that this bound, apart from the polylogarithmic factor, is tight. Clearly, there is some room for improvement. In fact, it is conceivable that $S_d(n)$ is $\Theta(n^d)$.

In conclusion, we thank Janos Pach for providing a crucial pointer.

References

1. G. Georgakopoulos and C. Papadimitriou. The 1-Steiner tree problem. *J. Algorithms* **8** (1987), 122–130.
2. G. Kalai. Intersection patterns of convex sets. *Israel J. Math.* **48** (1984), 161–174.
3. C. Monma and S. Suri. Transitions in geometric spanning trees. *Proc. 7th ACM Symp. on Computational Geometry*, 1991, pp. 239–249.
4. F. P. Preparata and M. I. Shamos. *Computational Geometry: An Introduction*. Springer-Verlag, New York, 1985.
5. A. C. Yao. On constructing minimum spanning trees in *k*-dimensional space and related problems. *SIAM J. Comput.* **11** (1982), 721–736.

Received September 17, 1992.

Discrete Comput Geom 12:35–48 (1994)

Discrete & Computational
Geometry
© 1994 Springer-Verlag New York Inc.

Computing the Ehrhart Polynomial of a Convex Lattice Polytope*

A. I. Barvinok

MSI, 409 College Avenue, Ithaca, NY 14850, USA
barvinok@msiadmin.cit.cornell.edu

Abstract. We prove that computation of any fixed number of highest coefficients of the Ehrhart polynomial of an integral polytope can be reduced in polynomial time to computation of the volumes of faces.

1. Introduction

The problem of counting integral points in polyhedra has been of interest for a long time. It is known that generally this problem is #*P*-hard. Even if we want to count integral points approximately with an exponentially large error, the problem still remains NP-hard [3]. In a recent paper [2] the author showed that if the dimension of a polytope is fixed then integral points in the polytope can be counted in polynomial time. In this paper we apply the technique of [2] further to deal with polytopes of varying dimension.

Let $\mathbb{Z}^d \subset \mathbb{R}^d$ be the standard integral lattice and let $P \subset \mathbb{R}^d$ be a polytope. We assume that P is *integral*, namely, its vertices belong to $\mathbb{Z}^d$. For $m \in \mathbb{N}$ we put $m \cdot P = \{m \cdot x : x \in P\}$. Then the number of integral points in $m \cdot P$ is a polynomial in $m \in \mathbb{N}$, called the *Ehrhart polynomial* (see, for example, Chapter 4 of [12]). So

$$\#\{m \cdot P \cap \mathbb{Z}^d\} = \sum_{j=0}^{d} e_j(P) \cdot m^j.$$

In this paper we study the coefficients $e_j(P)$ from the computational complexity point of view.

* This research was supported by the United States Army Research Office through the Army Center of Excellence for Symbolic Methods in Algorithmic Mathematics (ACSyAM), Mathematical Sciences Institute of Cornell University, Contract DAAL03-91-C-0027.

These coefficients naturally appear in many formulas of enumerative combinatorices (see, for example, [12]), therefore it might be interesting to compute them efficiently. It is well known that $e_d(P)$ is equal to the volume of P. The next coefficient $e_{d-1}(P)$ is half of the "surface area" of P, that is

$$e_{d-1}(P) = \tfrac{1}{2} \cdot \sum_G \operatorname{vol}_{d-1}(G),$$

where G ranges over all facets of P and the volume of a facet is measured intrinsically with respect to the lattice $\mathbb{Z}^d \cap A_G$, where A_G is the affine hull of G [9]. These observations show that computation of the two highest coefficients reduces to computation of the volumes of faces. From the results of [11] it follows that computation of $e_{d-2}(P)$ can also be reduced in polynomial time to computation of the volumes of faces ([11] does not deal with computational complexity but it contains an explicit expression of $e_{d-2}(P)$ in terms of the volumes and Dedekind sums; these sums, however, are known to be polynomially computable). We also know that $e_0(P) = 1$ for an arbitrary polytope P [9]. In this paper we prove that computation of any fixed number of the highest coefficients of the Ehrhart polynomial can be reduced to volume computation in polynomial time.

Let us assume that a d-dimensional integral polytope $P \subset \mathbb{R}^d$ is given by the set of linear inequalities

$$\textbf{(1.1)} \qquad P = \{x \in \mathbb{R}^d \colon \langle l_i, x\rangle \le a_i,\ i = 1, \ldots, m\},$$

where $l_i \in \mathbb{Z}^d$ and $a_i \in \mathbb{Z}$ for all i. Here $\langle \cdot, \cdot \rangle$ denotes the standard inner product in $\mathbb{R}^d$. We use the standard notion of *input size* (see, for example, [6]). Thus for the polytope P given by (1.1) we have

$$\text{size } P = O\left(d \cdot \sum_{i=1}^{m} (1 + \log(\|l_i\| + 1) + \log(|a_i| + 1))\right),$$

where $\|\cdot\|$ denotes the L_∞ norm in $\mathbb{R}^d$. Let us introduce the

Volume Computation Oracle.
Input: a polytope P given as in (1.1);
a set of indices $I \subset \{1, \ldots, m\}$ of cardinality s.
Output:

$$\begin{cases} \operatorname{vol}_{d-s} F & \text{if the set } F = \{x \in P \colon \langle l_i, x\rangle = a_i,\ i \in I\} \\ & \text{is a } (d-s)\text{-dimensional face of } P, \\ 0 & \text{otherwise.} \end{cases}$$

