

COMPUTING THE EHRHART QUASI-POLYNOMIAL OF A RATIONAL SIMPLEX

ALEXANDER BARVINOK

April 2005

We present a polynomial time algorithm to compute any fixed number of the highest coefficients of the Ehrhart quasi-polynomial of a rational simplex. Previously such algorithms were known for integer simplices and for rational polytopes of a fixed dimension. The algorithm is based on the formula relating the k th coefficient of the Ehrhart quasi-polynomial of a rational polytope to volumes of sections of the polytope by affine lattice subspaces parallel to k -dimensional faces of the polytope. We discuss possible extensions and open questions.

1. INTRODUCTION AND MAIN RESULTS

Let $P \subset \mathbb{R}^d$ be a rational polytope, that is, the convex hull of a finite set of points with rational coordinates. Let $t \in \mathbb{N}$ be a positive integer such that the vertices of the dilated polytope

$$tP = \left\{ tx : x \in P \right\}$$

are integer vectors. As is known, see, for example, Section 4.6 of [St97], there exist functions $e_i(P; \cdot) : \mathbb{N} \rightarrow \mathbb{Q}$, $i = 0, \dots, d$, such that

$$e_i(P; n+t) = e_i(P; n) \quad \text{for all } n \in \mathbb{N}$$

and

$$|nP \cap \mathbb{Z}^d| = \sum_{i=0}^d e_i(P; n)n^i \quad \text{for all } n \in \mathbb{N}.$$

The function on the right hand side is called the *Ehrhart quasi-polynomial* of P . It is clear that if $\dim P = d$ then $e_d(P; n) = \text{vol } P$. In this paper, we are interested in the computational complexity of the coefficients $e_i(P; n)$.

1991 *Mathematics Subject Classification.* 52C07, 05A15, 68R05.

Key words and phrases. Ehrhart quasi-polynomial, rational polytope, valuation, algorithm.

This research was partially supported by NSF Grant DMS 0400617.

If the dimension d is fixed in advance, the values of $e_i(P; n)$ for any given P , n , and i can be computed in polynomial time by interpolation, as implied by a polynomial time algorithm to count integer points in a polyhedron of a fixed dimension [B94a], [BP99].

If the dimension d is allowed to vary, it is an NP-hard problem to check whether $P \cap \mathbb{Z}^d \neq \emptyset$, let alone to count integer points in P . This is true even when P is a rational simplex, as exemplified by the knapsack problem see, for example, Section 16.6 of [Sc86]. If the polytope P is integral then the coefficients $e_i(P; n) = e_i(P)$ do not depend on n . In that case, for any k fixed in advance, computation of the Ehrhart coefficient $e_{d-k}(P)$ reduces in polynomial time to computation of the volumes of the $(d-k)$ -dimensional faces of P [B94b]. The algorithm is based on efficient formulas relating $e_{d-k}(P)$, volumes of the $(d-k)$ -dimensional faces, and cones of feasible directions at those faces, see [Mo93], [BP99], and [PT04]. In particular, if $P = \Delta$ is an integer simplex, there is a polynomial time algorithm for computing $e_{d-k}(\Delta)$ as long as k fixed in advance.

In this paper, we extend the last result to *rational* simplices (a d -dimensional rational simplex is the convex hull in \mathbb{R}^d of $(d+1)$ affinely independent points with rational coordinates).

- Let us fix an integer $k \geq 0$. The paper presents a polynomial time algorithm, which, given an integer $d \geq k$, a rational simplex $\Delta \subset \mathbb{R}^d$, and a positive integer n , computes the value of $e_{d-k}(\Delta; n)$.

We present the algorithm in Section 7 and discuss its possible extensions in Section 8.

In contrast to the case of an integral polytope, for a general rational polytope P computation of $e_i(P; n)$ cannot be reduced to computation of the volumes of faces and some functionals of the “angles” (cones of feasible direction) at the faces. A general result of McMullen [Mc78], see also [MS83] and [Mc93], asserts that the contribution of the i -dimensional face F of a rational polytope P to the coefficient $e_i(P; n)$ is a function of the volume of F , the cone of feasible directions of P at F , and the translation class of the affine hull $\text{aff}(F)$ of F modulo \mathbb{Z}^d .

Our algorithm is based on a new structural result, Theorem 1.3 below, relating the coefficient $e_{d-k}(P; n)$ to volumes of sections of P by affine lattice subspaces parallel to faces F of P with $\dim F \geq d-k$. Theorem 1.3 may be of interest in its own right.

(1.1) Valuations and polytopes. Let V be a d -dimensional real vector space and let $\Lambda \subset V$ be a lattice, that is, a discrete additive subgroup which spans V . A polytope $P \subset V$ is called a Λ -polytope or a *lattice polytope* if the vertices of P belong to Λ . A polytope $P \subset V$ is called Λ -rational or just *rational* if tP is a lattice polytope for some positive integer t .

For a set $A \subset V$, let $[A] : V \rightarrow \mathbb{R}$ be the indicator of A :

$$[A](x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

A complex-valued function ν on rational polytopes $P \subset V$ is called a *valuation* if it preserves linear relations among indicators of rational polytopes:

$$\sum_{i \in I} \alpha_i [P_i] = 0 \implies \sum_{i \in I} \alpha_i \nu(P_i) = 0,$$

where $P_i \subset V$ is a finite family of rational polytopes and α_i are rational numbers. We consider only Λ -valuations or *lattice valuations* ν that satisfy

$$\nu(P + u) = \nu(P) \quad \text{for all } u \in \Lambda,$$

see [MS83] and [Mc93].

A general result of McMullen [Mc78] states that if ν is a lattice valuation, $P \subset V$ is a rational polytope, and $t \in \mathbb{N}$ is a number such that tP is a lattice polytope then there exist functions $\nu_i(P; \cdot) : \mathbb{N} \rightarrow \mathbb{C}$, $i = 0, \dots, d$, such that

$$\nu(nP) = \sum_{i=0}^d \nu_i(P; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and

$$\nu_i(P; n+t) = \nu_i(P; n) \quad \text{for all } n \in \mathbb{N}.$$

Clearly, if we compute $\nu(mP)$ for $m = n, n+t, n+2t, \dots, n+dt$, we can obtain $\nu_i(P; n)$ by interpolation.

We are interested in the counting valuation E , where $V = \mathbb{R}^d$, $\Lambda = \mathbb{Z}^d$, and

$$E(P) = |P \cap \mathbb{Z}^d|$$

is the number of lattice points in P .

The idea of the algorithm is to replace valuation E by some other valuation, so that the coefficients $e_d(P; n), \dots, e_{d-k}(P; n)$ remain intact, but the new valuation can be computed in polynomial time on any given rational simplex Δ , so that the desired coefficient $e_{d-k}(\Delta; n)$ can be obtained by interpolation.

(1.2) Valuations E_L . Let $L \subset \mathbb{R}^d$ be a lattice subspace, that is, a subspace spanned by the points $L \cap \mathbb{Z}^d$. Suppose that $\dim L = k$ and let $pr : \mathbb{R}^d \rightarrow L$ be the orthogonal projection onto L . Let $P \subset \mathbb{R}^d$ be a rational polytope, let $Q = pr(P)$, $Q \subset L$, be its projection, and let $\Lambda = pr(\mathbb{Z}^d)$. Since L is a lattice subspace, $\Lambda \subset L$ is a lattice.

Let L^\perp be the orthogonal complement of L . Then $L^\perp \subset \mathbb{R}^d$ is a lattice subspace. We introduce the volume form vol_{d-k} on L^\perp which differs from the volume form inherited from \mathbb{R}^d by a scaling factor chosen so that the determinant of the lattice $\mathbb{Z}^d \cap L^\perp$ is 1. Consequently, the same volume form vol_{d-k} is carried by all translations $x + L^\perp$, $x \in \mathbb{R}^d$.

