COEFFICIENTS OF SYLVESTER'S DENUMERANT

V. BALDONI, N. BERLINE, J. A. DE LOERA, B. E. DUTRA, M. KÖPPE, AND M. VERGNE

ABSTRACT. For a given sequence $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, , \alpha_{N+1}]$ of $N+1$ positive integers, we consider the combinatorial function $E(\boldsymbol{\alpha})(t)$ that counts the nonnegative integer solutions of the equation $\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_N x_N + \alpha_{N+1} x_{N+1} = t$, where the right-hand side t is a varying nonnegative integer. It is well-known that $E(\boldsymbol{\alpha})(t)$ is a quasi-polynomial function in the variable t of degree N. In combinatorial number theory this function is known as Sylvester's *denumerant*.

Our main result is a new algorithm that, for every fixed number k, computes in polynomial time the highest $k+1$ coefficients of the quasi-polynomial $E(\boldsymbol{\alpha})(t)$ as *step polynomials* of t (a simpler and more explicit representation). Our algorithm is a consequence of a nice poset structure on the poles of the associated rational generating function for $E(\boldsymbol{\alpha})(t)$ and the geometric reinterpretation of some rational generating functions in terms of lattice points in polyhedral cones. Our algorithm also uses Barvinok's fundamental fast decomposition of a polyhedral cone into unimodular cones. This paper also presents a simple algorithm to predict the first truly periodic coefficient and concludes with a report of several computational experiments using an implementation of our algorithm in `LattE integrale`. We compare it with various `Maple` softwares for partial or full computation of the denumerant.

1. Introduction

Let $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_N, \alpha_{N+1}]$ be a sequence of positive integers. If t is a non-negative integer, we denote by $E(\boldsymbol{\alpha})(t)$ the number of solutions in nonnegative integers of the equation $\sum_{i=1}^{N+1} \alpha_i x_i = t$. In other words, $E(\boldsymbol{\alpha})(t)$ is the same as the number of partitions of the number t using the parts $\alpha_1, \alpha_2, \ldots, \alpha_N, \alpha_{N+1}$ (with repetitions allowed). This paper presents a new algorithm to compute individual coefficients of this function and uncovers new structure in generating functions that allows to compute their periodicity. Let us begin with some background and history before stating the precise results:

The combinatorial function $E(\boldsymbol{\alpha})(t)$ was called by J. Sylvester the *denumerant*. The denumerant $E(\boldsymbol{\alpha})(t)$ has a beautiful structure: it has been known since the times of Cayley and Sylvester that $E(\boldsymbol{\alpha})(t)$ is in fact a *quasi-polynomial*, i.e., it can be written in the form $E(\boldsymbol{\alpha})(t) = \sum_{i=0}^{N} E_i(t) t^i$, where $E_i(t)$ is a periodic function of t (a more precise description of the periods of the coefficients $E_i(t)$ will be given later). In other words, there exists a positive integer Q such that for t in the coset $q + Q\mathbb{Z}$, the function $E(\boldsymbol{\alpha})(t)$ coincides with a polynomial function of t. The study of the coefficients $E_i(t)$, in particular determining their periodicity, is a problem that has occupied various authors and it is the key focus of our investigations here.

Sylvester and Cayley first showed that the function can be written in the form $A(t)+U(t)$, where $A(t)$ is a polynomial in t of degree N and $U(t)$ is a periodic function of period the least common multiple of $\alpha_1, \ldots, \alpha_r$ (see [10, 11] and references therein). In 1943, E.T. Bell gave a

Key words and phrases. Denumerants, Ehrhart quasi-polynomials, restricted partitions, asymptotic behavior, polynomial-time algorithms.

simpler proof and remarked that the period Q is in the worst case given by the least common multiple of the α_i, but in general it can be smaller. A classical observation that goes back to I. Schur is that when the list $\boldsymbol{\alpha}$ consist of relatively prime numbers, then asymptotically

$$E(\boldsymbol{\alpha})(t) \approx \frac{t^N}{N!\alpha_1\alpha_2\cdots\alpha_{N+1}} \quad \text{as the number } t \to \infty.$$

Thus, in particular, there is a large enough integer F such that for any $t \geq F$, $E(\boldsymbol{\alpha})(t) > 0$ and there is a largest t for which $E(\boldsymbol{\alpha})(t) = 0$. Let us give a simple example:

Example 1.1. Let $\boldsymbol{\alpha} = [6, 2, 3]$. Then on each of the cosets $q + 6\mathbb{Z}$, the function $E(\boldsymbol{\alpha})(t)$ coincides with a polynomial $E^{[q]}(t)$. Here are the corresponding polynomials.

$$E^{[0]}(t) = \tfrac{1}{72}t^2 + \tfrac{1}{4}t + 1, \qquad E^{[1]}(t) = \tfrac{1}{72}t^2 + \tfrac{1}{18}t - \tfrac{5}{72},$$
$$E^{[2]}(t) = \tfrac{1}{72}t^2 + \tfrac{7}{36}t + \tfrac{5}{9}, \qquad E^{[3]}(t) = \tfrac{1}{72}t^2 + \tfrac{1}{6}t + \tfrac{3}{8},$$
$$E^{[4]}(t) = \tfrac{1}{72}t^2 + \tfrac{5}{36}t + \tfrac{2}{9}, \qquad E^{[5]}(t) = \tfrac{1}{72}t^2 + \tfrac{1}{9}t + \tfrac{7}{72}.$$

Naturally, the function $E(\boldsymbol{\alpha})(t)$ is equal to 0 if t does not belong to the lattice $\sum_{i=1}^{N+1} \mathbb{Z}\alpha_i \subset \mathbb{Z}$ generated by the integers α_i. So if g is the greatest common divisor of the α_i (which can be computed in polynomial time), and $\boldsymbol{\alpha}/g = [\frac{\alpha_1}{g}, \frac{\alpha_2}{g}, \ldots, \frac{\alpha_{N+1}}{g}]$ the formula $E(\boldsymbol{\alpha})(gt) = E(\boldsymbol{\alpha}/g)(t)$ holds, and we may assume that the numbers α_i span $\mathbb{Z}$ without changing the complexity of the problem. In other words, we may assume that the greatest common divisor of the α_i is equal to 1.

Our primary concern is how to compute $E(\boldsymbol{\alpha})(t)$, a problem has received a lot of attention. Computing the denumerant $E(\boldsymbol{\alpha})(t)$ as a close formula or evaluating it for specific t is relevant in several other areas of mathematics. In the combinatorics literature the denumerant has been studied extensively (see e.g., [10, 13, 24, 27] and the references therein). The denumerant plays an important role in integer optimization too [23, 25], where the problem is called an *equality-constrained knapsack*. In combinatorial number theory and the theory of partitions, the problem appears in relation to the *Frobenius problem* or the *coin-change problem* of finding the largest value of t with $E(\boldsymbol{\alpha})(t) = 0$ (see [17, 22, 26] for details and algorithms). Authors in the theory of numerical semigroups have also investigated the so called *gaps* or *holes* of the function (see [18] and references therein), which are values of t for which $E(\boldsymbol{\alpha})(t) = 0$, i.e., those positive integers t which cannot be represented by the α_i. For $N = 1$ the number of gaps is $(\alpha_1 - 1)(\alpha_2 - 1)/2$ but for larger N the problem is quite difficult.

Unfortunately, computing $E(\boldsymbol{\alpha})(t)$ or evaluating it are very challenging computational problems. Even deciding whether $E(\boldsymbol{\alpha})(t) > 0$ for a given t, is a well-known (weakly) NP-hard problem. Computing $E(\boldsymbol{\alpha})(t)$, i.e., determining the number of solutions for a given t, is $\#P$-hard. Computing the Frobenius number is also known to be NP-hard [26]. Likewise, for a given coset $q+Q\mathbb{Z}$, computing the polynomial $E^{[q]}(t)$ is NP-hard. Despite the difficulty to compute the function, in some special cases one can compute information efficiently. For example, the Frobenius number can be computed in polynomial time when $N + 1$ is fixed [22, 5]. At the same time for *fixed* $N + 1$ one can compute the entire quasi-polynomial $E(\boldsymbol{\alpha})(t)$ in polynomial time as a special case of a well-known result of Barvinok [6]. There are several papers exploring the practical computation of the Frobenius numbers (see e.g., [17] and the many references therein).

We are certainly not the first to use generating functions to compute $E(\boldsymbol{\alpha})(t)$. Already Ehrhart obtained formulas for $E(\boldsymbol{\alpha})(t)$ in terms of binomial coefficients using partial fraction decomposition. Similary, in [28] the authors propose another way to recover the coefficients of the quasipolynomial by a method they named *rigorous guessing*. In [28] quasipolynomials are represented as a function $f(t)$ given by q polynomials $f^{[1]}(t), f^{[2]}(t), \ldots, f^{[q]}(t)$ such that $f(t) = f^{[i]}(t)$ when $t \equiv i \pmod q$. To find the coefficients of the $f^{[i]}$ their method finds the first few terms of the Maclaurin expansion of the partial fraction decomposition to find enough evaluations of those polynomials and then recovers the coefficients of the $f^{[i]}$ as a result of solving a linear system. Here we are able to prove good complexity results and produced faster practical algorithms using the number theoretic nature of the question.

It should be noted that the polynomial-time complexity results for fixed N were achieved using a powerful geometric interpretation of $E(\boldsymbol{\alpha})(t)$ (which was the original way we encountered the problem too): The function $E(\boldsymbol{\alpha})(t)$ can also be thought of as the number of integral points in the N-dimensional simplex in $\mathbb{R}^{N+1}$ defined by $\Delta_{\boldsymbol{\alpha}} = \{\, [x_1, x_2, \ldots, x_N, x_{N+1}] : x_i \geq 0, \sum_{i=1}^{N+1} \alpha_i x_i = t \,\}$ with rational vertices $\mathbf{s}_i = [0, \ldots, 0, \frac{t}{\alpha_i}, 0, \ldots, 0]$. In this context, $E(\boldsymbol{\alpha})(t)$ is a very special case of the *Ehrhart function* (in honor of French mathematician Eugène Ehrhart who started its study [16]). Ehrhart functions count the lattice points inside a convex polytope P as it is dilated t times. All of the results we mentioned about $E(\boldsymbol{\alpha})(t)$ are in fact special cases of theorems from Ehrhart theory [8]. For example, the asymptotic result of I. Schur can be recovered from seeing that the highest-degree coefficient of $E_{\boldsymbol{\alpha}}(t)$ is just the normalized N-dimensional volume of the simplex $\Delta_{\boldsymbol{\alpha}}$. Our coefficients are very special cases of Ehrhart coefficients.

This paper is about the computation of the coefficients of $E(\boldsymbol{\alpha})(t)$. Here are our main results:

(1) It is clear that the leading coefficient is given by Schur's result. Our main result is a new algorithm for computing explicit formulas for more coefficients.

Theorem 1.2. *Given any fixed integer k, there is a polynomial time algorithm to compute the highest $k+1$ degree terms of the quasi-polynomial $E(\boldsymbol{\alpha})(t)$, that is*

$$\mathrm{Top}_k E(\boldsymbol{\alpha})(t) = \sum_{i=0}^{k} E_{N-i}(t) t^{N-i}.$$

The coefficients are recovered as step polynomial *functions of t.*

Note that the number Q of cosets for $E(\boldsymbol{\alpha})(t)$ can be exponential in the binary encoding size of the problem, and thus it is impossible to list, in polynomial time, the polynomials $E^{[q]}(t)$ for all the cosets $q + Q\mathbb{Z}$. That is why to obtain a polynomial time algorithm, the output is presented in the format of *step polynomials*, which we now introduce:

(i) We first define the function $\{s\} = s - \lfloor s \rfloor \in [0, 1)$ for $s \in \mathbb{R}$, where $\lfloor s \rfloor$ denotes the largest integer smaller or equal to s. The function $\{s+1\} = \{s\}$ is a periodic function of s modulo 1.

(ii) If r is rational with denominator q, the function $T \mapsto \{rT\}$ is a function of $T \in \mathbb{R}$ periodic modulo q. A function of the form $T \mapsto \sum_i c_i \{r_i T\}$ will be called a *step linear function*. If all the r_i have a common denominator q, this function is periodic modulo q.

(iii) Then consider the algebra generated over $\mathbb{Q}$ by such functions on $\mathbb{R}$. An element ϕ of this algebra can be written (not in a unique way) as

$$\phi(T) = \sum_{l=1}^{L} c_l \prod_{j=1}^{J_l} \{r_{l,j} T\}^{n_{l,j}}.$$

Such a function $\phi(T)$ will be called a *step polynomial*.

(iv) We will say that the step polynomial ϕ is of *degree* u if $\sum_j n_j \leq u$ for all set of indices I occurring in the formula for ϕ. We will say that ϕ is of *period* q if all the rational numbers r_j have common denominator q.

