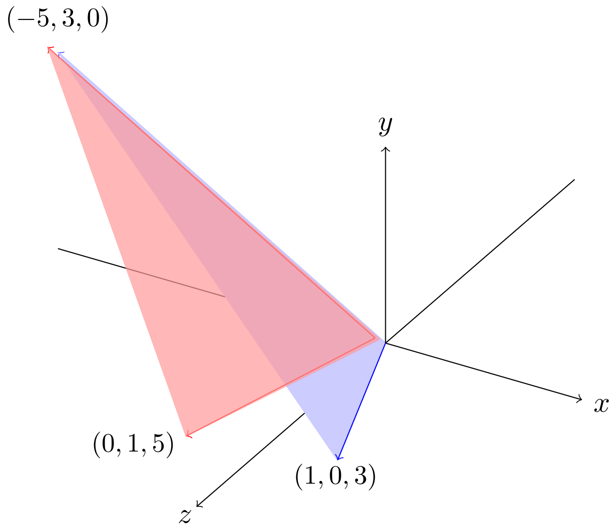
where

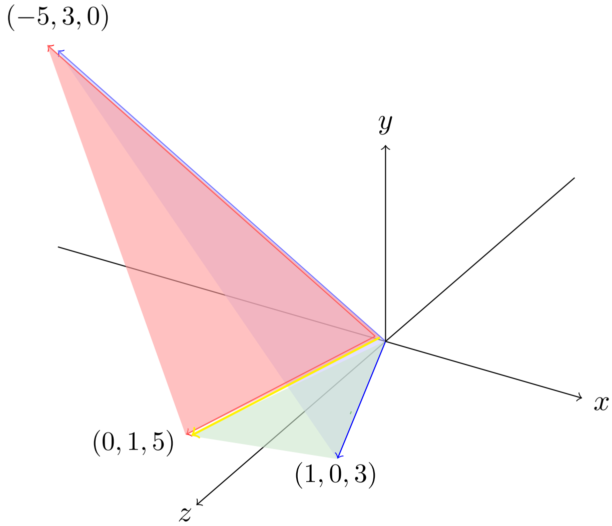
- $a_i = \begin{cases} z_2^{\frac{i}{\beta}} & \text{, if } \beta | i \text{ or } i = 0 \\ z_1^{\operatorname{rmd}((\alpha^{-1} \mod \beta)i,\beta)-\beta} z_2^{\operatorname{rmd}((\beta^{-1} \mod \alpha)i,\alpha)} & \text{, otherwise} \end{cases}$

- $b_i = \begin{cases} z_1^{-\beta} z_2^{\alpha} & \text{, if } i = 0 \\ z_1^{\operatorname{rmd}((\alpha^{-1} \mod \beta)i,\beta)-\beta} z_2^{\operatorname{rmd}((\beta^{-1} \mod \alpha)i,\alpha)} & \text{, otherwise} \end{cases}$









The main goal of this section is to prove the following theorem

Theorem 6.2.1. *Application of the Generalized Partial Fraction Decomposition*

$$\frac{1}{(1-z_1z_3^{\alpha})(1-z_2z_3^{\beta})} = \frac{P_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_1z_3^{\alpha})} - \frac{Q_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_2z_3^{\beta})} \tag{6.3}$$

on σ_C induces a signed cone decomposition of the cone $C = \mathbb{R}_+\{(1,0,\alpha),(0,1,\beta)\}$.

Proof Strategy:

- Determine the structure of the fundamental parallelepiped of the cones $\operatorname{co}((-\beta,\alpha,0),(1,0,\alpha))$ and $\operatorname{co}((-\beta,\alpha,0),(0,1,\beta))$
- Prove that the numerator polynomials in the GPFD are the generating functions of these fundamental parallelepipeds.

Denote by A the cone $\operatorname{co}((-\beta,\alpha,0),(1,0,\alpha))$ and by B the cone $\operatorname{co}((-\beta,\alpha,0),(0,1,\beta))$. In what follows we assume $\gcd(\alpha,\beta)=1$ as indicated in Theorem 4.4.4.

Funadamental Parallelepipeds

We define Φ_ζ to be the set $\Pi(B)\cap(\mathbb{Z}^2\times\{\zeta\})$, analogously to Π_ζ. As before we have (with a completely analogous proof) that $\Phi_\zeta=\{(x_1,x_2,\zeta)\in\mathbb{Z}^3|x_2=\frac{\zeta-x_1\alpha}{\beta},x_1\in\{-\beta+1,-\beta+2,\ldots,0\}\}$ and $|\Phi_\zeta|\le 1$.