We consider the following quantity

$$E_L(P) = \sum_{m \in \Lambda} \text{vol}_{d-k}(P \cap (m + L^\perp)) = \sum_{m \in Q \cap \Lambda} \text{vol}_{d-k}(P \cap (m + L^\perp))$$

(clearly, for $m \notin Q$ the corresponding terms are 0).

In words: we take all lattice translates of L^\perp , select those that intersect P and add the volumes of the intersections.

Clearly, E_L is a lattice valuation, so

$$E_L(nP) = \sum_{i=0}^d e_i(P, L; n) n^i$$

for some periodic functions $e_i(P, L; \cdot)$. If tP is an integer polytope for some $t \in \mathbb{N}$ then

$$e_i(P, L; n+t) = e_i(P, L; n) \quad \text{for all } n \in \mathbb{N}$$

and $i = 0, \dots, d$.

Note that if $L = \{0\}$ then $E_L(P) = \text{vol } P$ and if $L = \mathbb{R}^d$ then $E_L(P) = |P \cap \mathbb{Z}^d|$, so the valuations E_L interpolate between the volume and the number of lattice points as $\dim L$ grows.

We prove that $e_{d-k}(P; n)$ can be represented as a linear combination of $e_{d-k}(P, L; n)$ for some lattice subspaces L with $\dim L \leq k$.

(1.3) Theorem. *Let us fix an integer $k \geq 0$. Let $P \subset \mathbb{R}^d$ be a full-dimensional rational polytope and let t be a positive integer such that tP is an integer polytope. For a $(d-k)$ -dimensional face F of P let $\text{lin}(F) \subset \mathbb{R}^d$ be the $(d-k)$ -dimensional subspace parallel to the affine hull $\text{aff}(F)$ of F and let $L^F = (\text{lin } F)^\perp$ be its orthogonal complement, so $L^F \subset \mathbb{R}^d$ is a k -dimensional lattice subspace.*

Let \mathcal{L} be a finite collection of lattice subspaces which contains the subspaces L^F for all $(d-k)$ -dimensional faces F of P and is closed under intersections. For $L \in \mathcal{L}$ let $\mu(L)$ be integer numbers such that the identity

$$\left[\bigcup_{L \in \mathcal{L}} L \right] = \sum_{L \in \mathcal{L}} \mu(L) [L]$$

holds for the indicator functions of the subspaces from \mathcal{L} .

Let us define

$$\nu(nP) = \sum_{L \in \mathcal{L}} \mu(L) E_L(nP) \quad \text{for } n \in \mathbb{N}.$$

Then there exist functions $\nu_i(P; \cdot) : \mathbb{N} \longrightarrow \mathbb{Q}$, $i = 0, \dots, d$, such that

$$(1.3.1) \quad \nu(nP) = \sum_{i=0}^d \nu_i(P; n) n^i \quad \text{for all } n \in \mathbb{N},$$

$$(1.3.2) \quad \nu_i(P; n+t) = \nu_i(P; n) \quad \text{for all } n \in \mathbb{N},$$

and

$$(1.3.3) \quad e_{d-i}(P; n) = \nu_{d-i}(P; n) \quad \text{for all } n \in \mathbb{N} \quad \text{and } i = 0, \dots, k.$$

We prove Theorem 1.3 in Section 4 after some preparations in Sections 2 and 3.

Remark. Valuation E clearly does not depend on the choice of the scalar product in \mathbb{R}^d . One can observe that valuation ν of Theorem 1.3 admits a dual description which does not depend on the scalar product. Instead of \mathcal{L} , we consider the set \mathcal{L}^\vee of subspaces containing the subspaces $\text{lin}(F)$ and closed under taking sums of subspaces, and for $L \in \mathcal{L}^\vee$ we define $E_L^\vee(\cdot)$ as the sum of the volumes of sections of the polytope by the lattice affine subspaces parallel to L . Then

$$\nu = \sum_{L \in \mathcal{L}^\vee} \mu^\vee(L) E_L^\vee,$$

where μ^\vee are some integers computed from the set \mathcal{L}^\vee , partially ordered by inclusion.

However, using the explicit scalar product turns out to be more convenient.

The advantage of working with valuations E_L is that they are more amenable to computations.

- Let us fix an integer $k \geq 0$. We present a polynomial time algorithm, which, given an integer $d \geq k$, a d -dimensional rational simplex $\Delta \subset \mathbb{R}^d$, and a lattice subspace $L \subset \mathbb{R}^d$ such that $\dim L \leq k$, computes $E_L(\Delta)$.

We present the algorithm in Section 6 after some preparations in Section 5.

(1.4) The main ingredient of the algorithm to compute $e_{d-k}(\Delta; n)$.

Theorem 1.3 allows us to reduce computation of $e_{d-k}(\Delta; n)$ to that of $E_L(\Delta)$, where $L \subset \mathbb{R}^d$ is a lattice subspace and $\dim L \leq k$. Let us choose a particular lattice subspace L with $\dim L = j \leq k$.

If $P = \Delta$ is a simplex, then the description of the orthogonal projection $Q = pr(\Delta)$ onto L can be computed in polynomial time. Moreover, one can compute in polynomial time a decomposition of Q into a union of non-intersecting polyhedral

pieces Q_i , such that $\text{vol}_{d-j}(pr^{-1}(x))$ is a polynomial on each piece Q_i . Thus computing $E_L(\Delta)$ reduces to computing the sum

$$\sum_{m \in Q_i \cap \Lambda} \phi(m),$$

where ϕ is a polynomial with $\deg \phi = d - j$, $Q_i \subset L$ is a polytope with $\dim Q_i = j \leq k$ and $\Lambda \subset L$ is a lattice. The sum is computed by applying the technique of “short rational functions” for lattice points in polytopes of a fixed dimension, cf. [BW03], [BP99], and [D+04].

The algorithm for computing the sum of a polynomial over integer points in a polytope is discussed in Section 5.

2. THE FOURIER EXPANSIONS OF E AND E_L

Let V be a d -dimensional real vector space with the scalar product $\langle \cdot, \cdot \rangle$ and the corresponding Euclidean norm $\| \cdot \|$. Let $\Lambda \subset V$ be a lattice and let $\Lambda^* \subset V$ be the *dual* or the *reciprocal* lattice

$$\Lambda^* = \left\{ x \in V : \langle x, y \rangle \in \mathbb{Z} \text{ for all } y \in \Lambda \right\}.$$

For $\tau > 0$, we introduce the *theta function*

$$\begin{aligned} \theta_\Lambda(x, \tau) &= \tau^{d/2} \sum_{m \in \Lambda} \exp \{ -\pi \tau \|x - m\|^2 \} \\ &= (\det \Lambda)^{-1} \sum_{l \in \Lambda^*} \exp \{ -\pi \|l\|^2 / \tau + 2\pi i \langle l, x \rangle \}, \quad \text{where } x \in V. \end{aligned}$$

The last inequality is the reciprocity relation for theta series (essentially, the Poisson summation formula), see, for example, Section 69 of [Be61].

For a polytope P , let $\text{int } P$ denote the relative interior of P and let $\partial P = P \setminus \text{int } P$ be the boundary of P .