One can see that the *step polynomial* representation is much more economical than writing the individual polynomials for each coset of the period. For example instead of six polynomial "pieces" for $E(\boldsymbol{\alpha})(t)$ we can simply write a single step polynomial:

$$\frac{1}{72}\,t^2 + \left(\frac{1}{4} - \frac{\{-\frac{t}{3}\}}{6} - \frac{\{\frac{t}{2}\}}{6}\right) t + \left(1 - \frac{3}{2}\,\{-\tfrac{t}{3}\} - \frac{3}{2}\,\{\tfrac{t}{2}\} + \frac{1}{2}\,\left(\{-\tfrac{t}{3}\}\right)^2 + \{-\tfrac{t}{3}\}\{\tfrac{t}{2}\} + \frac{1}{2}\,\left(\{\tfrac{t}{2}\}\right)^2\right)$$

Our results come after an earlier result of Barvinok [7] who first proved a similar theorem valid for all simplices. Also in [3], the authors presented a polynomial-time algorithm to compute the coefficient functions of $\mathrm{Top}_k E(P)(t)$ for any simple polytope P (given by its rational vertices) in the form of *step polynomials* defined as above. We note that both of these earlier papers use the geometry of the problem very strongly; instead our new algorithm is different as it uses more of the number-theoretic structure of the special case at hand. There is a marked advantage of our algorithms over the work in [7]: We compute using the step polynomials all the possibilities of $E^{[q]}(t)$ while [7] recovers a single piece for given q. More important, our new algorithm is much easier to implement. Another relevant prior work (also useful for comparison) is our algorithm *LattE Top-Ehrhart* presented in [3]. In that paper we extend Barvinok's results of [7] to weighted Ehrhart quasipolynomials via variation of his original approach. The other important ingredient used in the efficient computation of the top coefficients is the reinterpretation of some generating functions in terms of lattice points in cones. This allows us to apply the polynomial-time signed cone decomposition of Barvinok for simplicial cones of fixed dimension k [6].

(2) Although the main result is computational, interesting mathematics comes into play: The new algorithm uses directly the residue theorem in one complex variable, which can be applied more efficiently as a consequence of a rich poset structure on the set of poles of the associated rational generating function for $E(\boldsymbol{\alpha})(t)$ (see Subsection 2.3). Our analysis of the high-order poles of the generating function associated to $E(\boldsymbol{\alpha})(t)$ allows us to decide what is the highest-degree coefficient of $E(\boldsymbol{\alpha})(t)$ that is truly periodic; we obtain:

Theorem 1.3. *Given a list of non-negative integer numbers $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_{N+1}]$, let ℓ be the greatest integer for which there exists a sublist $\boldsymbol{\alpha}_J$ with $|J| = \ell$, such that its greatest common divisor is not 1. Then for $k \geq \ell$ the coefficient of degree k is constant while the coefficient of degree $\ell - 1$ is strictly periodic in the quasipolynomial $E(\boldsymbol{\alpha})(t)$. Moreover, if the numbers α_i are given with their prime factorization, then detecting ℓ can be done in polynomial time.*

Example 1.4. We apply the theorem above to investigate the question of periodicity of the denumerant coefficients in the case of the classical partition problem $E([1,2,3,\dots,m])(t)$. It is well-know that this coincides with the classical problem of finding the number of partitions of the integer t into at most m parts usually denoted $p_m(t)$ (see [2]). In this case Theorem 1.3 predicts indeed that the highest-degree periodic Ehrhart coefficient of the partition function $p_m(t)$ is the term of degree $\lceil m/2 \rceil$. This follows from the theorem because the even numbers in the set $\{1,2,3,\dots,m\}$ form the largest sublist with gcd two.

(3) The paper closes with an extensive collection of computational experiments (Section 5). We constructed a dataset of over 760 knapsacks and show our new algorithm is the fastest available method for computing the top k terms in the Ehrhart quasipolynomial. Our implementation of the new algorithm is made available as a part of the free software `LattE integrale`, version 1.7.[1]

2. The residue formula for $E(\boldsymbol{\alpha})(t)$

Let us begin fixing some notation. If $\phi(z)\,\mathrm{d}z$ is a meromorphic one form on $\mathbb{C}$, with a pole at $z=\zeta$, we write

$$\mathrm{Res}_{z=\zeta}\,\phi(z)\,\mathrm{d}z = \frac{1}{2\pi i}\int_{C_\zeta}\phi(z)\,\mathrm{d}z,$$

where C_ζ is a small circle around the pole ζ. If $\phi(z)=\sum_{k\geq k_0}\phi_k z^k$ is a Laurent series in z, we denote by $\mathrm{res}_{z=0}$ the coefficient of z^{-1} of $\phi(z)$. Cauchy's formula implies that $\mathrm{res}_{z=0}\,\phi(z) = \mathrm{Res}_{z=0}\,\phi(z)\,\mathrm{d}z$.

2.1. A residue formula for $E(\boldsymbol{\alpha})(t)$.

Let $\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\dots,\alpha_{N+1}]$ be a list of integers. Define

$$F(\boldsymbol{\alpha})(z) := \frac{1}{\prod_{i=1}^{N+1}(1-z^{\alpha_i})}.$$

Denote by $\mathcal{P}=\bigcup_{i=1}^{N+1}\{\,\zeta\in\mathbb{C}:\zeta^{\alpha_i}=1\,\}$ the set of poles of the meromorphic function $F(\boldsymbol{\alpha})$ and by $p(\zeta)$ the order of the pole ζ for $\zeta\in\mathcal{P}$.

Note that because the α_i have greatest common divisor 1, we have $\zeta=1$ as a pole of order $N+1$, and the other poles have order strictly smaller.

Theorem 2.1. *Let $\boldsymbol{\alpha}=[\alpha_1,\alpha_2,\dots,\alpha_{N+1}]$ be a list of integers with greatest common divisor equal to 1, and let*

$$F(\boldsymbol{\alpha})(z) := \frac{1}{\prod_{i=1}^{N+1}(1-z^{\alpha_i})}.$$

If t is a non-negative integer, then

$$E(\boldsymbol{\alpha})(t) = -\sum_{\zeta\in\mathcal{P}}\mathrm{Res}_{z=\zeta}\,z^{-t-1}F(\boldsymbol{\alpha})(z)\,\mathrm{d}z \tag{2.1}$$

and the ζ-term of this sum is a quasi-polynomial function of t with degree less than or equal to $p(\zeta)-1$.

[1] Available under the GNU General Public License at `https://www.math.ucdavis.edu/~latte/`.

Proof. For $|z|<1$, we write $\frac{1}{1-z^{\alpha_i}} = \sum_{u=0}^{\infty} z^{u\alpha_i}$ so that $F(\boldsymbol{\alpha})(z) = \sum_{t\geq 0} E(\boldsymbol{\alpha})(t) z^t$.

For a small circle $|z|=\epsilon$ of radius ϵ around 0, the integral of $z^k\,\mathrm{d}z$ is equal to 0 except if $k=-1$, when it is $2\pi i$. Thus

$$E(\boldsymbol{\alpha})(t) = \frac{1}{2\pi i}\int_{|z|=\epsilon} z^{-t} F(\boldsymbol{\alpha})(z)\frac{\mathrm{d}z}{z} = \frac{1}{2\pi i}\int_{|z|=\epsilon} z^{-t}\prod_{i=1}^{N+1}\frac{1}{(1-z^{\alpha_i})}\frac{dz}{z}.$$

Because the α_i are positive integers, and t a non-negative integer, there are no residues at $z=\infty$ and we obtain Equation (2.1) by applying the residue theorem (for a reference about computational complex analysis see [19, 20, 21].

Write $E_\zeta(t) := -\operatorname{Res}_{z=\zeta} z^{-t}F(\boldsymbol{\alpha})(z)\frac{\mathrm{d}z}{z}$; then the dependence in t of $E_\zeta(t)$ comes from the expansion of z^{-t} near $z=\zeta$. We write $z=\zeta+y$, so that

$$E_\zeta(t) = -\operatorname{Res}_{y=0}(\zeta+y)^{-t}F(\boldsymbol{\alpha})(\zeta+y)\frac{\mathrm{d}y}{\zeta+y}.$$

As the pole of $F(\boldsymbol{\alpha})(\zeta+y)$ at $y=0$ is of order $p(\zeta)$, to compute the residue at $y=0$, we only need to expand in y the function $(\zeta+y)^{-t-1}$ and take the coefficient of $y^{p(\zeta)-1}$. Now from the generalized Newton binomial theorem, for $k=t+1$ the function $(\zeta+y)^{-k} = \sum_{n=0}^{\infty}\zeta^{-k-n}y^n$. From this expression one can recover the desired coefficient.

One can easily check that the dependence in t of our residue is a quasi-polynomial with degree less than or equal to $p(\zeta)-1$. We thus obtain the result. □

2.2. **Poles of high and low order.** Given an integer $0\leq k\leq N$, we partition the set of poles $\mathcal{P}$ in two disjoint sets according to the order of the pole:

$$\mathcal{P}_{>N-k} = \{\,\zeta : p(\zeta)\geq N+1-k\,\}, \qquad \mathcal{P}_{\leq N-k} = \{\,\zeta : p(\zeta)\leq N-k\,\}.$$

Example 2.2. (a) Let $\boldsymbol{\alpha}=[98,59,44,100]$, so $N=3$, and let $k=1$. Then $\mathcal{P}_{>N-k}$ consists of poles of order greater than 2. Of course $\zeta=1$ is a pole of order 4. Note that $\zeta=-1$ is a pole of order 3. So $\mathcal{P}_{>N-k} = \{\,\zeta : \zeta^2=1\,\}$.

(b) Let $\boldsymbol{\alpha}=[6,2,2,3,3]$, so $N=4$, and let $k=2$. Let $\zeta_6 = \mathrm{e}^{2\pi i/6}$ be a primitive 6th root of unity. Then $\zeta_6^6=1$ is a pole of order 5, ζ_6 and ζ_6^5 are poles of order 1, and ζ_6^2, $\zeta_6^3=-1$, ζ_6^4 are poles of order 3. Thus $\mathcal{P}_{>N-k}=\mathcal{P}_{>2}$ is the union of $\{\,\zeta:\zeta^2=1\,\}=\{-1,1\}$ and $\{\,\zeta:\zeta^3=1\,\}=\{\zeta_6^2,\zeta_6^4,\zeta_6^6=1\}$.

According to the disjoint decomposition $\mathcal{P}=\mathcal{P}_{\leq N-k}\cup\mathcal{P}_{>N-k}$, we write

$$E_{\mathcal{P}_{>N-k}}(t) = -\sum_{\zeta\in\mathcal{P}_{>N-k}}\operatorname{Res}_{z=\zeta} z^{-t-1}F(\boldsymbol{\alpha})(z)\,\mathrm{d}z$$

and

$$E_{\mathcal{P}_{\leq N-k}}(t) = -\sum_{\zeta\in\mathcal{P}_{\leq N-k}}\operatorname{Res}_{z=\zeta} z^{-t-1}F(\boldsymbol{\alpha})(z)\,\mathrm{d}z.$$

The following proposition is a direct consequence of Theorem 2.1.

Proposition 2.3. *We have*

$$E(\boldsymbol{\alpha})(t) = E_{\mathcal{P}_{>N-k}}(t) + E_{\mathcal{P}_{\leq N-k}}(t),$$

where the function $E_{\mathcal{P}_{\leq N-k}}(t)$ is a quasi-polynomial function in the variable t of degree strictly less than $N-k$.

Thus for the purpose of computing $\mathrm{Top}_k E(\boldsymbol{\alpha})(t)$ it is sufficient to compute the function $E_{\mathcal{P}_{>N-k}}(t)$. This function is computable in polynomial time, as stated in the main result of our paper:

Theorem 2.4. *Let k be a fixed number. Then the coefficient functions of the quasi-polynomial function $E_{\mathcal{P}_{>N-k}}(t)$ are computable in polynomial time as step polynomials of t.*

We prove the theorem in the rest of this section and the next.

2.3. **The poset of the high-order poles.** We first rewrite our set $\mathcal{P}_{>N-k}$. Note that if ζ is a pole of order $\geq p$, this means that there exist at least p elements α_i in the list $\boldsymbol{\alpha}$ so that $\zeta^{\alpha_i} = 1$. But if $\zeta^{\alpha_i} = 1$ for a set $I \subseteq \{1, \ldots, N+1\}$ of indices i, this is equivalent to the fact that $\zeta^f = 1$, for f the greatest common divisor of the elements $\alpha_i, i \in I$.

Now let $\mathcal{I}_{>N-k}$ be the set of subsets of $\{1, \ldots, N+1\}$ of cardinality greater than $N-k$. Note that when k is fixed, the cardinality of $\mathcal{I}_{>N-k}$ is a polynomial function of N. For each subset $I \in \mathcal{I}_{>N-k}$, define f_I to be the greatest common divisor of the corresponding sublist α_i, $i \in I$. Let $\mathcal{G}_{>N-k}(\boldsymbol{\alpha}) = \{\, f_I : I \in \mathcal{I}_{>N-k} \,\}$ be the set of integers so obtained and let $G(f) \subset \mathbb{C}^\times$ be the group of f-th roots of unity,

$$G(f) = \{\, \zeta \in \mathbb{C} : \zeta^f = 1 \,\}.$$

The set $\{\, G(f) : f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha}) \,\}$ forms a poset $\tilde{P}_{>N-k}$ (partially ordered set) with respect to reverse inclusion. That is, $G(f_i) \preceq_{\tilde{P}_{>N-k}} G(f_j)$ if $G(f_j) \subseteq G(f_i)$ (the i and j become swapped). Notice $G(f_j) \subseteq G(f_i) \Leftrightarrow f_j$ divides f_i. Even if $\tilde{P}_{>N-k}$ has a unique minimal element, we add an element $\hat{0}$ such that $\hat{0} \preceq G(f)$ and call this new poset $P_{>N-k}$.

