ON COUNTING INTEGRAL POINTS IN A CONVEX RATIONAL POLYTOPE

JEAN B. LASSERRE AND EDUARDO S. ZERON

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 algorithms provides the Ehrhart polynomial of a convex integer polytope \( \Omega \). 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 \( \Omega \) 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 \( \Omega \) 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 (1994), Barvinok and Pommersheim (1999), Beck (2000, 2002), Beck, Diaz and Robins (2002), Brion (1988), Brion and Vergne (1997), Kantor and Khovanskii (1993), and Khovanskii and Pukhlikov (1993). In particular, using generating functions, Brion and Vergne (1997, p. 801) provide generalized residue formulae that yield closed form expressions for \( f(b) \) and further exploit them in Baldoni-Silva and Vergne (2001) for particular cases like flow polytopes. Beck (2000) and Beck, Diaz and Robins (2002) also provide a complete analysis based on residue techniques for the case of a tetrahedron (\( m = 1 \)) and 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 (1994) proposed a conceptual algorithm for rational polytopes with polynomial time computational complexity when the dimension \( n \) is fixed. This algorithm requires knowledge of the vertices \( v \) of \( \Omega \) and uses a special representation due to Brion (1988) of the generating function \( g(c) := \sum_{x \in \Omega \cap \mathbb{Z}^n} c^x \) of the number of integral points in \( \Omega \). Essential in the procedure is the triangulation of certain closed convex cones into unimodular cones (see, e.g., Barvinok and Pommersheim 1999, Theor. 4.4). Alternatively, Brion and Vergne’s formula (1997, p. 801) could also be exploited in this manner. As mentioned in Baldoni-Silva and Vergne (2001), it requires many steps (in particular, one has to build up chambers maximal cones) in a subdivision of a closed convex cone into polyhedral cones (Brion and Vergne 1997).

The approach. The proposed approach is conceptually very simple and does not require explicit knowledge of the vertices of \( \Omega \). Following ideas already developed in, e.g., Beck (2000) and Brion and Vergne (1997), and instead of working in the space \( \mathbb{R}^n \) of primal
variables $x_i$, we rather work in the space $\mathbb{C}^n$ of dual variables $z_i$ associated with the $m$ nontrivial constraints that define the polytope (by trivial constraint we mean the nonnegativity constraint $x \geq 0$). Thus, in a sense, this approach might be seen as “dual” to the ones working in $\mathbb{R}^n$. Indeed, one considers the generating function of $f(b)$ instead of the generating function $g(c) := \sum_{c \in \mathbb{N}^n} c^t$, as in Barvinok (1994).

We consider the (multidimensional) $\mathbb{Z}$-transform $\mathcal{F}(z)$ of $f(b)$ (as it appears in Brion and Vergne 1997). The dimension of the complex vectors $z$ is $m$, the number of nontrivial constraints in the half-space description of the polytope.

We do not exploit the general formulae for $f(b)$ (e.g., as provided in Brion and Vergne 1997) but rather evaluate $f(b)$ numerically by computing the inverse $\mathbb{Z}$-transform of $\mathcal{F}$ at point $b$ by $m$ (one-dimensional) complex integrations with respect to one variable at a time.

The $m$-dimensional inversion with respect to (w.r.t.) $(z_1, \ldots, z_m)$ is done in $m$ steps, where step $k$ consists of several one-dimensional complex integrations w.r.t. the variable $z_k$. These one-dimensional integrations are performed by repeated application of Cauchy’s Residue Theorem. In fact, we provide two variants of an inversion algorithm and analyze their respective advantages. This approach is similar in spirit to the Laplace transform algorithm in Lasserre and Zeron (2001) for computing the volume of a convex rational polytope. In particular, we provide concrete recipes on several possible ways on how to apply Cauchy’s Residue Theorem as efficiently as possible.

In addition, and as a by-product, one of the two algorithms that we propose provides the Ehrhart polynomial of $\Omega$ for an integer polytope $\Omega$. We also briefly describe an approximation procedure with no occurrence of multiple poles all along the (therefore simplified) integration process.

Finally, we consider an alternative method still based on the $\mathbb{Z}$-transform $\mathcal{F}(z)$ but which avoids its complex integration. It is purely algebraic and uses the Hilbert Nullstellensatz to provide a special decomposition of the $\mathbb{Z}$-transform of $f(b)$ into certain partial fractions. As the integration of 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 1974 and Kollár 1988). 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 analyze 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 $c^t$ and $A^t$ 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

\begin{align}
(2.1) & \quad z^u := z_1^{u_1} z_2^{u_2} \cdots z_m^{u_m}, \\
(2.2) & \quad \ln(z) := [\ln(z_1), \ln(z_2), \ldots, \ln(z_m)].
\end{align}

As mentioned in the introduction, we consider the convex polytope

\begin{equation}
(2.3) \quad \Omega(y) = \{x \in \mathbb{R}^n \mid Ax = y; x \geq 0\},
\end{equation}
where \( y \in \mathbb{Z}^n \) and \( A \in \mathbb{Z}^{n \times m} \), and we want to compute the number of points \( x \in \mathbb{N}^m \) of \( \Omega(y) \), that is, the cardinality of the set

\[
\mathbb{N}^m \cap \Omega(y).
\]

We will actually calculate the following related function

\[
y \mapsto f(y) := \sum_{x \in \mathbb{N}^m \cap \Omega(y)} \mathbf{e}^x,
\]

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

We trivially have that \( f(y) \) is equal to the cardinality of \( \mathbb{N}^m \cap \Omega(y) \) when \( c = 0 \) (and for more details on \( f(y) \) (with \( c = 0 \)) the reader is referred to Beck 2000). Moreover, as observed in Barvinok and Pommersheim (1999), taking \( c \) very small and rounding \( f(y) \) to the nearest integer (or taking an appropriate residue) will give the number of points \( x \in \mathbb{N}^m \) of \( \Omega(y) \).

Of course, computing the number of points \( x \in \mathbb{N}^m \) of the convex polytope

\[
\Omega_1(y) = \{ x \in \mathbb{R}^m_+ \mid A_1 x \leq y \}
\]

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

Remark 2.1. The set \( \Omega(y) \) in (2.3) is a convex polytope, that is, a compact convex polyhedron, if and only if its recession cone \( \{ x \in \mathbb{R}^m_+ \mid Ax = 0 \} \) is the singleton \( \{0\} \) (see, e.g., Hiriart-Urruty and Lemarechal 1993). By a specialized version of Farkas Lemma due to Carver, the latter is in turn equivalent to stating that the cone

\[
\mathbb{K} := \{ u \in \mathbb{R}^m \mid A'u > 0 \}
\]

is not empty (see, e.g., Schrijver 1986, (33), p. 95).

