Counting with rational generating functions

Sven Verdoolaege and Kevin Woods

May 10, 2007

Abstract

We examine two different ways of encoding a counting function, as a rational generating function and explicitly as a function (defined piecewise using the greatest integer function). We prove that, if the degree and number of input variables of the (quasi-polynomial) function are fixed, there is a polynomial time algorithm which converts between the two representations. Examples of such counting functions include Ehrhart quasi-polynomials, vector partition functions, integer points in parametric polytopes, and projections of the integer points in parametric polytopes. For this last example, this algorithm provides the first known way to compute the explicit function in polynomial time. We rely heavily on results of Barvinok, and also of Verdoolaege, Seghir, Beyls, et al.

1 Introduction

We are interested in a wide variety of functions of the form

$$c : \mathbb{Z}^n \to \mathbb{Q}.$$

Most examples, including Ehrhart quasi-polynomials and vector partition functions, will count some combinatorial object. The function $c(\mathbf{s})$ can be encoded in at least two different ways: either as an explicit function or as a generating function

$$f(\mathbf{x}) = \sum_{\mathbf{s}=(s_1,\ldots,s_n)\in\mathbb{Z}^n} c(\mathbf{s}) x_1^{s_1} \cdots x_n^{s_n} = \sum_{\mathbf{s}\in\mathbb{Z}^n} c(\mathbf{s})\mathbf{x}^{\mathbf{s}}.$$

Example 1.1. Consider the generating function

$$f(x) = \frac{1}{1-x^2} = 1 + x^2 + x^4 + \cdots = \sum_{s \in \mathbb{Z}} c(s) x^s.$$

The corresponding function can be represented explicitly as

$$c(s) = \begin{cases} 0, & \text{if } s < 0 \\ 0, & \text{if } s \geq 0 \text{ and } s \text{ odd} \\ 1, & \text{if } s \geq 0 \text{ and } s \text{ even.} \end{cases}$$

□

Mathematicians often encode a function as a rational generating function, such as $f(x) = \frac{1}{1-x^2}$ in Example 1.1, which is a compact representation of a (possibly infinite) Laurent power series $\sum_{\mathbf{s} \in \mathbb{Z}^n} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}}$, where $c(\mathbf{s}) \in \mathbb{Z}^n$. This has the advantage that we may apply many computational tools to manipulate our rational generating function and obtain information from it (see, for example, [BW03]). An explicit function representation for $c(\mathbf{s})$, on the other hand, has the advantage of being easily evaluated for a particular value of $\mathbf{s}$. Such a representation is therefore preferred in the compiler community (see, for example, [VSB+07]).

We will show that these ways of representing a function are "the same," in the sense that one can convert between the rational function and explicit function representations in polynomial time (if the degree and number of variables of the function is fixed). Let us be more precise about the specific representations we will use for generating functions and explicit functions.

Definition 1.2. By a *rational generating function* $f(\mathbf{x})$, we will mean a function given to us in the form

$$f(\mathbf{x}) = \sum_{i \in I} \alpha_i \frac{\mathbf{x}^{\mathbf{p}_i}}{(1 - \mathbf{x}^{\mathbf{b}_{i1}})(1 - \mathbf{x}^{\mathbf{b}_{i2}}) \cdots (1 - \mathbf{x}^{\mathbf{b}_{ik_i}})}, \tag{1.3}$$

where $\mathbf{x} \in \mathbb{C}^n$, I is a finite set, $\alpha_i \in \mathbb{Q}$, $\mathbf{p}_i \in \mathbb{Z}^n$, and $\mathbf{b}_{ij} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$.

Definition 1.4. A *step-polynomial* $g : \mathbb{Z}^n \to \mathbb{Q}$ is a function written in the form

$$g(\mathbf{s}) = \sum_{j=1}^{m} \alpha_j \prod_{k=1}^{d_j} \lfloor \langle \mathbf{a}_{jk}, \mathbf{s} \rangle + b_{jk} \rfloor,$$

where $\alpha_j \in \mathbb{Q}$, $\mathbf{a}_{jk} \in \mathbb{Q}^n$, $b_{jk} \in \mathbb{Q}$, $\langle \cdot, \cdot \rangle$ is the standard inner product, and $\lfloor \cdot \rfloor$ is the greatest integer function. We say that the *degree* of $g(\mathbf{s})$ is $\max_j \{ d_j \}$.

A *piecewise step-polynomial* $c : \mathbb{Z}^n \to \mathbb{Q}$ is a collection of polyhedra Q_i (which may not all be full dimensional) together with corresponding functions $g_i : Q_i \cap \mathbb{Z}^n \to \mathbb{Q}$ such that

1. the $\text{int}(Q_i)$ partition $\mathbb{Q}^n$ (where $\text{int}(Q)$ is the relative interior of Q in the affine space it lies in)
2. $c(\mathbf{s}) = g_i(\mathbf{s})$, for $\mathbf{s} \in \text{int}(Q_i) \cap \mathbb{Z}^n$, and
3. each g_i is a step-polynomial.

We say that the degree of $c(\mathbf{s})$ is $\max_i \deg g_i$. Working with the relative interiors of the polyhedra allows us not to worry about the value of the function at the intersection of two polyhedra.

For example, the explicit function $c(s)$ in Example 1.1 can be written as the piecewise step-polynomial

$$c(s) = \begin{cases} 1 + \left\lfloor \frac{s}{2} \right\rfloor - \left\lfloor \frac{s+1}{2} \right\rfloor, & \text{if } s > 0 \\ 1, & \text{if s=0} \\ 0, & \text{if } s < 0. \end{cases}$$

We must be careful when speaking of a correspondence between a rational generating function and a piecewise step-polynomial, because a generating function may have different Laurent power series expansions which converge on different regions of $\mathbb{C}^n$. For example, if $f(x) = \frac{1}{1-x}$ then

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

are Laurent power series expansions convergent for $\|x\| < 1$ and $\|x\| > 1$, respectively.

We state the main theorem, and then provide several examples of rational generating functions and piecewise step-polynomials.

Theorem 1.5. *Fix n and k. There is a polynomial time algorithm which, given a rational generating function $f(\mathbf{x})$ in the form (1.3) with n variables and each $k_i \leq k$ and given $\mathbf{l} \in \mathbb{Z}^n$ such that $\langle \mathbf{l}, \mathbf{b}_{ij} \rangle \neq 0$ for all i and j,*

computes the piecewise step-polynomial $c : \mathbb{Z}^n \to \mathbb{Q}$ *with degree at most* k *such that*

$$f(\mathbf{x}) = \sum_{\mathbf{s} \in \mathbb{Z}^n} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}}$$

is the Laurent power series expansion of $f(\mathbf{x})$ *convergent on a neighborhood of* $\mathbf{e}^{\mathbf{l}} = (e^{l_1}, e^{l_2}, \ldots, e^{l_n})$*, with* e *the base of the natural logarithmic function.*

Conversely, there is a polynomial time algorithm which, given a piecewise step-polynomial $c : \mathbb{Z}^n \to \mathbb{Q}$ *of degree at most* k *such that* $f(\mathbf{x}) = \sum_{\mathbf{s} \in \mathbb{Z}^n} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}}$ *converges on some nonempty open subset of* $\mathbb{C}^n$*, computes the rational generating function* $f(\mathbf{x})$ *in the form (1.3) with* $k_i \leq k$*.*

The proof of the first half of this theorem will use several ideas from [BP99]. Section 3 will be devoted to the proof of the theorem, after we lay the groundwork in Section 2. Note that applying the theorem twice (in one direction and then the other) will in general not result in the exact same representation of the rational generating function or piecewise step-polynomial. We are unaware of any canonical form for either rational generating functions or piecewise step-polynomials that can be computed in polynomial time.

As there may be many functions with the same generating function representation (convergent on different neighborhoods), we need to find an appropriate $\mathbf{l}$ value when we want to convert a given rational generating function to an explicit representation. If we know that the function $c(\mathbf{s})$ is only nonzero for $\mathbf{s}$ in some polyhedron Q such that Q does not contain any straight lines, then we may take any $\mathbf{l}$ such that $\langle \mathbf{l}, \mathbf{b}_{ij} \rangle \neq 0$ for all i, j and such that

$$Q \cap \{ \mathbf{x} \in \mathbb{Q}^n \mid \langle \mathbf{l}, \mathbf{x} \rangle \geq 0 \}$$

is bounded. Such an $\mathbf{l}$ will give us the desired Laurent power series expansion $\sum_{\mathbf{s}} c(\mathbf{s})\, \mathbf{x}^{\mathbf{s}}$. In Example 1.1, we could take $l = -1$.

