ON COUNTING INTEGRAL POINTS IN A CONVEX RATIONAL POLYTOPE

JEAN B. LASSERRE AND EDUARDO S. ZERON

ABSTRACT. Given a convex rational polytope $\Omega(b) := \{x \in \mathbb{R}^n_+ \mid Ax = b\}$, we consider the function $b \mapsto f(b)$, which counts the nonnegative integral points of $\Omega(b)$. A closed form expression of its $\mathbb{Z}$-transform $z \mapsto \mathcal{F}(z)$ is easily obtained so that $f(b)$ can be computed as the inverse $\mathbb{Z}$-transform of $\mathcal{F}$. We then provide two variants of an inversion algorithm. As a by-product, one of the algorithm provides the Ehrhart polynomial of a convex integer polytope Ω. We also provide an alternative that avoids the complex integration of $\mathcal{F}(z)$ and whose main computational effort is to solve a linear system. This latter approach is particularly attractive for relatively small values of m, where m is the number of nontrivial constraints (or rows of A).

1. INTRODUCTION

In this paper, we are interested in the number $f(b)$ of nonnegative integral points $x \in \mathbb{Z}^n \cap \Omega$ where Ω is the convex *rational* polytope $\{x \in \mathbb{R}^n_+ \mid Ax = b\}$ (that is, the entries of A and b are all in $\mathbb{Z}$).

Counting integral points (or, more generally, lattice points) of a convex polytope Ω is an important problem in computational geometry (and operations research as well, in view of its connection with integer programming) which has received much attention in recent years (see e.g. the works of Barvinok [2, 3], Beck [5], Beck, Diaz and Robins [6], Brion [7], Brion and Vergne [8]), Kantor and Khovanskii [12], Khovanskii and Pukhlikov [13]). In particular, using generating functions, Brion and Vergne [8, p. 801] provide generalized residue formulae that yield closed form expressions for $f(b)$ and further exploited in Baldoni-Silva and Vergne [1] for particular cases like flow polytopes. Beck [5] and Beck Diaz and Robins [6] also provide a complete analysis based on residue techniques for the case of a tetrahedron ($m = 1$) and also mention the possibility of evaluating $f(b)$ for general polytopes by means of residues.

In principle, these theoretical results can be exploited to devise an algorithm to compute $f(b)$ numerically. For instance, Barvinok [2] proposed a conceptual algorithm for *rational* polytopes with polynomial time computational complexity when the dimension n is fixed. This algorithm requires

Date: September 20, 2002.

Research partially supported by the ECOS-Nord (France)-ANUIES (México) Educational and Scientific Cooperation Program PM98M02; and Cinvestav (México).

each term of the decomposition is easy, the main work is the computation of the coefficients of the polynomials involved in this decomposition, which reduces to solving a linear system as bounds on the degree of the polynomials in this decomposition are available (see e.g. Seidenberg [17] and Kollár [14]). This approach might be a viable alternative, particularly for relatively small values of m.

The paper is organized as follows. In §2 we provide an explicit expression of the $\mathbb{Z}$-transform $\mathcal{F}$ of $f(b)$. In §3 we describe and analyse an algorithm to invert the so-called *associated* $\mathbb{Z}$*-transform* of f. For illustration purposes, a simple example is worked out in §4 and a general algorithm is outlined in §5. An approximate algorithm with a simplified integration process is also presented in §6. Finally, an alternative approach is presented in §7.

2. The $\mathbb{Z}$ transform of f

The notation $\mathbb{R}_+$ stands for the usual positive closed cone of $\mathbb{R}$. As usual, $\mathbb{Z}$ denotes the set of relative integers and $\mathbb{Z}_+ = \mathbb{N} = \{0, 1, 2, \ldots\}$ the set of natural numbers. We denote by c' and A' the respective transpose of the vector c and the matrix A. Finally, given any two vectors $z \in \mathbb{C}^m$ and $u \in \mathbb{Z}^m$, the notation z^u and $\ln(z)$ stands (respectively) for

$$z^u := z_1^{u_1} z_2^{u_2} \cdots z_m^{u_m}, \tag{2.1}$$

$$\ln(z) := [\ln(z_1), \ln(z_2), \ldots, \ln(z_m)]. \tag{2.2}$$

As mentioned in the introduction, we consider the convex polytope

$$\Omega(y) = \{x \in \mathbb{R}^n \mid Ax = y; \quad x \geq 0\}, \tag{2.3}$$

where $y \in \mathbb{Z}^m$ and $A \in \mathbb{Z}^{n \times m}$, and we want to compute the number of points $x \in \mathbb{N}^n$ of $\Omega(y)$, that is, the cardinality of the set

$$\mathbb{N}^n \cap \Omega(y). \tag{2.4}$$

We will actually calculate the following related function

$$y \mapsto f(y) := \sum_{\mathbb{N}^n \cap \Omega(y)} \mathrm{e}^{c'x}. \tag{2.5}$$

for a given vector $c \in \mathbb{R}^n$.