We want to compute the exact value of \( f(y) \) and as we will see, an appropriate tool to analyze such a function is the \( \mathbb{Z} \)-transform. Thus, the \( m \)-dimensional two-sided \( \mathbb{Z} \)-transform, \( \mathcal{F} : \mathbb{C}^m \rightarrow \mathbb{C} \), of \( f \) is defined by the Laurent series

\[
z \mapsto \mathcal{F}(z) := \sum_{y \in \mathbb{Z}^m} f(y) z^{-y},
\]

with \( z^{-y} \) as in (2.1).

Now let \( e_m = (1, 1, \ldots) \) be the unit vector in \( \mathbb{R}^m \). We have the following result:

Theorem 2.2. Let \( f \) and \( \mathcal{F} \) be as in (2.5) and (2.8) respectively, with \( c \leq A'u_o \) for some \( u_o \in \mathbb{K} \). Then:

\[
\mathcal{F}(z) = \prod_{k=1}^{n} \frac{1}{1 - e^{z_k - A_{1k}} z_2 - A_{2k} z_3 - \cdots - A_{mk} z_m},
\]

on the domain

\[
(|z_1|, |z_2|, \ldots, |z_m|) \in \{ \beta \in \mathbb{R}^m_+ \mid A' \ln(\beta) > c \}.
\]

Moreover, for every \( y \in \mathbb{Z}^n \),

\[
f(y) = \frac{1}{(2\pi i)^m} \int_{|z_1|=w_1} \cdots \int_{|z_m|=w_m} \mathcal{F}(z) z^{-c y} dz,
\]

where the real constant vector \( w \in \mathbb{R}^m_+ \) satisfies \( A' \ln(w) > c \).
PROOF. Apply the definition (2.8) of $\cal F$ to obtain

$$\cal F(z) = \sum_{y \in \mathbb{Z}^n} z^{-y} \left[ \sum_{x \in \mathbb{N}^m} e^{y \cdot x} \right] = \sum_{x \in \mathbb{N}^m} e^{y \cdot x} z^{-(Ax)}.$$ 

On the other hand, notice that

$$e^{y \cdot x} z^{-(Ax)} = \prod_{k=1}^m \left( e^{y \cdot z_k - A_{1k} z_k - A_{2k} z_2 - \ldots - A_{mk} z_m} \right)^{y_k}.$$ 

Hence, the conditions $|z_1^{A_{11}} z_2^{A_{12}} \ldots z_m^{A_{1m}}| > e^{y_k}$ for $k = 1, 2, \ldots, n$, or equivalently, $A'(\ln |z_1|, \ln |z_2|, \ldots, \ln |z_m|) > c$, yields

$$\cal F(z) = \prod_{k=1}^n \sum_{x \in \mathbb{N}^m} e^{y_i z_k - A_{1k} z_k - A_{2k} z_2 - \ldots - A_{mk} z_m} \frac{1}{1 - e^{y_i z_k - A_{1k} z_k - A_{2k} z_2 - \ldots - A_{mk} z_m}}$$

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 than $-1$, 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 $\beta := e^{2\pi i}$). $\square$

3. Inversion of the $\mathbb{Z}$-transform $\cal F$. Theorem 2.2 allows us to compute $f(y)$ for $y \in \mathbb{Z}^n$ via (2.11), that is, by computing the inverse $\mathbb{Z}$-transform of $\cal F(z)$ at the point $y$. Moreover, we can directly calculate (2.11) by using Cauchy’s Residue Theorem because $\cal F(z)$ 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 $y \in \mathbb{Z}^n$ is such that $y_1 \neq 0$. We may also suppose (without loss of generality) that each $y_i$ is a multiple of $y_1$ (taking 0 to be a multiple of any other integer). Otherwise, we just need to multiply each constraint $(Ax)_i = y_i$ by $y_1 \neq 0$, when $i = 2, 3, \ldots, m$, 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. Thus, the inversion problem is reduced to evaluate, at the point $t := y_1$, the function $g : \mathbb{Z} \to \mathbb{N}$ defined by

$$g(t) := f(Dt) = \frac{1}{(2\pi i)^m} \int_{|z_1|=w_1} \cdots \int_{|z_1|=w_1} \cal F(z) z^{D_1-1} dz,$$

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

Consider the following simple change of variables. Let $p = z^D$ and $d = w^p$ in (3.1), so that $z_j = p \prod_{j=2}^m z_j^{D_j}$ and

$$g(t) = \frac{1}{(2\pi i)^m} \int_{|z_1|=w_1} \cdots \int_{|z_1|=w_1} \left[ \int_{|p|=d} p^{t-1} \cal F dp \right] dz_2 \cdots dz_m,$$
where
\begin{equation}
\mathcal{F} = \mathcal{F}\left(p \prod_{j=2}^{m} z_j^{-D_j}, z_2, \ldots, z_m\right) \prod_{j=2}^{m} z_j^{-D_j}.
\end{equation}

We can rewrite \( g(t) \) as follows
\begin{equation}
g(t) = \frac{1}{2\pi i} \int_{|p|=\sigma} p^{t-1} \mathcal{G}(p) \, dp, \quad \text{with}
\end{equation}
\begin{equation}
\mathcal{G}(p) := \frac{1}{2\pi i} \int_{|z|=w_2} \cdots \int_{|z|=w_m} \mathcal{F} \, dz_2 \cdots dz_m,
\end{equation}
and \( \mathcal{G} \) is called the associated \( \mathbb{Z} \)-transform of \( f \) with respect to \( D \).