Example 1.6. Let $P \subset \mathbb{Q}^d$ be a rational polytope, and let

$$c_P(s) = \#(sP \cap \mathbb{Z}^d),$$

where sP is P dilated by a factor of s.

Then Ehrhart proved [Ehr62] that $c_P(s)$ is a quasi-polynomial, that is, there is a $\mathcal{D} \in \mathbb{Z}_+$ and polynomial functions $g_0(s), g_1(s), \ldots, g_{\mathcal{D}-1}(s)$ such that

$$c_P(s) = g_j(s) \text{ for } s \equiv j \,(\text{mod } \mathcal{D}).$$

The generating function $\sum_{s=0}^{\infty} c_P(s)x^s$ can be computed in polynomial time, and this has been implemented in LattE (see [DLHTY04]). Computing some explicit function representation of $c_P(s)$ in worst-case exponential time has been implemented in [CL98] and computing $c_P(s)$ as a piecewise step-polynomial in polynomial time had been implemented in [VSB+07].

Example 1.7. In particular, let $P \subset \mathbb{Q}^2$ be $\left[0, \frac{1}{2}\right] \times \left[0, \frac{1}{2}\right]$.

Then

$$c_P(s) = \left\lfloor \frac{1}{2}s + 1 \right\rfloor^2, \text{ for } s \geq 0,$$

and we have that

$$\sum_{s=0}^{\infty} c_P(s)x^s = \frac{2}{(1-x)(1-x^2)^2} - \frac{1}{(1-x)(1-x^2)},$$

which can be verified by hand. □

Example 1.8. Given $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d \in \mathbb{N}^n$, let $c : \mathbb{Z}^n \to \mathbb{Z}$ be the *vector partition function*, defined by

$$c(\mathbf{s}) = \#\left\{ \boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_d) \in \mathbb{N}^d \mid \mathbf{s} = \lambda_1\mathbf{a}_1 + \lambda_2\mathbf{a}_2 + \cdots + \lambda_d\mathbf{a}_d \right\},$$

i.e., the number of ways an integer vector $\mathbf{s}$ can be written as a nonnegative combination of the $\mathbf{a}_i$.

Then the generating function representation of $c(\mathbf{s})$ is very simple:

$$f(\mathbf{x}) = \frac{1}{(1-\mathbf{x}^{\mathbf{a}_1})(1-\mathbf{x}^{\mathbf{a}_2})\cdots(1-\mathbf{x}^{\mathbf{a}_d})}.$$

The piecewise step-polynomial representation of $c(\mathbf{s})$ can also be computed in polynomial time (see Corollary 3.1 or [VSB+07]). Beck [Bec04] describes a general technique for computing vector partition functions, based on partial fraction expansions of $f(\mathbf{x})$. He does not provide a complexity analysis, but standard techniques for computing partial fractions [Hen74] are exponential, even for fixed dimensions.

Example 1.9. In particular, consider the number of ways to partition an integer s into 2's and 5's, i.e., $a_1 = 2$ and $a_2 = 5$. Then the generating function representation is

$$f(x) = \frac{1}{(1-x^2)(1-x^5)},$$

and

$$c(s) = \begin{cases} 0, & \text{if } s < 0 \\ \left\lfloor \frac{1}{2}s + 1 \right\rfloor + \left\lfloor -\frac{2}{5}s \right\rfloor, & \text{if } s \geq 0, \end{cases}$$

which, again, can be verified by hand. □

Both Ehrhart quasi-polynomials and vector partition functions are special cases of counting integer points in *parametric polytopes*. In general, we let $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$ be a rational polyhedron such that, for all $\mathbf{s} \in \mathbb{Q}^n$, the set $P_\mathbf{s} = \{\mathbf{t} \in \mathbb{Q}^d \mid (\mathbf{s}, \mathbf{t}) \in P\}$ is bounded, and we define the function $c : \mathbb{Z}^n \to \mathbb{Z}$ by

$$c(\mathbf{s}) = \#(P_\mathbf{s} \cap \mathbb{Z}^d) = \#\left\{\mathbf{t} \in \mathbb{Z}^d \mid (\mathbf{s}, \mathbf{t}) \in P\right\}. \tag{1.10}$$

We call P a parametric polytope, because, if $P = \left\{(\mathbf{s}, \mathbf{t}) \in \mathbb{Q}^n \times \mathbb{Q}^d \mid A\mathbf{s} + B\mathbf{t} \leq \mathbf{c}\right\}$ for some matrices $A \in \mathbb{Z}^{m \times n}$, $B \in \mathbb{Z}^{m \times d}$ and vector $\mathbf{c} \in \mathbb{Z}^m$, then

$$P_\mathbf{s} = \left\{\mathbf{t} \in \mathbb{Q}^d \mid B\mathbf{t} \leq \mathbf{c} - A\mathbf{s}\right\},$$

so as $\mathbf{s}$ varies, the polytope $P_\mathbf{s}$ varies by changing the right hand sides of its defining inequalities.

Both a piecewise step-polynomial representation for $c(\mathbf{s})$ and its generating function, $\sum_\mathbf{s} c(\mathbf{s})\mathbf{x}^\mathbf{s}$, can be computed in polynomial time, as the following two propositions state.

Proposition 1.11 ([VSB+07])**.** *Fix n and d. There is a polynomial time algorithm which, given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$, computes the piecewise step-polynomial*

$$c(\mathbf{s}) = \#(P_\mathbf{s} \cap \mathbb{Z}^d)$$

with degree at most d.

Proposition 1.12. *Fix n and d. There is a polynomial time algorithm which, given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$ such that*

$$f(\mathbf{x}) = \sum_{\mathbf{s} \in \mathbb{Z}^n} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}}$$

converges on some nonempty open subset of $\mathbb{C}^n$, computes $f(\mathbf{x})$ as a rational generating function of the form (1.3) with the k_i at most d.

In Section 2 we recall the key ideas of the proof of Proposition 1.11 from [VSB+07], drawing heavily from the ideas in [BP99]. Proposition 1.12 is an immediate consequence of [BP99, Theorem 4.4] and the monomial substitution from [BW03] and will be proved in Section 3.

We may also look at *projections* of the integer points in a parametric polytope. Let $P \subset \mathbb{Q}^n \times \mathbb{Q}^d \times \mathbb{Q}^m$ be a rational polytope, and define the function $c : \mathbb{Z}^n \to \mathbb{Z}$ by

$$c(\mathbf{s}) = \#\left\{\mathbf{t} \in \mathbb{Z}^d \mid \exists \mathbf{u} \in \mathbb{Z}^m : \ (\mathbf{s}, \mathbf{t}, \mathbf{u}) \in P\right\}.$$

If $P_{\mathbf{s}} = \left\{(\mathbf{t}, \mathbf{u}) \in \mathbb{Q}^d \times \mathbb{Q}^m \mid (\mathbf{s}, \mathbf{t}, \mathbf{u}) \in P\right\}$ and the projection $\pi : \mathbb{Q}^d \times \mathbb{Q}^m \to \mathbb{Q}^d$ is defined by $\pi(\mathbf{t}, \mathbf{u}) = \mathbf{t}$, then

$$c(\mathbf{s}) = \#\big(\pi(P_{\mathbf{s}} \cap \mathbb{Z}^{d+m})\big).$$

It follows from [BW03] that the generating function, $\sum_{\mathbf{s}} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}}$, can be computed in polynomial time (for fixed n, d, and m). Therefore, we have as a corollary to Theorem 1.5 that the piecewise step-polynomial can be computed in polynomial time.

Corollary 1.13. *Let n, d, and m be fixed. There is a polynomial time algorithm which, given a polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d \times \mathbb{Q}^m$, computes the piecewise step-polynomial*

$$c(\mathbf{s}) = \#\left\{\mathbf{t} \in \mathbb{Z}^d \mid \exists \mathbf{u} \in \mathbb{Z}^m : \ (\mathbf{s}, \mathbf{t}, \mathbf{u}) \in P\right\}$$

with degree at most $n + d + m$.

We will prove this corollary at the end of Section 3.

2 Computing Piecewise Step-Polynomials for Parametric Polytopes

In this section, we recall the main elements of the proof of Proposition 1.11 from [BP99] and [VSB+07]. That is, given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$, we define $P_{\mathbf{s}} = \{\mathbf{t} \in \mathbb{Q}^d \mid (\mathbf{s}, \mathbf{t}) \in P\}$, for $\mathbf{s} \in \mathbb{Z}^n$, and we want to compute

$$c(\mathbf{s}) = \#(P_{\mathbf{s}} \cap \mathbb{Z}^d)$$

as a piecewise step-polynomial. We demonstrate each step with a running example and formulate an extended version of the final step for use in Section 3.