Again, we measure the volume of a face F intrinsically. Namely, let A_F be the affine hull of F. Choosing a point from $\mathbb{Z}^d \cap A_F$ as the origin, let us consider A_F as a linear space. Then $\mathbb{Z}^d \cap A_F$ is a lattice and we scale the volume so that the parallelopiped spanned by a basis of this lattice has volume 1. Our main result is the following:

(1.2) Theorem. *Let us fix $k \in \mathbb{N}$. Then, for any integral polytope P given by* (1.1), *the coefficient $e_{d-k}(P)$ can be computed using $O(m^k)$ calls for the* Volume Computation Oracle *and a number of arithmetic operations which is polynomial in size P. The size of each number involved in the algorithm is bounded by a polynomial in size P.*

The problem of volume computation is #P-hard [4]. Moreover, the size of the volume is not necessarily bounded by a polynomial in the size of the polytope [8]. However, if we restrict ourselves to a class of integral polytopes, then the size of the volume of any face of such a polytope is bounded by a polynomial in the input size (since it is a rational number whose denominator is at most $d!$). Therefore our Oracle is well defined in the context of Theorem 1.2. Although introduction of the Volume Computation Oracle which could solve #P-complete problems seems to be too strong an assumption, it is unavoidable. Already computation of the highest coefficient of the Ehrhart polynomial reduces to volume computation. We note that volume computation generally seems to be somewhat easier than counting integral points. For example, the volume of a simplex can be computed by the explicit formula in the straightforward way whereas integral points counting is far less obvious. Theorem 1.2, however, implies the following result.

(1.3) Corollary. *Let us fix $k \in \mathbb{N}$. For any given integral simplex $\Delta \subset \mathbb{R}^d$ the coefficient $e_{d-k}(\Delta)$ can be computed in polynomial time.*

Theorem 1.2 implies, in particular, that integral points in an integral polytope can be counted in polynomial time if the dimension d is fixed. This result is already contained in [2]. However, the present algorithm gives a better estimate of complexity. For a d-dimensional simplex Δ we get $(d \cdot \text{size } \Delta)^{O(d)}$ rather than $(\text{size } \Delta)^{O(d^2)}$ from [2].

In the first version of this paper [1] a weaker result was obtained by using a sort of "harmonic analysis on polytopes." The present paper uses a completely different approach based on some identities from [10]. We describe Morelli's identities in Section 2. To show that these identities lead to efficient algorithms we apply a technique of "cone decompositions" developed earlier in [2]. We describe this technique in Section 3. A new ingredient is an effective construction of a "generic subspace" required for Morelli's identities. This construction is described in Section 4. In Section 5 we prove Theorem 1.2 and give some estimates for the complexity of counting integral points in a simplex.

(1.4) Definitions and Notation. By co S we denote the conic hull of the set $S \subset \mathbb{R}^d$. Thus

$$\text{co } S = \left\{x = \sum_i \lambda_i \cdot s_i \colon \lambda_i \ge 0,\ s_i \in S \text{ for all } i\right\}.$$

By $\#S$ we denote the cardinality of the set S. A *polyhedral cone* is a conic hull of finitely many integral vectors from $\mathbb{R}^d$. If $K = \text{co}\{u_1, \dots, u_m\} \subset \mathbb{R}^d$, where $u_i \in \mathbb{R}^d$ for $i = 1, \dots, m$, then we say that the cone K is *generated* by $u_1, \dots, u_m$ and call the vectors $u_1, \dots, u_m$ *generators* of K. In what follows we consider only *rational* cones, that is, the cones generated by integral vectors. Similarly, a subspace is called *rational* if it is generated by integral vectors. We assume that the cone is given by its generators. A cone $K = \text{co}\{u_1, \dots, u_m\}$ is *simple* if $u_1, \dots, u_m$ are linearly independent. By Lin S we denote the linear hull of $S \subset \mathbb{R}^d$. A discrete additive subgroup $\Lambda \subset \mathbb{R}^d$ is called a *lattice*. Each lattice Λ has a *basis*, that is, a set of linearly independent vectors $u_1, \dots, u_m \in \Lambda$ such that

$$\Lambda = \left\{x = \sum_{i=1}^{m} \lambda_i \cdot u_i \colon \lambda_i \in \mathbb{Z}\right\}.$$

Then m is called the *rank* of Λ. The volume of the parallelopiped spanned by a basis of Λ is called the *determinant* of the lattice Λ. Thus

$$\det \Lambda = |u_1 \wedge \cdots \wedge u_m|.$$

A simple cone $K = \text{co}\{u_1, \dots, u_m\}$ is called *primitive* if $u_1, \dots, u_m$ is a basis of the lattice $\Lambda = \text{Lin } K \cap \mathbb{Z}^d$. Then $u_1, \dots, u_m$ are called *primitive generators* of K.

