CHAPTER 1

Introduction

The two main objects of these notes are the *standard integer lattice* $\mathbb{Z}^d \subset \mathbb{R}^d$ consisting of points with integer coordinates and a *polyhedron* $P \subset \mathbb{R}^d$ consisting of points satisfying a finite set of linear inequalities. The unifying topic is how to count integer points in a *polytope* (bounded polyhedron). For example, we conclude by inspection that the polygon P in Figure 1 contains seven integer points, or, in other words, that $|P \cap \mathbb{Z}^2| = 7$.

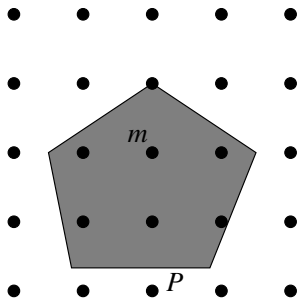

FIGURE 1. The integer lattice $\mathbb{Z}^2 \subset \mathbb{R}^2$, a polygon $P \subset \mathbb{R}^2$, and an integer point $m \in P$.

As the dimensions of our polytopes grow and their analytic descriptions become more complicated, "by inspection" no longer works and we need a theory. The first step towards such a theory is to realize that the number of $|P \cap \mathbb{Z}^d|$ of integer points in a d-dimensional polytope $P \subset \mathbb{R}^d$ is a *valuation*, that is

$$|P \cap \mathbb{Z}^d| = |P_1 \cap \mathbb{Z}^d| + |P_2 \cap \mathbb{Z}^d| - |Q \cap \mathbb{Z}^d| \quad \text{provided}$$
$$P = P_1 \cup P_2 \quad \text{and} \quad Q = P_1 \cap P_2.$$

This observation allows us to cut a given polytope into simpler pieces, enumerate integer points in those pieces and then obtain the total number of points by carefully accounting for various overlapping parts. This is indeed very useful, but not good enough: it turns out that for many polytopes there is no way to dissect them into a reasonably few simple pieces. We need more freedom in "cutting and pasting" of polyhedra.

What we need, is to be able to extend the valuation property further to *unbounded polyhedra*, since it turns out that only unbounded polyhedra (namely *cones*) are simple enough to deal with, as far as the integer point enumeration is concerned. This requires us to somehow make sense of the number of integer points in an unbounded polyhedron. Fortunately, a way of counting for infinite sets has long been known under the name of *generating functions*.

With an integer point $m = (\mu_1, \ldots, \mu_d)$ in $\mathbb{R}^d$ we associate a monomial $\mathbf{x}^m = x_1^{\mu_1} \cdots x_d^{\mu_d}$ in d variables $x_1, \ldots, x_d$. We consider the sum

$$\sum_{m \in P \cap \mathbb{Z}^d} \mathbf{x}^m, \tag{1.1}$$

where P is a polyhedron and $\mathbb{Z}^d \subset \mathbb{R}^d$ is the standard integer lattice. We will show that for *rational polyhedra* P (that is, polyhedra defined by linear inequalities with integer coefficients) if the series (1.1) converges for some $\mathbf{x}$, it converges to a *rational function* $f(P, \mathbf{x})$. Moreover, we will be able to define a rational function $f(P, \mathbf{x})$ even if the series (1.1) does not converge for any $\mathbf{x}$. If P is bounded, we obtain the number $|P \cap \mathbb{Z}^d|$ of integer points in P by computing the value of $f(P, \mathbf{x})$ at $x_1 = \cdots = x_d = 1$.

Let us see how this theory plays out in the familiar though admittedly not very exciting case of $d = 1$.

Suppose that $P_+ = [0, +\infty)$ is the positive ray. With every non-negative integer m we associate a monomial x^m and consider the sum over non-negative integer m, see Figure 2.

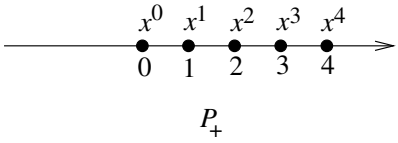

FIGURE 2. Points on the positive ray P_+.