Recall that \( \mathcal{F}(\hat{z}) \) is well defined on the domain given by conditions (2.10), so the domain of definition of \( \mathcal{F} \) is given by the conditions
\begin{equation}
\left( |p| \prod_{j=2}^{m} |z_j|^{-D_j}, |z_2|, \ldots, |z_m| \right) \in \{ \beta \in \mathbb{R}_+^m \mid \mathbb{A}' \ln(\beta) > c \}.
\end{equation}

### 3.1.1. The Ehrhart polynomial.
Consider the convex polytope \( \Omega_1(y) \) defined in (2.6) with \( y = D \) and the dilated polytope \( t\Omega_1(D) := \{ tx \mid x \in \Omega_1(D) \} \). Then with \( A := [A_1 | I] \) and \( c := 0 \), consider the function \( t \mapsto g(t) \) defined in (3.1).

When \( \Omega_1(D) \) is an integer polytope (an integer polytope has all its vertices in \( \mathbb{Z}^m \)) then \( g \) is a polynomial in \( t \), that is,
\begin{equation}
g(t) = a_0 t^n + a_{n-1} t^{n-1} + \cdots + a_0,
\end{equation}
with \( a_0 = 1 \) and \( a_n = \text{volume}(\Omega_1(D)) \). It is called the Ehrhart polynomial of \( \Omega_1(D) \) (see, e.g., Barvinok and Pommersheim 1999, and Ehrhart 1967).

On the other hand, if \( \Omega_1(D) \) is not an integer polytope (i.e., \( \Omega_1(D) \) has rational vertices), then the function \( t \mapsto g(t) \) is a quasipolynomial, that is, a polynomial in the variable \( t \) as in (3.6), but now with coefficients \( \{ a_i(t) \} \) that are periodic functions of \( t \), as in the illustrative example (4.5) below.

### 3.1.2. Inversion of the associated \( \mathbb{Z} \)-transform.
To compute \( g(t) \) we proceed as follows.
- We first compute \( \mathcal{G}(p) \) in (3.4), in \( m-1 \) steps, where each step \( k \) is a one-dimensional integration w.r.t. \( z_k \), \( k = 2, \ldots, m \).
- We then compute \( g(t) \) in (3.3), a one-dimensional integration w.r.t. \( p \).

At each of these steps, the one-dimensional complex integrals are evaluated by Cauchy’s Residue Theorem that we describe in the present context.

### 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) that we have to integrate several times (at each step and along a circle \( |z| = w \)) a rational function of the following kind:
\begin{equation}
R(z) = \frac{\alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n}{\prod_{k=1}^{m} (z - \beta_k)^{\delta_k}},
\end{equation}
where each \( d_k \) and \( \delta_k \) are positive integers. This rational function can obviously be rewritten as follows:
\begin{equation}
R(z) = \frac{\alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n}{\prod_{k=1}^{m} (z - \beta_k)^{\delta_k}}.
\end{equation}
where each \( \eta_k \) is a positive integer and the coefficients \( \beta_k^* \) are pairwise distinct. We can integrate (3.8) by using Cauchy’s Residue Theorem, which can be done in several ways, 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

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

However, calculating residues in (3.9) is not always a simple task, mainly when some \( \eta_k \) 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

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

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

\[
(3.11) \quad \frac{R(1/v)}{v^2} = \frac{\alpha_1 v^{\eta_1} + \alpha_2 v^{\eta_2 - 1} + \cdots + \alpha_o v^{\eta_o}}{v^{o_3} \prod_{k=1}^{o_3} (1 - v\beta_k)^{\eta_k}},
\]

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

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

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 hand, combining the above sum with (3.9) allows us to calculate the integral of \( R \) along the circle \( |z| = w \) by considering residues of poles outside the integration path. Recall that \( o_4 \leq 1 \) is given by (3.11). Hence,

\[
(3.13) \quad R(z) = Q_0(z) + \sum_{k=1}^{o_3} \frac{Q_k(z)}{(z^{\delta_k} - \beta_k)^{\delta_k}};
\]

where \( Q_0 \) and each \( Q_j \) are polynomials; degree of \( Q_k \) is strictly less than \( d_k \delta_k \) for every \( k = 1, 2, \ldots, o_2 \); and exponents \( d_k \) and \( \delta_k \) are given by (3.7). Previous expansion of \( R \) can be done in time polynomial with respect to its numerator degree, and in time exponential with respect to its denominator degree. On the other hand, we now integrate each term of \( R \) along a circle \( |z| = w \). Suppose that \( |\beta_k| \neq w^{\delta_k} \) for every \( k = 1, 2, \ldots, o_2 \). Notice that
the integral of $Q_\delta(z)$ is equal to zero because it is a polynomial. Moreover, from (3.9) and (3.12), we have that:

$$\int_{|z|=w} \frac{Q_\delta(z)}{(z^{\delta_k} - \beta_k)^{\delta_k}} dz = 0 \quad \text{if } |\beta_k| > w^{\delta_k} \text{ or } \deg(Q_\delta) \leq \delta_k d_k - 2.$$  

Therefore,

$$\frac{1}{2\pi i} \int_{|z|=w} R(z) \frac{dz}{z} = \sum_{|\beta_k| < w^{\delta_k}} (\delta_k d_k - 1)-\text{coefficient of } Q_\delta,$$

where each $Q_\delta$ is given by (3.13) and we suppose that the $(\delta_k d_k - 1)$-coefficient of $Q_\delta$ is equal to zero if $\deg(Q_\delta) \leq \delta_k d_k - 2$.

Before we outline the algorithm in the general case we briefly illustrate the method on a simple example.

4. Illustrative example. Consider the following convex rational polytope with three $(m=3)$ nontrivial constraints.

$$\Omega_4(te_3) := \{ x \in \mathbb{R}^3_+ \mid x_1 + x_2 \leq t; \ -2x_1 + 2x_2 \leq t \text{ and } 2x_1 - x_2 \leq t \}.$$  

With

$$c = 0, \quad A := \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ -2 & 2 & 0 & 1 & 0 \\ 2 & -1 & 0 & 0 & 1 \end{bmatrix},$$

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

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

where

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

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.