We trivially have that $f(y)$ is equal to the cardinality of $\mathbb{N}^n \cap \Omega(y)$ when $c = 0$ (and for more details on $f(y)$ (with $c = 0$) the reader is referred to Beck [4]). Morever, as observed in Barvinok and Pommersheim [3], taking c very small and rounding $f(y)$ to the nearest integer (or taking an appropriate residue) will give the number of points $x \in \mathbb{N}^n$ of $\Omega(y)$.

Of course, computing the number of points $x \in \mathbb{N}^n$ of the convex polytope

$$\Omega_1(y) = \{x \in \mathbb{R}_+^n \mid A_1 x \leq y\} \tag{2.6}$$

for some $A_1 \in \mathbb{Z}^{m \times n}$, reduces to computing the cardinality of $\mathbb{N}^n \cap \Omega(y)$ with Ω as in (2.3) and with $A := [A_1 \mid I]$ ($I \in \mathbb{N}^{m \times m}$ being the identity matrix).

Hence, the conditions $|z_1^{A_{1k}} z_2^{A_{2k}} \dots z_m^{A_{mk}}| > \mathrm{e}^{c_k}$ for $k = 1, 2, \cdots n$, or equivalently, $A'(\ln|z_1|, \ln|z_2|, \dots, \ln|z_m|) > c$, yields

$$\begin{aligned} \mathcal{F}(z) &= \prod_{k=1}^{n} \sum_{x_k=0}^{\infty} \left(\mathrm{e}^{c_k} z_1^{-A_{1k}} z_2^{-A_{2k}} \cdots z_m^{-A_{mk}} \right)^{x_k} \\ &= \prod_{k=1}^{n} \frac{1}{(1 - \mathrm{e}^{c_k} z_1^{-A_{1k}} z_2^{-A_{2k}} \cdots z_m^{-A_{mk}})} \end{aligned}$$

which is (2.9). Finally, equation (2.11) is obtained by analyzing the integral $\int_{|z|=r} z^w dz$ with $r > 0$. This integral is equal to $2\pi i$ only if $w = -1$, whereas if w is any integer different of -1, then the integral is equal to zero. It remains to show that indeed, the domain $\{\beta \in \mathbb{R}_+^n \mid A' \ln(\beta) > c\}$ is not empty. But this follows directly from our choice of the vector c and from Remark 2.1 (take $\beta := \mathrm{e}^{2u_0}$). □

3. Inversion of the $\mathbb{Z}$-transform $\mathcal{F}$

Theorem 2.2 allows us to compute $f(y)$ for $y \in \mathbb{Z}^m$ via (2.11), that is, by computing the inverse $\mathbb{Z}$-transform of $\mathcal{F}(z)$ at the point y. Moreover, we can directly calculate (2.11) by using Cauchy's Residue Theorem because $\mathcal{F}(z)$ is a rational function with only a *finite* number of poles (with respect to one variable at a time). We will call this technique *the direct $\mathbb{Z}$ inverse.* We will get back to this in §5.2.

On the other hand, we can also simplify the inverse problem and invert what we call the *associated $\mathbb{Z}$-transform* which yields some advantages when compared to the direct inversion (see the discussion in §5.2).

3.1. The *associated* $\mathbb{Z}$-transform.

Assume with no loss of generality that $y \in \mathbb{Z}^m$ is such that $y_1 \neq 0$. We may also suppose (without lost of generality) that each y_i is a multiple of y_1 (taking 0 to be multiple of any other integer). Otherwise, we just need to multiply each constraint $(Ax)_i = y_i$ by $y_1 \neq 0$ when $i = 2, 3, \dots, m$, so that the new matrix A and vector y still have entries in $\mathbb{Z}$.

Hence, there exists a vector $D \in \mathbb{Z}^m$ with first entry $D_1 = 1$ and such that $y = Dy_1$. Notice that D may have entries equal to zero or even negative, but not the first one. The inversion problem is thus reduced to evaluate, at the point $t := y_1$, the function $g : \mathbb{Z} \to \mathbb{N}$ defined by

$$g(t) := f(Dt) = \frac{1}{(2\pi i)^m} \int_{|z_m|=w_m} \cdots \int_{|z_1|=w_1} \mathcal{F}(z) z^{Dt - e_m} dz, \tag{3.1}$$

where $\mathcal{F}$ is given in (2.9), $e_m := (1, 1, \cdots)$ is the unit vector in $\mathbb{R}^m$ and the real (fixed) vector $w \in \mathbb{R}_+^m$ satisfies $A' \ln(w) > c$. The following technique permits us to calculate (3.1).