Definition 6.2.2. We define Π_ζ to be the set $\Pi(A)\cap(\mathbb{Z}^2\times\{\zeta\})$.

The following lemma says that there is at most one lattice point in $\Pi(A)$ at any given height (x_3-value).

Lemma 6.2.2. $\Pi_\zeta=\{(x_1,x_2,\zeta)\in\mathbb{Z}^3|x_1=\frac{\zeta-x_2\beta}{\alpha},x_2\in\{0,1,\ldots,\alpha-1\}\}$. *Moreover* $|\Pi_\zeta|\le 1$.

Proof. Let $(x_1,x_2,x_3)\in\Pi(A)\cap\mathbb{Z}^3$. Then there exist $k,l\in[0,1)$ such that $k(-\beta,\alpha,0)+l(1,0,\alpha)=(x_1,x_2,x_3)\in\mathbb{Z}^3$. $\begin{cases}x_1=l-k\beta\\x_2=k\alpha\\x_3=l\alpha\end{cases}\to\begin{cases}x_1=\frac{\zeta}{\alpha}-k\beta\\x_2\in[0,\alpha)\cap\mathbb{Z}\\l=\frac{x_3}{\alpha}\end{cases}\to\begin{cases}x_1=\frac{x_3-x_2\beta}{\alpha}\\x_2\in\{0,1,\ldots,\alpha-1\}\\x_3\in\{0,1,\ldots,\alpha-1\}\end{cases}$

Fix $x_3=\zeta\in\{0,1,\ldots,\alpha-1\}$. Assume $|\Pi_\zeta|>1$ and let $(x_1',x_2',\zeta),(x_1'',x_2'',\zeta)\in\Pi_\zeta$. Then $\begin{cases}\alpha|\zeta-x_2'\beta\\\alpha|\zeta-x_2''\beta\end{cases}\to\alpha|x_2'\beta-x_2''\beta\to\begin{cases}\alpha|\beta(x_2'-x_2'')\\\gcd(\alpha,\beta)=1\end{cases}\to\alpha|x_2'-x_2''$

Since $|x_2'-x_2''|<\alpha$ we have a contradiction. Thus $|\Pi_\zeta|\le 1$. ☐

Definition 6.2.3. We define Φ_ζ to be the set $\Pi(B)\cap(\mathbb{Z}^2\times\{\zeta\})$.

The following lemma says that there is at most one lattice point in $\Phi(B)$ at any given height (z-value).

Lemma 6.2.3. $\Phi_\zeta=\{(x,y,\zeta)\in\mathbb{Z}^3|y=\frac{\zeta-x\alpha}{\beta},x\in\{-\beta+1,-\beta+2,\ldots,0\}\}$. *Moreover* $|\Phi_\zeta|\le 1$.

Proof. Let $(x,y,z)\in\Pi(B)\cap\mathbb{Z}^3$. Then there exist $k,l\in[0,1)$ such that $k(-\beta,\alpha,0)+l(0,1,\beta)=(x,y,z)\in\mathbb{Z}^3$. $\begin{cases}x=-k\beta\\y=l+k\alpha\\z=l\beta\end{cases}\to\begin{cases}x\in(-\beta,0]\cap\mathbb{Z}\\y=\frac{\zeta}{\beta}-k\alpha\\l=\frac{z}{\beta}\end{cases}\to\begin{cases}x\in\{-\beta+1,-\beta+2,\ldots,0\}\\y=\frac{\zeta}{\beta}-k\alpha\\l\in\{0,1,\ldots,\beta-1\}\end{cases}$

Fix $z=\zeta\in\{0,1,\ldots,\beta-1\}$. Assume $|\Phi_\zeta|>1$ and let $(x_1,y_1,\zeta),(x_2,y_2,\zeta)\in\Phi_\zeta$. Then $\begin{cases}\beta|\zeta-x_1\alpha\\\beta|\zeta-x_2\alpha\end{cases}\to\beta|x_1\alpha-x_2\alpha\to\begin{cases}\beta|\alpha(x_1-x_2)\\\gcd(\alpha,\beta)=1\end{cases}\to\beta|x_1-x_2$

Since $|x_1-x_2|<\beta$ we have a contradiction. Thus $|\Phi_\zeta|\le 1$.

☐

The first summand

Our goal is to show that $\sigma_A = \frac{P_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_1z_3^{\alpha})}$.