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

where

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

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 $\tilde{\mathcal{F}}$ along the circle $|z_1| = z_1^*$ with a positive orientation. It is easy to see that (taking $p := p^*$ and $z_2 := z_2^*$ constant) $\tilde{\mathcal{F}}$ has two poles located on the circle of radius $|z_3 p|^{1/2} > z_3^*$, and three poles located on the circles of radii $1 < z_3^*$, $|z_2^{-1} p| > z_3^*$ and $|z_3^{-1} p^{-1}| < z_3^*$. Therefore, 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

\begin{equation}
I_1(p, z_2) = \frac{z_2 p^2}{(p - z_2)(z_2 - 1)(p - z_3^*)(z_3^* - p)}.
\end{equation}

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 analyzing the pole $z_2 := p^{1/3}$ (recall Equation (3.12)). We obtain

\begin{equation}\nonumber
\frac{-p^3}{(p - 1)(p^2 - 1)^2}.
\end{equation}

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 (3.14). Expanding the second term of $I_1$ into simple fractions, yields

\begin{align*}
\frac{p^5}{(z_2 - 1)(p^2 - 1)(1 - p)(p^3 - 1)} &+ \frac{(2p^7 + 2p^4 + 3p^3 + p^2 + p)^2}{(z_2 - p)(p - 1)^3(p + 1)^4(p^2 + 1)} \\
&+ \frac{Q_1(z, p) + Q_2(z, p)}{(z_2^* - p^*)^2}.
\end{align*}

Obviously, we only calculate those terms with denominator $(z_2 - 1)$ or $(z_2^* - p)$.

As a result, the associated $\mathcal{Z}$-transform $\mathcal{Z}(p)$ is given by

\begin{equation}\nonumber
\mathcal{Z}(p) = \frac{-p^3}{(p - 1)^3(p + 1)^2} - \frac{p^5}{(p - 1)^3(p + 1)^4(p^3 - 1)} \\
+ \frac{2p^3 + 2p^4 + 3p^3 + p^2 + p}{(p - 1)^3(p + 1)^4(p^2 + 1)}.
\end{equation}

Finally, it remains to integrate $\mathcal{Z}(p)p^{t-1}$ along the circle $|p| = p^*$. Observe that $\mathcal{Z}(p)p^{t-1}$ has poles when $p$ is equal to 1, $-1$, $i = \sqrt{-1}$, $-i$, $\sigma = e^{2\pi i/3}$ and $\bar{\sigma}$. Therefore, for $t \in \mathbb{Z}_+$, we finally obtain

\begin{equation}
(4.5)
g(t) = \frac{17t^2}{48} + \frac{41t}{48} + \frac{139}{288} + \frac{t(-1)^t}{16} + \frac{9(-1)^t}{32} \\
+ \frac{\sqrt{2}}{8} \cos\left(\frac{\pi t}{2} + \frac{\pi}{4}\right) + \frac{2}{9} \cos\left(\frac{2\pi t}{3} + \frac{\pi}{3}\right).
\end{equation}

Notice that we are using the following two identities which can be easily calculated.

\begin{align*}
\sqrt{2} \cos\left(\frac{\pi t}{2} + \frac{\pi}{4}\right) &= \frac{(i - 1)i^l}{2i} + \frac{(i + 1)(-i)^l}{2i}, \\
2 \cos\left(\frac{2\pi t}{3} + \frac{\pi}{3}\right) &= \frac{(\sigma - 1)\sigma^l}{\sigma - \bar{\sigma}} + \frac{(\bar{\sigma} - 1)\bar{\sigma}^l}{\sigma - \bar{\sigma}}.
\end{align*}
It is now easy to count the number \( f(te) = g(t) \) of points \( x \in \mathbb{N}^2 \) of \( \Omega(te) \).

\[
\begin{align*}
f(0) &= 139 + 9 + 1 = 1 \quad 288 + 32 + 8 + 9 = 1, \\
f(e) &= 17 + 4.1 = 1 \quad 48 + 48 + 139 = 1 \quad 16 - 32 - 8 - 9 = 1, \\
f(2e) &= 68 + 82 + 139 = 2 \quad 48 + 288 + 2 + 9 = 1 \quad 32 - 8 + 9 = 4.
\end{align*}
\]

**The Ehrhart polynomial.** Observe that in (4.5) the function \( t \mapsto g(t) \) is a *quasipolynomial* because the linear and constant term have periodic coefficients. However, with \( t = 12 \), one may check that the rational polytope \( \Omega_1(te) \) is, in fact, an *integer* polytope, that is, all its vertices are in \( \mathbb{Z}^n \).

Therefore, \( \Omega_1(12e) \) is the \( t \)-dilated polytope of \( \Omega_1(12e) \) and \( \tilde{g}(t) := g(12t) \) with \( g(t) \) as in (4.5), and is thus the Ehrhart polynomial of \( \Omega_1(12e) \) (see Ehrhart 1967, and Barvinok and Pommersheim 1999). We obtain

\[ \tilde{g}(t) = 51t^2 + 11t + 1, \]

and indeed, \( 51 \) is the volume of \( \Omega_1(12e) \), and the constant term is 1 as it should be (see the discussion in §3.1.1).

**5. A general algorithm.** Here we 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 \( \hat{f} \) which is well-defined on the open domain

\[ E_1 = \{ (z_k := \beta_k e^{i\theta}) \in \mathbb{C}^m \mid \beta \in \mathbb{R}^m, A' \ln(\beta) > c \}. \]

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, that \( y_i \neq 0 \) divides every other entry \( y_j \). That is, \( y = D y_1 \), where the first entry of the vector \( D \in \mathbb{Z}^m \) is equal to one. Then, we calculate the associated \( \mathbb{Z} \)-transform \( \hat{f} \) by doing the change of variable \( p = e^D \) and dividing by \( z_2 z_3 \cdots z_m \), as in (3.2). From this change of variable we can deduce that

\[ \hat{f}(z_2, z_3, \ldots, z_m, p) \text{ is well defined on a domain } E_2 \subset \mathbb{C}^m. \]

The algorithm consists of

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

- a final step to integrate \( \hat{g}(p) \) 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 least time consuming one. That is, we first try (3.9) or (3.12), and choose to use (3.14) if we have to deal with fractional exponents (recall that Cauchy’s Residue Theorem cannot be applied to nonanalytic functions).
5.1.2. Removable singularities. Let us analyze integral (3.4) because it needs some care to handle removable singularities. Suppose we have calculated the following partial integration, $2 \leq s \leq m$,

$$I_s^* = \frac{1}{(2\pi i)^{s-1}} \int_{|z_2|=w_2} \cdots \int_{|z_s|=w_s} \hat{f} \, dz_2 \cdots dz_s.$$ 

$I_s^*$ is analytic on $E_2 \cap ((w_2, \ldots, w_j) \times \mathbb{C}^{m-s+1})$, because $\hat{f}$ is analytic on the open domain $E_2$, and each integration path $|z_i| = w_i$ is a compact circle. However, some care is needed. Had we set $w_2 = w_3 = 2$ and $d = 8$ (instead of $w_2 = w_3 = 2$ and $d = 5$) in the above example, both terms (4.3) and (4.4) of $I_1$ have three poles given by $z_2^3 := p$, exactly on the path of integration (recall that $|z_2| = |p|^{3/5} = 2$). Those poles are called removable singularities because $I_1$ is actually analytic there and we only need to add together both terms of $I_1$.