(2.1) Lemma. *Let $P \subset V$ be a full-dimensional polytope such that $\partial P \cap \Lambda = \emptyset$. Then*

$$\begin{aligned} |P \cap \Lambda| &= \lim_{\tau \rightarrow +\infty} \int_P \theta_\Lambda(x, \tau) dx \\ &= (\det \Lambda)^{-1} \lim_{\tau \rightarrow +\infty} \sum_{l \in \Lambda^*} \exp \{ -\pi \|l\|^2 / \tau \} \int_P \exp \{ 2\pi i \langle l, x \rangle \} dx. \end{aligned}$$

Proof. As is known (cf., for example, Section B.5 of [La02]), as $\tau \rightarrow +\infty$, the function $\theta_\Lambda(x, \tau)$ converges in the sense of distributions to the sum of the delta-functions concentrated at the points $m \in \Lambda$. Therefore, for every smooth function $\phi : \mathbb{R}^d \rightarrow \mathbb{R}$ with a compact support, we have

$$(2.1.1) \quad \lim_{\tau \rightarrow +\infty} \int_{\mathbb{R}^d} \phi(x) \theta_\Lambda(x, \tau) dx = \sum_{m \in \Lambda} \phi(m).$$

Since $\partial P \cap \Lambda = \emptyset$, we can replace ϕ by the indicator function $[P]$ in (2.1.1). \square

Remark. If $\partial P \cap \Lambda \neq \emptyset$, the limit still exists but then it counts every lattice point $m \in \partial P$ with the weight equal to the “solid angle” of m at P , since every term $\exp\{-\pi\tau\|x - m\|^2\}$ is spherically symmetric about m . This connection between the solid angle valuation and the theta function was described by the author in the unpublished paper [Ba92] (the paper is very different from paper [B94b] which has the same title) and independently discovered by Diaz and Robins [DR94]. Diaz and Robins used a similar approach based on Fourier analysis to express coefficients of the Ehrhart polynomial of an integer polytope in terms of cotangent sums [DR97]. Banaszczyk [B93a] obtained asymptotically optimal bounds in transference theorems for lattices by using a similar approach with theta functions, with the polytope P replaced by a Euclidean ball.

The formula of Lemma 2.1 can be considered as the Fourier expansion of the counting valuation.

We need a similar result for valuation E_L defined in Section 1.2.

(2.2) Lemma. *Let $P \subset \mathbb{R}^d$ be a full-dimensional polytope and let $L \subset \mathbb{R}^d$ be a lattice subspace with $\dim L = k$. Let $pr : \mathbb{R}^d \rightarrow L$ be the orthogonal projection onto L , let $Q = pr(P)$, and let $\Lambda = pr(\mathbb{Z}^d)$, so $\Lambda \subset L$ is a lattice in L . Suppose that $\partial Q \cap \Lambda = \emptyset$.*

Then

$$E_L(P) = \lim_{\tau \rightarrow +\infty} \sum_{l \in L \cap \mathbb{Z}^d} \exp\{-\pi\|l\|^2/\tau\} \int_P \exp\{2\pi i \langle l, x \rangle\} dx.$$

Proof. We observe that $L \cap \mathbb{Z}^d = \Lambda^*$. For a vector $x \in \mathbb{R}^d$, let x_L be the orthogonal projection of x onto L . Applying the reciprocity relation for theta functions in L , we write

$$\begin{aligned} & \sum_{l \in L \cap \mathbb{Z}^d} \exp\{-\pi\|l\|^2/\tau + 2\pi i \langle l, x \rangle\} \\ &= \sum_{l \in L \cap \mathbb{Z}^d} \exp\{-\pi\|l\|^2/\tau + 2\pi i \langle l, x_L \rangle\} \\ &= (\det \Lambda) \tau^{k/2} \sum_{m \in \Lambda} \exp\{-\pi\tau\|x_L - m\|^2\}. \end{aligned}$$

As is known (cf., for example, Section B.5 of [La02]), as $\tau \rightarrow +\infty$, the function

$$g_\tau(x) = \tau^{k/2} \sum_{m \in \Lambda} \exp\{-\pi\tau\|x_L - m\|^2\}$$

converges in the sense of distributions to the sum of the delta-functions concentrated on the subspaces $m + L^\perp$ (this is the set of points where $x_L = m$) for $m \in \Lambda$.

Therefore, for every smooth function $\phi : \mathbb{R}^d \rightarrow \mathbb{R}$ with a compact support, we have

$$(2.2.1) \quad \lim_{\tau \rightarrow +\infty} \int_{\mathbb{R}^d} \phi(x) g_\tau(x) dx = \sum_{m \in \Lambda} \int_{m+L^\perp} \phi(x) d_{L^\perp} x,$$

where $d_{L^\perp} x$ is the Lebesgue measure on $m + L^\perp$ induced from \mathbb{R}^d .

Since $\partial Q \cap \Lambda = \emptyset$, each subspace $m + L^\perp$ for $m \in \Lambda$ either intersects the interior of P or is at least some distance $\epsilon = \epsilon(P, L) > 0$ away from P . Hence we may replace ϕ by the indicator $[P]$ in (2.2.1).

Recall from Section 1.2 that measuring volumes in $m + L^\perp$, we scale the volume form in L^\perp induced from \mathbb{R}^d so that the determinant of the lattice $L^\perp \cap \mathbb{Z}^d$ is 1. One can observe that $\det \Lambda$ provides the required normalization factor, so

$$(\det \Lambda) \int_{m+L^\perp} [P](x) d_{L^\perp}(x) = \text{vol}_{d-k}(P \cap (m + L^\perp)).$$

The proof now follows. □

Remark. If $\partial Q \cap \Lambda \neq \emptyset$ the limit still exists but then for $m \in \partial Q \cap \Lambda$ the volume $\text{vol}_{d-k}(P \cap (m + L^\perp))$ is counted with the weight defined as follows: we find the minimal (under inclusion) face F of P such that $m + L^\perp$ is contained in $\text{aff}(F)$ and let the weight equal to the solid angle of P at F .

3. EXPONENTIAL VALUATIONS

Let V be a d -dimensional Euclidean space, let $\Lambda \subset V$ be a lattice and let Λ^* be the reciprocal lattice. Let us choose a vector $l \in \Lambda^*$ and let us consider the integral

$$\Phi_l(P) = \int_P \exp\{2\pi i \langle l, x \rangle\} dx,$$

where dx is the Lebesgue measure in V . Note that for $l = 0$ we have $\Phi_l(P) = \Phi_0(P) = \text{vol } P$. We have

$$\Phi_l(P + a) = \exp\{2\pi i \langle l, a \rangle\} \Phi_l(P) \quad \text{for all } a \in V.$$

It follows that Φ_l is a Λ -valuation on rational polytopes $P \subset V$.

If $l \neq 0$ then the following lemma (essentially, Stokes' formula) shows that Φ_l can be expressed as a linear combination of exponential valuations on the facets of P . The proof can be found, for example, in [B93b].

(3.1) Lemma. *Let $P \subset V$ be a full-dimensional polytope. For a facet Γ of P , let $d_\Gamma x$ be the Lebesgue measure on $\text{aff}(\Gamma)$, and let p_Γ be the unit outer normal to Γ . Then, for every $l \in V \setminus 0$, we have*

$$\int_P \exp\{2\pi i \langle l, x \rangle\} dx = \sum_{\Gamma} \frac{\langle l, p_\Gamma \rangle}{2\pi i \|l\|^2} \int_{\Gamma} \exp\{2\pi i \langle l, x \rangle\} d_\Gamma x,$$

where the sum is taken over all facets Γ of P .

Let $F \subset P$ be an i -dimensional face of P . Recall that by $\text{lin}(F)$ we denote the i -dimensional subspace of \mathbb{R}^d that is parallel to the affine hull $\text{aff}(F)$ of F . We need the following result.

(3.2) Theorem. *Let $P \subset V$ be a rational full-dimensional polytope and let t be a positive integer such that tP is a lattice polytope. Let $\epsilon \geq 0$ be a rational number and let $a \in V$ be a vector. Let us choose $l \in \Lambda^*$. Then there exist functions $f_i(P, \epsilon, a, l; \cdot) : \mathbb{N} \longrightarrow \mathbb{C}$, $i = 0, \dots, d$, such that*

$$(3.2.1) \quad \Phi_l((n + \epsilon)P + a) = \sum_{i=0}^d f_i(P, \epsilon, a, l; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and

$$(3.2.2) \quad f_i(P, \epsilon, a, l; n + t) = f_i(P, \epsilon, a, l; n) \quad \text{for all } n \in \mathbb{N}$$

and $i = 0, \dots, d$.

Suppose that $f_{d-k}(P, \epsilon, a, l; n) \neq 0$ for some n . Then there exists a $(d - k)$ -dimensional face F of P such that l is orthogonal to $\text{lin}(F)$.