In terms of the group $G(f)$ we have thus $\mathcal{P}_{>N-k} = \bigcup_{f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})} G(f)$. This is, of course, not a disjoint union, but using the inclusion–exclusion principle, we can write the characteristic function of the set $\mathcal{P}_{>N-k}$ as a linear combination of characteristic functions of the sets $G(f)$:

$$[\mathcal{P}_{>N-k}] = \sum_{f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})} \mu_{>N-k}(f)[G(f)],$$

where $\mu_{>N-k}(f) := -\mu'_{>N-k}(\hat{0}, G(f))$ and $\mu'_{>N-k}(x, y)$ is the standard Möbius function for the poset $P_{>N-k}$:

$$\begin{aligned} &\mu'_{>N-k}(s,s) = 1 && \forall s \in P_{>N-k}, \\ &\mu'_{>N-k}(s,u) = -\sum_{s \preceq t \prec u} \mu'_{>N-k}(s,t) && \forall s \prec u \text{ in } P_{>N-k}. \end{aligned}$$

For simplicity, $\mu_{>N-k}$ will be called the *Möbius function* for the poset $P_{>N-k}$ and will be denoted simply by $\mu(f)$. We also have the relationship

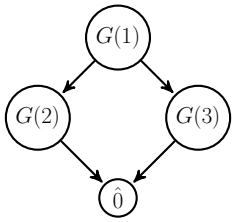
$$\begin{aligned} \mu(f) &= -\mu'_{>N-k}(\hat{0}, G(f)) \\ &= 1 + \sum_{\hat{0} \prec G(t) \prec G(f)} \mu'_{>N-k}(\hat{0}, G(t)) \\ &= 1 - \sum_{\hat{0} \prec G(t) \prec G(f)} -\mu'_{>N-k}(\hat{0}, G(t)) \\ &= 1 - \sum_{\hat{0} \prec G(t) \prec G(f)} \mu(t) \end{aligned}$$

Example 2.5 (Example 2.2, continued)**.**

(a) Here we have $\mathcal{I}_{>N-k} = \mathcal{I}_{>2} = \big\{\{1,2,3\},\{1,2,4\},\{1,3,4\},\{2,3,4\},\{1,2,3,4\}\big\}$ and $\mathcal{G}_{>N-k}(\boldsymbol{\alpha}) = \{1,1,2,1,1\} = \{1,2\}$. Accordingly, $\mathcal{P}_{>N-k} = G(1) \cup G(2)$. The poset $P_{>2}$ is

The arrows denote subsets, that is $G(1) \subset G(2)$ and $\hat{0}$ can be identified with the unit circle. The Möbius function μ is simply given by $\mu(1) = 0$, $\mu(2) = 1$, and so $[\mathcal{P}_{>N-k}] = [G(2)]$.

(b) Now $\mathcal{I}_{>N-k} = \mathcal{I}_{>2} = \big\{\{1,2,3\},\{1,2,4\},\ldots,\{3,4,5\},\{1,2,3,4\},\{1,2,3,5\},\{1,2,4,5\},\{1,3,4,5\},\{2,3,4,5\},\{1,2,3,4,5\}\big\}$ and thus $\mathcal{G}_{>N-k}(\boldsymbol{\alpha}) = \{2,3,1,1\} = \{1,2,3\}$. Hence $\mathcal{P}_{>N-k} = G(1) \cup G(2) \cup G(3) = \{1\} \cup \{-1,1\} \cup \{\zeta_3, \zeta_3^2, 1\}$, where $\zeta_3 = \mathrm{e}^{2\pi i/3}$ is a primitive 3rd root of unity.



The Möbius function μ is then $\mu(3) = 1$, $\mu(2) = 1$, $\mu(1) = -1$, and thus $[\mathcal{P}_{>N-k}] = -[G(1)] + [G(2)] + [G(3)]$.

Theorem 2.6. *Given a list $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_{N+1}]$ and a fixed integer k, then the values for the Möbius function for the poset $P_{>N-k}$ can be computed in polynomial time.*

Proof. First find the greatest common divisor of all sublists of the list $\boldsymbol{\alpha}$ with size greater than $N-k$. Let V be the set of integers obtained from all such greatest common divisors. We note that each node of the poset $P_{>N-k}$ is a group of roots of unity $G(v)$. But it is labeled by a non-negative integer v.

Construct an array M of size $|V|$ to keep the value of the Möbius function. Initialize M to hold the Möbius values of infinity: $M[v] \leftarrow \infty$ for all $v \in V$. Then call Algorithm 1 below with findMöbius$(1, V, M)$.

Algorithm 1 terminates because the number of nodes v with $M[v] = \infty$ decreases to zero in each iteration. To show correctness, consider a node v in the poset P_{N-k}. If v covers $\hat{0}$, then we must have $M[v] = 1$ as there is no other $G(w)$ with $G(f) \subset G(w)$. Else if v does not cover $\hat{0}$, we set $M[v]$ to be 1 minus the sum $\sum_{w:v|w} M[w]$ which guarantees that the poles in $G(v)$ are only counted once because $\sum_{w:v|w} M[w]$ is how many times $G(v)$ is a subset of another element that has already been counted.

Algorithm 1 findMöbius(n, V, M)

Input: n: the label of node $G(n)$ in the poset $\tilde{P}_{>N-k}$
Input: V: list of numbers in the poset $\tilde{P}_{>N-k}$
Input: M: array of current Möbius values computed for $P_{>N-k}$
Output: updates the array M of Möbius values
1: **if** $M[n] < \infty$ **then**
2: **return**
3: **end if**
4: $L \leftarrow \{ v \in V : n \mid v \} \setminus \{n\}$
5: **if** $L = \emptyset$ **then**
6: $M[n] \leftarrow 1$
7: **return**
8: **end if**
9: $M[n] \leftarrow 0$
10: **for all** $v \in L$ **do**
11: findMöbius(v, L, M)
12: $M[n] \leftarrow M[n] + M[v]$
13: **end for**
14: $M[n] \leftarrow 1 - M[n]$

The number of sublists of $\boldsymbol{\alpha}$ considered is $\binom{N}{1} + \binom{N}{2} + \cdots + \binom{N}{k} = O(N^k)$, which is a polynomial for k fixed. For each sublist, the greatest common divisor of a set of integers is computed in polynomial time. Hence $|V| = O(N^k)$. Notice that lines 4 to 14 of Algorithm 1 are executed at most $O(|V|)$ times as once a $M[v]$ value is computed, it is never recomputed. The number of additions on line 12 is $O(|V|^2)$ while the number of divisions on line 4 is also $O(|V|^2)$. Hence this algorithm finds the Möbius function in $O(|V|^2) = O(N^{2k})$ time where k is fixed. □

Let us define for any positive integer f

$$E(\boldsymbol{\alpha}, f)(t) = -\sum_{\zeta^f=1} \mathrm{Res}_{z=\zeta}\, z^{-t-1} F(\boldsymbol{\alpha})(z)\, \mathrm{d}z.$$

Proposition 2.7. *Let k be a fixed integer, then*

$$E_{\mathcal{P}_{>N-k}}(t) = -\sum_{f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})} \mu(f) E(\boldsymbol{\alpha}, f)(t). \tag{2.2}$$

Thus we have reduced the computation to the fast computation of $E(\boldsymbol{\alpha}, f)(t)$.

3. Polyhedral reinterpretation of the generating function $E(\boldsymbol{\alpha}, f)(t)$

To complete the proof of Theorem 2.4 we need only to prove the following proposition.

Proposition 3.1. *For any integer $f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})$, the coefficient functions of the quasi-polynomial function $E(\boldsymbol{\alpha}, f)(t)$ and hence $E_{\mathcal{P}_{>N-k}}(t)$ are computed in polynomial time as step polynomials of t.*

By the previous proposition we know we need to compute the value of $E(\boldsymbol{\alpha}, f)(t)$. Our goal now is to demonstrate that this function can be thought of as the generating function of

the lattice points inside a convex cone. This is a key point to guarantee good computational bounds. Before we can do that we review some preliminaries on generating functions of cones. We recall the notion of generating functions of cones; see also [3].

Let $V = \mathbb{R}^r$ provided with a lattice Λ, and let V^* denote the dual space. A (rational) simplicial cone $\mathfrak{c} = \mathbb{R}_{\geq 0}\mathbf{w}_1 + \cdots + \mathbb{R}_{\geq 0}\mathbf{w}_r$ is a cone generated by r linearly independent vectors $\mathbf{w}_1, \ldots, \mathbf{w}_r$ of Λ. We consider the semi-rational affine cone $\mathbf{s} + \mathfrak{c}$, $\mathbf{s} \in V$. Let $\boldsymbol{\xi} \in V^*$ be a dual vector such that $\langle \boldsymbol{\xi}, \mathbf{w}_i \rangle < 0,\ 1 \leq i \leq r$. Then the sum

$$S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi}) = \sum_{\mathbf{n} \in (\mathbf{s}+\mathfrak{c}) \cap \Lambda} \mathrm{e}^{\langle \boldsymbol{\xi}, \mathbf{n} \rangle}$$

is summable and defines an analytic function of $\boldsymbol{\xi}$. It is well known that this function extends to a meromorphic function of $\boldsymbol{\xi} \in V^*_{\mathbb{C}}$. We still denote this meromorphic extension by $S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi})$.

Example 3.2. Let $V = \mathbb{R}$ with lattice $\mathbb{Z}$, $\mathfrak{c} = \mathbb{R}_{\geq 0}$, and $s \in \mathbb{R}$. Then

$$S(s + \mathbb{R}_{\geq 0}, \mathbb{Z})(\xi) = \sum_{n \geq s} \mathrm{e}^{n\xi} = \mathrm{e}^{\lceil s \rceil \xi} \frac{1}{1 - \mathrm{e}^{\xi}}.$$

Using the function $\{x\} = x - \lfloor x \rfloor$, we find $\lceil s \rceil = s + \{-s\}$ and can write

$$\mathrm{e}^{-s\xi} S(s + \mathbb{R}_{\geq 0}, \mathbb{Z})(\xi) = \frac{\mathrm{e}^{\{-s\}\xi}}{1 - \mathrm{e}^{\xi}}. \tag{3.1}$$

Recall the following result:

Theorem 3.3. *Consider the semi-rational affine cone* $\mathbf{s}+\mathfrak{c}$ *and the lattice* Λ. *The series* $S(\mathbf{s}+\mathfrak{c}, \Lambda)(\boldsymbol{\xi})$ *is a meromorphic function of* $\boldsymbol{\xi}$ *such that* $\prod_{i=1}^{r} \langle \boldsymbol{\xi}, \mathbf{w}_i \rangle S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi})$ *is holomorphic in a neighborhood of* $\mathbf{0}$.

Let $\mathbf{t} \in \Lambda$. Consider the translated cone $\mathbf{t}+\mathbf{s}+\mathfrak{c}$ of $\mathbf{s}+\mathfrak{c}$ by $\mathbf{t}$. Then we have the covariance formula

$$S(\mathbf{t} + \mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi}) = \mathrm{e}^{\langle \boldsymbol{\xi}, \mathbf{t} \rangle} S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi}). \tag{3.2}$$

Because of this formula, it is convenient to introduce the following function.

Definition 3.4. Define the function

$$M(\mathbf{s}, \mathfrak{c}, \Lambda)(\boldsymbol{\xi}) = \mathrm{e}^{-\langle \boldsymbol{\xi}, \mathbf{s} \rangle} S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi}).$$

Thus the function $\mathbf{s} \mapsto M(\mathbf{s}, \mathfrak{c}, \Lambda)(\boldsymbol{\xi})$ is a function of $\mathbf{s} \in V/\Lambda$ (a periodic function of $\mathbf{s}$) whose values are meromorphic functions of $\boldsymbol{\xi}$.

There is a very special and important case when the function $M(\mathbf{s}, \mathfrak{c}, \Lambda)(\boldsymbol{\xi}) = \mathrm{e}^{-\langle \boldsymbol{\xi}, \mathbf{s} \rangle} S(\mathbf{s} + \mathfrak{c}, \Lambda)(\boldsymbol{\xi})$ is easy to write down. A *unimodular* cone, is a cone $\mathfrak{u}$ whose primitive generators $\mathbf{g}^{\mathfrak{u}}_i$ form a basis of the lattice Λ. We introduce the following notation.