Example 2.1. Consider the parametric polytope

$$P = \left\{ (\mathbf{s}, \mathbf{t}) \in \mathbb{Q}^2 \times \mathbb{Q}^2 \;\middle|\; \begin{pmatrix} -1 & 2 \\ 1 & -1 \\ 0 & 0 \\ 0 & 0 \end{pmatrix} \mathbf{s} + \begin{pmatrix} 1 & -2 \\ -1 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \mathbf{t} \geq \mathbf{0} \right\}.$$

We want to compute a piecewise step-polynomial representation of

$$c(\mathbf{s}) = \#(P_{\mathbf{s}} \cap \mathbb{Z}^2) = \#\left\{\mathbf{t} \in \mathbb{Z}^2 \mid (\mathbf{s}, \mathbf{t}) \in P\right\}.$$

□

Our main tool will be a slightly different sort of generating function than we have been using. If $S \subset \mathbb{Z}^d$ is a set of integer vectors, then define its generating function to be

$$f(S; \mathbf{x}) = \sum_{\mathbf{t} \in S} \mathbf{x}^{\mathbf{t}} = \sum_{(t_1, \ldots, t_d) \in S} x_1^{t_1} x_2^{t_2} \cdots x_d^{t_d}.$$

In our previous notation, this is the generating function for $c(\mathbf{t})$ such that $c(\mathbf{t}) = 1$ for $t \in S$ and $c(\mathbf{t}) = 0$ otherwise.

Our proof of Proposition 1.11 will have two main steps.

- First, we will calculate the generating function $f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{x})$ as a rational generating function, and we will examine how it changes as $\mathbf{s}$ varies (Propositions 2.4 and 2.11).

- Second, we will calculate

$$c(\mathbf{s}) = \#(P_{\mathbf{s}} \cap \mathbb{Z}^d) = f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{1}),$$

  by appropriately substituting $\mathbf{x} = \mathbf{1}$.

In order to calculate the generating function $f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{x})$, it is necessary to know what the vertices of $P_{\mathbf{s}}$ are.

Example 2.2. Consider the parametric polytope P from Example 2.1.

For a given $\mathbf{s}$, the vertices of $P_{\mathbf{s}}$ can be obtained as the intersections of pairs of facets of $P_{\mathbf{s}}$. The facets $t_1 = 0$ and $t_1 - 2t_2 = s_1 - 2s_2$, for example, intersect at the point $\mathbf{v}_1 = (0, -s_1/2 + s_2)$. This point is not always *active*, that is, actually a vertex of $P_{\mathbf{s}}$. It is active exactly when $2s_2 \geq s_1 \geq 0$ (for all other values of $\mathbf{s}$, $\mathbf{v}_1 \notin P_{\mathbf{s}}$). We similarly find the vertices $\mathbf{v}_2 = (0, 0)$, $\mathbf{v}_3 = (s_1 - s_2, 0)$, $\mathbf{v}_4 = (s_1 - 2s_2, 0)$, $\mathbf{v}_5 = (0, -s_1 + s_2)$ and $\mathbf{v}_6 = (s_1, s_2)$, active on the domains $2s_2 \geq s_1 \geq s_2$, $s_1 \geq s_2 \geq 0$, $s_1 \geq 2s_2 \geq 0$, $s_2 \geq s_1 \geq 0$, and $s_1, s_2 \geq 0$, respectively. Combining all of the inequalities, we have the regions

$$\begin{aligned} Q_1 &= \{\, \mathbf{s} \mid 2s_2 \geq s_1 \geq s_2 \,\} \\ Q_2 &= \{\, \mathbf{s} \mid s_1 \geq 2s_2 \geq 0 \,\} \\ Q_3 &= \{\, \mathbf{s} \mid s_2 \geq s_1 \geq 0 \,\}. \end{aligned}$$

For $\mathbf{s} \in Q_1$, the polyhedron $P_{\mathbf{s}}$ has active vertices $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_6$; for $\mathbf{s} \in Q_2$, it has active vertices $\mathbf{v}_3, \mathbf{v}_6, \mathbf{v}_4$; and for $\mathbf{s} \in Q_3$, it has active vertices $\mathbf{v}_1, \mathbf{v}_5, \mathbf{v}_6$. On the boundary of the Q_i, there is more than one possible description of the vertices (any is fine).

Figure 2.3 shows the decomposition, the vertices active in each Q_i, and the evolution of the vertices as the value of $\mathbf{s}$ changes.

□

As the example suggests, and as shown in [VSB+07], we can find polyhedra Q_i such that the $\text{int}(Q_i)$ partition $\mathbb{Q}^n$ and, for any $\mathbf{s}$ in the relative interior of a given polyhedron Q_i, the polytopes $P_{\mathbf{s}}$ will have a fixed set of vertices given by affine transformations of $\mathbf{s}$ (where an affine transformation $T : \mathbb{Q}^n \to \mathbb{Q}^d$ is given by $T(\mathbf{s}) = T'(\mathbf{s}) + \mathbf{v}$ such that T' is a linear transformation and $\mathbf{v} \in \mathbb{Q}^d$). These Q_i will be the pieces of our piecewise step-polynomial. This is the content of the following proposition.

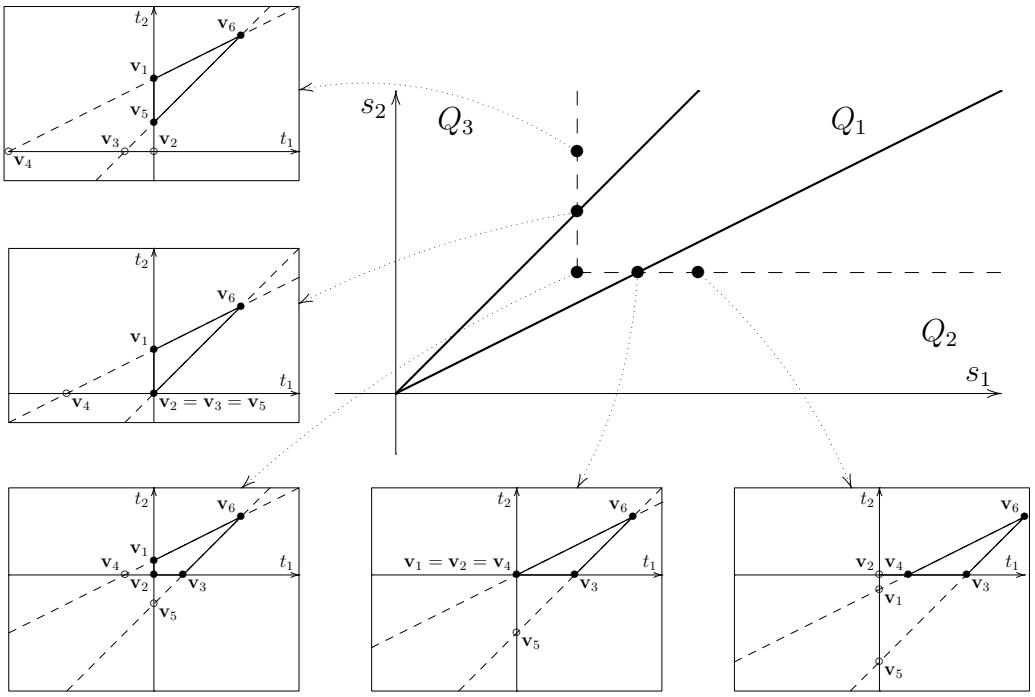

Figure 2.3: The decomposition and the vertices of the parametric polytope from Example 2.2.

Proposition 2.4 (Decomposition)**.** *Fix d and n. There exists a polynomial time algorithm, which, given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$, finds polyhedra Q_i whose relative interiors partition $\mathbb{Q}^n$, and, for each i, computes a collection of affine transformations $T_{i1}, T_{i2}, \ldots, T_{im_i} : \mathbb{Q}^n \to \mathbb{Q}^d$, such that, for $\mathbf{s} \in \operatorname{int} Q_i$, the vertices of $P_\mathbf{s}$ are $T_{i1}(\mathbf{s}), T_{i2}(\mathbf{s}), \ldots, T_{im_i}(\mathbf{s})$.*

Algorithms to compute the parametric vertices and the chambers can be found in [LW97] and [CL98] respectively. A proof of the polynomial time complexity is given in [VSB+07].

Now we can concentrate on computing $f(P_\mathbf{s} \cap \mathbb{Z}^d; \mathbf{x})$, given that $\mathbf{s}$ is in the relative interior of a particular Q_i. As a first step, we examine how to compute the generating function of an easy set: the integer points in a *unimodular cone*. The general case of a polyhedron is based on a reduction to these unimodular cones.