Proof. Since

$$\Phi_l(P + a) = \exp\{2\pi i \langle l, a \rangle\} \Phi_l(P),$$

without loss of generality we assume that $a = 0$. We will denote $f_i(P, \epsilon, 0, l; n)$ just by $f_i(P, \epsilon, l; n)$.

We proceed by induction on d . For $d = 0$ the statement of the theorem obviously holds. Suppose that $d \geq 1$. If $l = 0$ then $\Phi_l((n + \epsilon)P) = (n + \epsilon)^d \text{vol } P$ and the statement holds as well.

Suppose that $l \neq 0$. For a facet Γ of P , let $\Lambda_\Gamma = \Lambda \cap \text{lin}(\Gamma)$ and let l_Γ be the orthogonal projection of l onto $\text{lin}(\Gamma)$. Thus Λ_Γ is a lattice in the $(d - 1)$ -dimensional Euclidean space $\text{lin}(\Gamma)$ and $l_\Gamma \in \Lambda_\Gamma^*$, so we can define valuations Φ_{l_Γ} on $\text{lin}(\Gamma)$. Since tP is a lattice polytope, for every facet Γ there is a vector $u_\Gamma \in V$ such that

$$\text{lin}(\Gamma) = \text{aff}(t\Gamma) - tu_\Gamma \quad \text{and} \quad tu_\Gamma \in \Lambda.$$

Let $\Gamma' = \Gamma - u_\Gamma$, so $\Gamma' \subset \text{lin}(\Gamma)$ is a Λ_Γ -rational $(d - 1)$ -dimensional polytope such that $t\Gamma'$ is a Λ_Γ -polytope. We have

$$(n + \epsilon)\Gamma = (n + \epsilon)\Gamma' + (n + \epsilon)u_\Gamma.$$

Applying Lemma 3.1 to $(n + \epsilon)P$, we get

$$\Phi_l((n + \epsilon)P) = \sum_{\Gamma} \psi(\Gamma, l; n) \Phi_{l_\Gamma}((n + \epsilon)\Gamma'),$$

where

$$\psi(\Gamma, l; n) = \frac{\langle l, p_\Gamma \rangle}{2\pi i \|l\|^2} \exp\{2\pi i (n + \epsilon) \langle l, u_\Gamma \rangle\}$$

and the sum is taken over all facets Γ of P .

Since $tu_\Gamma \in \Lambda$ and $l \in \Lambda^*$, we have

$$\psi(\Gamma, l; n+t) = \psi(\Gamma, l; n) \quad \text{for all } n \in \mathbb{N}.$$

Hence, applying the induction hypothesis, we may write

$$f_i(P, \epsilon, l; n) = \sum_{\Gamma} \psi(\Gamma, l; n) f_i(\Gamma', \epsilon, l_\Gamma; n) \quad \text{for all } n \in \mathbb{N}$$

and $i = 0, \dots, d-1$ and $f_d(P, \epsilon, l; n) \equiv 0$. Hence (3.2.1)-(3.2.2) follows by the induction hypothesis.

If $f_{d-k}(P, \epsilon, l; n) \neq 0$ then there is a facet Γ of P such that $f_{d-k}(\Gamma', \epsilon, l_\Gamma; n) \neq 0$. By the induction hypothesis, there is a face F' of Γ' such that $\dim F' = d-k$, and l_Γ is orthogonal to $\text{lin}(F')$. Then $F = F' + u_\Gamma$ is a $(d-k)$ -dimensional face of P , $\text{lin}(F') = \text{lin}(F)$ and l is orthogonal to $\text{lin}(F)$, which completes the proof. \square

4. PROOF OF THEOREM 1.3

First, we discuss some ideas relevant to the proof.

(4.1) Shifting a valuation by a polytope. Let V be a d -dimensional real vector space, let $\Lambda \subset V$ be a lattice, and let ν be a Λ -valuation on rational polytopes. Let us fix a rational polytope $R \subset V$. McMullen [Mc78] observed that the function μ defined by

$$\mu(P) = \nu(P + R)$$

is a Λ -valuation on rational polytopes P . Here “+” stands for the Minkowski sum:

$$P + R = \left\{ x + y : x \in P, y \in R \right\}.$$

This result follows since the transformation $P \mapsto P + R$ preserves linear dependencies among indicators of polyhedra, cf. [MS83].

Let t be a positive integer such that tP is a lattice polytope. McMullen [Mc78] deduced that there exist functions $\nu_i(P, R; \cdot) : \mathbb{N} \rightarrow \mathbb{C}$, $i = 0, \dots, d$, such that

$$\nu(nP + R) = \sum_{i=0}^d \nu_i(P, R; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and

$$\nu_i(P, R; n+t) = \nu_i(P, R; n) \quad \text{for all } n \in \mathbb{N}.$$

(4.2) Continuity properties of valuations E and E_L . Let $R \subset \mathbb{R}^d$ be a full-dimensional rational polytope containing the origin in its interior. Then for every polytope $P \subset \mathbb{R}^d$ and every $\epsilon > 0$ we have $P \subset (P + \epsilon R)$. We observe that

$$|(P + \epsilon R) \cap \mathbb{Z}^d| = |P \cap \mathbb{Z}^d|,$$

for all sufficiently small $\epsilon > 0$. If P is a rational polytope, the supporting affine hyperplanes of the facets of nP for $n \in \mathbb{N}$ are split among finitely many translation classes modulo \mathbb{Z}^d . Therefore, there exists $\delta = \delta(P, R) > 0$ such that

$$|(nP + \epsilon R) \cap \mathbb{Z}^d| = |nP \cap \mathbb{Z}^d| \quad \text{for all } 0 < \epsilon < \delta \quad \text{and all } n \in \mathbb{N}.$$

We also note that for every rational subspace $L \subset \mathbb{R}^d$, we have

$$\lim_{\epsilon \rightarrow 0^+} E_L(P + \epsilon R) = E_L(P).$$

We will use the perturbation $P \mapsto P + \epsilon R$ to push valuations E and E_L into a sufficiently generic position, so that we can apply Lemmas 2.1–2.2 without having to deal with various boundary effects. This is somewhat similar in spirit to the idea of [BS05].

(4.3) Linear identities for quasi-polynomials. Let us fix positive integers t and d . Suppose that we have a possibly infinite family of quasi-polynomials $p_l : \mathbb{N} \rightarrow \mathbb{C}$ of the type

$$p_l(n) = \sum_{i=0}^d p_i(l; n) n^i \quad \text{for all } n \in \mathbb{N},$$

where functions $p_i(l; \cdot) : \mathbb{N} \rightarrow \mathbb{C}$, $i = 0, \dots, d$, satisfy

$$p_i(l; n) = p_i(l; n + t) \quad \text{for all } n \in \mathbb{N}.$$

Suppose further that $p : \mathbb{N} \rightarrow \mathbb{C}$ is yet another quasi-polynomial

$$p(n) = \sum_{i=0}^d p_i(n) n^i \quad \text{where } p_i(n + t) = p_i(n) \quad \text{for all } n \in \mathbb{N}.$$

Finally, suppose that $c_l(\cdot) : \mathbb{R}_+ \rightarrow \mathbb{C}$ is a family of functions and that

$$p(n) = \lim_{\tau \rightarrow +\infty} \sum_l c_l(\tau) p_l(n) \quad \text{for all } n \in \mathbb{N}$$

and that the series converges absolutely for every $n \in \mathbb{N}$ and every $\tau > 0$.

Then we claim that for $i = 0, \dots, d$ we have

$$p_i(n) = \lim_{\tau \rightarrow +\infty} \sum_l c_l(\tau) p_i(l; n) \quad \text{for all } n \in \mathbb{N}$$

and that the series converges absolutely for every $n \in \mathbb{N}$ and every $\tau > 0$.