Proposition 6.2.4. $\sigma_{\Pi(A)} = P_{\alpha,\beta}$.

Proof. Given that for $(x,y,z) \in \Pi(A)$ we have $\alpha > z \in \mathbb{N}$, we need to prove the following three statements (since $\Pi_\zeta = \emptyset$ for $\zeta \geq \alpha$)

1. If $\zeta = 0$ then $\sigma_{\Pi_\zeta} = 1 = a_0$.
2. Let $\zeta \in \{1,2,\ldots,\alpha-1\}$ such that $\beta|\zeta$. Then $\sigma_{\Pi_\zeta} = z_2^{\frac{\lambda}{\beta}} z_3^{\zeta} = a_\zeta z_3^{\zeta}$.
3. Let $\zeta \in \{1,2,\ldots,\alpha-1\}$ such that $\beta \nmid \zeta$. Then $\sigma_{\Pi_\zeta} = a_\zeta z_3^{\zeta}$.

Proof of statement 1.

Using the equations from the proof of Lemma 6.2.2 we have

$$\begin{cases} x_1 = l - k\beta \\ x_2 = k\alpha \\ 0 = l\alpha \end{cases} \xrightarrow{l=0} \begin{cases} k\beta \in \mathbb{Z} \\ k\alpha \in \mathbb{Z} \end{cases} \xrightarrow{\exists n \in \mathbb{N}} \begin{cases} k\beta \in \mathbb{Z} \\ k = \frac{n}{\alpha} \end{cases} \rightarrow \begin{cases} \frac{n\beta}{\alpha} \in \mathbb{Z} \\ k = \frac{n}{\alpha} \end{cases} \rightarrow \begin{cases} \alpha|n \text{ or } \alpha|\beta \\ k = \frac{n}{\alpha} \end{cases}$$

$$\xrightarrow{\gcd(\alpha,\beta)=1} \begin{cases} \alpha|n \\ \frac{n}{\alpha} = k \in [0,1) \end{cases}$$

Thus $k = 0$, $x = y = \lambda = 0$ and $\sigma_{\Pi_0} = 1$.

By the definition of a_0 we have that $a_0 = 1$.

□ of statement 1.

Proof of statement 2.

From Lemma 6.2.2 we know that $|\Pi_\zeta| \leq 1$ and if equality holds the lattice point is of the form $(\frac{\zeta - y\beta}{\alpha}, y, \zeta)$ for some $y \in \{0,1,\ldots,\alpha-1\}$.

Let $x_2 = \frac{\zeta}{\beta}$. Since $\zeta < \alpha$ we have that $y \in \{0,1,\ldots,\alpha-1\}$. Moreover $x_1 = \frac{\zeta - x_2\beta}{\alpha} = \frac{\zeta - \frac{\lambda}{\beta}\beta}{\alpha} = 0 \in \mathbb{Z}$, which means that $(0, \frac{\zeta}{\beta}, \zeta) \in \Pi_\zeta$.

Then $\sigma_{\Pi_\zeta} = z_2^{\frac{\zeta}{\beta}} z_3^{\zeta}$, which by definition is $a_\zeta z_3^{\zeta}$.

□ of statement 2.

Proof of statement 3.

We will proceed in two steps. First show that $\mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta, \alpha)$ is the x_2-coordinate of a lattice point in Π_ζ and then that $\mathrm{rmd}((\alpha^{-1} \mod \beta)\zeta, \beta) - \beta$ is the x_1-coordinate of a lattice point in Π_ζ. Since $|\Pi_\zeta| \leq 1$, we have that $\sigma_{\Pi_\zeta} = a_\zeta z_3^{\zeta}$.

- In order to prove that $\mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta, \alpha)$ is the x_2-coordinate of a lattice point in Π_ζ we have to show that

(a) $\mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta, \alpha) \in \{0, 1, \dots, \alpha - 1\}$

(b) $\frac{\zeta - \left(\mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta,\alpha)\right)\beta}{\alpha} \in \mathbb{Z}$

Let $y = \mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta, \alpha)$. By the definition of division by α, the remainder x_2 is in $\{0, 1, \dots, \alpha - 1\}$.

By the definitions of remainder and modular inverse we have

$x_2 = r\zeta - \alpha m$ for some $m \in \mathbb{Z}$ and r such that $r\beta = \alpha n + 1$ for some $n \in \mathbb{Z}$.