Definition 2.5. Let $\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_d \in \mathbb{Z}^d$ be a basis for the lattice $\mathbb{Z}^d$, and let $\beta_i \in \mathbb{Q}$, for $1 \le i \le d$. We define the *rational unimodular cone*

$$K = \left\{ \mathbf{x} \in \mathbb{Q}^d \mid \langle \mathbf{c}_i, \mathbf{x} \rangle \le \beta_i \text{ for } 1 \le i \le d \right\}.$$

This cone may have a vertex which is not at the origin. Let $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_d$ be the *negative dual basis* of $\mathbb{Z}^d$, so that

$$\langle \mathbf{u}_i, \mathbf{c}_j \rangle = \begin{cases} -1, & \text{if } i = j \\ 0, & \text{if } i \neq j. \end{cases}$$

If β_i were zero, for all i, then K would be the cone with vertex at the origin defined by

$$K = \left\{ \lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \cdots + \lambda_d \mathbf{u}_d \;\mid\; \boldsymbol{\lambda} \ge \mathbf{0} \right\},$$

we would have that

$$K \cap \mathbb{Z}^d = \left\{ \lambda_1 \mathbf{u}_1 + \lambda_2 \mathbf{u}_2 + \cdots + \lambda_d \mathbf{u}_d \;\mid\; \boldsymbol{\lambda} \in \mathbb{Z}^d_{\ge 0} \right\},$$

and therefore

$$f(K \cap \mathbb{Z}^d; \mathbf{x}) = \frac{1}{(1 - \mathbf{x}^{\mathbf{u}_1})(1 - \mathbf{x}^{\mathbf{u}_2}) \cdots (1 - \mathbf{x}^{\mathbf{u}_d})}.$$

In the general case, where the β_i are not necessarily zero, we have that

$$f(K \cap \mathbb{Z}^d; \mathbf{x}) = \frac{\mathbf{x}^{\mathbf{p}}}{(1 - \mathbf{x}^{\mathbf{u}_1})(1 - \mathbf{x}^{\mathbf{u}_2}) \cdots (1 - \mathbf{x}^{\mathbf{u}_d})}, \tag{2.6}$$

where $\mathbf{p} = -\sum_{i=1}^{d} \lfloor \beta_i \rfloor \, \mathbf{u}_i$ (see [BP99]). This greatest integer function in the definition of $\mathbf{p}$ is where the greatest integer function in our step-polynomial will come from. Note also that the denominator of this generating function does not depend on the β_i, only on the $\mathbf{c}_i$.

We want to reduce our problem, which is finding the generating function $f(P_\mathbf{s} \cap \mathbb{Z}^d; \mathbf{x})$ where $P_\mathbf{s}$ is a polyhedron, to the easy problem of finding the generating function for a unimodular cone. We can first reduce to the case of (not necessarily unimodular) cones using Brion's Theorem [Bri88], which states that the generating function of a polytope is equal to the sum of the generating functions of its *vertex cones*. These vertex cones are formed by the supporting hyperplanes of the polytope that intersect in a given vertex (see Figure 2.9 for an example). Next, we use Barvinok's unimodular decomposition [Bar94] to write the generating function of each vertex cone as a (signed) sum of generating functions of unimodular cones.

Example 2.7. Consider once more the parametric polytope P from Examples 2.1 and 2.2. We want to compute the generating function of this parametric polytope. Consider specifically region Q_3 from Example 2.2 with active vertices $\mathbf{v}_1 = (0, -s_1/2 + s_2)$, $\mathbf{v}_5 = (0, -s_1 + s_2)$ and $\mathbf{v}_6 = (s_1, s_2)$. The polytope corresponding to $\mathbf{s} = (3, 4) \in C_3$ is shown in Figure 2.9 together with the vertex cones, $\text{cone}(P_\mathbf{s}, \mathbf{v}_i)$, at each active vertex. Brion's theorem tells us that

$$f(P_\mathbf{s} \cap \mathbb{Z}^2; \mathbf{x}) = f\big(\text{cone}(P_\mathbf{s}, \mathbf{v}_1) \cap \mathbb{Z}^2; \mathbf{x}\big) + f\big(\text{cone}(P_\mathbf{s}, \mathbf{v}_5) \cap \mathbb{Z}^2; \mathbf{x}\big) + f\big(\text{cone}(P_\mathbf{s}, \mathbf{v}_6) \cap \mathbb{Z}^2; \mathbf{x}\big).$$

The vertex cones at $\mathbf{v}_5$ and $\mathbf{v}_6$ are unimodular, but the one at $\mathbf{v}_1$ is not. We therefore need to apply Barvinok's unimodular decomposition to $\text{cone}(P_\mathbf{s}, \mathbf{v}_1)$, which yields

$$f\big(\text{cone}(P_\mathbf{s}, \mathbf{v}_1) \cap \mathbb{Z}^2; \mathbf{x}\big) = \frac{\mathbf{x}^{(-2\lfloor \frac{s_1}{2} - s_2 \rfloor + s_1 - 2s_2, -\lfloor \frac{s_1}{2} - s_2 \rfloor)}}{(1 - \mathbf{x}^{(1,0)})(1 - \mathbf{x}^{(2,1)})} - \frac{\mathbf{x}^{(0, -\lfloor \frac{s_1}{2} - s_2 \rfloor)}}{(1 - \mathbf{x}^{(1,0)})(1 - \mathbf{x}^{(0,1)})}. \tag{2.8}$$

We refer to [BP99, DLHTY04, Köp07, KV07] for details on how to perform Barvinok's decomposition. Table 2.10 lists the generating functions of all vertex cones.

□

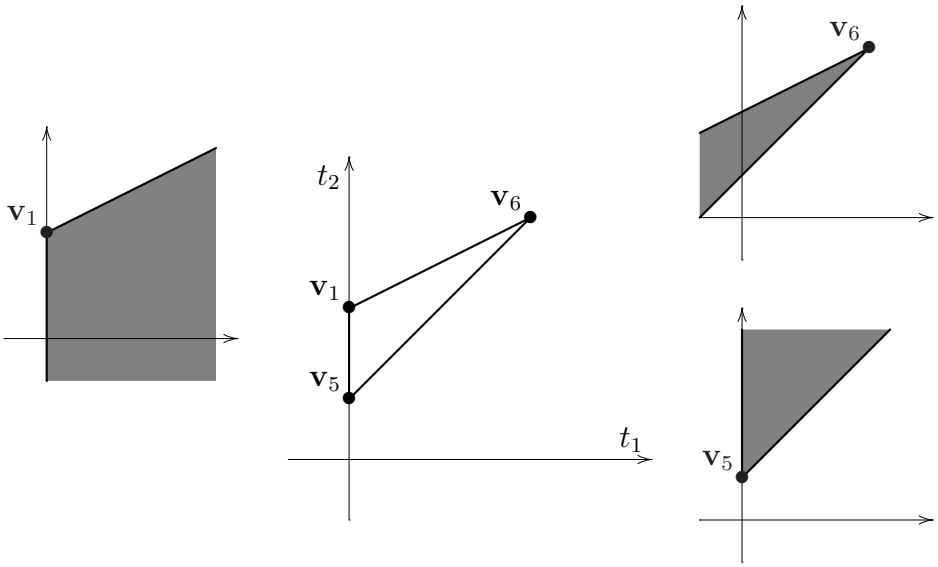

Figure 2.9: $P_{(3,4)}$ and its vertex cones

Vertex $\mathbf{v}_i$	$f\big(\operatorname{cone}(P_{\mathbf{s}}, \mathbf{v}_i) \cap \mathbb{Z}^d; \mathbf{x}\big)$
$\mathbf{v}_1 = (0, -s_1/2 + s_2)$	$\frac{\mathbf{x}^{(-2\lfloor \frac{s_1}{2} - s_2 \rfloor + s_1 - 2s_2, -\lfloor \frac{s_1}{2} - s_2 \rfloor)}}{(1-\mathbf{x}^{(1,0)})(1-\mathbf{x}^{(2,1)})} - \frac{\mathbf{x}^{(0, -\lfloor \frac{s_1}{2} - s_2 \rfloor)}}{(1-\mathbf{x}^{(1,0)})(1-\mathbf{x}^{(0,1)})}$
$\mathbf{v}_2 = (0, 0)$	$\frac{\mathbf{x}^{(0,0)}}{(1-\mathbf{x}^{(0,1)})(1-\mathbf{x}^{(1,0)})}$
$\mathbf{v}_3 = (s_1 - s_2, 0)$	$\frac{\mathbf{x}^{(s_1 - s_2, 0)}}{(1-\mathbf{x}^{(1,0)})(1-\mathbf{x}^{(-1,0)})}$
$\mathbf{v}_4 = (s_1 - 2s_2, 0)$	$\frac{\mathbf{x}^{(s_1 - 2s_2, 0)}}{(1-\mathbf{x}^{(2,1)})(1-\mathbf{x}^{(1,0)})}$
$\mathbf{v}_5 = (0, -s_1 + s_2)$	$\frac{\mathbf{x}^{(0, -s_1 + s_2)}}{(1-\mathbf{x}^{(0,1)})(1-\mathbf{x}^{(1,1)})}$
$\mathbf{v}_6 = (s_1, s_2)$	$\frac{\mathbf{x}^{(s_1, s_2)}}{(1-\mathbf{x}^{(-2,-1)})(1-\mathbf{x}^{(-1,-1)})}$

Table 2.10: The generating function of each vertex cone

When we do this in general, the end result is the following proposition, a rephrasing of Theorem 4.4 of [BP99].