This follows since $p_i(n)$, respectively $p_i(l; n)$, can be expressed as linear combinations of $p(m)$, respectively $p_l(m)$, for $m = n, n+t, \dots, n+td$ with the coefficients depending on m, n, t , and d only.

Now we are ready to prove Theorem 1.3.

(4.4) Proof of Theorem 1.3. Let us fix a rational polytope $P \subset \mathbb{R}^d$ as defined in the statement of the theorem. For $L \in \mathcal{L}$ let $P_L \subset L$ be the orthogonal projection of P onto L and let $\Lambda_L \subset L$ be the orthogonal projection of \mathbb{Z}^d onto L .

Let $a \in \text{int } P$ be a rational vector and let

$$R = P - a.$$

Hence R is a rational polytope containing the origin in its interior. Let R_L denote the orthogonal projection of R onto L .

Since P is a rational polytope and \mathcal{L} is a finite set of rational subspaces, there exists $\delta = \delta(P, R) > 0$ such that for all $0 < \epsilon < \delta$ and all $n \in \mathbb{N}$, we have

$$(1) \quad (nP + \epsilon R) \cap \mathbb{Z}^d = nP \cap \mathbb{Z}^d \quad \text{and} \quad \partial(nP + \epsilon R) \cap \mathbb{Z}^d = \emptyset \quad \text{for all } n \in \mathbb{N}$$

and for all $L \in \mathcal{L}$, we have

$$(2) \quad (nP_L + \epsilon R_L) \cap \Lambda_L = nP_L \cap \Lambda_L \quad \text{and} \quad \partial(nP_L + \epsilon R_L) \cap \Lambda_L = \emptyset \quad \text{for all } n \in \mathbb{N},$$

cf. Section 4.2. Let us choose any rational $0 < \epsilon < \delta$.

Because of (1), we can write

$$(3) \quad |(nP + \epsilon R) \cap \mathbb{Z}^d| = \sum_{i=0}^d e_i(P; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and by Lemma 2.1 we get

$$(4) \quad |(nP + \epsilon R) \cap \mathbb{Z}^d| = \lim_{\tau \rightarrow +\infty} \sum_{l \in \mathbb{Z}^d} \exp\{-\pi \|l\|^2 / \tau\} \Phi_l(nP + \epsilon R),$$

where Φ_l are the exponential valuations of Section 3. Since Φ_l is a \mathbb{Z}^d -valuation, by Section 4.1 there exist functions $f_i(P, \epsilon, l; \cdot) : \mathbb{N} \rightarrow \mathbb{C}$, $i = 0, \dots, d$, such that

$$(5) \quad \Phi_l(nP + \epsilon R) = \sum_{i=0}^d f_i(P, \epsilon, l; n) n^i \quad \text{for } n \in \mathbb{N}$$

and

$$(6) \quad f_i(P, \epsilon, l; n + t) = f_i(P, \epsilon, l; n) \quad \text{for all } n \in \mathbb{N}.$$

Moreover, we can write

$$nP + \epsilon R = nP + \epsilon(P - a) = (n + \epsilon)P - \epsilon a.$$

Therefore, by Theorem 3.2, for $i \leq k$ we have $f_{d-i}(P, \epsilon, l; n) = 0$ unless $l \in L^F$ for some face F of P with $\dim F = d - k$.

Therefore, combining (3)–(6) and Section 4.3, we obtain for all $0 \leq i \leq k$ and all $n \in \mathbb{N}$

$$\begin{aligned} e_{d-i}(P; n) &= \lim_{\tau \rightarrow +\infty} \sum_{l \in \mathbb{Z}^d} \exp \{ -\pi \|l\|^2 / \tau \} f_{d-i}(P, \epsilon, l; n) \\ &= \lim_{\tau \rightarrow +\infty} \sum_{l \in \bigcup_{L \in \mathcal{L}} (L \cap \mathbb{Z}^d)} \exp \{ -\pi \|l\|^2 / \tau \} f_{d-i}(P, \epsilon, l; n), \end{aligned}$$

since vectors $l \in \mathbb{Z}^d$ outside of subspaces $L \in \mathcal{L}$ contribute 0 to the sum. Therefore, for $0 \leq i \leq k$ and all $n \in \mathbb{N}$

$$(7) \quad e_{d-i}(P; n) = \lim_{\tau \rightarrow +\infty} \sum_{L \in \mathcal{L}} \mu(L) \sum_{l \in L \cap \mathbb{Z}^d} \exp \{ -\pi \|l\|^2 / \tau \} f_{d-i}(P, \epsilon, l; n)$$

On the other hand, because of (2), by Lemma 2.2 we get for all $L \in \mathcal{L}$ and all $n \in \mathbb{N}$

$$(8) \quad E_L(nP + \epsilon R) = \lim_{\tau \rightarrow +\infty} \sum_{l \in L \cap \mathbb{Z}^d} \exp \{ -\pi \|l\|^2 / \tau \} \Phi_l(nP + \epsilon R).$$

Since E_L are \mathbb{Z}^d -valuations, by Section 4.1 there exist functions $e_i(P, \epsilon, L; \cdot) : \mathbb{N} \rightarrow \mathbb{Q}$, $i = 0, \dots, d$, such that

$$(9) \quad E_L(nP + \epsilon R) = \sum_{i=0}^d e_i(P, \epsilon, L; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and

$$(10) \quad e_i(P, \epsilon, L; n+t) = e_i(P, \epsilon, L; n) \quad \text{for all } n \in \mathbb{N}.$$

Combining (5)–(6) and (8)–(10), by Section 4.3 we conclude

$$e_{d-i}(P, \epsilon, L; n) = \lim_{\tau \rightarrow +\infty} \sum_{l \in L \cap \mathbb{Z}^d} \exp \{ -\pi \|l\|^2 / \tau \} f_{d-i}(P, \epsilon, l; n) \quad \text{for all } n \in \mathbb{N}.$$

Therefore, by (7), for $0 \leq i \leq k$ we have

$$(11) \quad e_{d-i}(P; n) = \sum_{L \in \mathcal{L}} \mu(L) e_{d-i}(P, \epsilon, L; n) \quad \text{for all } n \in \mathbb{N}.$$

Since E_L is a \mathbb{Z}^d -valuation, there exist functions $e_i(P, L; \cdot) : \mathbb{N} \rightarrow \mathbb{Q}$, $i = 0, \dots, d$, such that

$$(12) \quad E_L(nP) = \sum_{i=0}^d e_i(P, L; n) n^i \quad \text{for all } n \in \mathbb{N}$$

and

$$e_i(P, L; n + t) = e_i(P, L; n) \quad \text{for all } n \in \mathbb{N}.$$

Let us choose an $m \in \mathbb{N}$. Substituting $n = m, m + t, \dots, m + dt$ in (12), we obtain $e_i(P, L; m)$ as a linear combination of $E_L(nP)$ with coefficients depending on n, m, t , and d only. Similarly, substituting $n = m, m + t, \dots, m + dt$ in (9), we obtain $e_i(P, \epsilon, L; m)$ as the same linear combination of $E_L(nP + \epsilon R)$. Since volumes are continuous functions, in view of (2) (see also Section 4.2), we get

$$\lim_{\epsilon \rightarrow 0^+} E_L(nP + \epsilon R) = E_L(nP) \quad \text{for } n = m, m + t, \dots, m + dt.$$

Therefore,

$$\lim_{\epsilon \rightarrow 0^+} e_i(P, \epsilon, L; m) = e_i(P, L; m) \quad \text{for all } m \in \mathbb{N}.$$

Taking the limit as $\epsilon \rightarrow +0$ in (11), we obtain for $0 \leq i \leq k$

$$e_{d-i}(P; n) = \sum_{L \in \mathcal{L}} \mu(L) e_{d-i}(P, L; n) \quad \text{for all } n \in \mathbb{N}.$$

To complete the proof, we note that

$$\nu_{d-i}(P, L; n) = \sum_{L \in \mathcal{L}} \mu(L) e_{d-i}(P, L; n).$$

□

5. SUMMING UP A POLYNOMIAL OVER INTEGER POINTS IN A RATIONAL POLYTOPE

Let us fix a positive integer k and let us consider the following situation. Let $Q \subset \mathbb{R}^k$ be a rational polytope, let $\text{int } Q$ be the relative interior of Q and let $f : \mathbb{R}^k \rightarrow \mathbb{R}$ be a polynomial with rational coefficients. We want to compute the value

$$(5.1) \quad \sum_{m \in \text{int } Q \cap \mathbb{Z}^k} f(m).$$

We claim that as soon as the dimension k of the polytope Q is fixed, there is a polynomial time algorithm to do that. We assume that the polytope Q is a given by the list of its vertices and the polynomial f is given by the list its coefficients.