3.2. **Calculating integrals by residues.** One of the easiest ways of calculating (3.3) and (3.4) is to use Cauchy's Residue Theorem. In our context, we have to use this theorem at each of the m one-dimensional integration steps. We are going to see (cf. example in §4 below) that we have to integrate several times (at each step and along a circle $|z| = w$) a rational function of the following kind:

$$R(z) = \frac{\alpha_0 + \alpha_1 z + \ldots + \alpha_{o_1} z^{o_1}}{\prod_{k=1}^{o_2} (z^{d_k} - \beta_k)^{\delta_k}}, \tag{3.7}$$

where each d_k and δ_k are positive integers. This rational function can obviously be re-written as follows:

$$R(z) = \frac{\alpha_0 + \alpha_1 z + \ldots + \alpha_{o_1} z^{o_1}}{\prod_{k=1}^{o_3} (z - \beta_k^*)^{\eta_k}}, \tag{3.8}$$

where each η_k is a positive integer and the coefficients β_k^* are pairwise distinct. We can integrate (3.8) by using Cauchy 's Residue Theorem, which can be done in several ways, for instance, by the three different techniques (a), (b) and (c) proposed below.

(a) One way to proceed is as follows. Suppose that $w > 0$ and $|\beta_k^*| \neq w$ for $k = 1, 2, \ldots, o_3$. Then

$$\frac{1}{2\pi i} \int_{|z|=w} R(z)\, dz = \sum_{|\beta_k^*|<w} \text{Res } (R, \beta_k^*). \tag{3.9}$$

However, calculating residues in (3.9) is not always a simple task, mainly when some η_k is large. Therefore, we next propose an alternative technique.

(b) Consider a real number $w^* > 0$ big enough to ensure $|\beta_k^*| < w^*$ for every $k = 1, 2, \ldots, o_3$. Then

$$\sum_{k=1}^{o_3} \text{Res } (R, \beta_k^*) = \frac{1}{2\pi i} \int_{|z|=w^*} R(z)\, dz = \frac{1}{2\pi i} \int_{|v|=1/w^*} \frac{R(1/v)\, dv}{v^2}.$$

Notice that the change of variable $z = 1/v$ gives us a negative sign in last integral, but this sign gets canceled because we also change the orientation of the integration path. Moreover, the function

$$\frac{R(1/v)}{v^2} = \frac{\alpha_0 v^{o_1} + \alpha_1 v^{o_1 - 1} + \ldots + \alpha_{o_1}}{v^{o_4} \prod_{k=1}^{o_3} (1 - v\beta_k)^{\eta_k}}, \tag{3.10}$$

$$o_4 = 2 + o_1 - (\eta_1 + \eta_2 + \ldots + \eta_{o_3}), \tag{3.11}$$

is analytic inside the circle $|v| = 1/w^*$ when $o_4 \leq 0$ because $|\beta_k^*| < w^*$ for every $k = 1, 2, \ldots, o_3$. Hence:

$$\sum_{k=1}^{o_3} \text{Res } (R, \beta_k^*) = \begin{cases} 0 & \text{if } o_4 \leq 0, \\ \alpha_{o_1} & \text{if } o_4 = 1. \end{cases}$$

We may not wish calculate the above sum when $o_4 \geq 2$, because it can become too complicated; namely, we have to calculate the $(o_4 - 1)$ derivative of $R(1/v)v^{o_4 - 2}$, and it is obviously prohibitive for large o_4. On the other

and by Theorem 2.2, we have to calculate the inverse $\mathbb{Z}$-transform of :

$$\mathcal{F} = \frac{z_1 z_2 z_3}{(z_1-1)(z_2-1)(z_3-1)(1-z_1^{-1}z_2^2 z_3^{-2})(1-z_1^{-1}z_2^{-2}z_3)}, \tag{4.1}$$

where

$$\begin{cases} |z_j| > 1 \text{ for } j = 1,2,3, \\ |z_1 z_2^{-2} z_3^2| > 1, \\ |z_1 z_2^2 z_3^{-1}| > 1. \end{cases} \tag{4.2}$$

We wish to work with rational functions whose denominator's degree is the smallest possible, so we are going to fix $z_1 = p/(z_2 z_3)$ and divide by $z_2 z_3$ (see 3.2) because z_1 has the exponents with smallest absolute value.