As a general reference to lattice algorithms we use [6].

2. Morelli's Formulas

In this section we briefly describe some results of [10]. Morelli's formulas provide an expression

$$e_{d-k}(P) = \sum_F \text{vol}_{d-k}(F) \cdot \mu(P, F),$$

where F ranges over the set of all $(d-k)$-dimensional faces of P and $\mu(P, F)$ is a certain function which is determined by the supporting cone of P at F. Actually, μ is an additive measure on rational polyhedral cones in $\mathbb{R}^d$. We describe this measure in detail.

Let us consider the set $\mathscr{C}_k$ of all k-dimensional rational polyhedral cones K in $\mathbb{R}^d$. Morelli defines a measure μ on $\mathscr{C}_k$. For $K \in \mathscr{C}_k$, the value of $\mu(K)$ is a rational real-valued function on the Grassmanian $\mathbf{G}_{d-k+1}(\mathbb{R}^d)$ of all $(d-k+1)$-dimensional subspaces in $\mathbb{R}^d$. If $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$ is a regular point of the function $\mu(K)$, then by $\mu_G(K)$ we denote the real number that is the value of the function $\mu(K)$ at the point G. Before we describe this measure we recall one useful notion.

(2.1) Todd Polynomial. *Todd polynomial* $\text{td}_k(x_1, \dots, x_d)$ is defined as the coefficient of t^k in the following expansion:

$$\text{(2.1.1)} \qquad \prod_{i=1}^{d} \frac{t \cdot x_i}{1 - \exp\{-t \cdot x_i\}} = \sum_{k=0}^{+\infty} t^k \cdot \text{td}_k(x_1, \dots, x_d).$$

So, $\text{td}_k(x_1, \dots, x_d)$ is a symmetric homogeneous polynomial with rational coefficients of degree k. In Section 5 we need the following simple result.

(2.1.2) Lemma. *For any given d, $k \in \mathbb{N}$ and for any rational nonzero numbers $x_1, \dots, x_d$ the value of $\text{td}_k(x_1, \dots, x_d)$ can be computed in time which is polynomial in d, k, and the input size of $x_1, \dots, x_d$.*

Proof. For given $x_1, \dots, x_d$ the value of $\text{td}_k(x_1, \dots, x_d)$ is equal to the kth coefficient of the Taylor expansion of the univariate function from the left-hand side of (2.1.1). Replacing $\exp\{-t \cdot x_i\}$ by the first $k+1$ terms of its Taylor expansion we compute the desired value in the straightforward way. □

First we define the function $\mu(K)$ for a *primitive* cone K.

(2.2) Primitive Cones. Let $K = \text{co}\{u_1, \dots, u_k\} \subset \mathbb{R}^d$ be a primitive cone with the primitive generators $u_1, \dots, u_k \in \mathbb{Z}^d$. Let

$$K^* = \{x \in \mathbb{R}^d \colon \langle x, y \rangle \geq 0 \text{ for all } y \in K\} \subset \mathbb{R}^d$$

be the conjugate cone. The cone K^* contains a $(d-k)$-dimensional subspace

$$V = \{x \in \mathbb{R}^d \colon \langle x, y \rangle = 0 \text{ for all } y \in K\}.$$

For $s = 1, \dots, k$ let us define a linear $(d-k+1)$-dimensional subspace $E_s \subset \mathbb{R}^d$:

$$E_s = \{x \in \mathbb{R}^d \colon \langle x, u_j \rangle = 0 \text{ for } j = 1, \dots, s-1, s+1, \dots, k\}.$$

Let us choose a basis $x_1, \dots, x_{d-k}$ of V. For each $s = 1, \dots, k$ we construct an oriented basis $B_s = (b_1^s, \dots, b_{d-k+1}^s)$ of the $(d-k+1)$-dimensional lattice $E_s \cap \mathbb{Z}^d$. We assume that the orientation of B_s is the same as that of the basis $x_1, \dots, x_{d-k}, \bar{u}_s$, where $\bar{u}_s$ is the orthogonal projection of u_s onto E_s.