Then $x_2 = r\zeta - \alpha m \Leftrightarrow \beta x_2 = \beta r\zeta - \alpha\beta m \Leftrightarrow \beta x_2 = (\alpha n + 1)\zeta - \alpha\beta m \Leftrightarrow \beta x_2 = \alpha n\zeta + \zeta - \alpha\beta m \Leftrightarrow \zeta - \beta x_2 = \alpha(\beta m - n\zeta) \Leftrightarrow \frac{\zeta - \beta x_2}{\alpha} = \beta m - n\zeta \in \mathbb{Z}$

- In order to prove that $\mathrm{rmd}((\alpha^{-1} \mod \beta)\zeta, \beta) - \beta$ is the x_1-coordinate of a lattice point in Π_ζ we have to show that there exist $x_2 \in \{0, 1, \dots, \alpha - 1\}$ such that $\mathrm{rmd}((\alpha^{-1} \mod \beta)\zeta, \beta) - \beta = \frac{\zeta - x_2\beta}{\alpha}$.

  By definition $\rho = r\zeta - \beta m$ for some $m \in \mathbb{Z}$ and r such that $\alpha r = \beta n + 1$ for some $n \in \mathbb{Z}$. Then we want to prove that $\rho - \beta = \frac{\zeta - x_2\beta}{\alpha}$ which means

  $r\zeta - \beta m - \beta = \frac{\zeta - x_2\beta}{\alpha}$. We have

  $r\zeta - \beta m - \beta = \frac{\zeta - x_2\beta}{\alpha} \Leftrightarrow \alpha r\zeta - \alpha\beta m - \alpha\beta = \zeta - x_2\beta \Leftrightarrow \beta n\zeta + \zeta - \alpha\beta m - \alpha\beta = \zeta - x_2\beta \Leftrightarrow \beta n\zeta + \zeta - \alpha\beta m - \alpha\beta = \zeta - x_2\beta \Leftrightarrow x_2 = \alpha(m + 1) - n\zeta$.

  (a) $x_2 \in \mathbb{Z}$

  (b) By the definition of division $m + 1 > \frac{r\zeta}{\beta} \Rightarrow m > \frac{r\zeta}{\beta} - 1 \Rightarrow m > \frac{\left(\frac{\beta n+1}{\alpha}\right)\zeta}{\beta} - 1 \Rightarrow m > \frac{\beta n\zeta + \zeta}{\alpha\beta} - 1 \Rightarrow m > \frac{\beta n\zeta}{\alpha\beta} - 1 \Rightarrow m > \frac{n\zeta}{\alpha} - 1 \Rightarrow \alpha(m + 1) > n\zeta \Rightarrow \alpha(m + 1) - n\zeta > 0$

  (c) Since $\beta \nmid \zeta$ we have $0 \neq \rho = r\zeta - m\beta$. Moreover $\zeta < \alpha$. Thus $\zeta < \alpha\rho \Rightarrow \frac{\zeta}{\alpha} < \rho \Rightarrow 0 < \rho - \frac{\zeta}{\alpha} \Rightarrow m\beta < m\beta + \rho - \frac{\zeta}{\alpha} \Rightarrow m\beta < r\zeta - \frac{\zeta}{\alpha} \Rightarrow m\beta < \frac{(n\beta+1)\zeta}{\alpha} - \frac{\zeta}{\alpha} \Rightarrow m\beta < \frac{n\beta\zeta}{\alpha} \Rightarrow m < \frac{n\zeta}{\alpha} \Rightarrow \alpha m < n\zeta \Rightarrow \alpha m + \alpha < n\zeta + \alpha \Rightarrow \alpha(m + 1) - n\zeta < \alpha$

$\square$ of statement 3.

$\square$

Corollary 6.2.5. *From Proposition 6.2.4 and Lemma* **??** *we have that* $\sigma_A = \frac{P_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_1z_3^{\alpha})}$.

The second summand

Our goal is to show that $\sigma_B = \frac{Q_{\alpha,\beta}+1-z_1^{-\beta}z_2^{\alpha}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_1z_3^{\alpha})}$.

Proposition 6.2.6. $\sigma_{\Pi(B)} = Q_{\alpha,\beta} + 1 - z_1^{-\beta}z_2^{\alpha}$.

Proof. Given that for $(x, y, z) \in \Pi(A)$ we have $\alpha > z \in \mathbb{N}$, w We need to prove the following two statements (since $\Phi_\zeta = \emptyset$ for $\zeta \geq \beta$)

1. $\sigma_{\Phi_0} = 1$ and $b_0 = z_1^{-\beta}z_2^{\alpha}$.