$$\widehat{\mathcal{F}} = \frac{z_3 p^2}{(z_2^{-1}p - z_3)(z_2-1)(z_3-1)(z_3 - z_2^3 p^{-1})(z_2 p - z_3^2)},$$

where

$$\begin{cases} |p| > |z_2 z_3|, \\ |z_3 p| > |z_2^3| > 1, \\ |z_2 p| > |z_3^2| > 1. \end{cases}$$

Notice that $z_2^* = z_3^* = 2$ and $p^* = 5$ is a solution of the previous system of inequalities. We are going to calculate (3.3) and (3.4) by fixing $w_2 = z_2^*$, $w_3 = z_3^*$ and $d = p^*$. Let us integrate $\widehat{\mathcal{F}}$ along the circle $|z_3| = z_3^*$ with a positive orientation. It is easy to see that (taking $p := p^*$ and $z_2 := z_2^*$ constant) $\widehat{\mathcal{F}}$ has two poles located on the circle of radius $|z_2 p|^{1/2} > z_3^*$, and three poles located on the circles of radii $1 < z_3^*$, $|z_2^{-1}p| > z_3^*$ and $|z_2^3 p^{-1}| < z_3^*$. Whence, we can consider poles inside the circle $|z_3| = z_3^*$, in order to avoid analyzing the pole $z_3 := (z_2 p)^{1/2}$ with fractional exponent. This yields

$$I_1(p, z_2) = \frac{z_2 p^2}{(p - z_2)(z_2 - 1)(p - z_2^3)(z_2 - p^{-1})} \tag{4.3}$$

$$+ \frac{z_2^3 p^5}{(p^2 - z_2^4)(z_2 - 1)(z_2^3 - p)(p^3 - z_2^5)}. \tag{4.4}$$

Next, we integrate I_1 along the circle $|z_2| = z_2^*$. Taking $p := p^*$ as a constant, the first term of I_1 has poles on circles of radii $|p| > z_2^*$, $1 < z_2^*$, $|p|^{1/3} < z_2^*$ and $|p|^{-1} < z_2^*$. We consider poles outside the circle $|z_2| = z_2^*$, in order to avoid analysing the pole $z_2 := p^{1/3}$ (recall equation (3.12)). We obtain

$$\frac{-p^3}{(p-1)(p^2-1)^2}.$$

The second term of I_1 has poles on circles of radii $|p|^{1/2} > z_2^*$, $1 < z_2^*$, $|p|^{1/3} < z_2^*$ and $|p|^{3/5} > z_2^*$. Notice that we have poles with fractional exponents inside and outside the integration path $|z_2| = z_2^*$, so we use equation

Therefore, $\Omega_1(12te_3)$ is the t-dilated polytope of $\Omega_1(12e_3)$ and $\tilde{g}(t) := g(12t)$ with $g(t)$ as in (4.5), is thus the Ehrhart polynomial of $\Omega_1(12e_3)$ (see Ehrhart [10], Barvinok and Pommersheim [3]). We obtain

$$\tilde{g}(t) = 51t^2 + 11t + 1, \tag{4.6}$$

and indeed, 51 is the volume of $\Omega_1(12e_3)$ and the constant term is 1 as it should be (see the discussion in §4.6).

5. A GENERAL ALGORITHM

We here describe a general algorithm, and in fact, two variants. The first one is via the inversion of the associated $\mathbb{Z}$-transform whereas the second one is the direct inversion of the $\mathbb{Z}$-transform.

5.1. The inverse associated $\mathbb{Z}$-transform algorithm.

5.1.1. *Sketch of the algorithm.* We want to calculate the inverse $\mathbb{Z}$-transform f of an analytic function $\mathcal{F}$ which is well defined on the open domain

$$E_1 = \left\{(z_k := \beta_k e^{i\theta_k}) \in \mathbb{C}^m \mid \beta, \theta \in \mathbb{R}^m,\ A' \ln(\beta) > c\right\};$$

see (2.9), (2.10) and (2.11). Moreover, we simplify our problem of calculating $f(y)$ with $y \in \mathbb{Z}^m$ by supposing, let us say, that $y_1 \neq 0$ divides every other entry y_j. That is, $y = Dy_1$ where the first entry of the vector $D \in \mathbb{Z}^m$ is equal to one. Then, we calculate the associated $\mathbb{Z}$-transform $\widehat{\mathcal{F}}$ by doing the change of variable $p = z^D$ and dividing by $z_2 z_3 \cdots z_m$, as in (3.2). From this change of variable we can deduce that

$$\widehat{\mathcal{F}}(z_2, z_3, \ldots, z_m, p) \text{ is well defined on a domain } E_2 \subset \mathbb{C}^m.$$

The algorithm consists of

- $m-1$ intermediate steps to compute $\mathcal{G}(p)$ in (3.4) by successive one-dimensional integrations w.r.t. $z_2, z_3, \ldots, z_m$, respectively, using either equation (3.9), or (3.12), or (3.14) (cf. (a), (b) and (c) in §3.2).