Let us choose vectors $g_1, \dots, g_{d-k+1} \in \mathbb{R}^d$. For $s = 1, \dots, k$ we define a $(d-k+1) \times (d-k+1)$ matrix M^s as follows:

$$M^s(i, j) = \langle b_i^s, g_j \rangle$$

for $i, j = 1, \dots, d-k+1$. Put $f_s = \det M^s$. Let us put

$$\mu_{g_1,\dots,g_k}(K) = \frac{\mathrm{td}_k(f_1,\dots,f_k)}{f_1\cdots f_k}.$$

Thus $\mu_{g_1,\dots,g_k}(K)$ is a rational function in $g_1,\dots,g_{d-k+1}$. Formally, μ depends also on the choice of B_s. However, since td_k is a homogeneous polynomial of degree k, we observe that the value of $\mu_{g_1,\dots,g_k}(K)$ actually depends on the linear subspace $G \subset \mathbb{R}^d$ generated by $g_1,\dots,g_{d-k+1}$ only. Thus for $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$ we put $\mu_G(K) = \mu_{g_1,\dots,g_{d-k+1}}(K)$ where $g_1,\dots,g_{d-k+1}$ is a basis of G. We observe that a "generic" $(d-k+1)$-dimensional subspace G is a regular point of the function $\mu(K)$.

Morelli shows that μ is an additive measure.

(2.3) Theorem [10]. *Let $K \subset \mathbb{R}^d$ be a k-dimensional rational cone. Let*

$$K = \bigcup_{i\in I_1} K_i$$

and

$$K = \bigcup_{i\in I_2} K_i$$

be decompositions of the cone K into the union of finitely many primitive k-dimensional cones K_i, $i \in I_1$ (resp. K_i, $i \in I_2$), with pairwise disjoint interiors. Then

$$\sum_{i\in I_1} \mu(K_i) = \sum_{i\in I_2} \mu(K_i)$$

as rational functions on the Gassmanian $\mathbf{G}_{d-k+1}(\mathbb{R}^d)$ of $(d-k+1)$-dimensional subspaces in $\mathbb{R}^d$.

Since every rational polyhedral K cone can be decomposed into the union of finitely many primitive cones K_i with pairwise disjoint interiors (see, for example, Section 2.6 of [5]) we can correctly define

$$\mu(K) = \sum_{i\in I} \mu(K_i).$$

Thus $\mu(K)$ is a rational function in $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$.

(2.4) Definition. Let $P \subset \mathbb{R}^d$ be a convex d-dimensional polytope. For a $(d-k)$-dimensional face $F \subset P$ of P we define the supporting cone $K(F, P)$ as the cone of

feasible directions. Let y be an arbitrary p
F. We put $K(F, P) = \{x \in \mathbb{R}^d: y + \varepsilon \cdot x \in P$
$K^*(F, P)$ we denote the conjugate cone. Th

(2.5) Theorem [10]. *Let $P \subset \mathbb{R}^d$ be an inte*

$$e_{d-k}(P) = \sum_F \mathrm{vol}_{d-k}($$

where the sum is taken over all $(d-k)$-dimens
side is a constant function in $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$

3. Decomposition of Rational Cones

In this section we show that any rational
represented in polynomial time as a "linear
a set $S \subset \mathbb{R}^d$ by $\chi_S: \mathbb{R}^d \to \{0, 1\}$ we denote the

$$\chi_S(x) = \begin{cases} 1 & \text{if} \\ 0 & \text{o} \end{cases}$$

(3.1) Definition. Let K, K_i, $i \in I$, be a finite
cones in $\mathbb{R}^d$ and let ε_i, $i \in I$, be a family of in

$$K = \sum_{i\in I} \varepsilon_i \cdot$$

if and only if the identity

$$\chi_K = \sum_{i\in I} \varepsilon_i \cdot$$

holds for all $x \in \mathbb{R}^d$ except possibly a finite u
subspaces.

Thus, if $K = \bigcup_{i\in I} K_i$, where K_i, $i \in I$, are
pairwise disjoint interors, we have that $K =$
standard corollary of Theorem 2.3.

(3.2) Lemma. *Let*

$$K = \sum_{i\in I} \varepsilon_i \cdot$$

for $i, j = 1, \ldots, d-k+1$. Put $f_s = \det M^s$. Let us put

$$\mu_{g_1,\ldots,g_k}(K) = \frac{\mathrm{td}_k(f_1, \ldots, f_k)}{f_1 \cdots f_k}.$$

Thus $\mu_{g_1,\ldots,g_k}(K)$ is a rational function in $g_1, \ldots, g_{d-k+1}$. Formally, μ depends also on the choice of B_s. However, since td_k is a homogeneous polynomial of degree k, we observe that the value of $\mu_{g_1,\ldots,g_k}(K)$ actually depends on the linear subspace $G \subset \mathbb{R}^d$ generated by $g_1, \ldots, g_{d-k+1}$ only. Thus for $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$ we out $\mu_G(K) = \mu_{g_1,\ldots,g_{d-k+1}}(K)$ where $g_1, \ldots, g_{d-k+1}$ is a basis of G. We observe that a "generic" $(d-k+1)$-dimensional subspace G is a regular point of the function $\iota(K)$.

Morelli shows that μ is an additive measure.