The corresponding generating function is given by the formula for the infinite geometric series:

$$\sum_{m=0}^{+\infty} x^m = \frac{1}{1-x} \quad \text{provided} \quad |x| < 1,$$

so we say that

$$f(P_+, x) = \frac{1}{1-x}.$$

Similarly, for the negative ray $P_- = (-\infty, 0]$, we get

$$\sum_{m=-\infty}^{0} x^m = \frac{1}{1-x^{-1}} \quad \text{provided} \quad |x| > 1,$$

see Figure 3, so we say that

$$f(P_-, x) = \frac{1}{1-x^{-1}}.$$

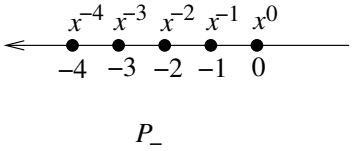

FIGURE 3. Points on the negative ray P_-.

Let us consider integer points on the line $\mathbb{R}^1$, see Figure 4. Although the series

$$\sum_{m=-\infty}^{+\infty} x^m$$

does not converge for any x, we are able to find the rational function $f(\mathbb{R}^1, x)$ using the valuation property. Indeed, we have

$$\mathbb{R}^1 = P_+ \cup P_- \quad \text{and} \quad P_+ \cap P_- = \{0\}.$$

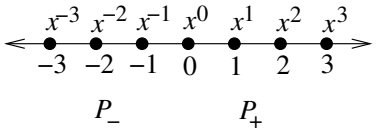

FIGURE 4. Points on the line $\mathbb{R}^1$.

Hence we must have

$$\begin{aligned} f(\mathbb{R}^1, x) = f(P_+, x) + f(P_-, x) - x^0 &= \frac{1}{1-x} + \frac{1}{1-x^{-1}} - 1 \\ &= \frac{1}{1-x} - \frac{x}{1-x} - 1 = 0. \end{aligned}$$

Now, let us do some counting. For some integers $k < n$ let us consider the interval $P = [k, n]$, $P \subset \mathbb{R}^1$, which is a bona fide one-

dimensional polytope. We do some cutting and pasting to represent the interval as a combination of unbounded polyhedra, see Figure 5. In terms of formal power series we have

$$\sum_{m=k}^{n} x^m = \sum_{m=k}^{+\infty} x^k + \sum_{m=-\infty}^{n} x^m - \sum_{m=-\infty}^{+\infty} x^m.$$

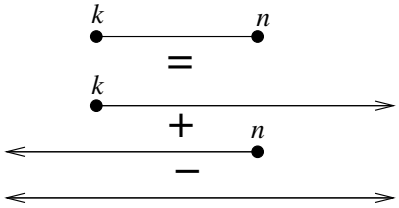

FIGURE 5. Representing the interval as a sum of two rays minus a line.

The valuation property tells us that we must have

$$f(P, x) = f(k + P_+,\ x) + f(n + P_-,\ x) - f(\mathbb{R}^1,\ x),$$

where $k + P_+$ and $n + P_-$ are the respective translations of the positive ray P_+ by k and of the negative ray P_- by n. It is not hard to convince ourselves that we must have

$$f(k + P_+,\ x) = x^k f(P_+, x) = \frac{x^k}{1 - x} \quad \text{and} \quad f(n + P_-,\ x) = x^n f(P_-, x) = \frac{x^n}{1 - x^{-1}}.$$

Together with the identity $f(\mathbb{R}^1, x) = 0$ this gives us the familiar formula for the sum of a finite geometric series:

$$\sum_{m=k}^{n} x^m = f(P, x) = \frac{x^k}{1 - x} + \frac{x^n}{1 - x^{-1}} - 0 = \frac{x^k - x^{n+1}}{1 - x}. \tag{1.2}$$

Finally, to compute the number $|P \cap \mathbb{Z}|$ of integer points on the interval, we substitute $x = 1$ in the expression for $f(P, x)$. After a moment of hesitation, we apply l'Hospital's rule and conclude that $|P \cap \mathbb{Z}| = n - k + 1$, which we knew all along.