For an integer point $m = (\mu_1, \dots, \mu_k)$, let

$$\mathbf{x}^m = x_1^{\mu_1} \cdots x_k^{\mu_k} \quad \text{for } \mathbf{x} = (x_1, \dots, x_k)$$

be the Laurent monomial in k variables $\mathbf{x} = (x_1, \dots, x_k)$. We use the following result [BP99].

(5.2) The short rational function algorithm. Let us fix k . There is a polynomial time algorithm, which, given a rational polytope $Q \subset \mathbb{R}^k$ computes the generating function (Laurent polynomial)

$$S(Q; \mathbf{x}) = \sum_{m \in \text{int } Q \cap \mathbb{Z}^k} \mathbf{x}^m$$

in the form

$$S(Q; \mathbf{x}) = \sum_{i \in I} \epsilon_i \frac{\mathbf{x}^{a_i}}{(1 - \mathbf{x}^{b_{i1}}) \cdots (1 - \mathbf{x}^{b_{ik}})},$$

where $a_i \in \mathbb{Z}^k$, $b_{ij} \in \mathbb{Z}^k \setminus \{0\}$ and $\epsilon_i \in \mathbb{Q}$. In particular, the number $|I|$ of fractions is bounded by a polynomial in the input size of Q .

Our first step is computing the generating function

$$S(Q, f; \mathbf{x}) = \sum_{m \in Q \cap \mathbb{Z}^k} f(m) \mathbf{x}^m.$$

Our approach is similar to that of [D+04].

(5.3) The algorithm for computing $S(Q, f; \mathbf{x})$. We observe that

$$S(Q, f; \mathbf{x}) = f \left(x_1 \frac{\partial}{\partial x_1}, \dots, x_k \frac{\partial}{\partial x_k} \right) S(Q; \mathbf{x}).$$

We compute $S(Q; \mathbf{x})$ as in Section 5.2.

Let $a = (\alpha_1, \dots, \alpha_k)$ be an integer vector, let $b_j = (\beta_{j1}, \dots, \beta_{jk})$ be non-zero integer vectors for $j = 1, \dots, k$ and let $\gamma_1, \dots, \gamma_k$ be positive integers. Then

$$\begin{aligned} & \left(x_i \frac{\partial}{\partial x_i} \right) \frac{\mathbf{x}^a}{(1 - \mathbf{x}^{b_1})^{\gamma_1} \cdots (1 - \mathbf{x}^{b_k})^{\gamma_k}} \\ &= \alpha_i \frac{\mathbf{x}^a}{(1 - \mathbf{x}^{b_1})^{\gamma_1} \cdots (1 - \mathbf{x}^{b_k})^{\gamma_k}} + \sum_{j=1}^k \gamma_j \beta_{ji} \frac{\mathbf{x}^{a+b_j}}{(1 - \mathbf{x}^{b_j})^{\gamma_j+1}} \prod_{s \neq j} \frac{1}{(1 - \mathbf{x}^{b_s})^{\gamma_s}}. \end{aligned}$$

Consecutively applying the above formula and collecting similar fractions, we compute

$$f \left(x_1 \frac{\partial}{\partial x_1}, \dots, x_k \frac{\partial}{\partial x_k} \right) \frac{\mathbf{x}^a}{(1 - \mathbf{x}^{b_1}) \cdots (1 - \mathbf{x}^{b_k})}$$

as an expression of the type

$$(5.3.1) \quad \sum_j \rho_j \frac{\mathbf{x}^{a_j}}{(1 - \mathbf{x}^{b_1})^{\gamma_{j1}} \cdots (1 - \mathbf{x}^{b_k})^{\gamma_{jk}}},$$

where $\rho_j \in \mathbb{Q}$, $\gamma_{j1}, \dots, \gamma_{jk}$ are non-negative integers satisfying $\gamma_{j1} + \dots + \gamma_{jk} \leq k + \deg f$ and a_j are vectors of the type

$$a_j = a + \mu_1 b_1 + \dots + \mu_k b_k,$$

where μ_i are non-negative integers and $\mu_1 + \dots + \mu_k \leq \deg f$. The number of terms in (5.3.1) is bounded by $(\deg f)^{O(k)}$, which shows that for a k fixed in advance, the algorithm runs in polynomial time.

Consequently, $S(Q, f; \mathbf{x})$ is computed in polynomial time.

Formally speaking, to compute the sum (5.1), we have to substitute $x_i = 1$ into the formula for $S(Q, f; \mathbf{x})$. This, however, cannot be done in a straightforward way since $\mathbf{x} = (1, \dots, 1)$ is a pole of every fraction in the expression for $S(Q, f; \mathbf{x})$. Nevertheless, the substitution can be done via efficient computation of the relevant residue of $S(Q, f; \mathbf{x})$ as described in [B94a] and [BW03].

(5.4) The algorithm for computing the sum. The output of Algorithm 5.3 represents $S(Q, f; \mathbf{x})$ in the general form

$$S(Q, f; \mathbf{x}) = \sum_{i \in I} \epsilon_i \frac{\mathbf{x}^{a_i}}{(1 - \mathbf{x}^{b_{i1}})^{\gamma_{i1}} \dots (1 - \mathbf{x}^{b_{ik}})^{\gamma_{ik}}},$$

where $\epsilon_i \in \mathbb{Q}$, $a_i \in \mathbb{Z}^k$, $b_{ij} \in \mathbb{Z}^k \setminus \{0\}$, and $\gamma_{ij} \in \mathbb{N}$ such that $\gamma_{i1} + \dots + \gamma_{ik} \leq k + \deg f$ for all $i \in I$.

Let us choose a vector $l \in \mathbb{Q}^k$, $l = (\lambda_1, \dots, \lambda_k)$ such that $\langle l, b_{ij} \rangle \neq 0$ for all i, j (such a vector can be computed in polynomial time, cf. [B94a]). For a complex τ , let

$$\mathbf{x}(\tau) = (e^{\tau \lambda_1}, \dots, e^{\tau \lambda_k}).$$

We want to compute the limit

$$\lim_{\tau \rightarrow 0} G(\tau) \quad \text{for} \quad G(\tau) = S(Q, f; \mathbf{x}(\tau)).$$

In other words, we want to compute the constant term of the Laurent expansion of $G(\tau)$ around $\tau = 0$.

Let us consider a typical fraction

$$\frac{\mathbf{x}^a}{(1 - \mathbf{x}^{b_1})^{\gamma_1} \dots (1 - \mathbf{x}^{b_k})^{\gamma_k}}.$$

Substituting $\mathbf{x}(\tau)$, we get the expression

$$(5.4.1) \quad \frac{e^{\alpha \tau}}{(1 - e^{\tau \beta_1})^{\gamma_1} \dots (1 - e^{\tau \beta_k})^{\gamma_k}},$$

where $\alpha = \langle a, l \rangle$ and $\beta_i = \langle b_i, l \rangle$ for $i = 1, \dots, k$. The order of the pole at $\tau = 0$ is $D = \gamma_1 + \dots + \gamma_k \leq k + \deg f$. To compute the constant term of the Laurent expansion of (5.4.1) at $\tau = 0$, we do the following.