2.3) Theorem [10]. *Let $K \subset \mathbb{R}^d$ be a k-dimensional rational cone. Let*

$$K = \bigcup_{i \in I_1} K_i$$

nd

$$K = \bigcup_{i \in I_2} K_i$$

e decompositions of the cone K into the union of finitely many primitive k-imensional cones K_i, $i \in I_1$ (resp. K_i, $i \in I_2$), with pairwise disjoint interiors. Then

$$\sum_{i \in I_1} \mu(K_i) = \sum_{i \in I_2} \mu(K_i)$$

; rational functions on the Gassmanian $\mathbf{G}_{d-k+1}(\mathbb{R}^d)$ of $(d-k+1)$-dimensional ıbspaces in $\mathbb{R}^d$.

Since every rational polyhedral K cone can be decomposed into the union of ıitely many primitive cones K_i with pairwise disjoint interiors (see, for example, ection 2.6 of [5]) we can correctly define

$$\mu(K) = \sum_{i \in I} \mu(K_i).$$

ıus $\mu(K)$ is a rational function in $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$.

4) Definition. Let $P \subset \mathbb{R}^d$ be a convex d-dimensional polytope. For a $(d-k)$-nensional face $F \subset P$ of P we define the supporting cone $K(F, P)$ as the cone of feasible directions. Let y be an arbitrary point in the relative interior of the face F. We put $K(F, P) = \{x \in \mathbb{R}^d : y + \varepsilon \cdot x \in P$ for all sufficiently small $\varepsilon > 0\}$. By $K^*(F, P)$ we denote the conjugate cone. Thus $\dim K^*(F, P) = k$.

(2.5) Theorem [10]. *Let $P \subset \mathbb{R}^d$ be an integral polytope. Then*

$$e_{d-k}(P) = \sum_F \mathrm{vol}_{d-k}(F) \cdot \mu(K^*(F, P)),$$

where the sum is taken over all $(d-k)$-dimensional faces F of P. Thus the right-hand side is a constant function in $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$ whose value is equal to $e_{d-k}(P)$.

3. Decomposition of Rational Cones

In this section we show that any rational cone of a fixed dimension can be represented in polynomial time as a "linear combination" of primitive cones. For a set $S \subset \mathbb{R}^d$ by $\chi_S: \mathbb{R}^d \to \{0, 1\}$ we denote the characteristic function of S, that is,

$$\chi_S(x) = \begin{cases} 1 & \text{if } x \in S, \\ 0 & \text{otherwise.} \end{cases}$$

(3.1) Definition. Let K, K_i, $i \in I$, be a finite family of k-dimensional polyhedral cones in $\mathbb{R}^d$ and let ε_i, $i \in I$, be a family of integral numbers. We write

$$K = \sum_{i \in I} \varepsilon_i \cdot K_i$$

if and only if the identity

$$\chi_K = \sum_{i \in I} \varepsilon_i \cdot \chi_{K_i}$$

holds for all $x \in \mathbb{R}^d$ except possibly a finite union of rational $(k-1)$-dimensional subspaces.

Thus, if $K = \bigcup_{i \in I} K_i$, where K_i, $i \in I$, are k-dimensional rational cones with pairwise disjoint interors, we have that $K = \sum_{i \in I} K_i$. The following result is the standard corollary of Theorem 2.3.

(3.2) Lemma. *Let*

$$K = \sum_{i \in I} \varepsilon_i \cdot K_i$$

e a representation of a k-dimensional rational polyhedral cone $K \subset \mathbb{R}^d$ into a linear combination of primitive k-dimensional cones K_i, $i \in I$. Then

$$\mu(K) = \sum_{i \in I} \varepsilon_i \cdot \mu(K_i).$$

Proof. Let Γ_j, $j \in J$, be a finite (possibly empty) union of $(k-1)$-dimensional ubspaces from Definition 3.1. Let us subdivide all possible k-dimensional intersecions $(K \cap) \bigcap_{i \in I_1} K_i$, $I_1 \subset I$, into primitive k-dimensional cones K_α, $\alpha \in A$, with airwise disjoint interiors so that Γ_j does not intersect the interior of K_α for all j and . Thus each cone can be represented as a union $K = \bigcup_{\alpha \in A_0} K_\alpha$, $K_i = \bigcup_{\alpha \in A_i} K_\alpha$, o that, for any $\alpha \in A$,

$$\sum_{i : \alpha \in A_i} \varepsilon_i = \begin{cases} 1 & \text{if } \alpha \in A_0, \\ 0 & \text{otherwise.} \end{cases}$$

'he proof then follows by Theorem 2.3. □

It is well known that a k-dimensional polyhedral cone $K \subset \mathbb{R}^d$ can be reresented as a union of simple cones K_i with pairwise disjoint interiors. If k is xed, then this can be done in polynomial time. Our aim is to show that if k is xed, then a simple rational k-dimensional cone can be represented as a linear ombination of primitive cones in polynomial time. Here we basically follow [2], lthough we present a somewhat weaker construction since we do not care about oints in a $(k-1)$-dimensional set.

We discuss the input size of our problem. For a simple cone $K = \text{co}\{u_1, \dots, u_k\}$, here $u_i \in \mathbb{Z}^d$, we have size $K = O(d \cdot \sum_{i=1}^d (1 + \log(\|u_i\| + 1)))$, where $\|\cdot\|$ is the L_∞ orm on $\mathbb{R}^d$.