2. If $\zeta \in \{1, 2, \dots, \beta - 1\}$, then $\sigma_{\Phi_\zeta} = a_\zeta z_3^\zeta$.

Proof of statement 1.

The proof is analogous to that of Proposition 6.2.4

$$\begin{cases} x_1 = -k\beta \\ x_2 = l + k\alpha \\ 0 = l\beta \end{cases} \xrightarrow{l=0} \begin{cases} k\beta \in \mathbb{Z} \\ k\alpha \in \mathbb{Z} \end{cases} \xrightarrow{\exists n \in \mathbb{N}} \begin{cases} k\beta \in \mathbb{Z} \\ k = \frac{n}{\alpha} \end{cases} \rightarrow \begin{cases} \frac{n\beta}{\alpha} \in \mathbb{Z} \\ k = \frac{n}{\alpha} \end{cases} \rightarrow \begin{cases} \alpha | n \text{ or } \alpha | \beta \\ k = \frac{n}{\alpha} \end{cases}$$

$$\xrightarrow{\gcd(\alpha,\beta)=1} \begin{cases} \alpha | n \\ \frac{n}{\alpha} = k \in [0, 1) \end{cases}$$

Thus $k = 0$, $x_1 = x_2 = \lambda = 0$ and $\sigma_{\Phi_0} = 1$.

By the definition of b_0 we have that $b_0 = z_1^{-\beta} z_2^\alpha$.

□ of statement 1.

Proof of statement 2.

We need to show that $\Pi(A) = \Phi(B)$ for $\zeta \in \{1, 2, \dots, \beta - 1\}$.

From the analysis in the proof of Proposition 6.2.4, we know that $(\mathrm{rmd}((\alpha^{-1} \mod \beta)\zeta, \beta) - \beta, \mathrm{rmd}((\beta^{-1} \mod \alpha)\zeta, \alpha), \zeta)$ is in Π_ζ for $\zeta \in \{0, 1, \dots, \beta - 1\} \subset \{0, 1, \dots, \alpha - 1\}$.

The proof follows from the fact that $x_1 = \frac{\zeta - x_2\beta}{\alpha} \Leftrightarrow x_2 = \frac{\zeta - x_1\alpha}{\beta}$.

□ of statement 2.

□

Note. The statement $\sigma_{\Pi(B)} = Q_{\alpha,\beta} + 1 - z_1^{-\beta} z_2^\alpha$ means that $\frac{Q_{\alpha,\beta}}{(1 - z_1^{-\beta} z_2^\alpha)(1 - z_2 z_3^\beta)}$ is the generating function of the cone B, ignoring the lattice points with x-coordinate equal to 0.

For this we observe that there are no lattice points on the ray generated by $(-\beta, \alpha, 0)$. Thus the cone B is half-open.

Proof. of Theorem 6.2.1

The proof follows from Proposition 6.2.4, Proposition 6.2.6, Note 6.2 and considering the signs in the two summands of Equation 6.3.

□

Note. One can see the full signed decomposition in the generating function level as follows:

$\sigma_C = \sigma_A - \sigma_B + \sigma_{\mathrm{co}((0,1,\beta))}$

According to the previous analysis $\sigma_A = \frac{P_{\alpha,\beta}}{(1 - z_1^{-\beta} z_2^\alpha)(1 - z_1 z_3^\alpha)}$

Since $\sigma_{\mathrm{co}((0,1,\beta))} = \frac{1}{(1-z_2 z_3^{\beta})}$ we have $-\sigma_B + \sigma_{\mathrm{co}((0,1,\beta))} = -\frac{Q_{\alpha,\beta}+1-z_1^{-\beta}z_2^{\alpha}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_2 z_3^{\beta})} + \frac{1}{(1-z_2 z_3^{\beta}} = -\frac{Q_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_2 z_3^{\beta})}$ which gives

$$\frac{1}{(1-z_1 z_3^{\alpha})(1-z_2 z_3^{\beta})} = \frac{P_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_1 z_3^{\alpha})} - \frac{Q_{\alpha,\beta}}{(1-z_1^{-\beta}z_2^{\alpha})(1-z_2 z_3^{\beta})} \tag{6.4}$$

In other words, $Q_{\alpha,\beta}$ encodes the inclusion-exclusion step for the cone $\mathrm{co}((0,1,\beta))$.