- a final step to integrate $\mathcal{G}(p)$ in (3.3) (integration w.r.t. p).

We obviously fix a real vector $(w_2, w_3, \ldots, w_m, d) \in E_2 \cap \mathbb{R}^m$ in order to compute previous integrals; it is easy to see that $E_2 \cap \mathbb{R}^m \neq \emptyset$ from the definition (3.5) of E_2.

Of course, at each step, we want to use among the equations (3.9), (3.12) and (3.14), the less time consuming one. That is, we first try (3.9) or (3.12) and rather choose to use (3.14) if we have to deal with fractional exponents (recall that Cauchy 's Residue Theorem cannot be applied to non-analytic functions).

As for the associated $\mathbb{Z}$ inverse algorithm of §5.1, the algorithm consists of m successive steps to compute (2.11), where step k is a one-dimensional integration w.r.t. z_k, for all $k = 1, \ldots, m$.

In order to integrate $\mathcal{F}$ in (2.11), we first define the integration path by fixing a real vector $(w_1, w_2, \ldots, w_m) \in E_1 \cap \mathbb{R}^m$. From the definition (2.10) of E_1 it follows that $E_1 \cap \mathbb{R}^m \neq \emptyset$.

Of course, at each step, we want to use among the equations (3.9), (3.12) and (3.14), the less time consuming one. However, in contrast to the associated transform algorithm, in the present context, equations (3.12) and (3.14) may become really time prohibitive, so we are almost restricted to use only equation (3.9).

Moreover, the function I_s^* obtained in the s-th steep ($1 \leq s < m$) is analytic on $E_1 \cap (\{(w_1, \ldots, w_s)\} \times \mathbb{C}^{m-s})$, because $\mathcal{F}$ is analytic on E_1, and each integration path $|z_j| = w_j$ is a compact circle (cf. §5.1.2). Hence, we add together all terms of I_s^* which have *removable singularities*, where in the present case, *removable singularities* means either poles on the path of integration $|z_{s+1}| = w_{s+1}$ or variables with *fractional* exponent.

We illustrate below this algorithm by analyzing again the convex polytope $\Omega(te_3)$ presented in §4.

Example 5.1. Consider the polytope $\Omega_1(te_3)$ already treated in §4 (with $c = 0$). We have to calculate (2.11) when $\mathcal{F}$ is given by (4.1). Notice that $z_1^* = 3$ and $z_2^* = z_3^* = 2$ is a solution of (4.2), so we are going to integrate (2.11) by fixing $w_1 = 3$ and $w_2 = w_3 = 2$. Let us integrate

$$\mathcal{F}(z)z^{(t-1)e_3} = \frac{z_1^{t+1} z_2^{t+2} z_3^{t+2}}{(z_1 - 1)(z_2 - 1)(z_3 - 1)(z_1 z_3^2 - z_2^2)(z_2^2 - z_1^{-1} z_3)}$$

first along $|z_2| = w_2$. Supposing z_1 and z_3 constant, we have poles located on circles of radii $1 < w_2$, $|z_1^{1/2} z_3| > w_3$ and $|z_1^{-1} z_3|^{1/2} < w_3$. Now, we do not want to consider poles outside the integration path, as in (3.12), because the work required increases with t; see the paragraph just before equation (3.12). Moreover, we do not want to decompose $\mathcal{F}(z)z^{(t-1)e_3}$ into a sum of simple fractions either, as in (3.13), because this expansion is done in time polynomial in the parameter t *as well.* Therefore, we may wish to consider only inside poles (the alternative (c) in §3.2), which yields

$$\begin{aligned} I_1(z_1, z_3) = & \frac{z_1^{t+1} z_3^{t+2}}{(z_1 - 1)(z_3 - 1)(z_1 z_3^2 - 1)(1 - z_1^{-1} z_3)} \\ & + \frac{z_1^{(t+1)/2} z_2^{(3t+5)/2}}{2\,(z_1 - 1)(z_3 - 1)(z_1^{-1/2} z_3^{1/2} - 1)(z_1 z_3^2 - z_1^{-1} z_3)} \\ & - \frac{(-1)^t z_1^{(t+1)/2} z_2^{(3t+5)/2}}{2\,(z_1 - 1)(z_2 - 1)(-z_1^{-1/2} z_3^{1/2} - 1)(z_1 z_3^2 - z_1^{-1} z_3)}. \end{aligned}$$