Proposition 2.11. *Fix d. There exists a polynomial time algorithm, which, given a parametric polyhedron $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$ and a polyhedral region Q such that for $\mathbf{s} \in Q$ the vertices of $P_{\mathbf{s}} = \{\mathbf{t} \in \mathbb{Q}^d \mid (\mathbf{s}, \mathbf{t}) \in P\}$ are given by affine transformations $T_1(\mathbf{s}), T_2(\mathbf{s}), \cdots, T_m(\mathbf{s})$, computes the generating function*

$$f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{x}) = \sum_{i \in I} \varepsilon_i \frac{\mathbf{x}^{\mathbf{p}_i(\mathbf{s})}}{(1 - \mathbf{x}^{\mathbf{b}_{i1}})(1 - \mathbf{x}^{\mathbf{b}_{i2}}) \cdots (1 - \mathbf{x}^{\mathbf{b}_{id}})},$$

where $\varepsilon \in \{-1, 1\}$, $\mathbf{b}_{ij} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$, and each coordinate of $\mathbf{p}_i(\mathbf{s}) : \mathbb{Z}^n \to \mathbb{Z}^d$ is a step-polynomial of degree one, for each i.

Now that we know how to compute $f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{x})$, all that remains is to evaluate it at $\mathbf{x} = \mathbf{1}$.

Example 2.12. Consider once more the parametric polytope P from Examples 2.1, 2.2, and 2.7.

We have already computed $f\big(P_{\mathbf{s}} \cap \mathbb{Z}^2; \mathbf{x}\big)$, and we now compute the value $f\big(P_{\mathbf{s}} \cap \mathbb{Z}^2; \mathbf{1}\big)$. We cannot simply plug in $\mathbf{x} = \mathbf{1}$, because $\mathbf{1}$ is a pole of some of the rational functions. Instead, we make a suitable substitution, in this case $\mathbf{x} = (t+1, t+1)$ (chosen carefully so that none of the denominators become identically zero), and take the limit as t approaches zero. To compute this limit, we can simply compute, for each term in the sum constituting $f\big(P_{\mathbf{s}} \cap \mathbb{Z}^2; t+1, t+1\big)$, the constant term in the Laurent series expansion at $t = 0$.

For example, substituting $\mathbf{x} = (t+1, t+1)$ into the second term in (2.8), we obtain

$$-\frac{(1+t)^{-\lfloor \frac{s_1}{2} \rfloor + s_2}}{(1-(1+t))(1-(1+t))}.$$

Since the denominator, in this case, is exactly t^2, the constant term in the Laurent expansion is simply the coefficient of t^2 in the expansion of the numerator, i.e.,

$$-\frac{(-\lfloor \frac{s_1}{2} \rfloor + s_2)(-\lfloor \frac{s_1}{2} \rfloor + s_2 - 1)}{2} = -\frac{1}{2}\left\lfloor \frac{s_1}{2} \right\rfloor^2 - \frac{s_2^2}{2} + \left\lfloor \frac{s_1}{2} \right\rfloor s_2 - \frac{1}{2}\left\lfloor \frac{s_1}{2} \right\rfloor + \frac{s_2}{2}.$$

The other terms are handled similarly. Note that this is the place where the step polynomials show up in full force. The contribution of each vertex cone

Vertex $\mathbf{v}_i$	$f\big(\operatorname{cone}(P_{\mathbf{s}}, \mathbf{v}_i) \cap \mathbb{Z}^d; \mathbf{1}\big)$ (if v_i is active)
$\mathbf{v}_1 = (0, -s_1/2 + s_2)$	$\frac{s_1^2}{6} + \frac{s_1 s_2}{3} - s_1 \left\lfloor \frac{s_1}{2} \right\rfloor - \frac{s_1}{2} - \frac{s_2}{3} + \left\lfloor \frac{s_1}{2} \right\rfloor^2 + \left\lfloor \frac{s_1}{2} \right\rfloor + \frac{2}{9}$
	$-\frac{1}{2} \left\lfloor \frac{s_1}{2} \right\rfloor^2 - \frac{s_2^2}{2} + \left\lfloor \frac{s_1}{2} \right\rfloor s_2 - \frac{1}{2} \left\lfloor \frac{s_1}{2} \right\rfloor + \frac{s_2}{2}$
$\mathbf{v}_2 = (0, 0)$	0
$\mathbf{v}_3 = (s_1 - s_2, 0)$	$-\frac{s_1^2}{4} + \frac{s_1 s_2}{2} - \frac{s_2^2}{4} + \frac{1}{8}$
$\mathbf{v}_4 = (s_1 - 2s_2, 0)$	$\frac{s_1^2}{6} - \frac{2s_1 s_2}{3} - \frac{s_1}{2} + \frac{2s_2^2}{3} + s_2 + \frac{2}{9}$
$\mathbf{v}_5 = (0, -s_1 + s_2)$	$\frac{s_1^2}{4} - \frac{s_1 s_2}{2} + \frac{s_1}{2} + \frac{s_2^2}{4} - \frac{s_2}{2} + \frac{1}{8}$
$\mathbf{v}_6 = (s_1, s_2)$	$\frac{s_1^2}{12} + \frac{s_1 s_2}{6} + \frac{s_1}{2} + \frac{s_2^2}{12} + \frac{s_2}{2} + \frac{47}{72}$

Table 2.13: The contribution of each vertex cone to the constant term of the Laurent expansion

to the constant term of the Laurent expansion is listed in Table 2.13. The final step-polynomial in each chamber is computed using Brion's Theorem as the sum of the appropriate step-polynomials from this table. The final result is shown in Figure 2.14.

□

In general, we use the following lemma, which is more general than strictly needed here, but which allows for an incremental computation as discussed after the lemma and which we will also need in Section 3. The lemma is a special case of the monomial substitution theorem [BW03, Theorem 2.6]. We provide a slightly different proof, which lends itself more easily to an implementation. It is an extension of an idea from [DLHTY04], which is in itself a variation of the idea used in [Bar94].

Lemma 2.15 (Specialization)**.** *Let us fix k. There exists a polynomial time algorithm which, given a rational generating function $f(\mathbf{x})$ of the form (1.3) and an m with $0 \leq m \leq d$ such that $g(\mathbf{z}) := f(z_1, \ldots, z_m, 1, \ldots, 1)$ is an analytic function on some nonempty open subset of $\mathbb{C}^m$, computes $g(\mathbf{z})$ in*

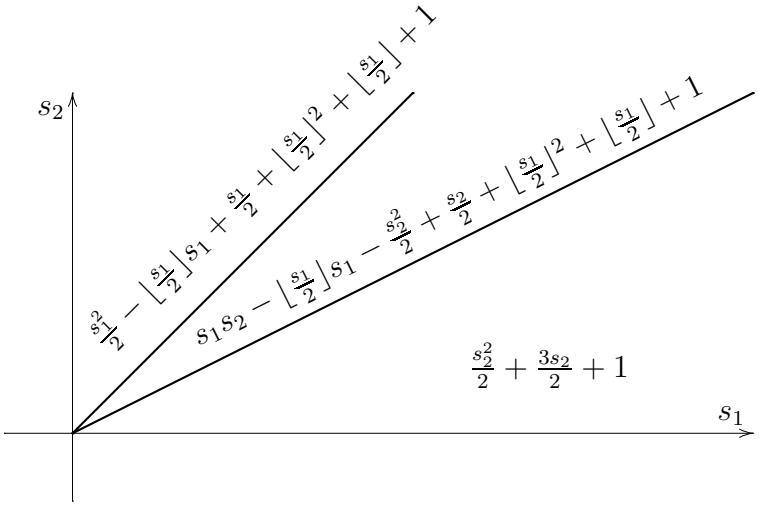

Figure 2.14: The enumerator of $P_{\mathbf{s}}$, a step-polynomial in each chamber

the same form, i.e.,

$$g(\mathbf{z}) = \sum_{i' \in I'} \beta_{i'} \frac{\mathbf{z}^{\mathbf{q}_{i'}}}{(1 - \mathbf{z}^{\mathbf{d}_{i'1}})(1 - \mathbf{z}^{\mathbf{d}_{i'2}}) \cdots (1 - \mathbf{z}^{\mathbf{d}_{i'k_{i'}}})}, \tag{2.16}$$

where $k_{i'} \leq k$, $\mathbf{z} \in \mathbb{C}^m$, $\beta_{i'} \in \mathbb{Q}$, $\mathbf{q}_{i'} \in \mathbb{Z}^m$, *and* $\mathbf{d}_{i'j'} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$.