Fortunately, removable singularities is a pathological case which happens with probability zero in a set of problems with randomly generated data $A \in \mathbb{Z}^{m \times n}$, and this issue could be ignored in practice.

However, for the sake of mathematical rigor, we must provide a solution. This has actually been done already. Indeed, if any term of $I_s^*$ has poles on the integration path $|z_{s+1}| = w_{s+1}$ or $|p| = d$, we only need to add together all terms which have poles there. For example, adding both terms of $I_1$ together, we get

$$I_1(p, z_2) = \frac{p^2 z_2 (p^2 + p^2 z_2^2 - p z_2^3 - z_2^5)}{(p - z_2)(z_2 - 1)(z_2 - p^{-1})(p^2 - z_2^3)(p^3 - z_2^5)}.$$ 

Therefore, taking $p := d$ as a constant, we have that $I_1$ actually has poles only on circles of radii $|p| > w_2$, $1 < w_2$, $|p|^{1/3} < w_2$, $|p|^{1/2} > w_2$, and $|p|^{3/5} > w_2$. We consider poles inside the circle $|z_2| = z_2^*$, getting the associated $\mathbb{Z}$-transform

$$\mathbb{Z}(p) = \frac{p^3 (1 + 2p + p^2 + p^3)}{(p - 1)^2 (p + 1) (p^3 - 1)} - \frac{p^6}{(p - 1)^3 (p + 1)^2 (p^2 + 1)},$$ 

which can be easily checked to be equal to the one obtained above. We need only to move terms around.

5.2. Direct $\mathbb{Z}$ inverse algorithm. We calculated the inverse $\mathbb{Z}$-transform of (4.1) via the associated $\mathbb{Z}$-transform, because it seems to be the easier way. However, we could have computed the integral (2.11) directly. That is, we could have computed the inverse $\mathbb{Z}$-transform (4.1) at the point $y$.

5.2.1. Sketch of the algorithm. In the general case, we want to compute the inverse $\mathbb{Z}$-transform $f$ of an analytic function $\hat{f}$, which is well defined on an open domain $E_1 \subset \mathbb{C}^n$; see (2.9), (2.10), and (2.11).

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 $\hat{f}$ 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 $E_1 \cap \mathbb{R}^m \neq \emptyset$.

At each step, we want to use among the Equations (3.9), (3.12), and (3.14), the least time-consuming one. However, in contrast to the associated transform algorithm, in the present context, Equations (3.12) and (3.14) may become excessively time prohibitive, so we are almost restricted to using only Equation (3.9).

Moreover, the function $I_s^*$ obtained in the $s$th step ($1 \leq s < m$) is analytic on $E_1 \cap ((w_1, \ldots, w_s) \times \mathbb{C}^{m-s})$, because $\hat{f}$ 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 \( I^\ast \) which have removable singularities, where in the present case, removable singularities means either poles on the path of integration \( |z_{e+1}| = w_{e+1} \) or variables with fractional exponent.

We illustrate this algorithm by analyzing again the convex polytope \( \Omega(t e_3) \) presented in §4.

**Example 5.1.** Consider the polytope \( \Omega(1 t e_3) \) 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 \( z_3^* = z_3^3 = 2 \) 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

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

first along \( |z_2| = w_2 \). Supposing \( z_1 \) and \( z_3 \) constant, we have poles located on circles of radii \( 1 < w_2 \), \( |z_2/z_3| > w_3 \) and \( |z_1^{-1} z_3|^{1/2} < w_3 \). 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

\[
I_i(z_1, z_3) = \frac{z_1^{t+1} z_3^{t+2}}{(z_1 - 1) (z_3 - 1) (z_1 z_3^2 - 1) (1 - z_1^{-1} z_3)}
+ \frac{z_1^{(t+1)/2} z_3^{(3t+5)/2} (z_1 z_3^2 - z_1^{-1} z_3)}{2 (z_1 - 1) (z_3 - 1) (z_3 - z_1) (z_1^2 z_3 - 1)}
\]

We cannot work with fractional exponents, for neither \( z_1^{1/2} z_3^{1/2} \) nor \( z_1 z_3^{1/2} \) are analytic at zero, so we adopt the same remedy suggested in §5.1.2, i.e., we add together the last two terms, and we obtain

\[
I_i(z_1, z_3) = \frac{z_1^{t+2} z_3^{t+2}}{(z_1 - 1) (z_3 - 1) (z_1 z_3^2 - 1) (z_1 - z_3)}
+ \frac{z_1^{(t+1)/2} z_3^{(3t+3)/2} Q(z_1, z_3)}{2 (z_1 - 1) (z_3 - 1) (z_3 - z_1) (z_1^2 z_3 - 1)},
\]

where

\[
Q(z_1, z_3) = z_1^{-1/2} z_3^{1/2} + 1 + (z_1^{-1/2} z_3^{-1/2} - 1).
\]

Notice that \( I_i \) has no more fractional exponents, for its second term’s numerator is equal to

\[
\begin{cases}
2 z_1^{t/2} z_3^{t/2} & \text{if } t \text{ is even,} \\
2 z_1^{(t+5)/2} z_3^{(3t+3)/2} & \text{if } t \text{ is odd.}
\end{cases}
\]

To simplify the exposition, we fix the value of \( t \), say \( t = 120 \), for instance. Then

\[
I_i(z_1, z_3) = \frac{z_1^{122} z_3^{122}}{(z_1 - 1) (z_3 - 1) (z_1 z_3^2 - 1) (z_1 - z_3)}
+ \frac{z_1^{62} z_3^{182}}{(z_1 - 1) (z_3 - 1) (z_3 - z_1) (z_1^2 z_3 - 1)}.
\]
We integrate the first term of $I_1$ along $|z_1| = w_1$, so we suppose $z_1 := 2$ constant, and we have poles on circles of radii $1 < w_1$, $|z_2| < w_1$ and $|z_3| < w_1$. We get

$$I(z_3) := \frac{-z_3^{122}}{(z_3 - 1)^2(z_3 + 1)} + \frac{z_3^{120}}{(z_3 - 1)^2(z_3 + 1)(z_3 - 1)} + \frac{z_3^{344}}{(z_3 - 1)^3(z_3 + 1)(z_3 - 1)}.$$