Definition 3.5. Let $\mathfrak{u}$ be a unimodular cone with primitive generators $\mathbf{g}^{\mathfrak{u}}_i$ and let $\mathbf{s} \in V$. Then, write $\mathbf{s} = \sum_i s_i \mathbf{g}^{\mathfrak{u}}_i$, with $s_i \in \mathbb{R}$, and define

$$\{-\mathbf{s}\}_{\mathfrak{u}} = \sum_i \{-s_i\} \mathbf{g}^{\mathfrak{u}}_i.$$

Thus $\mathbf{s}+\{-\mathbf{s}\}_{\mathfrak{u}} = \sum_i \lceil s_i \rceil \mathbf{g}_i^{\mathfrak{u}}$. Note that if $\mathbf{t} \in \Lambda$, then $\{-(\mathbf{s}+\mathbf{t})\}_{\mathfrak{u}} = \{-\mathbf{s}\}_{\mathfrak{u}}$. Thus, $\mathbf{s} \mapsto \{-\mathbf{s}\}_{\mathfrak{u}}$ is a function on V/Λ with value in V. For any $\boldsymbol{\xi} \in V^*$, we then find

$$S(\mathbf{s}+\mathfrak{u},\Lambda)(\boldsymbol{\xi}) = \mathrm{e}^{\langle \boldsymbol{\xi},\mathbf{s}\rangle}\mathrm{e}^{\langle \boldsymbol{\xi},\{-\mathbf{s}\}_{\mathfrak{u}}\rangle}\frac{1}{\prod_j(1-\mathrm{e}^{\langle \boldsymbol{\xi},\mathbf{g}_j^{\mathfrak{u}}\rangle})}$$

and thus

$$M(\mathbf{s},\mathfrak{u},\Lambda)(\boldsymbol{\xi}) = \mathrm{e}^{\langle \boldsymbol{\xi},\{-\mathbf{s}\}_{\mathfrak{u}}\rangle}\frac{1}{\prod_j(1-\mathrm{e}^{\langle \boldsymbol{\xi},\mathbf{g}_j^{\mathfrak{u}}\rangle})}. \tag{3.3}$$

For a general cone $\mathfrak{c}$, we can decompose its characteristic function $[\mathfrak{c}]$ as a signed sum of characteristic functions of unimodular cones, $\sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}}[\mathfrak{u}]$, modulo characteristic functions of cones containing lines. As shown by Barvinok (see [6] for the original source and [8] for a great new exposition), if the dimension r of V is fixed, this decomposition can be computed in polynomial time. Then we can write

$$S(\mathbf{s}+\mathfrak{c},\Lambda)(\boldsymbol{\xi}) = \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}}\, S(\mathbf{s}+\mathfrak{u},\Lambda)(\boldsymbol{\xi}).$$

Thus we obtain, using Formula (3.3),

$$M(\mathbf{s},\mathfrak{c},\Lambda)(\boldsymbol{\xi}) = \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}}\, \mathrm{e}^{\langle \boldsymbol{\xi},\{-\mathbf{s}\}_{\mathfrak{u}}\rangle}\frac{1}{\prod_j(1-\mathrm{e}^{\langle \boldsymbol{\xi},\mathbf{g}_i^{\mathfrak{u}}\rangle})}. \tag{3.4}$$

Here $\mathfrak{u}$ runs through all the unimodular cones occurring in the decomposition of $\mathfrak{c}$, and the $\mathbf{g}_i^{\mathfrak{u}} \in \Lambda$ are the corresponding generators of the unimodular cone $\mathfrak{u}$.

Remark 3.6. For computing explicit examples, it is convenient to make a change of variables that leads to computations in the standard lattice $\mathbb{Z}^r$. Let B be the matrix whose columns are the generators of the lattice Λ; then $\Lambda = B\mathbb{Z}^r$.

$$\begin{aligned} M(\mathbf{s},\mathfrak{c},\Lambda)(\boldsymbol{\xi}) &= \mathrm{e}^{-\langle \boldsymbol{\xi},\mathbf{s}\rangle} \sum_{\mathbf{n}\in(\mathbf{s}+\mathfrak{c})\cap B\mathbb{Z}^r} \mathrm{e}^{\langle \boldsymbol{\xi},\mathbf{n}\rangle} \\ &= \mathrm{e}^{-\langle B^\top\boldsymbol{\xi},B^{-1}\mathbf{s}\rangle} \sum_{\mathbf{x}\in(B^{-1}(\mathbf{s}+\mathfrak{c})\cap\mathbb{Z}^r} \mathrm{e}^{\langle B^\top\boldsymbol{\xi},\mathbf{x}\rangle} = M(B^{-1}\mathbf{s},B^{-1}\mathfrak{c},\mathbb{Z}^r)(B^\top\boldsymbol{\xi}). \end{aligned}$$

3.1. **Back to the computation of $E(\boldsymbol{\alpha},f)(t)$.** After the preliminaries we will see how to rewrite $E(\boldsymbol{\alpha},f)(t)$ in terms of lattice points of simplicial cones. This will require some suitable manipulation of the initial form of $E(\boldsymbol{\alpha},f)(t)$. So we introduce some notation.

Definition 3.7. Let k be fixed. For $f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})$, define

$$\mathcal{F}(\boldsymbol{\alpha},f,T)(x) = \sum_{\zeta^f=1} \frac{\zeta^{-T}}{\prod_{i=1}^{N+1}(1-\zeta^{\alpha_i}\mathrm{e}^{\alpha_i x})},$$

$$\mathcal{E}(\boldsymbol{\alpha},f)(t,T) = -\operatorname{res}_{x=0} \mathrm{e}^{-tx}\mathcal{F}(\boldsymbol{\alpha},f,T)(x),$$

and

$$E_i(f)(T) = \operatorname{res}_{x=0} \frac{(-x)^i}{i!}\mathcal{F}(\boldsymbol{\alpha},f,T)(x).$$

Writing $z = \zeta \mathrm{e}^x$ and changing coordinates in residues, we obtain immediately:

$$E(\boldsymbol{\alpha}, f)(t) = \mathcal{E}(\boldsymbol{\alpha}, f)(t, T)\big|_{T=t}. \tag{3.5}$$

The dependence in T of $\mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$ is through ζ^T. As $\zeta^f = 1$, the function $\mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$ is a periodic function of T modulo f whose values are meromorphic functions of x. Since the pole in x is of order at most $N+1$, we can rewrite $\mathcal{E}(\boldsymbol{\alpha}, f)(t, T)$ in terms of $E_i(f)(T)$ and prove:

Theorem 3.8. *Let k be fixed. Then for $f \in \mathcal{G}_{>N-k}(\boldsymbol{\alpha})$ we can write*

$$\mathcal{E}(\boldsymbol{\alpha}, f)(t, T) = \sum_{i=0}^{N} t^i E_i(f)(T)$$

with $E_i(f)(T)$ a step polynomial of degree less than or equal to $N - i$ and periodic of T modulo f. This step polynomial can be computed in polynomial time.

It is now clear that once we have proved Theorem 3.8, then the proof of Theorem 2.4 will follow. Writing everything out, for m such that $0 \le m \le N$, the coefficient of t^m in the Ehrhart quasi-polynomial is given by

$$E_m(T) = -res_{x=0} \frac{(-x)^m}{m!} \sum_{f \in \mathcal{G}_{>m}(\alpha)} \mu(f) \sum_{\{\zeta; \zeta^f = 1\}} \frac{\zeta^{-T}}{\prod (1 - \zeta^{\alpha_i} \mathrm{e}^{\alpha_i x})} \tag{3.6}$$

As an example, we see that E_N is independent of T because $\mathcal{G}_{>N}(\alpha) = \{1\}$; thus E_N is a constant. We now concentrate on writing the function $\mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$ more explicitly.

Definition 3.9. For a list $\boldsymbol{\alpha}$ and integers f and T, define meromorphic functions of $x \in \mathbb{C}$ by:

$$\mathcal{B}(\boldsymbol{\alpha}, f)(x) := \frac{1}{\prod_{i:\ f | \alpha_i} (1 - \mathrm{e}^{\alpha_i x})},$$

$$\mathcal{S}(\boldsymbol{\alpha}, f, T)(x) := \sum_{\zeta:\ \zeta^f = 1} \frac{\zeta^{-T}}{\prod_{i:\ f \nmid \alpha_i} (1 - \zeta^{\alpha_i} \mathrm{e}^{\alpha_i x})}.$$

Thus

$$\mathcal{F}(\boldsymbol{\alpha}, f, T)(x) = \mathcal{B}(\boldsymbol{\alpha}, f)(x)\, \mathcal{S}(\boldsymbol{\alpha}, f, T)(x).$$

The expression we obtained will allow us to compute $\mathcal{F}(\boldsymbol{\alpha}, f, T)$ by relating $S(\boldsymbol{\alpha}, f, T)$ to a generating function of a cone. This cone will have fixed dimension when k is fixed.

3.2. $E(\boldsymbol{\alpha}, f)(t)$ **as the generating function of a cone in fixed dimension.** To this end, let f be an integer from $\mathcal{G}_{>N-k}(\boldsymbol{\alpha})$. By definition, f is the greatest common divisor of a sublist of $\boldsymbol{\alpha}$. Thus the greatest common divisor of f and the elements of $\boldsymbol{\alpha}$ which are *not* a multiple of f is still equal to 1. Let $J = J(\boldsymbol{\alpha}, f)$ be the set of indices $i \in \{1, \dots, N+1\}$ such that α_i is indivisible by f, i.e., $f \nmid \alpha_i$. Note that f by definition is the greatest common divisor of all except at most k of the integers α_j. Let r denote the cardinality of J; then $r \le k$. Let $V_J = \mathbb{R}^J$ and let V_J^* denote the dual space. We also define the sublist $\boldsymbol{\alpha}_J = [\alpha_i]_{i \in J}$ of elements of $\boldsymbol{\alpha}$ indivisible by f and view it as a vector in V_J^*.

Definition 3.10. For an integer T, define the meromorphic function of $\boldsymbol{\xi} \in V_J^*$,

$$Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi}) = \sum_{\zeta\colon \zeta^f=1} \frac{\zeta^{-T}}{\prod_{j\in J(\boldsymbol{\alpha},f)}(1-\zeta^{\alpha_j}\mathrm{e}^{\xi_j})}.$$

Remark 3.11. Observe that $Q(\boldsymbol{\alpha}, f, T)$ can be restricted at $\boldsymbol{\xi} = \boldsymbol{\alpha}_J x$, for $x \in \mathbb{C}$ generic, to give $\mathcal{S}(\boldsymbol{\alpha}, f, T)(x)$.

We find that $Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi})$ is the discrete generating function of an affine shift of the standard cone relative to a certain lattice in V_J, which we define as:

$$\Lambda(\boldsymbol{\alpha}, f) = \big\{\, \mathbf{y} \in \mathbb{Z}^J : \langle \boldsymbol{\alpha}_J, \mathbf{y}\rangle = \sum_{j\in J} y_j\alpha_j \in \mathbb{Z}f \,\big\}. \tag{3.7}$$

Consider the map $\phi\colon \mathbb{Z}^J \to \mathbb{Z}/\mathbb{Z}f$, $\mathbf{y} \mapsto \langle \boldsymbol{\alpha}, \mathbf{y}\rangle + \mathbb{Z}f$. Its kernel is the lattice $\Lambda(\boldsymbol{\alpha}, f)$. Because the greatest common divisor of f and the elements of $\boldsymbol{\alpha}_J$ is 1, by Bezout's theorem there exist $s_0 \in \mathbb{Z}$ and $\mathbf{s} \in \mathbb{Z}^J$ such that $1 = \sum_{i\in J} s_i\alpha_i + s_0 f$. Therefore, the map ϕ is surjective, and therefore the index $|\mathbb{Z}^J : \Lambda(\boldsymbol{\alpha}, f)|$ equals f.

Theorem 3.12. *Let $\boldsymbol{\alpha} = [\alpha_1, \dots, \alpha_{N+1}]$ be a list of positive integers and f be the greatest common divisor of a sublist of $\boldsymbol{\alpha}$. Let $J = J(\boldsymbol{\alpha}, f) = \{\, i : f \nmid \alpha_i \,\}$. Let $s_0 \in \mathbb{Z}$ and $\mathbf{s} \in \mathbb{Z}^J$ such that $1 = \sum_{i\in J} s_i\alpha_i + s_0 f$ using Bezout's theorem. Let T be an integer, and $\boldsymbol{\xi} \in V_J^*$. Then*

$$Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi}) = f\, M\big(-T\mathbf{s}, \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi}).$$

Remark 3.13. The function $Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi})$ is a function of T periodic modulo f. Since $f\mathbb{Z}^J$ is contained in $\Lambda(\boldsymbol{\alpha}, f)$, the element $f\mathbf{s}$ is in the lattice $\Lambda(\boldsymbol{\alpha}, f)$, and we see that the right hand side is also a periodic function of T modulo f.

Proof of Theorem 3.12. Consider $\boldsymbol{\xi} \in V_J^*$ with $\xi_j < 0$. Then we can write the equality

$$\frac{1}{\prod_{j\in J}(1-\zeta^{\alpha_j}\mathrm{e}^{\xi_j})} = \prod_{j\in J}\sum_{n_j=0}^{\infty} \zeta^{n_j\alpha_j}\mathrm{e}^{n_j\xi_j}.$$

So

$$Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi}) = \sum_{\mathbf{n}\in\mathbb{Z}^J_{\geq 0}} \Big(\sum_{f\colon \zeta^f=1} \zeta^{\sum_j n_j\alpha_j - T}\Big)\mathrm{e}^{\sum_{j\in J} n_j\xi_j}.$$

We note that $\sum_{f\colon \zeta^f=1} \zeta^m$ is zero except if $m \in \mathbb{Z}f$, when this sum is equal to f. Then we obtain that $Q(\boldsymbol{\alpha}, f, T)$ is the sum over $\mathbf{n} \in \mathbb{Z}^J_{\geq 0}$ such that $\sum_j n_j\alpha_j - T \in \mathbb{Z}f$. The equality $1 = \sum_{j\in J} s_j\alpha_j + s_0 f$ implies that $T \equiv \sum_j ts_j\alpha_j$ modulo f, and the condition $\sum_j n_j\alpha_j - T \in \mathbb{Z}f$ is equivalent to the condition $\sum_j (n_j - Ts_j)\alpha_j \in \mathbb{Z}f$.