This one-dimensional exercise shows in a nutshell some important features of the general theory. First, higher-dimensional analogues of the strange identity

$$f(\mathbb{R}^1, x) = \sum_{m=-\infty}^{+\infty} x^m = 0 \tag{1.3}$$

turn out to be indispensable in dealing with unbounded polyhedra in $\mathbb{R}^d$. Second, the representation of Figure 5 turns out to be one degenerate case of a rich family of identities for higher-dimensional polyhedra. Finally, substituting $\mathbf{x} = (1, \dots, 1)$ in $f(P, \mathbf{x})$ in higher dimensions also requires an appropriate version of l'Hospital's rule, though the answer, in general, is far from obvious. There are, of course, important phenomena in higher dimensions that cannot be observed in dimension 1.

Formula (1.2) writes a potentially long (for $n-k$ large) polynomial in x as a short rational function in x. We will see that for a general polyhedron P the sum (1.1) can be written as a short rational function, with the term "short" defined appropriately. Let us consider a 2-dimensional example: a triangle Δ in the plane with the vertices at $A = (0, 0)$, $B = (0, 100)$ and $C = (100, 0)$. One can show that

$$\sum_{m \in \Delta \cap \mathbb{Z}^2} \mathbf{x}^m = \frac{1}{(1-x_1)(1-x_2)} + \frac{x_2^{100}}{(1-x_2^{-1})(1-x_1x_2^{-1})} + \frac{x_1^{100}}{(1-x_1^{-1})(1-x_1^{-1}x_2)}$$

and this formula will be seen as belonging to the same family of formulas as formula (1.2). Incidentally, the three terms of the right-hand side are the sums over the angles of the triangle, see Figure 6.

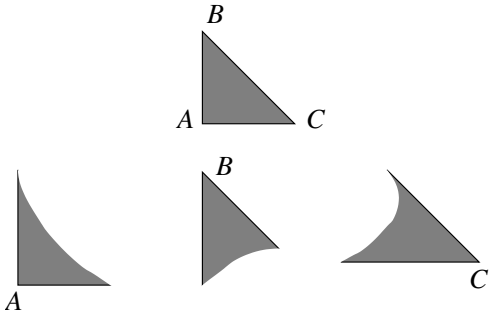

FIGURE 6. A triangle and its angles.

Exercises below describe some interesting examples of short rational functions encoding long series.

Problems

1. Let a and b be coprime positive integers and let

$$S = \Big\{ m_1 a + m_2 b : \quad m_1, m_2 \in \mathbb{Z}_+ \Big\}$$

be the set (semigroup) of all linear combinations of a and b with non-negative integer coefficients m_1 and m_2. Prove that

$$\sum_{m \in S} x^m = \frac{1 - x^{ab}}{(1 - x^a)\,(1 - x^b)} \quad \text{for} \quad |x| < 1.$$

2*. Let a, b, and c be coprime positive integers and let

$$S = \Big\{ m_1 a + m_2 b + m_3 c : \quad m_1, m_2, m_3 \in \mathbb{Z}_+ \Big\}$$

be the set of all linear combinations of a, b, and c with non-negative integer coefficients m_1, m_2, and m_3. Prove that there exist integers p_1, p_2, p_3, p_4 and p_5, not necessarily distinct, such that

$$\sum_{m \in S} x^m = \frac{1 - x^{p_1} - x^{p_2} - x^{p_3} + x^{p_4} + x^{p_5}}{(1 - x^a)\,(1 - x^b)\,(1 - x^c)} \quad \text{for} \quad |x| < 1.$$

Hint: See [**De03**].

3. Let a, b, c, and d be coprime positive integers and let

$$S = \Big\{ m_1 a + m_2 b + m_3 c + m_4 d : \quad m_1, m_2, m_3, m_4 \in \mathbb{Z}_+ \Big\}$$

be the set of all linear combinations of a, b, c, and d with non-negative integer coefficients m_1, m_2, m_3, and m_4.

a) Prove that

$$\sum_{m \in S} x^m = \frac{p(x)}{(1 - x^a)\,(1 - x^b)\,(1 - x^c)\,(1 - x^d)}$$

for some polynomial p and all $|x| < 1$.

b*) Prove that the number of monomials in the polynomial p above can be arbitrarily large, depending on a, b, c, and d.

Hint: See [**SW86**].

Problem 3 shows that the pattern of Problems 1 and 2 breaks down for semigroups with four or more generators. Nevertheless, the more general phenomenon that the series has a "short rational generating function representation" still holds, see [**BW03**].