Finally, we integrate $I(z_3)$ along $|z_3| = w_3$. The integral of its second term is equal to zero due to (3.12), whereas the first and third integral yield

$$- \frac{29281}{8} + \frac{1}{8} + \frac{88208}{9} + \frac{1}{9} = 6141.$$

Next, we integrate the second term of $I_1(z_1, z_3)$ along the circle $|z_3| = w_3$, so we have poles on circles of radii $1 < w_3$, $|z_1| > w_3$ and $|z_1^2| < w_3$. This yields

$$I(z_1) := \frac{-z_1^{122}}{(z_1 - 1)^3(z_1 + 1)} + \frac{z_1^{300}}{(z_1 - 1)^2(z_1 + 1)(z_1 - 1)}.$$

Again, the integral of the second term of $I(z_1)$ along $|z_1| = w_1$ is equal to zero due to (3.12), whereas the first term gives us

$$- \frac{7441}{8} + \frac{1}{8} = -930.$$

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

$$f(120e_3) = 6141 - 930 \quad \text{[by direct inversion]}$$

$$= \frac{17 * 120^2}{48} + \frac{41 * 120}{48} + \frac{139}{288} + \frac{120}{16} + \frac{9}{32} + \frac{1}{8} + \frac{1}{9} \quad \text{[by (4.5)].}$$

5.2.2. Which $Z$-inverse should be used? As a final comparison between the direct inversion of the $Z$-transform and the inversion of the associated $Z$-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 $Z$-transform $\mathcal{F}$, we need not suppose that there exists an entry $y_i \neq 0$, which divides every other entry. However, for practical efficiency of the algorithm, we are forced to use the only integration technique (c) in §3.2.

(ii) On the other hand, the inversion of the associated $Z$-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 $Z$-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 $\sum_{i_1, \ldots, i_k} \Delta^{1, 2, \ldots, k}(i_1, i_2, \ldots, i_k)$, where

$$\Delta^{1, 2, \ldots, k}(i_1, i_2, \ldots, i_k) := \det \begin{bmatrix} A_{i_1} & A_{i_2} & \cdots & A_{i_k} \\ A_{2i_1} & A_{2i_2} & \cdots & A_{2i_k} \\ \vdots & \vdots & \ddots & \vdots \\ A_{ki_1} & A_{ki_2} & \cdots & A_{ki_k} \end{bmatrix}.$$
where \( i_j \in \{1, \ldots, n\} \) and the \( i_j \)'s are pairwise distinct. Therefore, as we have at most \( \binom{n}{s} \) such determinants, we roughly have at most \( O(Kn^s) \) poles with the coefficient \( K := \max_{i_1, \ldots, i_s} |\Delta_{1, \ldots, s}(i_1, i_2, \ldots, i_s)| \) (which is a polynomial in the data). Therefore, the total number of poles is \( O(Mn^s) \) 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 avoidance of the occurrence of multiple poles during the integration procedure, as shown in the next section.

6. An approximate inversion of the \( \mathbb{Z} \)-transform. We have seen in §3.2 that the integration procedure can become complex, particularly when multiple poles are encountered at some stage of the algorithm. Fortunately, one may avoid the occurrence of multiple poles by invoking an approximation of the cost function \( c \) in the expression of \( \mathcal{F}(z) \).

The main idea of this algorithm is to calculate an approximate value of (2.5). That is, instead of considering a fixed value of the vector \( c \), we will calculate the inverse \( \mathbb{Z} \)-transform of

\[
\tilde{F}(z) = \prod_{k=1}^{n} \frac{1}{1 - e^{d_k z_1^{-A_{1k}} \cdots z_m^{-A_{mk}}}},
\]

where the vector \( d \) is allowed to lie in an open ball centered at \( c \) and with radius small enough.

In order to simplify the exposition let us assume that every entry of \( A \) is positive. Recall that we are calculating integral in Equation (2.11) along the integration paths \( |z_j| = w_j \), where the fixed vector \( w \in \mathbb{R}^m_+ \) satisfies \( A' \ln(w) > c \). So fix a radius \( r > 0 \), small enough to ensure that \( A' \ln(w) > d \) for every \( d \) in the open ball \( B(c, r) \subset \mathbb{R}^n \). Then, we calculate the integral

\[
\hat{f}(y) = \frac{1}{(2\pi i)^m} \int_{|z_j|=w_1} \cdots \int_{|z_m|=w_m} \tilde{F}(z) z_1^{-r_1} \cdots z_m^{-r_m} \, dz,
\]

by choosing a vector \( d \in B(c, r) \) that makes calculations easier.

For example, we can always choose \( d \in B(c, r) \) in such a way that the real numbers:

\[
|e^{d_k z_2^{-A_{1k}} \cdots z_m^{-A_{mk}}} 1/A_{1k}|, \quad k = 1, \ldots, n
\]

are pairwise distinct. This condition automatically implies that the poles of \( z_1 \mapsto \tilde{F}(z) \) are simple. Moreover, we can calculate the following decomposition:

\[
\tilde{F}(z) = \sum_{k=1}^{n} \frac{Q_k(z_1^{-1})}{1 - e^{d_k z_1^{-A_{1k}} \cdots z_m^{-A_{mk}}}},
\]

for some real-valued polynomials

\[
Q_k(z_1^{-1}) = \sum_{j=1}^{A_{1k}-1} \sum_{j=1}^{A_{jk}-1} Q_{jk} z_1^{-j}, \quad k = 1, \ldots, n,
\]

where each coefficient \( Q_{jk} \) is constant with respect to variable \( z_1 \). Hence,

\[
\tilde{F}(z) = \sum_{k=1}^{n} \sum_{j=1}^{A_{1k}-1} \sum_{x \in \mathbb{N}} Q_{kj} e^{d_k x} z_1^{-j-A_{1k}x} z_2^{-A_{2k}x} \cdots z_m^{-A_{mk}x}.
\]
Integrating with respect to $z_1$, we obtain

$$
\frac{1}{2\pi i} \int_{|z_1|=w_1} \tilde{F}(z)z^{-e_m} \, dz_1
= \sum_{k=1}^{n} \sum_{j=1}^{A_{kk}-1} Q_{kj} z_2^{-A_{kk}x_0-1} \cdots z_m^{-A_{mk}x_0-1} \left\{ \begin{array}{ll}
eq 0 & \text{if } x_0 = (y - j)/A_{kk} \in \mathbb{N} \\
0 & \text{otherwise.} \end{array} \right.
$$