We see that the point $\mathbf{n} - T\mathbf{s}$ is in the lattice $\Lambda(\boldsymbol{\alpha}, f)$ as well as in the cone $-T\mathbf{s} + \mathbb{R}^J_{\geq 0}$ (as $n_j \geq 0$). Thus our function $Q(\boldsymbol{\alpha}, f, T)(\boldsymbol{\xi})$ is equal to $f\,\mathrm{e}^{\langle \boldsymbol{\xi}, T\mathbf{s}\rangle} S\big(-T\mathbf{s} + \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi}) = f\, M\big(-T\mathbf{s} + \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi})$. □

3.3. **Unimodular decomposition in the dual space.** The cone $\mathbb{R}^J_{\geq 0}$ is in general not unimodular with respect to the lattice $\Lambda(\boldsymbol{\alpha}, f)$. By decomposing $\mathbb{R}^J_{\geq 0}$ in cones $\mathfrak{u}$ that are unimodular with respect to $\Lambda(\boldsymbol{\alpha}, f)$, modulo cones containing lines, we can write

$$M\big(-T\mathbf{s}, \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big) = \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}} M(-T\mathbf{s}, \mathfrak{u}, \Lambda),$$

where $\epsilon_{\mathfrak{u}} \in \{\pm 1\}$. This decomposition can be computed using Barvinok's algorithm in polynomial time for fixed k because the dimension $|J|$ is at most k.

Remark 3.14. For this particular cone and lattice, this decomposition modulo cones containing lines is best done using the "dual" variant of Barvinok's algorithm, as introduced by [15] (see also [9]). This is in contrast to the "primal" variant described in [12] and [4]. To explain this, let us determine the index of the cone $\mathbb{R}^J_{\geq 0}$ in the lattice $\Lambda = \Lambda(\boldsymbol{\alpha}, f)$; the worst-case complexity of the signed cone decomposition is bounded by a polynomial in the logarithm of this index.

Let B be a matrix whose columns form a basis of Λ, so $\Lambda = B\mathbb{Z}^J$. Then $|\mathbb{Z}^J : \Lambda| = |\det B| = f$. By Remark 3.6, we find

$$M\big(-T\mathbf{s}, \mathbb{R}^J_{\geq 0}, \Lambda\big)(\boldsymbol{\xi}) = M(-TB^{-1}\mathbf{s}, B^{-1}\mathbb{R}^J_{\geq 0}, \mathbb{Z}^J)(B^{\top}\boldsymbol{\xi}).$$

Let $\mathfrak{c}$ denote the cone $B^{-1}\mathbb{R}^J_{\geq 0}$, which is generated by the columns of B^{-1}. Since B^{-1} is not integer in general, we find generators of $\mathfrak{c}$ that are primitive vectors of $\mathbb{Z}^J$ by scaling each of the columns by an integer. Certainly $|\det B|B^{-1}$ is an integer matrix, and thus we find that the index of the cone $\mathfrak{c}$ is bounded above by f^{r-1}. We can easily determine the exact index as follows. For each $i \in J$, the generator $\mathbf{e}_i$ of the original cone $\mathbb{R}^J_{\geq 0}$ needs to be scaled so as to lie in the lattice Λ. The smallest multiplier $y_i \in \mathbb{Z}_{>0}$ such that $\langle \boldsymbol{\alpha}_J, y_i\mathbf{e}_i\rangle \in \mathbb{Z}f$ is $y_i = \operatorname{lcm}(\alpha_i, f)/\alpha_i$. Thus the index of $\mathbb{R}^J_{\geq 0}$ in $\mathbb{Z}^J$ is the product of the y_i, and finally the index of $\mathbb{R}^J_{\geq 0}$ in Λ is

$$\frac{1}{|\mathbb{Z}^r : \Lambda|}\prod_{i\in J}\frac{\operatorname{lcm}(\alpha_i, f)}{\alpha_i} = \frac{1}{f}\prod_{i\in J}\frac{\operatorname{lcm}(\alpha_i, f)}{\alpha_i}.$$

Instead we consider the dual cone, $\mathfrak{c}^\circ = \{\,\boldsymbol{\eta} \in V_J^* : \langle \boldsymbol{\eta}, \mathbf{y}\rangle \geq 0 \text{ for } \mathbf{y} \in \mathfrak{c}\,\}$. We have $\mathfrak{c}^\circ = B^{\top}\mathbb{R}^J_{\geq 0}$. Then the index of the dual cone $\mathfrak{c}^\circ$ equals $|\det B^{\top}| = f$, which is much smaller than f^{r-1}.

Following [15], we now compute a decomposition of $\mathfrak{c}^\circ$ in cones $\mathfrak{u}^\circ$ that are unimodular with respect to $\mathbb{Z}^J$, modulo lower-dimensional cones,

$$[\mathfrak{c}^\circ] \equiv \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}}[\mathfrak{u}^\circ] \quad \text{(modulo lower-dimensional cones)}.$$

Then the desired decomposition follows:

$$[\mathfrak{c}] \equiv \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}}[\mathfrak{u}] \quad \text{(modulo cones with lines)}.$$

Because of the better bound on the index of the cone on the dual side, the worst-case complexity of the signed decomposition algorithm is reduced. This is confirmed by computational experiments.

Remark 3.15. Although we know that the meromorphic function $M\big(-T\mathbf{s}, \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi})$ restricts via $\boldsymbol{\xi} = \boldsymbol{\alpha}_J x$ to a meromorphic function of a single variable x, it may happen that the individual functions $M\big(-T\mathbf{s}, \mathfrak{u}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi})$ do not restrict. In other words, the line $\boldsymbol{\alpha}_J x$ may be entirely contained in the set of poles. If this is the case, we can compute (in polynomial time) a regular vector $\boldsymbol{\beta} \in \mathbb{Q}^J$ so that all functions $M\big(-T\mathbf{s} + \mathfrak{u}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\xi})$ occurring can be evaluated on $(\boldsymbol{\alpha}_J + \epsilon\boldsymbol{\beta})x$.

3.4. **The periodic dependence in T.** Now let us analyze the dependence in T of the functions $M(-T\mathbf{s}, \mathfrak{u}, \Lambda(\boldsymbol{\alpha}, f))$, where $\mathfrak{u}$ is a unimodular cone. Let the generators be $\mathbf{g}_i^{\mathfrak{u}}$, so the elements $\mathbf{g}_i^{\mathfrak{u}}$ form a basis of the lattice $\Lambda(\boldsymbol{\alpha}, f)$. Recall that the lattice $f\mathbb{Z}^r$ is contained in $\Lambda(\boldsymbol{\alpha}, f)$. Thus as $\mathbf{s} \in \mathbb{Z}^r$, we have $\mathbf{s} = \sum_i s_i \mathbf{g}_i^{\mathfrak{u}}$ with $fs_i \in \mathbb{Z}$ and hence $\{-T\mathbf{s}\}_{\mathfrak{u}} = \sum_i \{-Ts_i\}\mathbf{g}_i^{\mathfrak{u}}$ with $\{-Ts_i\}$ a function of T periodic modulo f.

Thus the function $T \mapsto \{-T\mathbf{s}\}_{\mathfrak{u}}$ is a step linear function, modulo f, with value in V. We then write

$$M(-T\mathbf{s}, \mathfrak{u})(\boldsymbol{\xi}) = \mathrm{e}^{\langle \boldsymbol{\xi}, \{T\mathbf{s}\}_{\mathfrak{u}} \rangle} \prod_{j=1}^{r} \frac{1}{(1 - \mathrm{e}^{\langle \boldsymbol{\xi}, \mathbf{g}_j \rangle})},$$

and hence finally

$$\mathcal{F}(\boldsymbol{\alpha}, f, T)(x) = f\, M\big(-T\mathbf{s}, \mathbb{R}^J_{\geq 0}, \Lambda(\boldsymbol{\alpha}, f)\big)(\boldsymbol{\alpha}_J x) \prod_{j\colon f | \alpha_j} \frac{1}{(1 - \mathrm{e}^{\alpha_j x})}.$$

This is a meromorphic function of the variable x. Near $x = 0$, it is of the form

$$\sum_{\mathfrak{u}} \exp\{l_{\mathfrak{u}}(T)x\} h(x)/x^{N+1}$$

where $h(x)$ is holomorphic in x and $l_{\mathfrak{u}}(T)$ is a step linear function of T, modulo f. Thus to compute

$$E_i(f)(T) = \mathrm{res}_{x=0} \frac{(-x)^i}{i!} \mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$$

we only have to expand the function $x \mapsto \exp\{l_{\mathfrak{u}}(T)x\}$ up to the power x^{N-i}. This expansion can be done in polynomial time. We thus see that as stated in Theorem 3.8, $E_i(f)(T)$ is a step polynomial of degree less than or equal to $(N - i)$, which is periodic of T modulo f. This completes the proof of Theorem 3.8 and thus the proof of Theorem 2.4.

4. Recovering the first periodic coefficient

Now that we have the main algorithmic result we can prove some consequences to the description of the periodicity of the coefficients. In this section, we determine the largest degree with a truly periodic coefficient and we give a polynomial time algorithm for computing it. This will complete the proof of Theorem 1.3.

Theorem 4.1. *Given as input a list of integers $\boldsymbol{\alpha} = [\alpha_1, \ldots, \alpha_{N+1}]$ with their prime factorization $\alpha_i = p_1^{a_{i1}} p_2^{a_{i2}} \cdots p_n^{a_{in}}$, there is a polynomial time algorithm to find all of the largest sublists where the greatest common divisor is not one. Moreover, if ℓ denotes the size of the largest sublists with greatest common divisor different from one, then (1) there are polynomially many such sublists, (2) the poset $\tilde{P}_{>\ell-1}$ is a fan (a poset with a maximal element and adjacent atoms), and (3) the Möbius function for $P_{>\ell-1}$ is $\mu(f) = 1$ if $G(f) \neq G(1)$ and $\mu(1) = 1 - (|\mathcal{G}_{>\ell-1}(\boldsymbol{\alpha})| - 1)$.*

Proof. Consider the matrix $A = [a_{ij}]$. Let $c_{i_1}, \ldots, c_{i_k}$ be column indices of A that denote the columns that contain the largest number of non-zero elements among the columns. Let $\boldsymbol{\alpha}^{(c_{i_j})}$ be the sublist of $\boldsymbol{\alpha}$ that corresponds to the rows of A where column c_{i_j} has a non-zero entry. Each $\boldsymbol{\alpha}^{(c_{i_j})}$ has greatest common divisor different from one. If ℓ is the size of the largest sublist of $\boldsymbol{\alpha}$ with greatest common divisor different from one, then there are ℓ many α_i's that share a common prime. Hence each column c_{i_1} of A has ℓ many non-zero elements.

Then each $\boldsymbol{\alpha}^{(c_{i_j})}$ is a largest sublist where the greatest common divisor is not one. Note that more than one column index c_i might produce the same sublist $\boldsymbol{\alpha}^{(c_{i_j})}$. The construction of A, counting the non-zero elements of each column, and forming the sublist indexed by each c_{i_j} can be done in polynomial time in the input size.

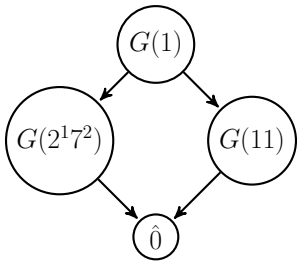
To show the poset $\tilde{P}_{>\ell-1}$ is a fan, let $\mathcal{G} = \{1, f_1, \ldots, f_m\}$ be the set of greatest common divisors of sublists of size $> \ell - 1$. Each f_i corresponds to a greatest common divisor of a sublist $\boldsymbol{\alpha}^{(i)}$ of $\boldsymbol{\alpha}$ with size ℓ. We cannot have $f_i \mid f_j$ for $i \neq j$ because if $f_i \mid f_j$, then f_i is also the greatest common divisor of $\boldsymbol{\alpha}^{(i)} \cup \boldsymbol{\alpha}^{(j)}$, a contradiction to the maximality of ℓ. Then the Möbius function is $\mu(f_i) = 1$, and $\mu(1) = 1 - m$.

As an aside, $\gcd(f_i, f_j) = 1$ for all $f_i \neq f_j$ as if $\gcd(f_i, f_j) \neq 1$, then we can take the union of the sublist that produced f_i and f_j thereby giving a larger sublist with greatest common divisor not equal to one, a contradiction. □

Example 4.2. $[2^2 7^4 41^1, 2^1 7^2 11^1, 11^4, 17^3]$ gives the matrix

$$\begin{pmatrix} 2 & 4 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 \end{pmatrix}$$

where the columns are the powers of the primes indexed by $(2, 7, 11, 17, 41)$. We see the largest sublists that have gcd not equal to one are $[2^2 7^4 41^1, 2^1 7^2 11^1]$ and $[2^1 7^2 11^1, 11^4]$. Then $\mathcal{G} = \{1, 2^1 7^2, 11\}$. The poset $P_{>1}$ is



and $\mu(1) = -1$, $\mu(11) = \mu(2^1 7^2) = 1$.

Proof of Theorem 1.3. Let ℓ be the greatest integer for which there exists a sublist $\boldsymbol{\alpha}_J$ with $|J| = \ell$, such that its gcd f is not 1. Then for $m \geq \ell$ the coefficient of degree m, $E_m(T)$, is constant because in Equation 3.6, $\mathcal{G}_{>m}(\boldsymbol{\alpha}) = \{1\}$. Hence $E_m(T)$ does not depend on T. We now focus on $E_{\ell-1}(T)$. To simplify Equation 3.6, we first compute the $\mu(f)$ values.