.3) Definition. Let $K = \text{co}\{u_1, \dots, u_k\}$ be a simple k-dimensional cone in $\mathbb{R}^d$ ven by its generators $u_1, \dots, u_k \in \mathbb{Z}^d$. Let us put $\Lambda = \text{Lin } K \cap \mathbb{Z}^d$. Thus Λ is a dimensional lattice. By Ind K we denote the index of the sublattice generated the vectors $u_1, \dots, u_k$ in the lattice Λ. In other words,

$$\text{Ind } K = \frac{|u_1 \wedge \cdots \wedge u_k|}{\det \Lambda},$$

ıere $|u_1 \wedge \cdots \wedge u_k|$ denotes the k-volume of the parallelopiped spanned by $, \dots, u_k$.

We conclude that K is primitive with the primitive generators $u_1, \dots, u_k$ if and ly if Ind $K = 1$. Besides, Ind K is polynomially computable, and therefore the lue of log Ind K is bounded by a polynomial in the input size of the cone K. ır algorithm is based on successive reduction of Ind K.

(3.4) Lemma (see [2]). *Let us fix $k \in \mathbb{N}$. Then a polynomial-time algorithm exists which, for any $d \in \mathbb{N}$, for any rational simple k-dimensional cone $K \subset \mathbb{R}^d$, computes k-dimensional simple cones K_i, $i \in I$, $\# I \le k$, and numbers $\delta_i \in \{+1, -1\}$ such that*

$$\text{(3.4.1)} \qquad K = \sum_{i \in I} \delta_i \cdot K_i,$$

$$\text{(3.4.2)} \qquad \text{Ind } K_i \le (\text{Ind } K)^{(k-1)/k} \quad \textit{for all} \quad i \in I,$$

$$\text{(3.4.3)} \qquad \text{size } K_i \le \text{size } K + O(d^2) \quad \textit{for all} \quad i \in I.$$

Proof. Let us consider the parallelopiped

$$\text{(3.4.4)} \qquad \Psi = \left\{ x = \sum_{i=1}^{k} \alpha_i \cdot u_i : |\alpha_i| \le (\text{Ind } K)^{-1/k} \right\}.$$

Thus Ψ is a centrally symmetric convex body whose k-dimensional volume is equal to $2^k \cdot \det \Lambda$, where $\Lambda = \mathbb{Z}^d \cap \text{Lin } K$. Therefore by Minkowski's theorem (see, for example, [6]) it contains a nonzero lattice vector $w \in \Lambda$. Choosing, if necessary, $-w$ instead of w we ensure that $w, u_1, \dots, u_k$ belong to certain open subspace in $\mathbb{R}^d$. Let us denote

$$I = \{ i \in [1:k] \text{: the vectors } u_1, \dots, u_{i-1}, w, u_{i+1}, \dots, u_k \text{ are linearly independent} \}.$$

For $i \in I$ let us put $K_i = \text{co}\{u_1, \dots, u_{i-1}, w, u_{i+1}, \dots, u_k\}$. We are going to prove that K_i satisfy (3.4.1)–(3.4.3). Let us put

$$I_+ = \{ i \in I \text{: the bases } (u_1, \dots, u_{i-1}, w, u_{i+1}, \dots, u_k) \text{ and } (u_1, \dots, u_{i-1}, u_i, u_{i+1}, u_k) \text{ have the same orientation} \}$$

and

$$I_- = I \backslash I_+.$$

Then we put

$$\delta_i = \begin{cases} 1 & \text{if } i \in I_+, \\ -1 & \text{if } i \in I_-. \end{cases}$$

Obviously we have

$$K = \sum_{i \in I} \delta_i \cdot K_i$$

nd (3.4.1) holds. Furthermore, if $w = \sum_{i=1}^{k} \alpha_i \cdot u_i$, then $|\alpha_i| \le (\text{Ind } K)^{-1/k}$ and we ave that

$$\begin{aligned}\text{Ind } K_i &= \frac{|u_1 \wedge \cdots \wedge u_{i-1} \wedge w \wedge u_{i+1} \wedge \cdots \wedge u_k|}{\det \Lambda}\\ &= \frac{|\alpha_i| \cdot |u_1 \wedge \cdots \wedge u_k|}{\det \Lambda}\\ &\le (\text{Ind } K)^{(k-1)/k}\end{aligned}$$

nd therefore (3.4.2) holds. Finally, (3.4.3) holds since obviously

$$\|w\| \le \|u_1\| + \cdots + \|u_k\|.$$

Now we must show that the vector w can be computed in polynomial time. ndeed, the problem of finding an integral nonzero vector in the parallelopiped Ψ reduces to integer programming in fixed dimension k. Let us construct a basis $b_1, \dots, b_k$ of the lattice Λ. This can be done in polynomial time (see [6]). We pproximate the parallelopiped Ψ by a rational parallelopiped Π. To do that, let s compute the basis $\{u_i^* \in \text{Lin } K: i = 1, \dots, k\}$ of Lin K conjugate to $\{u_1, \dots, u_k\}$, o $\langle u_i, u_j^* \rangle = \delta_{ij}$ for $i, j = 1, \dots, k$. Let D be the least common multiple of the enominators of coordinates of u_i^*, $i = 1, \dots, k$. We define the parallelopiped Π eplacing $(\text{Ind } K)^{-1\ k}$ in (3.4.4) by its rational approximation with error less than $/D$. This can be done in polynomial time as well. Then for $i = 1, \dots, k$ we solve problem of integer linear programming:

Find $\gamma = (\gamma_1, \dots, \gamma_k) \in \mathbb{Z}^k$
Such that: $\sum_{i=1}^{k} \gamma_i \cdot b_i \in \Pi$
and $\gamma_i \ge 1$.

For some i the program has a solution and then the point $w = \sum_{i=1}^{k} \gamma_i \cdot b_i$ is e desired nonzero integral vector from Ψ. Since k is fixed, a solution of the above rogram can be found in polynomial time (see [6] and [7]). □

Now we can prove the main result of this section.

.5) Theorem (see [2]). *Let us fix $k \in \mathbb{N}$. Then, for any $d \in \mathbb{N}$, for any simple tional k-dimensional cone $K \subset \mathbb{R}^d$, a family of k-dimensional primitive cones K_i, $\in I$, and integral numbers $\varepsilon_i \in \{1, -1\}$, $i \in I$, such that*

$$K = \sum_{i \in I} \varepsilon_i \cdot K_i$$

an be constructed in polynomial time.

Proof. We iterate the construction of Lemma 3.4. After the mth iteration we get a decomposition

$$K = \sum_{i \in I_m} \varepsilon_i \cdot K_i, \tag{3.5.1}$$

where $\# I_m \le k^m$, $\text{Ind } K_i \le (\text{Ind } K)^{((k-1)/k)^m}$, $\varepsilon_i \in \{-1, 1\}$, and size $K_i \le$ size $K + O(d^2 \cdot m)$. Let us choose the smallest integral m such that

$$m \ge \frac{-\log\log 1.9 + \log\log(\text{Ind } K)}{\log k - \log(k-1)}.$$

Then after the mth iteration we will have that $\text{Ind } K_i \le 1.9$ and therefore $\text{Ind } K_i = 1$ for all i in the representation (3.5.1). Now we observe that the complexity of our algorithm is linear in k^m. We have that

$$k^m \le C_1(k) \cdot (\log(\text{Ind } K))^{C_2(k)},$$

where

$$C_1(k) = \exp\left\{\left(\frac{-\log\log 1.9}{\log k - \log(k-1)} + 1\right) \cdot \log k\right\}, \qquad C_2(k) = \frac{\log k}{\log k - \log(k-1)}.$$

Thus for a fixed k the value of k^m is bounded by a polynomial in the size of K. □

4. Constructing a Regular Subspace

In this section we prove the following main result.

(4.1) Lemma. *A polynomial-time algorithm exists which, for any given $d, k, m \in \mathbb{N}$ and any given m primitive k-dimensional cones $K_i \subset \mathbb{R}^d$, $i = 1, \dots, m$, computes a $(d - k + 1)$-dimensional subspace $G \in \mathbf{G}_{d-k+1}(\mathbb{R}^d)$ which is a regular point for all the functions $\mu(K_i)$, $i = 1, \dots, m$.*

We deduce Lemma 4.1 from a more general statement about polynomials defined by their oracles. Such an object is a multivariate rational polynomial P given by a "black box" which for any given rational x computes the value $P(x)$. Besides we assume that an upper bound D of the degree of P is known. This approach is useful when we deal with various determinants. Indeed, a determinant can usually be computed rather efficiently whereas its straightforward expansion contains plenty of monomial terms. The following result shows that we can always compute in polynomial time a point which is not a root of any polynomial from a given family, provided for each polynomial we know at least one point which is not a root. We note that generally it is an open problem to determine in polynomial time whether a polynomial given by an oracle is not identically zero.

(4.2) Proposition. *For any finite set $\{P_\alpha : \alpha \in A\}$ of rational polynomials $P_\alpha : \mathbb{Q}^n \to \mathbb{Q}$ given by their oracles such that* $\deg P_\alpha \le D_\alpha$, $\alpha \in A$, *and for any given* $x_\alpha \in \mathbb{Q}^n$, $\alpha \in A$, *such that* $P_\alpha(x_\alpha) \neq 0$ *for* $\alpha \in A$ *a vector* $x \in \mathbb{Q}^n$ *such that* $P_\alpha(x) \neq 0$ *for all* $\alpha \in A$ *can be computed in time which is polynomial in* n, $\# A$, $\max\{D_\alpha : \alpha \in A\}$, *and in the maximum size of* x_α, $\alpha \in A$.