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

$$Q_{jk} = P(z_2^{-1}) \prod_{i=1}^{j} (1 - z_2^{-m} \beta_i)^{-1},$$

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

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 $\tilde{f}(y)$ 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

$$\tilde{F}(p^{-e_m}) = \sum_{y \in \mathbb{Z}^m} f(y)p^y = \prod_{k=1}^{n} \frac{1}{1 - e^{\alpha_k} p_1^{A_{kk}} \cdots p_m^{A_{mk}}}.$$

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

$$A^+_k := \begin{cases} A_{kj} & \text{if } A_{kj} \geq 0, \\ 0 & \text{otherwise,} \end{cases} \quad \text{and} \quad A^- := A^+ - A.$$

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. Recall that $p^{A^+_k} = p_1^{A_{kk}} \cdots p_m^{A_{mk}}$ as in (2.1). Hence, we can rewrite $\tilde{F}$ as

$$\tilde{F}(p^{-e_m}) = \prod_{k=1}^{n} \frac{p^{A^+_k}}{p^{A^-_k} - e^{\alpha_k} p^{A^+_k}}.$$

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

Assumption 7.1. Let $n > m$ and $a := n - m$. The solutions $s \in \mathbb{R}^m$ (whenever they exist) of the $m \choose a$ systems of linear equations

$$(s_1, \ldots, s_m)[A_{(j_1)} | A_{(j_2)} | \cdots | A_{(j_a)}] = (c_{(j_1)}, \ldots, c_{(j_a)}),$$

$1 \leq j_1 < j_2 < \cdots < j_a \leq n$, are pairwise distinct.

Obviously, Assumption 7.1 implies, in particular, that the $m \choose a$ polynomials

$$\prod_{k \neq j_1, \ldots, j_a} (p^{A^+_k} - e^{\alpha_k} p^{A^+_k}), \quad 1 \leq j_1 < j_2 < \cdots < j_m \leq n$$

have no common zero in $\mathbb{C}^m$. 

Therefore, by Hilbert’s Nullstellensatz, there exist \(^a\) real-valued polynomials \(Q_{j_1, \ldots, j_m} \in \mathbb{R}[p_1, \ldots, p_n]\) such that

\[
1 = \sum_{1 \leq j_1 < \cdots < j_m \leq a} Q_{j_1, \ldots, j_m}(p) \prod_{k \neq j_1, \ldots, j_m} (p^{A_{ik}} - e^{\alpha_i} p^{A_{ik}}).
\]

Moreover, bounds on the degree of the \(Q_{j_1, \ldots, j_m}\) are available (see, e.g., Seidenberg 1974 (Theorems 55–57, pp. 296–297) or Kollár 1988). For instance, in our present context, with \(r := \binom{m}{n}\), let \(d_1 \geq d_2 \geq \cdots \geq d_r\) be the degrees of the polynomials

\[
q_{j_1, \ldots, j_m}(p) := \prod_{k \neq j_1, \ldots, j_m} (p^{A_{ik}} - e^{\alpha_i} p^{A_{ik}}), \quad 1 \leq j_1 < \cdots < j_m \leq n.
\]

Then, for all \(1 \leq j_1 < \cdots < j_m \leq n\), the degree of

\[
Q_{j_1, \ldots, j_m}(p)q_{j_1, \ldots, j_m}(p),
\]

in (7.3) is bounded by \(d_1d_2 \cdots d_{m-r}d_r\) (see Kollár 1988).

So one may compute the coefficients of the polynomials \(Q_{j_1, \ldots, j_m}\) by solving a linear system that matches the terms of the same power in both sides of (7.3). In view of the above bound on the degree, this approach is realistic for relatively small values of \(m\) because the size of the resulting linear system grows rapidly with \(m\). Indeed, a real-valued polynomial of degree \(r\) in \(m\) variables may have as many as \(\binom{m+r}{m}\) coefficients.

Multiplying together Equations (7.2) and (7.3), we can deduce that

\[
\mathcal{F}(p^{-\epsilon_n}) = \sum_{1 \leq j_1 < \cdots < j_m \leq a} \frac{Q_{j_1, \ldots, j_m}(p) \prod_{i=1}^p (p^{A_{ik}} - e^{\alpha_i} p^{A_{ik}})}{\prod_{k=1}^n (p^{A_{ik}} - e^{\alpha_i} p^{A_{ik}})}
= \sum_{1 \leq j_1 < \cdots < j_m \leq a} \frac{Q_{j_1, \ldots, j_m}(p) p^{B(j_1, \ldots, j_m)}}{\prod_{k=1}^n (1 - e^{\alpha_i} p^{A_{ik}})},
\]

where

\[
B(j_1 \cdots j_m) := \sum_{k \neq j_1, \ldots, j_m} A_{ik}.
\]

Notice that \(|e^{\alpha_i} p^{A_{ik}}| < 1\) for \(k = 1, \ldots, n\), because of (2.10) and \(p = z^{-\epsilon_n}\), so that we have the expansion

\[
\prod_{k=j_1, \ldots, j_m} \frac{1}{1 - e^{\alpha_i} p^{A_{ik}}} = \sum_{x \in \mathbb{Z}^m} \prod_{k=1}^m e^{\alpha_i} e^{x_k} e^{p^{A_{ik}x_k}}.
\]