We compute the polynomial

$$q(\tau) = \sum_{i=0}^D \frac{\alpha^i}{i!} \tau^i$$

that is the truncation at τ^D of the Taylor series expansion of $e^{\alpha\tau}$. For $i = 1, \dots, k$ we compute the polynomial $p_i(\tau)$ with $\deg p_i = D$ such that

$$\frac{\tau}{1 - e^{\tau\beta_i}} = p_i(\tau) + \text{terms of higher order in } \tau$$

at $\tau = 0$. Consecutively multiplying polynomials $\pmod{\tau^{D+1}}$ we compute a polynomial $u(\tau)$ with $\deg u = D$ such that

$$q(\tau)p_1^{\gamma_1}(\tau) \cdots p_k^{\gamma_k}(\tau) \equiv u(\tau) \pmod{\tau^{D+1}}.$$

The coefficient of τ^D in $u(\tau)$ is the desired constant term of the Laurent expansion.

6. COMPUTING $E_L(\Delta)$

Let us fix a positive integer k . Let $\Delta \subset \mathbb{R}^d$ be a rational simplex given by the list of its vertices and let $L \subset \mathbb{R}^d$ be a rational subspace given its basis and such that $\dim L = k$. In this section, we describe a polynomial time algorithm for computing the value of $E_L(\Delta)$ as defined in Section 1.2.

Let $pr : \mathbb{R}^d \rightarrow L$ be the orthogonal projection. We compute the vertices of the polytope $Q = pr(\Delta)$ and a basis of the lattice $\Lambda = pr(\mathbb{Z}^d)$. For basic lattice algorithms see [Sc93] and [G+93].

As is known, as $x \in \Delta$ varies, the function

$$\phi(x) = \text{vol}_{d-k}(P_x) \quad \text{where} \quad P_x = (\Delta \cap (x + L^\perp))$$

is a piece-wise polynomial on Q . Our first step consists of computing a decomposition

$$(6.1) \quad Q = \bigcup_i C_i$$

such that $C_i \subset Q$ are rational polytopes (chambers) with pairwise disjoint interiors and polynomials $\phi_i : L \rightarrow \mathbb{R}$ such that $\phi_i(x) = \phi(x)$ for $x \in C_i$.

We observe that every vertex of P_x is the intersection of $x + L^\perp$ and some k -dimensional face F of Δ .

For every face G of Δ with $\dim G = k - 1$ and such that $\text{aff}(G)$ is not parallel to L^\perp , let us compute

$$A_G = \left\{ x \in L : x + L^\perp \cap \text{aff}(G) \neq \emptyset \right\}.$$

Then A_G is an affine hyperplane in L . Then number of different hyperplanes A_G is $d^{O(k)}$ and hence they cut Q into at most $d^{O(k^2)}$ polyhedral chambers C_i , cf. Section 6.1 of [Ma02]. As long as x stays within the relative interior of a chamber C_i , the strong combinatorial type of P_x does not change (the facets of P_x move parallel to themselves) and hence the restriction ϕ_i of ϕ onto C_i is a polynomial, cf. Section 5.1 of [Sc93]. Since in the $(d - k)$ -dimensional space $x + L^\perp$ the polytope P_x is defined by d linear inequalities, ϕ_i can be computed in polynomial time, see [GK94] and [B93b].

The decomposition 6.1 gives rise to the formula

$$[Q] = \sum_j [Q_j],$$

where Q_j are open faces of the chambers C_i (the number of such faces is bounded by a polynomial in d), cf. Section 6.1 of [Ma02]. Hence we have

$$E_L(\Delta) = \sum_j \sum_{m \in Q_j \cap \Lambda} \phi(m).$$

Each inner sum is the sum of a polynomial over lattice points in a polytope of dimension at most k . By a change of the coordinates, it becomes the sum over integer points in a rational polytope and we compute it as described in Section 5.

7. COMPUTING $e_{d-k}(\Delta; n)$

Let us fix a an integer $k \geq 0$. We describe our algorithm, which, given a positive integer $d \geq k$, a rational simplex $\Delta \subset \mathbb{R}^d$ (defined, for example, by the list of its vertices), and a positive integer n , computes the number $e_{d-k}(\Delta; n)$.

We use Theorem 1.3.

(7.1) Computing the set \mathcal{L} of subspaces. We compute subspaces L and numbers $\mu(L)$ described in Theorem 1.3. Namely, for each $(d - k)$ -dimensional face F of Δ , we compute a basis of the subspace $L^F = (\text{lin } F)^\perp$. Hence $\dim L^F \leq k$. Clearly, the number of distinct subspaces L^F is $d^{O(k)}$. We let \mathcal{L} be the set consisting of the subspaces L^F and all other subspaces obtained as intersections of L^F . We compute \mathcal{L} in k (or fewer) steps. Initially, we let

$$\mathcal{L} := \left\{ L^F : F \text{ is a } (d - k)\text{-dimensional face of } \Delta \right\}.$$

Then, on every step, we consider the previously constructed subspaces $L \in \mathcal{L}$, consider the pairwise intersections $L \cap L^F$ as F ranges over the $(d-k)$ -dimensional faces of Δ and add the obtained subspace $L \cap L^F$ to the set \mathcal{L} if it was not already there. If no new subspaces are obtained, we stop. Clearly, in the end of this process, we will obtain all subspaces L that are intersections of different L^{F_i} . Since $\dim L^F = k$, each subspace $L \in \mathcal{L}$ is an intersection of some k subspaces L^{F_i} . Hence the process stops after k steps and the total number $|\mathcal{L}|$ of subspaces is $d^{O(k^2)}$.

Having computed the subspaces $L \in \mathcal{L}$, we compute the numbers $\mu(L)$ as follows.

For each pair of subspaces $L_1, L_2 \in \mathcal{L}$ such that $L_1 \subseteq L_2$, we compute the number $\mu(L_1, L_2)$ recursively: if $L_1 = L_2$ we let $\mu(L_1, L_2) = 1$. Otherwise, we let

$$\mu(L_1, L_2) = - \sum_{\substack{L \in \mathcal{L} \\ L_1 \subseteq L \subsetneq L_2}} \mu(L_1, L).$$

In the end, for each $L \in \mathcal{L}$, we let

$$\mu(L) = \sum_{\substack{L_1 \in \mathcal{L} \\ L \subseteq L_1}} \mu(L, L_1).$$

Hence $\mu(L_i, L_j)$ are the values of the Möbius function on the set \mathcal{L} partially ordered by inclusion, so

$$\left[\bigcup_{L \in \mathcal{L}} L \right] = \sum_{L \in \mathcal{L}} \mu(L)[L]$$

follows from the Möbius inversion formula, cf. Section 3.7 of [St97].

Now, for each $L \in \mathcal{L}$ and $m = n, n+t, \dots, n+td$ we compute the values of $E_L(m\Delta)$ as in Section 6, compute

$$\nu(m\Delta) = \sum_{L \in \mathcal{L}} \mu(L) E_L(m\Delta)$$

and find $\nu_{d-k}(\Delta; n) = e_{d-k}(\Delta, n)$ by interpolation.

8. POSSIBLE EXTENSIONS AND FURTHER QUESTIONS

(8.1) Computing more general expressions. Let $P \subset \mathbb{R}^d$ be a rational polytope, let $\alpha \geq 0$ be a rational number, and let $u \in \mathbb{R}^d$ be a rational vector. One can show (cf. Section 4.1) that

$$\left| ((n+\alpha)P + u) \cap \mathbb{Z}^d \right| = \sum_{i=0}^d e_i(P, \alpha, u; n) n^i \quad \text{for all } n \in \mathbb{N},$$

where $e_i(P, \alpha, u; \cdot) : \mathbb{N} \rightarrow \mathbb{Q}$, $i = 0, \dots, d$, satisfy

$$e_i(P, \alpha, u; n+t) = e_i(P, \alpha, u; n) \quad \text{for all } n \in \mathbb{N},$$

provided $t \in \mathbb{N}$ is a number such that tP is an integer polytope. As long as k is fixed in advance, for given α, u, n , and a rational simplex $\Delta \subset \mathbb{R}^d$, one can compute $e_{d-k}(\Delta, \alpha, u; n)$ in polynomial time. Similarly, Theorem 1.3 and its proof extend to this more general situation in a straightforward way.