We cannot work with fractional exponents, for neither $z_1^{1/2}$ nor $z_3^{1/2}$ are analytic at zero, so we adopt the same remedy suggested in §5.1.2, i.e., we

Thus, we have have obtained $g(120)$, that we also compare with the one obtained in (4.5) with $t = 120$, by the inverse associated transform algorithm.

$$\begin{aligned} f(120e_3) &= 6141 - 930 \qquad \text{[by direct inversion]} \\ &= \frac{17 * 120^2}{48} + \frac{41 * 120}{48} + \frac{139}{288} + \frac{120}{16} + \frac{9}{32} + \frac{1}{8} + \frac{1}{9} \text{ [by (4.5)].} \end{aligned}$$

5.2.2. *Which $\mathbb{Z}$-inverse should be used?* As a final comparison between the direct inversion of the $\mathbb{Z}$-transform and the inversion of the associated $\mathbb{Z}$-transform, we can point out the following facts:

i) To compute $f(y)$ for $y \in \mathbb{Z}^m$ via the direct inversion of the $\mathbb{Z}$-transform $\mathcal{F}$, we need not suppose that there exists an entry $y_1 \neq 0$ which divides every other entry. However, for practical efficiency of the algorithm, we are condamned to use the only integration technique (c) in §3.2.

ii) On the other hand, the inversion of the associated $\mathbb{Z}$-transform gives us an explicit formula for $g(t) = f(Dt)$ (under the above restriction on the entries of y). Moreover, it is likely to be more time efficient because at each integration step, and depending on the data on hand, we may choose between the three alternative integration techniques (a), (b) or (c) in §3.2. As a by-product, we also obtain the Ehrhart polynomial of an integer polytope.

5.2.3. *Computational complexity.* We have not succeeded in getting an exact evaluation of the computational complexity of both algorithms (direct inversion and inversion of the associated $\mathbb{Z}$-transform). One important parameter to evaluate this complexity is the total number of poles that are considered at each of the m one-dimensional integration steps.

Basically, it turns out that in the worst case, the number of poles at step k is equal to $\sum_{i_1,\dots i_k} \Delta^{1,2,\dots k}(i_1 i_2 \dots i_k)$, where

$$\Delta^{1,2,\dots k}(i_1 i_2 \dots i_k) := \det \begin{bmatrix} A_{1i_1} & A_{1i_2} & . & A_{1i_k} \\ A_{2i_1} & A_{2i_2} & . & A_{2i_k} \\ . & . & . & . \\ A_{ki_1} & A_{ki_2} & . & A_{ki_k} \end{bmatrix}, \tag{5.1}$$

where $i_j \in \{1, \dots n\}$ and the i_j's are pairwise distinct. Therefore, as we have at most $\binom{n}{k}$ such determinants, we roughly have at most $O(Kn^k)$ poles with $K := \max_{i_1,\dots i_k} |\Delta^{1,2,\dots k}(i_1 i_2 \dots i_k)|$ (which is a polynomial in the data). Therefore, the total number of poles is $O(Mn^m)$ with M a polynomial in the data (exponential in the input size in computational complexity terminology). We also must evaluate the total work required in the integration techniques (a), (b) or (c) in §3.2, which is difficult because it involves expansions in fractions. Moreover, the extra work required for the eventual derivations needed in case of multiple poles may become complex very quickly. However, it is worth noticing that a careful choice of the vector c permits to

Integrating with respect to z_1, we obtain

$$\frac{1}{2\pi i}\int_{|z_1|=w_1} \widetilde{F}(z)z^{y-\mathrm{e}_m}dz_1 \;=\; \sum_{k=1}^{n}\sum_{j=1}^{A_{1k}-1} Q_{kj}\times$$
$$z_2^{y_2-A_{2k}x_0-1}\cdots z_m^{y_m-A_{mk}x_0-1}\begin{cases} \mathrm{e}^{d_k x_0} & \text{if } x_0=\frac{y-j}{A_{jk}}\in\mathbb{N}\\ 0 & \text{otherwise.}\end{cases}$$

Notice that each Q_{jk} is a real-valued rational fraction of the variables $z_2, z_3, \ldots z_n$. Therefore, we can write them as

$$Q_{jk} \;=\; P(z_2^{-1})\prod_{i=1}^{o_{jk}}\left(1-z_2^{-\alpha_i}\beta_i\right)^{-1},$$

where P is a real-valued polynomial of z_2^{-1}, each $\alpha_i\in\mathbb{N}$ and each β_i is constant with respect to z_2 and a real-valued rational function of variables $z_3, z_4, \ldots z_n$.