Moreover, writing

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

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

\[
\mathcal{F}(p^{-\epsilon_n}) = \sum_{1 \leq j_1 < \cdots < j_m \leq a} \sum_{\beta \in \mathbb{N}^m, \beta \leq M} \sum_{x \in \mathbb{Z}^m} Q_{j_1, \ldots, j_m}^{(\beta)} e^{\sum_{k=1}^m \alpha_i x_k} e^{p^{A_{ik}x_k}}
\]

with the square submatrices

\[
A(j_1 \cdots j_m) := [A_{j_1j_2}] \cdots [A_{j_1j_m}]
\]

for all \(1 \leq j_1 < j_2 \cdots < j_m \leq n\).
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 \( \beta + B(j_1 \cdots j_m) + A(j_1 \cdots j_m)x \) is equal to \( y \). That is, given the condition
\[
(7.5) \quad \beta_x := y - B(j_1 \cdots j_m) - A(j_1 \cdots j_m)x \in [0, M]^n,
\]
we have
\[
(7.6) \quad f(y) = \sum_{1 \leq j_1 \cdots j_m \leq n} \sum_{x \in \mathbb{N}^n} Q^{(\beta)}_{j_1, \ldots, j_m} \left\{ \begin{array}{ll} e^{\sum_i \epsilon_i x_i} \cdot x & \text{if } (7.5) \text{ holds,} \\ 0 & \text{otherwise.} \end{array} \right.
\]
Moreover, with the additional assumption that all the square submatrices \( A(j_1 \cdots j_m) \) are nonsingular, (7.6) simplifies, that is, considering the condition
\[
(7.7) \quad x_\beta := A(j_1 \cdots j_m)^{-1} [y - \beta - B(j_1 \cdots j_m)] \in \mathbb{N}^n,
\]
we now have
\[
(7.8) \quad f(y) = \sum_{1 \leq j_1 \cdots j_m \leq n} \sum_{p \in \mathbb{N}^m} Q^{(\beta)}_{j_1, \ldots, j_m} \left\{ \begin{array}{ll} e^{\sum_i \epsilon_i x_i} \cdot x & \text{if } (7.7) \text{ holds,} \\ 0 & \text{otherwise.} \end{array} \right.
\]

**Example 7.2.** Consider the matrices \( A = \begin{pmatrix} 1 & 2 & 1 \\ 1 & 2 & 1 \end{pmatrix} \) in \( \mathbb{R}^{2 \times 3} \), \( c = \ln(2)(1, 1, 1) \) in \( \mathbb{R}^3 \), and the convex polytope
\[
\Omega(b) := \{ x \in \mathbb{R}^3 | x_1 + 2x_2 + x_3 = b_1, \ 2x_1 + x_2 + x_3 = b_2, \ x \geq 0 \}.
\]
We obtain
\[
\mathcal{F}(p^{-\epsilon}) = \frac{1}{(1 - 2p_1p_2^2)(1 - 2p_1^2p_2)(1 - 2p_1p_2)},
\]
and
\[
1 = Q_{23}(p)(1 - 2p_1p_2^2) + Q_{13}(p)(1 - 2p_1^2p_2) + Q_{12}(z)(1 - 2p_1p_2),
\]
where
\[
Q_{23}(p) = 1 + 2p_1^2p_2, \quad Q_{13}(p) = 1 + 2p_1p_2^2 \quad \text{and} \quad Q_{12}(p) = -(1 + 2p_1p_2 + 4p_1^2p_2^2).
\]
Hence,
\[
f(y) = \sum_{A \in \mathbb{N}^3} 2^{y_1 + y_2 + y_3}
\]
\[
= \begin{cases} 2^{y_2} & \text{if } y_1 - y_2 \geq 0 \text{ and } 2y_2 - y_1 \geq 0 \\ 0 & \text{otherwise} \end{cases}
\]
\[
+ \begin{cases} 2^{y_1} & \text{if } y_1 - y_2 - 1 \geq 0 \text{ and } 2y_2 - y_1 \geq 0 \\ 0 & \text{otherwise} \end{cases}
\]
\[
+ \begin{cases} 2^{y_2} & \text{if } y_2 - y_1 \geq 0 \text{ and } 2y_1 - y_2 \geq 0 \\ 0 & \text{otherwise} \end{cases}
\]
\[
+ \begin{cases} 2^{y_1} & \text{if } y_2 - y_1 - 1 \geq 0 \text{ and } 2y_1 - y_2 \geq 0 \\ 0 & \text{otherwise} \end{cases}
\]
\[
- \begin{cases} 2^{(y_1 + y_2)/3} & \text{if } (2y_2 - y_1)/3 \in \mathbb{N} \text{ and } (2y_1 - y_2)/3 \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}
\]
Moreover, once the Cauchy’s Residue Theorem but where all calculations for \( b \) depend on \( b \) are useless for another \( b' \neq b \).

\[
- \begin{cases}
2^{(y_1+y_2+5)/3} & \text{if } (2y_2 - y_1 + 1)/3 \in \mathbb{N} \text{ and } (2y_1 - y_2 + 1)/3 \in \mathbb{N} \\
0 & \text{otherwise}
\end{cases}
- \begin{cases}
2^{(y_2+y_2+10)/3} & \text{if } (2y_2 - y_1 + 2)/3 \in \mathbb{N} \text{ and } (2y_1 - y_2 + 2)/3 \in \mathbb{N} \\
0 & \text{otherwise}.
\end{cases}
\]

7.2. Discussion. It worth noticing that in this approach, most of the computational effort is concentrated on the determination of the coefficients of the polynomials \( Q_{j_1,\ldots,j_n} \) in the Hilbert Nullstellensatz decomposition (7.3), which does not depend on the right-hand-side \( b \) of \( Ax = b \); indeed \( b \) is only involved in the final (and easy) evaluation (7.7)–(7.8). Moreover, once the \( Q_{j_1,\ldots,j_n} \) are calculated by solving a linear system, one may evaluate \( f(b) \) for any value of \( b \) at a cheap cost (like Brion and Vergne’s 1997 formula which is valid for all \( b \) in the same chamber). As already mentioned, this approach is particularly attractive for relatively small values of \( m \), otherwise the linear system to solve is too large.

At this stage, it is not clear whether this general method whose main work does not depend on \( b \) is preferable to the more specific associated \( \mathbb{Z} \)-inverse method that relies on Cauchy’s Residue Theorem but where all calculations for \( b \) are useless for another \( b' \neq b \).

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 (1994) 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 the fact that 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 \( m \).

Acknowledgment. The authors thank the anonymous referees for their many remarks that have been very helpful in writing this final version. Research for this paper was partially supported by the ECOS-Nord (France)-ANUIES (México) Educational and Scientific Cooperation Program PM98M02 and by CNR-CONACYT Grant 15059 (México).

References