Furthermore, if the vectors $\mathbf{b}_{ij}$ *and the numbers* α_i *in (1.3) are fixed, but the vectors* $\mathbf{p}_i$ *vary, then the vectors* $\mathbf{d}_{i'j'}$ *are fixed,* $\mathbf{q}_{i'}$ *each differ by a constant vector from some* $\mathbf{p}_i$, *and* $\beta_{i'}$ *are each a polynomial of degree at most* k *in the coordinates of some* $\mathbf{p}_i$.

Proof. The case $m = d$ is trivial, so we will assume $m < d$. Note that we cannot simply plug in the values 1, since $(z_1, \ldots, z_m, 1, \ldots, 1)$ may be a pole of some of the terms in (1.3). In fact, if $m = 0$, then it will be a pole of all those terms. We must take an appropriate limit as $(x_{m+1}, \ldots, x_n)$ approaches $(1, \ldots, 1)$. Consider

$$h(t) = f(z_1, \ldots, z_m, (1+t)^{\lambda_1}, \ldots, (1+t)^{\lambda_{d-m}}),$$

as a function of t only, where $\boldsymbol{\lambda} \in \mathbb{Z}^{d-m}$ is such that for each $i \in I$ either $(b_{i1}, \ldots, b_{im}) \neq \mathbf{0}$ or $\langle (b_{i,m+1}, \ldots, b_{id}), \boldsymbol{\lambda} \rangle \neq 0$. Such a $\boldsymbol{\lambda}$ can be found in polynomial time by choosing an appropriate point from the "moment curve"

as in [BP99, Algorithm 5.2]. Then $g(\mathbf{z})$ is simply the constant term in the Laurent power series expansion of $h(t)$ about $t = 0$. This is the sum of the constant terms in the Laurent power series expansions of

$$h_i(t) = \alpha_i \frac{\mathbf{z}^{\mathbf{p}'_i}(t+1)^{q_i}}{(1-\mathbf{z}^{\mathbf{b}'_{i1}}(t+1)^{v_{i1}})(1-\mathbf{z}^{\mathbf{b}'_{i2}}(t+1)^{v_{i2}})\cdots(1-\mathbf{z}^{\mathbf{b}'_{ik_i}}(t+1)^{v_{ik_i}})},$$

where, for $\mathbf{v} \in \{\, \mathbf{p}_i, \mathbf{b}_{ij} \,\}$, we write $\mathbf{v}'$ for the first m components of $\mathbf{v}$ and $\mathbf{v}''$ for the remaining $d-m$ components, and we let $q_i = \langle \mathbf{p}'', \mathbf{1} \rangle$ and $v_{ij} = \langle \mathbf{b}''_{ij}, \mathbf{1} \rangle$.

Consider a particular $h_i(t)$. Let r be the number of factors with $v_{ij} \neq 0$ but $\mathbf{b}'_{ij} = \mathbf{0}$. Then $h_i(t)$ has a pole of order r at $t = 0$. Therefore, we must compute the coefficient of t^r in the Taylor series expansion of $t^r h_i(t)$, which is analytic at $t = 0$.

Following [DLHTY04] we use the technique outlined in [Hen74, 241–247] (where it is applied to compute the residue of a function, i.e., the coefficient of the term t^{-1}). Let $t^r h_i(t) = \frac{P(t)}{Q(t)}$, where P and Q are polynomials. To compute the coefficients c_j in

$$\frac{P(t)}{Q(t)} =: c_0 + c_1 t + c_2 t^2 + \cdots,$$

expand $P(t)$ and $Q(t)$ as

$$\begin{aligned} P(t) &=: a_0 + a_1 t + a_2 t^2 + \cdots \\ Q(t) &=: b_0 + b_1 t + b_2 t^2 + \cdots \end{aligned}$$

and apply the recurrence relation

$$c_j = \frac{1}{b_0}\left(a_j - \sum_{i=1}^{j} b_i c_{j-i}\right).$$

Note that we only need to keep track of the first $r+1$ coefficients of $P(t)$ and $Q(t)$, and so this may be done in polynomial time. Examining the recursive process, we see that the lemma follows. □

Remark on the implementation of Lemma 2.15: Note that as argued by [DLHTY04], a $\boldsymbol{\lambda}$ from the moment curve may not be the most appropriate choice to use in an implementation since it is likely to have large coefficients. They therefore propose to construct a random vector with small coefficients

and check whether $\langle \mathbf{b}''_{ij}, \boldsymbol{\lambda} \rangle \neq 0$ for all i and j. (Or rather $\langle \mathbf{b}_{ij}, \boldsymbol{\lambda} \rangle \neq 0$, since $m = 0$ in their case.) Only after a fixed number of failed attempts would the implementation fall back onto the moment curve.

Both of these strategies have the disadvantage however that all the terms in (1.3) need to be available before the constant term of the first term can be computed. This may induce a large memory bottleneck. The authors of [DLHTY04] have therefore also implemented an alternative strategy where a random vector with larger coefficients is constructed at the beginning of the computation. If the coefficients are large enough, then the probability of having constructed an incorrect vector is close to zero. The disadvantage of this technique is that the coefficients are larger and that the computation has to be redone completely in the unlikely event the vector was incorrect.

We propose a different strategy which does not require all terms to be available, nor does it require the use of large coefficients. We simply repeatedly apply Lemma 2.15 for m' from $d-1$ down to m. In each application, we can simply use $\lambda = 1$, which is known to be valid in any case. □

We summarize the proof of Proposition 1.11.

Proof of Proposition 1.11. Given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$, apply Proposition 2.4 to obtain the decomposition $\{ Q_i \}$. For each region Q_i, apply Proposition 2.11 to obtain the corresponding generating function of $P_{\mathbf{s}}$, for $s \in Q_i$. The result is a collection of polyhedral regions Q_i such that, for $\mathbf{s} \in \operatorname{int}(Q_i) \cap \mathbb{Z}^n$,

$$f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{x}) = \sum_j \frac{\mathbf{x}^{\mathbf{p}_j(\mathbf{s})}}{(1 - \mathbf{x}^{\mathbf{u}_{j1}})(1 - \mathbf{x}^{\mathbf{u}_{j2}}) \cdots (1 - \mathbf{x}^{\mathbf{u}_{jd}})},$$

where $\mathbf{u}_{jl} \in \mathbb{Z}^d \setminus \{\mathbf{0}\}$ and the coordinates of $\mathbf{p}_j : \mathbb{Z}^n \to \mathbb{Z}^d$ are piecewise step-polynomials of degree one. All that remains is to use Lemma 2.15 with $m = 0$ to compute $c(\mathbf{s}) := f(P_{\mathbf{s}} \cap \mathbb{Z}^d; \mathbf{1})$ as a step-polynomial in $\mathbf{s}$, valid for $\mathbf{s} \in \operatorname{int} Q_i$. □

3 Equivalence of Rational Generating Functions and Piecewise Step-Polynomials

In this section, we prove Theorem 1.5, that we may convert between rational generating function and piecewise step-polynomial representations in polynomial time. In both directions, we reduce the problem to a set of counting problems to which we apply either Proposition 1.11 or Proposition 1.12. We first prove a special case of the first half of Theorem 1.5, as a corollary of Proposition 1.11.