Lemma 4.3. *For ℓ as in Theorem 1.3, the poset $\mathcal{G}_{>\ell-1}(\boldsymbol{\alpha})$ is a fan, with one maximal element 1 and adjacent elements f which are pairwise coprime. In particular, $\mu(f) = 1$ for $f \neq 1$.*

Proof. Let $\boldsymbol{\alpha}_{J_1}$, $\boldsymbol{\alpha}_{J_2}$ be two sublists of length ℓ with gcd's $f_1 \neq f_2$ both not equal to 1. If f_1 and f_2 had a nontrivial common divisor d, then the list $\boldsymbol{\alpha}_{J_1 \cup J_2}$ would have a gcd not equal to 1, in contradiction with its length being strictly greater than ℓ. □

Next we recall a fact about Fourier series and use it to show that each f-term in Equation 3.6 has smallest period f.

Lemma 4.4. *Let f be a positive integer and let $\phi(t)$ be a periodic function on $\mathbb{Z}/f\mathbb{Z}$ with Fourier expansion*

$$\phi(t) = \sum_{n=0}^{f-1} c_n \mathrm{e}^{2i\pi\frac{nt}{f}}.$$

If $c_n \neq 0$ for some n which is coprime to f then $\phi(t)$ has smallest period equal to f.

Proof. Assume $\phi(t)$ has period m with $f = qm$ and $q > 1$. We write its Fourier series as a function of period m.

$$\phi(t) = \sum_{j=0}^{m-1} c'_j \mathrm{e}^{2i\pi\frac{jt}{m}} = \sum_{j=0}^{m-1} c'_j \mathrm{e}^{2i\pi\frac{(jq)t}{f}}.$$

By uniqueness of the Fourier coefficients, we have $c_n = 0$ if n is not a multiple of q (and $c_{qj} = c'_j$). In particular, $c_n = 0$ if n is coprime to f, a contradiction. □

Lemma 4.5. *The f-term in (3.6) has smallest period f as a function of T.*

Proof. For $f = 1$, the statement is clear. Assume $f \neq 1$. We observe that the f-term in (3.6) is a periodic function (of period f) which is *given as the sum of its Fourier expansion* and is written as $\sum_{n=0}^{f-1} c_n \mathrm{e}^{-2i\pi\frac{nT}{f}}$ where

$$c_n = -\operatorname{res}_{x=0} \frac{(-x)^{\ell-1}}{(\ell-1)!\prod(1-\mathrm{e}^{-2i\pi\frac{n\alpha_j}{f}}\mathrm{e}^{\alpha_j x})}.$$

Consider a coefficient for which n is coprime to f. We decompose the product according to whether f divides α_j or not. The crucial observation is that there are exactly ℓ indices j such that f divides α_j, because of the maximality assumption on ℓ. Therefore $x = 0$ is a simple pole and the residue is readily computed. We obtain

$$c_n = \frac{(-1)^{\ell-1}}{(\ell-1)!} \frac{1}{\prod_{j:f\nmid\alpha_j}(1-\mathrm{e}^{2i\pi\frac{n\alpha_j}{f}})} \frac{1}{\prod_{j:f|\alpha_j}\alpha_j}.$$

Thus $c_n \neq 0$ for an n coprime with f. By Lemma 4.4, each f-term has minimal period f. □

As the various f's in $\mathcal{G}_{>\ell-1}(\alpha)$ different from 1 are pairwise coprime and have minimal period f, $E_{\ell-1}(T)$ has minimal period $\prod_{f\in\mathcal{G}_{>\ell-1}(\boldsymbol{\alpha})} f > 1$. □

5. Summary of the algorithm and computational experiments

In this last section we report on experiments using our algorithm. But first, let us review the key steps of the algorithm:

Given a sequence of integers $\boldsymbol{\alpha}$ of length $N+1$, we wish to compute the top $k+1$ coefficients of the quasi-polynomial $E(\boldsymbol{\alpha})(t)$ of degree N. Recall that

$$E(\boldsymbol{\alpha})(t) = \sum_{i=0}^{N} E_i(t) t^i$$

where $E_i(t)$ is a periodic function of t modulo some period q_i. We assume that greatest common divisor of the list $\boldsymbol{\alpha}$ is 1.

1. We have
$$E(\boldsymbol{\alpha})(t) = E_{\mathcal{P}_{>N-k}}(t) + E_{\mathcal{P}_{\leq N-k}}(t)$$
with $E_{\mathcal{P}_{\leq N-k}}(t)$ a periodic polynomial of degree strictly less than $N-k$. Computing the first $k+1$ coefficients means to compute $E_{\mathcal{P}_{>N-k}}(t)$.

2. By writing $[\mathcal{P}_{>N-k}] = \sum_{f\in\mathcal{F}_{>N-k}(\boldsymbol{\alpha})} \mu(f)[G(f)]$, we have
$$E_{\mathcal{P}_{>N-k}}(t) = \sum_{f\in\mathcal{F}_{>N-k}(\boldsymbol{\alpha})} \mu(f) E(f,\boldsymbol{\alpha})(t).$$

3. Fix f an integer. Write
$$\mathcal{F}(\boldsymbol{\alpha}, f, T)(x) = \sum_{\zeta^f=1} \frac{\zeta^{-T}}{\prod_{i=1}^{N+1}(1-\zeta^{\alpha_i}\mathrm{e}^{\alpha_i x})};$$
$$E(f,\boldsymbol{\alpha})(t) = \sum_i t^i E_i(f)(t) \text{ with}$$
$$E_i(f)(T) = \mathrm{res}_{x=0}(-x)^i/i!\cdot\mathcal{F}(\boldsymbol{\alpha}, f, T)(x).$$

4. We fix f and let r be the number of elements α_i such that α_i is not a multiple of f.
We then list such α_i in the list $\boldsymbol{\alpha} = [\alpha_1, \alpha_2, \ldots, \alpha_r]$.
We introduce a lattice $\Lambda := \Lambda(\boldsymbol{\alpha}, f) \subset \mathbb{Z}^r$ and an element $\mathbf{s}\in\mathbb{Z}^r$ so that $f\mathbf{s}\in\Lambda$.
We decompose the standard cone $\mathbb{R}^I_{\geq 0}$ as a signed decomposition, modulo cones containing lines, in unimodular cones $\mathfrak{u}$ for the lattice Λ obtaining
$$\mathcal{F}(\boldsymbol{\alpha}, f, T)(x) = \sum_{\mathfrak{u}} \epsilon_{\mathfrak{u}} M(T\mathbf{s}, \mathfrak{u}, \Lambda)(\boldsymbol{\alpha}_I x) \frac{1}{\prod_{i:\ f|\alpha_i}(1-\mathrm{e}^{\alpha_i x})}.$$

5. To compute $E_{N-i}(f)(T)$, we compute the Laurent series of $\mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$ at $x=0$ and take the coefficient in x^{-N-1+i} of this Laurent series. As the Laurent series of $\mathcal{F}(\boldsymbol{\alpha}, f, T)(x)$ starts by x^{-N-1}, if i is less than k, we just have to compute at most k terms of this Laurent series.

5.1. **Experiments.** We first wrote a preliminary implementation of our algorithm in `Maple`, which we call *M-Knapsack* in the following. Later we developed a faster implementation in C++, which is released as part of the `LattE integrale` software package, version 1.7, and is referred to as *LattE Knapsack* in the following. Both `LattE integrale` and *M-Knapsack* are available at `http://www.math.ucdavis.edu/~latte/software.php`

We report on two different benchmarks tests:

(1) We test the performance of the *M-Knapsack*[2], *LattE Knapsack*[3] and the *LattE Top-Ehrhart*[4] algorithm from [3] on a collection of over 750 knapsacks. The latter algorithm can compute the weighted Ehrhart quasi-polynomials for simplicial polytopes, and hence it is more general than the algorithm we present in this paper, but this is the only other available algorithm for computing coefficients directly. Note that the implementations of the *M-Knapsack* algorithm and the main computational part of the *LattE Top-Ehrhart* algorithm are in `Maple`, making comparisons between the two easier.

[2]Maple usage: coeff_Nminusk_knapsack(⟨knapsack list⟩, t, ⟨k value list⟩);

[3]Command line usage: ./topKnapsack -f ⟨knapsack file⟩ -o ⟨output file⟩ -k ⟨k value⟩

[4]Command line usage: ./integrate –valuation=top-ehrhart –top-ehrhart-save=⟨output file⟩ –num-coefficients=⟨k value⟩ ⟨knapsack file⟩

(2) Next, we run our algorithms on a few knapsacks that have been studied in the literature. We chose these examples because some of these problems are considered difficult in the literature. We also present a comparison with other available software that can also compute information of the denumerant $E_{\boldsymbol{\alpha}}(t)$ the code *CTEuclid6* [30] and *pSn* [28]. These routines use different mathematical ideas that those used in this paper. These `Maple` packages are also available at `http://www.math.ucdavis.edu/~latte/software.php`

All computations were performed on a 64-bit Ubuntu machine with 64 GB of RAM and eight Dual Core AMD Opteron 880 processors.

5.2. ***M-Knapsack* vs. *LattE Knapsack* vs. *LattE Top-Ehrhart*.** Here we compare our two implementations with the *LattE Top-Ehrhart* algorithm from [3]. We constructed a test set of 768 knapsacks. For each $3 \leq d \leq 50$, we constructed four families of knapsacks:

random-3: Five random knapsacks in dimension $d-1$ where $a_1 = 1$ and the other coefficients, $a_2, \ldots, a_d$, are 3-digit random numbers picked uniformly

random-15: Similar to the previous case, but with a 15-digit random number

repeat: Five knapsacks in dimension $d-1$ where $\alpha_1 = 1$ and all the other α_i's are the same 3-digit random number. These produce few poles and have a simple poset structure. These are among the simplest knapsacks that produce periodic coefficients.

partition: One knapsack in the form $\alpha_i = i$ for $1 \leq i \leq d$.

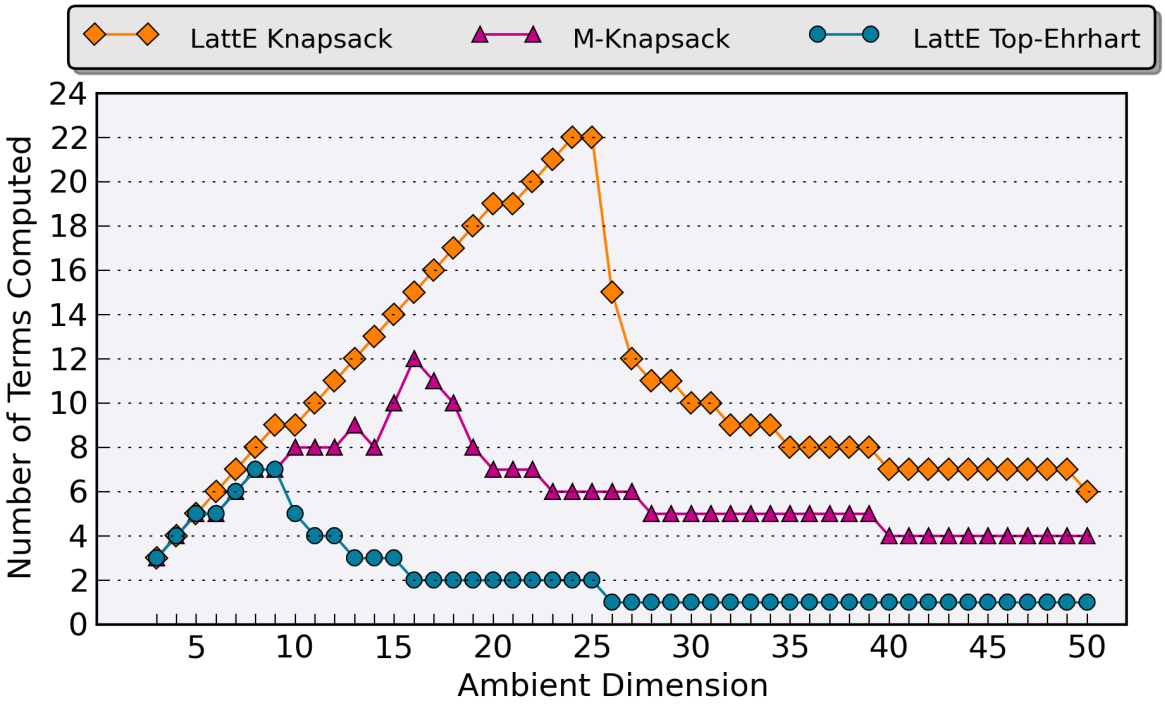
For each knapsack, we try to compute the highest degree term of the quasi-polynomial in under 200 seconds. If the computation is successful, we continue to compute the next highest degree term under a new 200 second limit. Once a term takes longer than 200 seconds to compute, we stop the program and start with a new knapsack. Figures 1, 2, 3, 4 show the maximum number of terms in the quasi-polynomial that can be computed when each term has a 200 second limit on the random-3, random-15, repeat, and partition knapsacks, respectively. For example, in Figure 1, for each of the five random 3-digit knapsacks in ambient dimension 50, the *LattE Knapsack* method computed at most 6 terms of an Ehrhart polynomial, the *M-Knapsack* computed at most four terms, and the *LattE Top-Ehrhart* method computed at most one term where each term took at most 200 seconds.