(8.2) Computing the generating function. Let $P \subset \mathbb{R}^d$ be a rational polytope. Then, for every $0 \leq i \leq d$, the series

$$\sum_{n=1}^{+\infty} e_i(P; n)t^n$$

converges to a rational function $f_i(P; t)$ for $|t| < 1$.

It is not clear whether $f_{d-k}(\Delta; t)$ can be efficiently computed as a “closed form expression” in any meaningful sense, although it seems that by adjusting the methods of Sections 5–7, for any given t such that $|t| < 1$ one can compute the value of $f_{d-k}(\Delta; t)$ in polynomial time (again, k is assumed to be fixed in advance).

(8.3) Extensions to other classes of polytopes. If k is fixed in advance, the coefficient $e_{d-k}(P; n)$ can be computed in polynomial time, if the rational polytope $P \subset \mathbb{R}^d$ is given by the list of its $d+c$ vertices or the list of its $d+c$ inequalities, where c is a constant fixed in advance. Similar result holds for rational parallelepipeds P , that is, for Minkowski sums of d rational intervals that do not lie in the same affine hyperplane in \mathbb{R}^d .

(8.4) Possible applications to integer programming and integer point counting. If $P \subset \mathbb{R}^m$ is a rational polytope given by the list of its defining linear inequalities, the problem of testing whether $P \cap \mathbb{Z}^m = \emptyset$ is a typical problem of integer programming, see [G+93] and [Sc86]. Moreover, a general construction of “aggregation” (see Section 16.6 of [Sc86] and Section 2.2 of [Sh97]) establishes a bijection between the sets $P \cap \mathbb{Z}^m$ and $\Delta \cap \mathbb{Z}^d$ provided P is defined by $d+1$ linear inequalities. Here $\Delta \subset \mathbb{R}^d$ a rational simplex whose definition is computable in polynomial time from that of P . It would be interesting to find out whether approximating valuation E by valuation ν of Theorem 1.3 for some $k \ll d$ and applying the algorithm of this paper to compute $\nu(\Delta)$ can be of any practical use to solve higher-dimensional integer programs and integer point counting problems. It could complement existing software packages [D+03] and [B+04] based on the “short rational functions” calculus.

REFERENCES

- [B93a] W. Banaszczyk, *New bounds in some transference theorems in the geometry of numbers*, Math. Ann. **296** (1993), 625–635.

- [B93b] A. Barvinok, *Computing the volume, counting integral points, and exponential sums*, Discrete Comput. Geom. **10** (1993), 123–141.
- [Ba92] A. Barvinok, *Computing the Ehrhart polynomial of a convex lattice polytope*, preprint TRITA-MAT-1992-0036 (1992), Royal Institute of Technology, Stockholm.
- [B94a] A. Barvinok, *A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed*, Math. Oper. Res. **19** (1994), 769–779.
- [B94b] A. Barvinok, *Computing the Ehrhart polynomial of a convex lattice polytope*, Discrete Comput. Geom. **12** (1994), 35–48.
- [BP99] A. Barvinok and J. Pommersheim, *An algorithmic theory of lattice points in polyhedra*, New perspectives in algebraic combinatorics (Berkeley, CA, 1996–97), Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, Cambridge, 1999, pp. 91–147.
- [BS05] M. Beck and F. Sottile, *Irrational proofs for three theorems of Stanley*, preprint arXiv math.CO/0501359 (2005).
- [Be61] R. Bellman, *A Brief Introduction to Theta Functions*, Athena Series: Selected Topics in Mathematics, Holt, Rinehart and Winston, New York, 1961.
- [BW03] A. Barvinok and K. Woods, *Short rational generating functions for lattice point problems*, J. Amer. Math. Soc. **16** (2003), 957–979.
- [B+04] K. Beyls, M. Bruynooghe, V. Loechner, R. Seghir, and S. Verdoolaege, *Analytical computation of Ehrhart polynomials: enabling more compiler analyses and optimizations*, see also <http://www.kotnet.org/~skimo/barvinok>, Proceedings of the 2004 International Conference on Compilers, Architecture, and Synthesis for Embedded Systems (CASES 2004), 2004, pp. 248–258.
- [D+03] J. De Loera, D. Haws, R. Hemmecke, P. Huggins, J. Tauzer, and R. Yoshida, *A User’s Guide for LattE v1.1, 2003*, software package LattE, available at <http://www.math.ucdavis.edu/~latte> (2003).
- [D+04] J. De Loera, R. Hemmecke, M. Köppe, and R. Weismantel, *Integer polynomial optimization in fixed dimension*, preprint arXiv math.OC/0410111 (2004).
- [DR94] R. Diaz and S. Robins, *Solid angles, lattice points, and the Fourier decomposition of polytopes*, manuscript (1994).
- [DR97] R. Diaz and S. Robins, *The Ehrhart polynomial of a lattice polytope*, Ann. of Math. (2) **145** (1997), 503–518; Erratum: 146 (1997), no. 1, 237.
- [GK94] P. Gritzmann and V. Klee, *On the complexity of some basic problems in computational convexity. II. Volume and mixed volumes*, Polytopes: Abstract, Convex and Computational (Scarborough, ON, 1993), NATO Adv. Sci. Inst. Ser. C. Math. Phys. Sci., vol. 440, Kluwer Acad. Publ., Dordrecht, 1994, pp. 373–466.
- [G+93] M. Grötschel, L. Lovász, and A. Schrijver, *Geometric Algorithms and*

- Combinatorial Optimization. Second edition*, Algorithms and Combinatorics, vol. 2, Springer-Verlag, Berlin, 1993.
- [La02] P.D. Lax, *Functional Analysis*, Pure and Applied Mathematics, Wiley-Interscience, New York, 2002.
- [Ma02] J. Matoušek, *Lectures on Discrete Geometry*, Graduate Texts in Mathematics, vol. 212, Springer-Verlag, New York, 2002.
- [Mc78] P. McMullen, *Lattice invariant valuations on rational polytopes*, Arch. Math. (Basel) **31** (1978/79), 509–516.
- [Mc93] P. McMullen, *Valuations and dissections*, Handbook of Convex Geometry, vol. B, North-Holland, Amsterdam, 1993, pp. 933–988.
- [Mo93] R. Morelli, *Pick's theorem and the Todd class of a toric variety*, Adv. Math. **100** (1993), 183–231.
- [MS83] P. McMullen and R. Schneider, *Valuations on convex bodies*, Convexity and its Applications, Birkhäuser, Basel, 1983, pp. 170–247.
- [PT04] J. Pommersheim and H. Thomas, *Cycles representing the Todd class of a toric variety*, J. Amer. Math. Soc. **17** (2004), 983–994.
- [Sc86] A. Schrijver, *Theory of Linear and Integer Programming*, Wiley-Interscience Series in Discrete Mathematics, John Wiley & Sons, Ltd., Chichester, 1986.
- [Sc93] R. Schneider, *Convex Bodies: the Brunn-Minkowski Theory*, Encyclopedia of Mathematics and its Applications, vol. 44, Cambridge University Press, Cambridge, 1993.
- [Sh97] V.N. Shevchenko, *Qualitative Topics in Integer Linear Programming*, Translated from the Russian by H. H. McFaden. Translations of Mathematical Monographs, 156, American Mathematical Society, Providence RI, 1997.
- [St97] R.P. Stanley, *Enumerative Combinatorics. Vol. 1*, Corrected reprint of the 1986 original. Cambridge Studies in Advanced Mathematics, 49, Cambridge University Press, Cambridge, 1997.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,
USA

E-mail address: `barvinok@umich.edu`