Corollary 3.1. *Fix d. There is a polynomial time algorithm which, given $\alpha \in \mathbb{Q}$, $\mathbf{p} \in \mathbb{Z}^n$, $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_d \in \mathbb{Z}^n \backslash \{\mathbf{0}\}$ and given $\mathbf{l} \in \mathbb{Z}^n$ such that $\langle \mathbf{l}, \mathbf{a}_i \rangle \neq 0$ for all i, computes the piecewise step-polynomial $c : \mathbb{Z}^n \to \mathbb{Q}$ such that*

$$f(\mathbf{x}) = \alpha \frac{\mathbf{x}^{\mathbf{p}}}{(1-\mathbf{x}^{\mathbf{a}_1})(1-\mathbf{x}^{\mathbf{a}_2})\cdots(1-\mathbf{x}^{\mathbf{a}_d})} = \sum_{\mathbf{s}\in\mathbb{Z}^n} c(\mathbf{s})\mathbf{x}^{\mathbf{s}}$$

is convergent on a neighborhood of $\mathbf{e}^{\mathbf{l}}$.

Proof. We may assume, without loss of generality, that $\langle \mathbf{l}, \mathbf{a}_i \rangle < 0$ for all i. Otherwise, if $\langle \mathbf{l}, \mathbf{a}_i \rangle > 0$ for some i, we would apply the identity

$$\frac{1}{1-\mathbf{x}^{\mathbf{a}_i}} = \frac{-\mathbf{x}^{-\mathbf{a}_i}}{1-\mathbf{x}^{-\mathbf{a}_i}}. \tag{3.2}$$

It suffices to prove this corollary for $\alpha = 1$ and $\mathbf{p} = \mathbf{0}$, because if $c'(\mathbf{s})$ is a piecewise step-polynomial representation of the generating function $g(\mathbf{x})$, then $\alpha \cdot c'(\mathbf{s}-\mathbf{p})$ is a piecewise step-polynomial representation of $\alpha \mathbf{x}^{\mathbf{p}} g(\mathbf{x}))$. Note that $\alpha = 1$ and $\mathbf{p} = \mathbf{0}$ mean that $c(\mathbf{s})$ is the vector partition function defined in Example 1.8.

We expand $f(\mathbf{x})$ as a product of infinite geometric series,

$$f(\mathbf{x}) = \prod_{i=1}^{d} (1 + \mathbf{x}^{\mathbf{a}_i} + \mathbf{x}^{2\mathbf{a}_i} + \cdots).$$

Then

$$f(\mathbf{e}^{\mathbf{l}}) = \prod_{i=1}^{d} (1 + e^{\langle \mathbf{l}, \mathbf{a}_i \rangle} + e^{2\langle \mathbf{l}, \mathbf{a}_i \rangle} + \cdots),$$

and this expansion is convergent on a neighborhood of $\mathbf{e}^{\mathbf{l}}$, since $\langle \mathbf{l}, \mathbf{a}_i \rangle < 0$. We see that we are looking to compute the function

$$c(\mathbf{s}) = \#\big\{\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_d) \in \mathbb{Z}^d_{\geq 0} \;\mid\; \mathbf{s} = \lambda_1 \mathbf{a}_1 + \lambda_2 \mathbf{a}_2 + \cdots + \lambda_d \mathbf{a}_d\big\}.$$

Let P be the parametric polytope

$$P = \big\{(\mathbf{s}, \boldsymbol{\lambda}) \in \mathbb{Q}^n \times \mathbb{Q}^d \;\mid\; \boldsymbol{\lambda} \geq \mathbf{0} \text{ and } \mathbf{s} = \lambda_1 \mathbf{a}_1 + \cdots + \lambda_d \mathbf{a}_d\big\}.$$

Then

$$c(\mathbf{s}) = \#\left\{\boldsymbol{\lambda} \in \mathbb{Z}^d \mid (\mathbf{s}, \boldsymbol{\lambda}) \in P\right\},$$

which can be computed as a piecewise step-polynomial using Proposition 1.11. The proof follows. □

Example 3.3. Consider the function

$$f(\mathbf{x}) = \frac{1}{(1 - \mathbf{x}^{(1,1)})(1 - \mathbf{x}^{(2,1)})(1 - \mathbf{x}^{(1,0)})(1 - \mathbf{x}^{(0,1)})},$$

which is the generating function of the vector partition function

$$c(\mathbf{s}) = \#\left\{\boldsymbol{\lambda} \in \mathbb{N}^4 \;\middle|\; \begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \boldsymbol{\lambda} = \mathbf{s}\right\}. \tag{3.4}$$

This is the same as the example from [Bec04, Section 4]. For a given $\mathbf{s} \in \mathbb{Z}^n$, the solution set $P_{\mathbf{s}} = \left\{\boldsymbol{\lambda} \in \mathbb{Q}^4 \;\middle|\; \boldsymbol{\lambda} \geq \mathbf{0} \text{ and } \begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \boldsymbol{\lambda} = \mathbf{s}\right\}$ is a two dimensional polytope in $\mathbb{Q}^4$, so it is helpful to convert it to a full-dimensional polytope in $\mathbb{Q}^2$ (without changing the number of integer points). To do this, extend the transformation matrix from (3.4) to

$$M = \begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

which is unimodular (that is, it has determinant ± 1 and so, as a linear transformation, it bijectively maps $\mathbb{Z}^4$ to $\mathbb{Z}^4$), and perform the change of

coordinates $\boldsymbol{\lambda} \mapsto \boldsymbol{\lambda}' = M\boldsymbol{\lambda}$. Then

$$\begin{aligned} c(\mathbf{s}) &= \#\left\{\boldsymbol{\lambda}' \in \mathbb{Z}^4 \;\middle|\; M^{-1}\boldsymbol{\lambda}' \geq 0 \text{ and } \begin{pmatrix} 1 & 2 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} M^{-1}\boldsymbol{\lambda}' = \mathbf{s}\right\} \\ &= \#\left\{\boldsymbol{\lambda}' \in \mathbb{Z}^4 \;\middle|\; M^{-1}\boldsymbol{\lambda}' \geq 0 \text{ and } \lambda'_1 = s_1, \lambda'_2 = s_2\right\} \\ &= \#\left\{(\lambda'_3, \lambda'_4) \in \mathbb{Z}^2 \;\middle|\; \begin{pmatrix} -1 & 2 & 1 & -2 \\ 1 & -1 & -1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_1 \\ s_2 \\ \lambda'_3 \\ \lambda'_4 \end{pmatrix} \geq \mathbf{0}\right\}. \end{aligned}$$

This is the enumeration problem that was our running example in the last section.

□

We will also need the following lemma.

Lemma 3.5. *Let $\Phi(m,d) = \binom{m}{0} + \binom{m}{1} + \cdots + \binom{m}{d}$. Then m hyperplanes in $\mathbb{Q}^d$ decompose the space into at most $\Phi(m,d)$ polyhedral chambers. Furthermore, if we fix d, then there is a polynomial time algorithm which, given m hyperplanes in $\mathbb{Q}^d$, computes the defining inequalities for each of these chambers.*

Proof. This lemma is well known, especially the first part, see, for example, Section 6.1 of [Mat02]. We prove both parts by induction on m. Certainly the statement is true for m=0. Suppose we have a collection of m hyperplanes $\mathcal{H}_1, \cdots, \mathcal{H}_m$, and assume that these decompose $\mathbb{Q}^d$ into at most $\Phi(m,d)$ polyhedral chambers whose defining inequalities may be determined in polynomial time. Let us then add a new hyperplane $\mathcal{H}_{m+1}$, which will split some of the old chambers in two. The chambers that it splits correspond exactly to the chambers that the m hyperplanes $\mathcal{H}_i \cap \mathcal{H}_{m+1} \subset \mathcal{H}_{m+1}$, for $1 \leq i \leq m$, decompose the $(d-1)$-dimensional space $\mathcal{H}_{m+1}$ into. Inductively, there are at most $\Phi(m,d-1)$ of these chambers in $\mathcal{H}_{m+1}$, and their descriptions may be computed in polynomial time. Therefore, the hyperplanes $\mathcal{H}_1, \cdots, \mathcal{H}_{m+1}$ decompose $\mathbb{Q}^m$ into at most $\Phi(m,d) + \Phi(m,d-1) = \Phi(m+1,d)$ chambers, and we may compute their descriptions in polynomial time. □

A generating function in the form (1.3) is simply the sum of terms like those in the statement of Corollary 3.1, so the first half of Theorem 1.5 follows from the following lemma.