In each knapsack family, we see that each algorithm has a "peak" dimension where after it, the number of terms that can be computed in under 200 seconds quickly decreases; for the *LattE Knapsack* method, this is around dimension 25 in each knapsack family. In each family, there is a clear order to which algorithm can compute the most: *LattE Knapsack* computes the most coefficients, while the *LattE Top-Ehrhart* method computes the least number of terms. In Figure 3, the simple poset structure helps every method to compute more terms, but the two `Maple` scripts seem to benefit more than the *LattE Knapsack* method.

Figure 4 demonstrates the power of the LattE implementation. Note that a knapsack of this particular form in dimension d does not start to have periodic terms until around $d/2$. Thus even though half of the coefficients are only constants we see that the *M-Knapsack* code cannot compute past a few periodic term in dimension 10–15 while the *LattE Knapsack* method is able to compute the entire polynomial.

In Figure 5 we plot the average speedup ratio between the *M-Knapsack* and *LattE Top-Ehrhart* implementations along with the maximum and minimum speedup ratios (we wrote both algorithms in `Maple`). The ratios are given by the time it takes *LattE Top-Ehrhart* to compute a term, divided by the time it takes *M-Knapsack* to compute the same term, where

FIGURE 1. Random 3-digit knapsacks: Maximum number of coefficients each algorithm can compute where each coefficient takes less than 200 seconds.



both times are between 0 and 200 seconds. For example, among all the terms computed in dimension 15 from random 15-digit knapsacks, the average speedup between the two methods was 8000, the maximum ratio was 20000, and the minimum ratio was 200. We see that in dimensions 3–10, there are a few terms for which the *LattE Top-Ehrhart* method was faster than the *M-Knapsack* method, but this only occurs for the highest degree terms. Also, after dimension 25, there is little variance in the ratios because the *LattE Top-Ehrhart* method is only computing one term. Similar results hold for the other knapsack families, and so their plots are omitted.

5.3. **Other examples.** Next we focus on ten problems listed in Table 1. Some of these selected problems have been studied before in the literature [1, 14, 30, 29]. Table 2 shows the time in seconds to compute the full Ehrhart quasipolynomial using the *M-Knapsack*, *LattE Knapsack* and *LattE Top-Ehrhart* codes with two other algorithms: *CTEuclid6* and *pSn*.

The *CTEuclid6* [5] algorithm [30] computes the lattice point count of a polytope, and supersedes an earlier algorithm in [29]. Instead of using Barvinok's algorithm to construct unimodular cones, the main idea used by the *CTEuclid6* algorithm to find the constant term in the generating function $F(\alpha)(z)$ relies on recursively computing partial fraction decompositions to construct the series. Notice that the *CTEuclid6* method only computes the number of integer points in one dilation of a polytope and not the full Ehrhart polynomial. We can estimate how long it would take to find the Ehrhart polynomial using an interpolation method by computing the time it takes to find one lattice point count times the periodicity

[5]Maple usage: CTEuclid($F(\boldsymbol{\alpha})(x)/x^b$, t, [x]); where $b = \alpha_1 + \cdots + \alpha_{N+1}$

FIGURE 2. Random 15-digit knapsacks: Maximum number of coefficients each algorithm can compute where each coefficient takes less than 200 seconds.

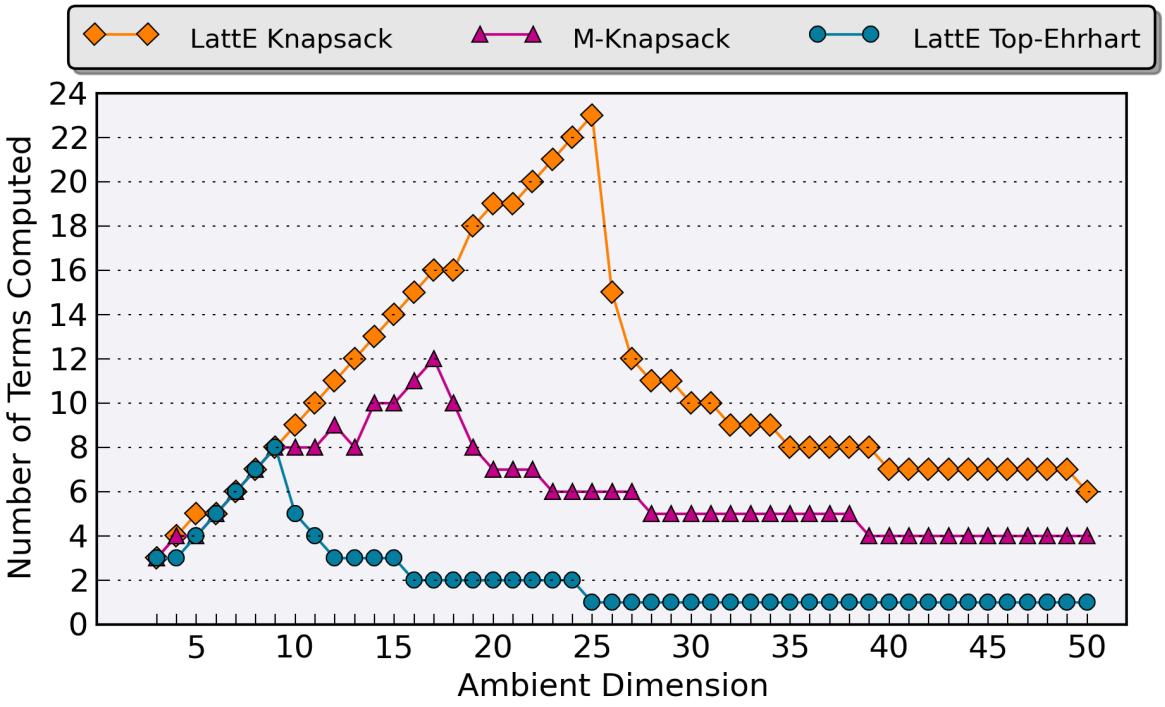


FIGURE 3. Repeat knapsacks: Maximum number of coefficients each algorithm can compute where each coefficient takes less than 200 seconds.

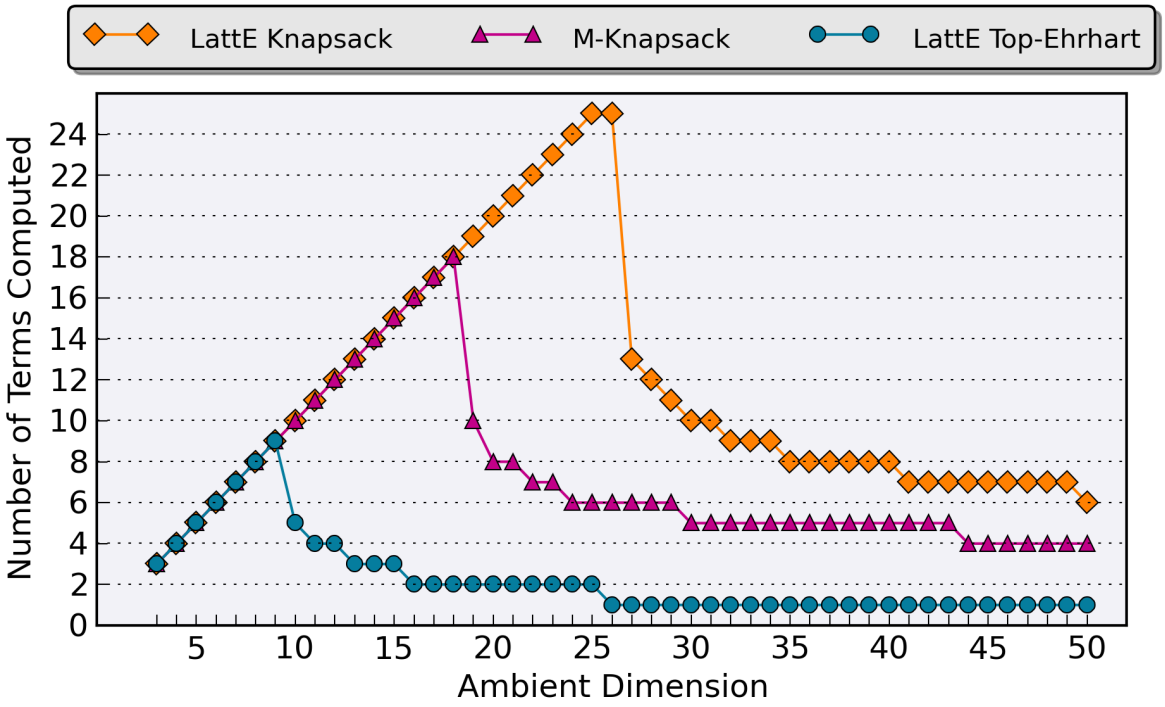


FIGURE 4. Partition knapsacks: Maximum number of coefficients each algorithm can compute where each coefficient takes less than 200 seconds.

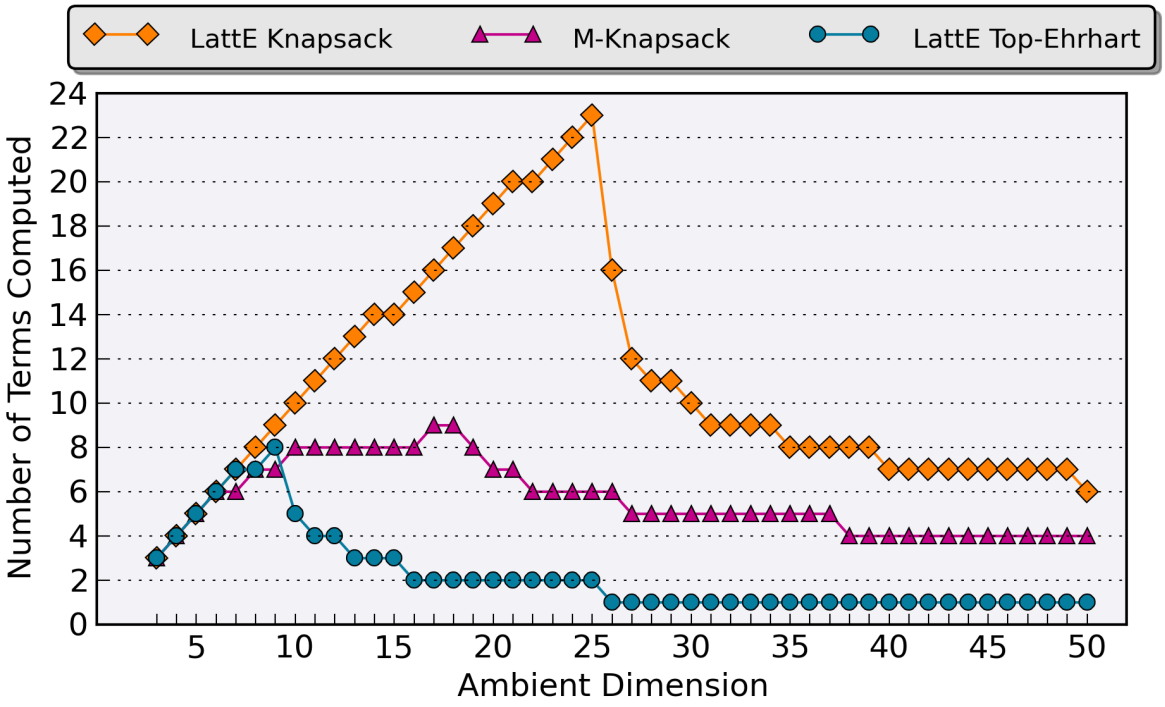
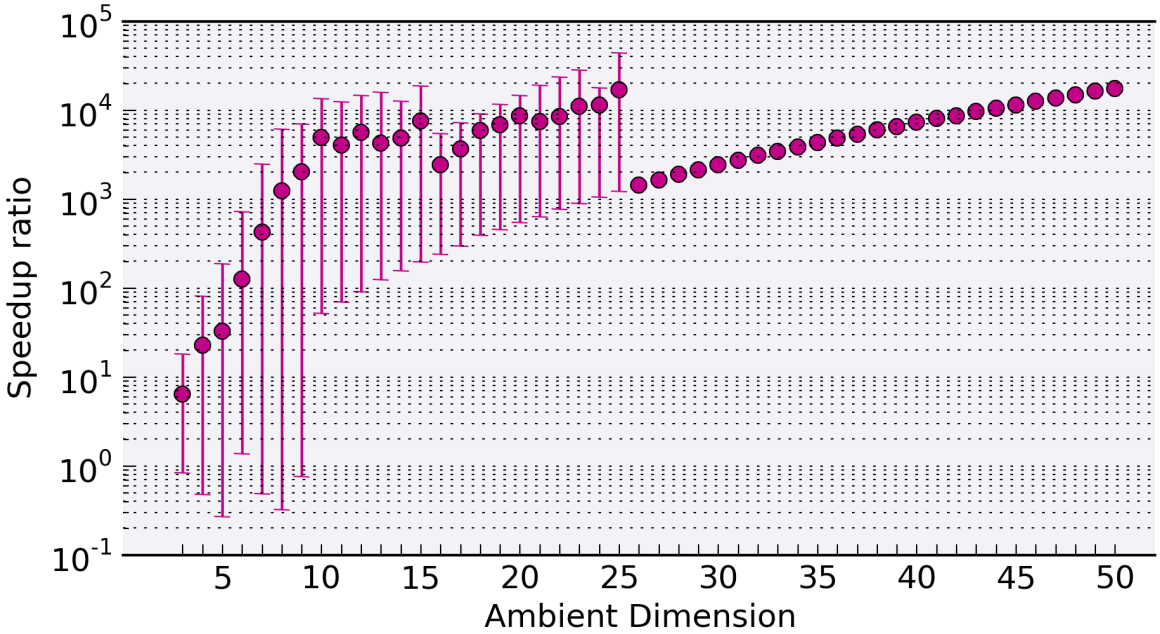


FIGURE 5. Average speedup ratio (dots) between the *M-Knapsack* and *LattE Top-Ehrhart* codes along with maximum and minimum speedup ratio bounds (vertical lines) for the random 15-digit knapsacks.



of the polynomial and degree. Hence, in Table 2, column "one point" refers to the running time of finding one lattice point count, while column "estimate" is an estimate for how long it would take to find the Ehrhart polynomial by interpolation. We see that the *CTEuclid6* algorithm is fast for finding the number of integer points in a knapsack, but this would lead to a slow method for finding the Ehrhart polynomial.