Chapter 7

Further Directions

During my visit at San Francisco State University, supported by the Austrian Marshall Plan Foundation, the following directions of research were explored:

- Algorithmic improvements by use of Brion's theorem and explicit geometric computations.
- Extensions of Partition Analysis for the simultaneous elimination of multiple λ's through the use of geometric arguments.
- Geometry based investigation of questions concerning Lecture Hall Partitions.
- Exploiting the structure of Hilbert basis for particular families of cones arising in the context of Lecture Hall Partitions.
- Connections of the APR decomposition with Dedekind-Carlitz polynomials

7.1 New Algorithms for Partition Analysis

Two new algorithms are available for partition analysis. One performs elimination of a single λ, which is suitable for recursive application for the efficient algorithmic solution of Linear Diophantine Systems. The algorithm follows traditional ideas employing though tools from polyhedral geometry.

The second algorithm performs simultaneous elimination of multiple λ's. It is still under development but first indications show that it is efficient. We note that it is the first algorithm in literature for the computation of the Ω operator applying multiple elimination.

7.2 Lecture Hall Partitions

In 1997, Bousquet-Mélou and Eriksson [5] initiated the study of lecture hall partitions, a fascinating family of partitions that yield a finite version of Euler's celebrated odd/distinct partition theorem. In subsequent work on $\mathbf{s}$-lecture hall partitions, they considered the self-reciprocal property for various associated generating functions, with the goal of characterizing those sequences $\mathbf{s}$ which give rise to generating functions of the form $((1-q^{e_1})(1-q^{e_2})\cdots(1-q^{e_n}))^{-1}$.

We continue this line of investigation, connecting their work to the more general context of Gorenstein cones. We focus on the Gorenstein condition for $\mathbf{s}$-lecture hall cones when $\mathbf{s}$ is a positive integer sequence generated by a second order homogeneous linear recurrence with initial values 0 and 1. Among such sequences $\mathbf{s}$, we prove that the n-dimensional $\mathbf{s}$-lecture hall cone is Gorenstein for all $n \geq 1$ if and only if $\mathbf{s}$ is an ℓ-sequence. One consequence is that among such sequences $\mathbf{s}$, unless $\mathbf{s}$ is an ℓ-sequence, the generating function for the $\mathbf{s}$-lecture hall partitions can have the form $((1-q^{e_1})(1-q^{e_2})\cdots(1-q_n^e))^{-1}$ for at most finitely many n.

We also establish several conjectures by Pensyl and Savage regarding the symmetry of h^*-vectors for $\mathbf{s}$-lecture hall polytopes.

7.3 Partial Fraction Decompositions and Geometry

The geometric interpretation of different types of partial fraction decompositions is a recurring question. On the other hand, partial fraction decomposition having specific properties induced by their geometry were also a goal. In particular the partial fraction decomposition method appearing in [3] along with the ones presented earlier in that report, were investigated.

A different line of research was that of constructing decompositions suitable for the $\Omega_{\geq}$ operator, while preserving structure, i.e. symmetry.

Bibliography

[1] G. Andrews, P. Paule, and A. Riese. MacMahon's Partition Analysis III: The Omega Package. *European J. Combin.*, 22:887–904, 2001.

[2] G. Andrews, P. Paule, and A. Riese. MacMahon's Partition Analysis VI: A New Reduction Algorithm. *Ann. Comb.*, 5:251–270, 2001.

[3] M. Beck. The partial-fractions method for counting solutions to integral linear systems. *Discrete and Computational Geometry*, 32:437–446, 2004. 10.1007/s00454-004-1131-5.

[4] M. Beck and S. Robins. *Computing the continuous discretely. Transl. from the English by Kord Eickmeyer. (Das Kontinuum diskret berechnen.)*. Springer-Lehrbuch. Berlin: Springer. xx, 242 p., 2008.

[5] M. Bousquet-Mélou and K. Eriksson. Lecture hall partitions. *Ramanujan J.*, 1(1):101–111, 1997.

[6] E. B. Elliott. On linear homogeneous diophantine equations. *Q J Pure Appl Math*, 136:348–377, 1903.

[7] M. Kauers and P. Paule. *The Concrete Tetrahedron.* Text and Monographs in Symbolic Computation. Springer Wien, 1st edition, 2011.

[8] P. A. MacMahon. *Combinatory Analysis.* Cambridge University Press, 1915.

[9] E. Miller and B. Sturmfels. *Combinatorial Commutative Algebra.* Graduate Texts in Mathematics. Springer, 2004.