Thus, as we already did for z_1, we can choose again a vector $d\in B(c,r)$ such that Q_{jk} has a decomposition as in (6.3), and repeat the same procedure until we obtain the value of $\widetilde{f}(y)$ for some vector $d\in\mathbb{R}^n$ close enough to c.

7. An alternative method

In this section we propose an alternative method which avoids complex integration and is purely algebraic. It is particularly attractive for small values of m.

7.1. **The method.** With $e_m=(1,1,\ldots)$ and doing the change of variables $z=p^{-e_m}$ in the functions (2.8) and (2.9), we obtain

$$\mathcal{F}(p^{-e_m}) \;=\; \sum_{y\in\mathbb{Z}^m} f(y)p^y \;=\; \prod_{k=1}^{n}\left[\frac{1}{1-\mathrm{e}^{c_k}p_1^{A_{1k}}p_2^{A_{2k}}\cdots p_m^{A_{mk}}}\right]. \tag{7.1}$$

Partition the matrix $A\in\mathbb{Z}^{m\times n}$ into its positive and negative parts $A^+, A^-\in\mathbb{N}^{m\times n}$, defined by

$$A^+_{ij} \;:=\; \begin{cases} A_{ij} & \text{if } A_{ij}\geq 0,\\ 0 & \text{otherwise,}\end{cases} \qquad \text{and} \qquad A^- \;:=\; A^+ - A.$$

The notation A_k stands for the k-th column of A for all $k=1,\ldots,n$. The same notation A^+_k and A^-_k applies to A^+ and A^- respectively. Besides, recall that $p^{A^+_k}=p_1^{A^+_{1k}}\cdots p_m^{A^+_{mk}}$ as in (2.1). Hence, we can rewrite $\mathcal{F}$ as

$$\mathcal{F}(p^{-e_m}) \;=\; \prod_{k=1}^{n}\left[\frac{p^{A^-_k}}{p^{A^-_k}-\mathrm{e}^{c_k}p^{A^+_k}}\right]. \tag{7.2}$$

In order to simplify the exposition, we make the following weak assumption.

Notice that $|e^{c_k} p^{A_k}| < 1$ for $k = 1, \ldots, n$, because of (2.10) and $p = z^{-e_m}$, so that we have the expansion

$$\prod_{k=j_1,\ldots,j_m} \frac{1}{1 - e^{c_k} p^{A_k}} = \sum_{x \in \mathbb{Z}^m} \prod_{k=1}^{m} e^{c_{j_k} x_k} p^{A_{(j_k)} x_k}.$$

Moreover, writing

$$Q_{j_1 \ldots j_m}(p) = \sum_{\beta \in \mathbb{N}^m, \beta \leq M} Q^{(\beta)}_{j_1 \ldots j_m} p^{\beta},$$

for some constant bound $M \in \mathbb{N}^m$, we get that

$$\mathcal{F}(p^{-e_m}) = \sum_{1 \leq j_1 < \ldots < j_m \leq n} \sum_{\substack{\beta \in \mathbb{N}^m, \\ \beta \leq M}} \sum_{x \in \mathbb{N}^m} Q^{(\beta)}_{j_1 \ldots j_m} \times e^{\sum_k c_{j_k} x_k} \, p^{\beta + B(j_1 \ldots j_m) + A(j_1 \ldots j_m) x}, \tag{7.4}$$

with the square submatrices

$$A(j_1 \ldots j_m) := [A_{(j_1)} | A_{(j_2)} | \cdots | A_{(j_m)}]$$

for all $1 \leq j_1 < j_2 \ldots < j_m \leq n$.

Finally, notice that the sums in equations (7.1) and (7.4) are equal. Hence, if we want to deduce the exact value of $f(y)$ from equation (7.4), we only have to sum up all the terms for which the exponent $\beta + B(j_1 \ldots j_m) + A(j_1 \ldots j_m)x$ is equal to y. That is, given the condition

$$\beta_x := y - B(j_1 \ldots j_m) - A(j_1 \ldots j_m) x \in [0, M]^m, \tag{7.5}$$

we have

$$f(y) = \sum_{1 \leq j_1 < \ldots < j_m \leq n} \sum_{x \in \mathbb{N}^m} Q^{(\beta_x)}_{j_1 \ldots j_m} \begin{cases} e^{\sum_k c_{j_k} x_k} & \text{if (7.5) holds,} \\ 0 & \text{otherwise.} \end{cases} \tag{7.6}$$