The *pSn* [6] algorithm of [28] computes the full Ehrhart quasi polynomial by using a partial fraction decomposition based method. More precisely the quasipolynomials are represented as a function $f(t)$ given by q polynomials $f^{[1]}(t), f^{[2]}(t), \ldots, f^{[q]}(t)$ such that $f(t) = f^{[i]}(t)$ when $t \equiv i \pmod{q}$. To find the coefficients of the $f^{[i]}$ their method finds the first few terms of the Maclaurin expansion of the partial fraction decomposition to find enough evaluations of those polynomials and then recovers the coefficients of each the $f^{[i]}$ as a result of solving a linear system. This algorithm goes back to Cayley and it was implemented in `Maple`. Looking at Table 2, we see that the *pSn* method is competitive with *LattE Knapsack* for knapsacks $1, 2, \ldots, 6$, and beats *LattE Knapsack* in knapsack 10. However, the *pSn* method is highly sensitive to the number of digits in the knapsack coefficients, unlike our *M-Knapsack* and *LattE Knapsack* methods. For example, the knapsacks $[1, 2, 4, 6, 8]$ takes 0.320 seconds to find the full Ehrhart polynomial, $[1, 20, 40, 60, 80]$ takes 5.520 seconds, and $[1, 200, 600, 900, 400]$ takes 247.939 seconds. Similar results hold for other three-digit knapsacks in dimension four. However, the partition knapsack $[1, 2, 3, \ldots, 50]$ only takes 102.7 seconds. Finally, comparing the two `Maple` scripts, the *LattE Top-Ehrhart* method outperforms the *M-Knapsack* method.

Table 2 ignores one of the main features of our algorithm: that it can compute just the top k terms of the Ehrhart polynomial. In Table 3, we time the computation for finding the top three and four terms of the Ehrhart polynomial on the knapsacks in Table 1. We immediately see that our *LattE Knapsack* method takes less than one thousandth of a second in each example. Comparing the two `Maple` scripts, *M-Knapsack* greatly outperforms *LattE Top-Ehrhart*. Hence, for a fixed k, the *LattE Knapsack* is the fastest method.

In summary, the *LattE Knapsack* is the fastest method for computing the top k terms of the Ehrhart polynomial. The *LattE Knapsack* method can also compute the full Ehrhart polynomial in a reasonable amount of time up to around dimension 25, and the number of digits in each knapsack coefficient does not significantly alter performance. However, if the coefficients each have one or two digits, the *pSn* method is faster, even in large dimensions.

[6] Maple usage: QPStoTrunc(pSn(⟨knapsack list⟩,n,j),n); where j is the smallest value in $\{100, 200, 500, 1000, 2000, 3000\}$ that produces an answer

TABLE 1. Ten selected instances

Problem	Data
#1	$[8, 12, 11]$
#2	$[5, 13, 2, 8, 3]$
#3	$[5, 3, 1, 4, 2]$
#4	$[9, 11, 14, 5, 12]$
#5	$[9, 10, 17, 5, 2]$
#6	$[1, 2, 3, 4, 5, 6]$
#7	$[12223, 12224, 36674, 61119, 85569]$
#8	$[12137, 24269, 36405, 36407, 48545, 60683]$
#9	$[20601, 40429, 40429, 45415, 53725, 61919, 64470, 69340, 78539, 95043]$
#10	$[5, 10, 10, 2, 8, 20, 15, 2, 9, 9, 7, 4, 12, 13, 19]$

TABLE 2. Computation times in seconds for finding the full Ehrhart polynomial using five different methods.

	LattE Knapsack	*M-Knapsack*	*LattE Top-Ehrhart*	CTEuclid6		pSn
				One point	estimate	
#1	0	0.316	0.160	0.004	3.168	0.328
#2	0.03	5.984	2.208	0.048	347.4	0.292
#3	0.02	4.564	0.148	0.031	9.60	0.212
#4	0.08	18.317	3.884	0.112	7761.6	0.496
#5	0.06	15.200	3.588	0.096	734.4	0.392
#6	0.11	37.974	8.068	0.088	31.68	0.336
#7	0.19	43.006	8.424	0.436	9.466×10^{20}	>30min
#8	1.14	1110.857	184.663	2.120	8.530×10^{20}	>30min
#9	>30min	>30min	>30min	>30min	>30min	>30min
#10	>30min	>30min	>30min	142.792	1.333×10^{9}	2.336

TABLE 3. Computation times in seconds for finding the top three and four terms of the Ehrhart polynomial

	Top 3 coefficients			Top 4 coefficients		
	LattE Knapsack	*M-Knapsack*	*LattE Top-Ehrhart*	*LattE Knapsack*	*M-Knapsack*	*LattE Top-Ehrhart*
#1	0	0.305	0.128	–	–	–
#2	0	0.004	0.768	0	0.096	1.356
#3	0	0.004	0.788	0	0.080	1.308
#4	0	0.003	0.792	0	0.124	1.368
#5	0	0.004	0.784	0	0.176	1.424
#6	0	0.004	1.660	0	0.088	2.976
#7	0	0.004	0.836	0	0.272	1.652
#8	0	0.068	1.828	0	0.112	3.544
#9	0	0.004	18.437	0	0.016	59.527
#10	0	0.012	142.104	0	0.044	822.187

Acknowledgments. We are grateful to Doron Zeilberger for his suggestions and comments. The work for this article was done in large part during a SQuaRE program at the American Institute of Mathematics, Palo Alto, in March 2012. V. Baldoni was partially supported by the Cofin 40%, MIUR. De Loera was partially supported by NSF grant DMS-0914107, M. Köppe was partially supported by NSF grant DMS-0914873. B. Dutra was supported by the NSF-VIGRE grant DMS-0636297. The support received is gratefully acknowledged.

References

[1] K. Aardal and A. K. Lenstra, *Hard equality constrained integer knapsacks*, Math. Oper. Res. **29** (2004), no. 3, 724–738. MR 2082626 (2005g:90085)

[2] G. E. Andrews, *The theory of partitions*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1998, Reprint of the 1976 original. MR 1634067 (99c:11126)

[3] V. Baldoni, N. Berline, J. A. De Loera, M. Köppe, and M. Vergne, *Computation of the highest coefficients of weighted Ehrhart quasi-polynomials of rational polyhedra*, Foundations of Computational Mathematics (2011), Published online 12 November 2011.

[4] V. Baldoni, N. Berline, M. Köppe, and M. Vergne, *Intermediate sums on polyhedra: Computation and real Ehrhart theory*, Mathematika **59** (2013), 1–22.

[5] A. Barvinok and K. Woods, *Short rational generating functions for lattice point problems*, J. Amer. Math. Soc. **16** (2003), no. 4, 957–979 (electronic). MR 1992831 (2004e:05009)

[6] A. I. Barvinok, *Polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed*, Mathematics of Operations Research **19** (1994), 769–779.

[7] ———, *Computing the Ehrhart quasi-polynomial of a rational simplex*, Math. Comp. **75** (2006), no. 255, 1449–1466.

[8] ———, *Integer points in polyhedra*, Zürich Lectures in Advanced Mathematics, European Mathematical Society (EMS), Zürich, Switzerland, 2008.

[9] A. I. Barvinok and J. E. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, New Perspectives in Algebraic Combinatorics (L. J. Billera, A. Björner, C. Greene, R. E. Simion, and R. P. Stanley, eds.), Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, Cambridge, 1999, pp. 91–147.

[10] M. Beck, I. M. Gessel, and T. Komatsu, *The polynomial part of a restricted partition function related to the Frobenius problem*, Electron. J. Combin. **8** (2001), no. 1, Note 7, 5 pp. (electronic). MR 1855876 (2002f:05017)

[11] E. T. Bell, *Interpolated denumerants and Lambert series*, Amer. J. Math. **65** (1943), 382–386. MR 0009043 (5,92a)

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

[13] L. Comtet, *Advanced combinatorics*, enlarged ed., D. Reidel Publishing Co., Dordrecht, 1974, The art of finite and infinite expansions. MR 0460128 (57 #124)

[14] J. A. De Loera, R. Hemmecke, J. Tauzer, and R. Yoshida, *Effective lattice point counting in rational convex polytopes*, Journal of Symbolic Computation **38** (2004), no. 4, 1273–1302.

[15] M. Dyer and R. Kannan, *On Barvinok's algorithm for counting lattice points in fixed dimension*, Mathematics of Operations Research **22** (1997), 545–549.

[16] E. Ehrhart, *Polynômes arithmétiques et méthode des polyèdres en combinatoire*, Birkhäuser Verlag, Basel, 1977, International Series of Numerical Mathematics, Vol. 35. MR 0432556 (55 #5544)

[17] D. Einstein, D. Lichtblau, A. Strzebonski, and S. Wagon, *Frobenius numbers by lattice point enumeration*, Integers **7** (2007), A15, 63. MR 2299816 (2008a:11031)

[18] R. Hemmecke, A. Takemura, and R. Yoshida, *Computing holes in semi-groups and its application to transportation problems*, Contributions to Discrete Mathematics **4** (2009), 81–91.

[19] P. Henrici, *Applied and computational complex analysis. Vol. 3*, Pure and Applied Mathematics (New York), John Wiley & Sons Inc., New York, 1986, Discrete Fourier analysis—Cauchy integrals—construction of conformal maps—univalent functions, A Wiley-Interscience Publication. MR 822470 (87h:30002)

[20] ———, *Applied and computational complex analysis. Vol. 1*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1988, Power series—integration—conformal mapping—location of zeros, Reprint of the 1974 original, A Wiley-Interscience Publication. MR 1008928 (90d:30002)
[21] ———, *Applied and computational complex analysis. Vol. 2*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1991, Special functions—integral transforms—asymptotics—continued fractions, Reprint of the 1977 original, A Wiley-Interscience Publication. MR 1164865 (93b:30001)
[22] R. Kannan, *Lattice translates of a polytope and the Frobenius problem*, Combinatorica **12** (1992), no. 2, 161–177. MR 1179254 (93k:52015)
[23] H. Kellerer, U. Pferschy, and D. Pisinger, *Knapsack problems*, Springer-Verlag, Berlin, 2004. MR 2161720 (2006d:90002)
[24] P. Lisoněk, *Denumerants and their approximations*, J. Combin. Math. Combin. Comput. **18** (1995), 225–232. MR 1334651 (96a:05009)
[25] S. Martello and P. Toth, *Knapsack problems*, Wiley-Interscience Series in Discrete Mathematics and Optimization, John Wiley & Sons Ltd., Chichester, 1990, Algorithms and computer implementations. MR 1086874 (92a:90006)
[26] J. L. Ramírez Alfonsín, *The Diophantine Frobenius problem*, Oxford Lecture Series in Mathematics and its Applications, vol. 30, Oxford University Press, Oxford, 2005. MR 2260521 (2007i:11052)
[27] J. Riordan, *An introduction to combinatorial analysis*, Dover Publications Inc., Mineola, NY, 2002, Reprint of the 1958 original [Wiley, New York; MR0096594 (20 #3077)]. MR 1949650
[28] A. Sills and D. Zeilberger, *Formulæ for the number of partitions of n into at most m parts (using the quasi-polynomial ansatz)*, Adv. in Appl. Math. **48** (2012), 640–645.
[29] G. Xin, *A fast algorithm for MacMahon's partition analysis*, Electr. J. Comb. **11** (2004), no. 1.
[30] G. Xin, *A Euclid style algorithm for MacMahon partition analysis*, e-print http://arxiv.org/abs/1208.6074, 2012.

Velleda Baldoni: Dipartimento di Matematica, Università degli studi di Roma "Tor Vergata", Via della ricerca scientifica 1, I-00133 Roma, Italy
E-mail address: baldoni@mat.uniroma2.it

Nicole Berline: Centre de Mathématiques Laurent Schwartz, École Polytechnique, 91128 Palaiseau Cedex, France
E-mail address: nicole.berline@math.polytechnique.fr

Jesús A. De Loera: Department of Mathematics, University of California, Davis, One Shields Avenue, Davis, CA, 95616, USA
E-mail address: deloera@math.ucdavis.edu

Brandon E. Dutra: Department of Mathematics, University of California, Davis, One Shields Avenue, Davis, CA, 95616, USA
E-mail address: bedutra@ucdavis.edu

Matthias Köppe: Department of Mathematics, University of California, Davis, One Shields Avenue, Davis, CA, 95616, USA
E-mail address: mkoeppe@math.ucdavis.edu

Michèle Vergne: Institut de Mathématiques de Jussieu, Théorie des Groupes, Case 7012, 2 Place Jussieu, 75251 Paris Cedex 05, France
E-mail address: vergne@math.jussieu.fr