Lemma 3.6. *Fix d. There is a polynomial time algorithm which, given piecewise step-polynomials $c_i : \mathbb{Z}^d \to \mathbb{Q}$, computes $c(\mathbf{s}) = \sum_i c_i(\mathbf{s})$ as a piecewise step-polynomial.*

Proof. Suppose $c_i(\mathbf{s})$ are given as piecewise step-polynomials, and let $c(\mathbf{s}) = \sum_i c_i(\mathbf{s})$. We would like to compute $c(\mathbf{s})$ as a piecewise step-polynomial. For each i, let $\{\langle \mathbf{a}_{ij}, \mathbf{x}\rangle \le b_{ij}\}_j$ be the collection of linear inequalities that define the chambers of the piecewise step-polynomial representation of $c_i(\mathbf{s})$. By Lemma 3.5, we can compute in polynomial time the chambers in $\mathbb{Q}^n$ determined by the collection of all inequalities $\{\langle \mathbf{a}_{ij}, \mathbf{x}\rangle \le b_{ij}\}_{i,j}$. These will be the chambers in the piecewise step-polynomial representation of $c(\mathbf{s})$. Within a particular chamber, each $c_i(\mathbf{s})$ is defined by

$$c_i(\mathbf{s}) = \sum_{j=1}^{n_i} \alpha_{ij} \prod_{k=1}^{d_{ij}} \lfloor \langle \mathbf{a}_{ijk}, \mathbf{s}\rangle + b_{ijk} \rfloor ,$$

where $\alpha_{ij} \in \mathbb{Q}$, $\mathbf{a}_{ijk} \in \mathbb{Q}^d$, and $b_{ijk} \in \mathbb{Q}$, and so $c(\mathbf{s}) = \sum_i c_i(\mathbf{s})$ is simply a sum of such functions. □

The first half of Theorem 1.5 is now proved. The second half of Theorem 1.5 depends on Proposition 1.12, which we prove now.

Proof of Proposition 1.12. Given a parametric polytope $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$, apply Theorem 4.4 of [BP99] (see Proposition 2.11) directly on P (that is, not considering P as a parametric polytope but as a polyhedron in its own right) to obtain the rational generating function

$$g(P \cap \mathbb{Z}^{n+d}; \mathbf{x}, \mathbf{y}) = \sum_{(\mathbf{s},\mathbf{t}) \in P \cap \mathbb{Z}^{n+d}} \mathbf{x}^{\mathbf{s}} \mathbf{y}^{\mathbf{t}}$$

in polynomial time. Then the generating function $f(\mathbf{x})$ can be obtained by substituting $\mathbf{y} = \mathbf{1}$, i.e.,

$$f(\mathbf{x}) = \sum_{\mathbf{s} \in \mathbb{Z}^n} c(\mathbf{s}) \mathbf{x}^{\mathbf{s}} = g\big(P \cap \mathbb{Z}^{n+d}; \mathbf{x}, \mathbf{1}\big).$$

We may perform this substitution in polynomial time using Lemma 2.15. The result is in the form (1.3). □

Given a piecewise step-polynomial $c(\mathbf{s})$, we would like to compute the rational generating function $f(\mathbf{x}) = \sum_{\mathbf{s}\in\mathbb{Z}^n} c(\mathbf{s})\mathbf{x}^{\mathbf{s}}$. It suffices to prove it for functions of the form

$$c(\mathbf{s}) = \begin{cases} \prod_{j=1}^{d} \lfloor \langle \mathbf{a}_j, \mathbf{s}\rangle + b_j \rfloor, & \text{for } \mathbf{s} \in Q \\ 0, & \text{for } \mathbf{s} \notin Q, \end{cases}$$

where Q is a rational polyhedron, $\mathbf{a}_j \in \mathbb{Q}^n$, and $b_j \in \mathbb{Q}$, because all piecewise step-polynomials may be written as linear combinations of functions of this form.

Let $P \subset \mathbb{Q}^n \times \mathbb{Q}^d$ be the polyhedron

$$P = \left\{(\mathbf{s},\mathbf{t}) \in \mathbb{Q}^n \times \mathbb{Q}^d \;\mid\; \mathbf{s} \in Q \text{ and } 1 \le t_j \le \langle \mathbf{a}_j, \mathbf{s}\rangle + b_j, \text{ for } 1 \le j \le d\right\}.$$

Then

$$c(\mathbf{s}) = \#\left\{\mathbf{t} \in \mathbb{Z}^d \mid (\mathbf{s},\mathbf{t}) \in P\right\},$$

and we may compute $f(\mathbf{x}) = \sum_{\mathbf{s}} c(\mathbf{s})\mathbf{x}^{\mathbf{s}}$ as a rational generating function using Proposition 1.12. The second half of Theorem 1.5 follows.

Finally, we prove Corollary 1.13.

Proof of Corollary 1.13. Let

$$S = \left\{(\mathbf{s},\mathbf{t}) \in \mathbb{Z}^n \times \mathbb{Z}^d \mid \exists \mathbf{u} \in \mathbb{Z}^m : \; (\mathbf{s},\mathbf{t},\mathbf{u}) \in P\right\}.$$

Then we may compute, in polynomial time, the generating function

$$f(S;\mathbf{x},\mathbf{y}) = \sum_{(\mathbf{s},\mathbf{t})\in S} \mathbf{x}^{\mathbf{s}}\mathbf{y}^{\mathbf{t}},$$

using Theorem 1.7 of [BW03]. Next we compute $f\big(S;\mathbf{x},\mathbf{1}\big)$ using Lemma 2.15, and the $c(\mathbf{s})$ that we desire to compute is the piecewise step-polynomial representation of this generating function. Applying Theorem 1.5, the proof follows (since P is bounded, $\sum_{\mathbf{s}} c(\mathbf{s})\mathbf{x}^{\mathbf{s}}$ converges everywhere to $f\big(S;\mathbf{x},\mathbf{1}\big)$, and so any $\mathbf{l}$ not orthogonal to any of $\mathbf{b}_{ij}$ can be used in the application of this theorem). □

Acknowledgements

We are grateful to Alexander Barvinok for several helpful discussions. We would also like to thank the anonymous referees for their help in improving the exposition of this manuscript.

References

[Bar94] Alexander Barvinok. A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. Oper. Res.*, 19(4):769–779, 1994.

[Bec04] Matthias Beck. The partial-fractions method for counting solutions to integral linear systems. *Discrete Comp. Geom.*, 32:437–446, 2004. (special issue in honor of Louis Billera).

[BP99] Alexander Barvinok and James Pommersheim. An algorithmic theory of lattice points in polyhedra. In *New Perspectives in Algebraic Combinatorics (Berkeley, CA, 1996–97)*, volume 38 of *Math. Sci. Res. Inst. Publ.*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.

[Bri88] Michel Brion. Points entiers dans les polyèdres convexes. *Ann. Sci. École Norm. Sup. (4)*, 21(4):653–663, 1988.

[BW03] Alexander Barvinok and Kevin Woods. Short rational generating functions for lattice point problems. *J. Amer. Math. Soc.*, 16(4):957–979 (electronic), 2003.

[CL98] Phillipe Clauss and Vincent Loechner. Parametric analysis of polyhedral iteration spaces. *Journal of VLSI Signal Processing*, 19(2):179–194, July 1998.

[DLHTY04] Jesús De Loera, Raymond Hemmecke, Jeremy Tauzer, and Ruriko Yoshida. Effective lattice point counting in rational convex polytopes. *Journal of Symbolic Computation*, 38(4):1273–1302, 2004.

[Ehr62] Eugène Ehrhart. Sur les polyèdres rationnels homothétiques à n dimensions. *C. R. Acad. Sci. Paris*, 254:616–618, 1962.

[Hen74] Peter Henrici. *Applied and computational complex analysis.* Pure and applied mathematics. Wiley-Interscience [John Wiley & Sons], New York, 1974. Volume 1: Power series—integration—conformal mapping—location of zeros, Pure and Applied Mathematics.

[Köp07] Matthias Köppe. A primal Barvinok algorithm based on irrational decompositions. *SIAM Journal on Discrete Mathematics*, 21(1):220–236, 2007.

[KV07] Matthias Köppe and Sven Verdoolaege. Computing parametric rational generating functions with a primal barvinok algorithm, 2007. manuscript in preparation.

[LW97] Vincent Loechner and Doran K. Wilde. Parameterized polyhedra and their vertices. *International Journal of Parallel Programming*, 25(6):525–549, December 1997.

[Mat02] Jiří Matoušek. *Lectures on Discrete Geometry*, volume 212 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[VSB+07] S. Verdoolaege, R. Seghir, K. Beyls, V. Loechner, and M. Bruynooghe. Counting integer points in parametric polytopes using barvinok's rational functions. *Algorithmica*, 2007. accepted for publication.

Department of Computer Science, K.U. Leuven, Belgium
Email: Sven.Verdoolaege@cs.kuleuven.be[1]

Department of Mathematics, Oberlin College, Oberlin, Ohio
Email: Kevin.Woods@oberlin.edu

[1]Currently at Leiden Institute of Advanced Computer Science, Universiteit Leiden, The Netherlands, sverdool@liacs.nl