Moreover, with the additional assumption that all the square submatrices $A(j_1 \ldots j_m)$ are non-singular, (7.6) simplifies, that is, considering the condition :

$$x_\beta := A(j_1 \ldots j_m)^{-1} [y - \beta - B(j_1 \ldots j_m)] \in \mathbb{N}^m, \tag{7.7}$$

we now have

$$f(y) = \sum_{1 \leq j_1 < \ldots < j_m \leq n} \sum_{\substack{\beta \in \mathbb{N}^m, \\ \beta \leq M}} Q^{(\beta)}_{j_1 \ldots j_m} \begin{cases} e^{\sum_k c_{j_k} [x_\beta]_k} & \text{if (7.7) holds,} \\ 0 & \text{otherwise.} \end{cases} \tag{7.8}$$

Example 7.2. Consider the matrices $A = \binom{1,2,1}{2,1,1}$ in $\mathbb{R}^{2 \times 3}$, $c = \ln(2)(1,1,1)$ in $\mathbb{R}^3$, and the convex polytope

$$\Omega(b) := \{x \in \mathbb{R}^3 \mid x_1 + 2x_2 + x_3 = b_1, \quad 2x_1 + x_2 + x_3 = b_2, \quad x \geq 0\}.$$

We obtain

$$\mathcal{F}(p^{-e_3}) = \frac{1}{(1 - 2p_1 p_2^2)(1 - 2p_1^2 p_2)(1 - 2p_1 p_2)},$$

8. Conclusion

We have presented an algorithm (in fact, three) for computing the number of nonnegative integral points in a convex rational polytope $\{x \in \mathbb{R}^n_+ \mid Ax \leq b\}$. They are all based on the inversion of some $\mathbb{Z}$-transform by means of residues. In contrast to the algorithm proposed by Barvinok [3] which works in the space $\mathbb{R}^n$ of *primal* variables x, we rather work in the space $\mathbb{R}^m$ of *dual* variables z associated with the m nontrivial constraints $Ax = b$. In addition, we need *not* know the vertices of the polytope explicitly. As such, it provides an alternative method. Despite we have not completely characterized the computational complexity of the algorithm, it might work for potentially large values of n and relatively small values of m, a context "dual" to that of Barvinok's algorithm which is polynomial in the problem size for *fixed* dimension n. Finally the (algebraic) alternative approach described in §7 does not use residues "directly" and is particularly attractive for relatively small values of m.

References

[1] W. Baldoni-Silva, M. Vergne. Residues formulae for volumes and Ehrhart polynomials of convex polytopes, arXiv:math.CO/0103097 v1, (2001).

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

[3] A.I. Barvinok, J.E. Pommersheim. An algorithmic theory of lattice points in polyhedra, in *New Perspectives in Algebraic Combinatorics*, MSRI Publications **38** (1999), 91–147.

[4] M. Beck. Multidimensional Ehrhart reciprocity, *J. Comb. Theory Ser. A* **97** (2002), 187–194.

[5] M. Beck. Counting Lattice Points by means of the Residue Theorem. *Ramanujan Journal* **4** (2000), 399–310.

[6] M. Beck, R. Diaz and S. Robins. The Frobenius problem, rational polytopes, and Fourier-Dedekind sums, *J. Numb. Theor.*, to appear.

[7] M. Brion. Points entiers dans les polyèdres convexes, *Ann. Ecol. Norm. Sup. (Sér. 4)* **21** (1988), 653–663.

[8] M. Brion, M. Vergne. Residue formulae, vector partition functions and lattice points in rational polytopes, *J. Amer. Math. Soc.* **10** (1997), 797–833.

[9] J.B. Conway. *Functions of a complex variable I*, 2nd ed., Springer, New York, (1978).

[10] E. Ehrhart. Sur un problème de géométrie diophantienne linéaire II, *J. Reine Angew. Math.* **227** (1967), 25–49.

[11] J.-B. Hiriart-Urruty, C. Lemarechal. *Convex Analysis and Minimization Algorithms I*, Springer-Verlag, Berlin, 1993.

[12] J-M. Kantor, A, Khovanskii. Une application du théorème de Riemann-Roch combinatoire au polynôme d'Ehrhart des polytopes entiers, *C.R. Acad. Sci. Paris (Série I)* **317** (1993), 501–507.

[13] A. Khovanskii, A. Pukhlikov. A Riemann-Roch theorem for integrals and sums of quasipolynomials over virtual polytopes, *St-Petersburg Math. J.* **4** (1993), 789–812.

[14] J. Kollár. Sharp effective Nullstellensatz, *J. Am. Math. Soc.* **1** (1988), 963–975.

[15] J.B. Lasserre, E.S. Zeron. A Laplace transform algorithm for the volume of a convex polytope, *J. ACM* **48** (2001), 1126–1140.