Proof. Let us put $D = \max\{D_\alpha : \alpha \in A\}$. We construct an algebraic curve $\gamma : \mathbb{Q} \to \mathbb{Q}^n$ which passes through all the points x_α, $\alpha \in A$. We may think of the elements of A as the integers $1, \dots, \# A$. Let us denote by $x_\alpha(j)$ the jth coordinate of x_α. Using standard interpolation we construct a polynomial $r_j(t)$, $t \in \mathbb{Q}$, $j = 1, \dots, n$, of degree $\# A - 1$ such that $r_j(\alpha) = x_\alpha(j)$ for $\alpha \in A$. Put $\gamma(t) = (r_1(t), \dots, r_n(t)) \in \mathbb{Q}^n$. Then $\gamma(\alpha) = x_\alpha$ for $\alpha \in A$. We observe that for $\alpha \in A$ the polynomial $p_\alpha(t) = P_\alpha(\gamma(t))$ is a univariate nonzero polynomial of degree at most $(\# A) \cdot D_\alpha$. Our algorithm is the following: we compute consecutively $\gamma(t)$, $t = 0, \dots, (\# A)^2 \cdot D$, and the corresponding values $P_\alpha(\gamma(t))$, $\alpha \in A$. For at least one $t = T \in [0 : (\# A)^2 \cdot D]$ all the values of $P_\alpha(\gamma(t))$, $\alpha \in A$, must be nonzero. We put $x = \gamma(T)$. □

Now we can prove Lemma 4.1.

Proof of Lemma 4.1. We use (2.2) and (4.2). Let us define first the set of indices A. An index $\alpha \in A$ is a tuple $\alpha = (i, s)$, where $i = 1, \dots, m$ and $s = 1, \dots, k$. For $\alpha = (i, s)$ we construct the polynomial P_α as follows. Choose the cone K_i. Construct an oriented basis $B_s = (b_1^s, \dots, b_{d-k+1}^s)$ as described in (2.2). This can be done in polynomial time (see [6] for lattice algorithms). Then P_α will be a polynomial in the coordinates of $g_1, \dots, g_{d-k+1} \in \mathbb{R}^d$ defined as f_s (see (2.2)). We observe that for any given $g_1, \dots, g_{d-k+1} \in \mathbb{R}^d$ the value of P_α can be computed using $O(d^3)$ arithmetic operations as the value of the $(d-k+1) \times (d-k+1)$ determinant. We also note that $\deg P_\alpha \le d - k + 1$. Our aim is to find a set of vectors $G = (g_1, \dots, g_{d-k+1})$ such that $P_\alpha(G) \neq 0$ for all $\alpha \in A$. To apply Proposition 4.2 we only need to construct a point x_α such that $P_\alpha(x_\alpha) \neq 0$. However, we can choose $x_\alpha = (b_1^s, \dots, b_d^s{}_{k+1})$. Indeed, the value of $P_\alpha(x_\alpha)$ is the determinant of the Gramm matrix of the basis B_s, and therefore is nonzero. □

5. Proof of the Main Result

Now we are ready to prove the main result of this paper.

Proof of Theorem 1.2. Our algorithm is the following. For each collection $I \subset [1:m]$: $\# I = k$ of indices, by applying the Volume Computation Oracle we check if $F_I = \{x \in P : \langle l_i, x \rangle = a_i,\ i \in I\}$ is a $(d-k)$-dimensional face of P and if so, we compute its volume. Then for each such a face F_I we find a set

$$J_I = \{i \in [1:m]: \text{the face } F_I \text{ belongs to the hyperplane } \langle l_i, x \rangle = a_i\}.$$

This can be done using linear programming or by applying the Oracle. For each face F_I let us put $K_I = \mathrm{co}\{l_i : i \in J_I\}$. Thus K_I is a rational k-dimensional polyhedral cone in $\mathbb{R}^d$. Then, using triangulation and Theorem 3.5, we compute in polynomial time a decomposition

$$K_I = \sum_{\alpha \in A_I} \varepsilon_\alpha \cdot K_\alpha,$$

where K_α, $\alpha \in A = \bigcup A_I$, is a primitive k-dimensional cone in $\mathbb{R}^d$. Using Lemma 4.1 we compute a $(d-k+1)$-dimensional subspace G which is a regular point for all the functions $\mu(K_\alpha)$, $\alpha \in A$. Then for all $\alpha \in A$ we compute the value $\mu_G(K_\alpha)$ as in (2.2), see also (2.1.2). Now we put

$$\mu_G(K_I) = \sum_{\alpha \in A_I} \varepsilon_\alpha \cdot \mu_G(K_\alpha).$$

Finally, we compute the coefficient $e_{d-k}(P)$ using Theorem 2.5. □

Now we discuss the problem of counting integral points in a d-dimensional integral simplex. Let $\Delta \subset \mathbb{R}^d$ be a d-dimensional integral simplex. Our approach gives the following complexity for the problem of counting integral points in Δ. Obviously, we have

$$\#(\Delta \cap \mathbb{Z}^d) = \sum_{j=0}^{d} e_j(\Delta).$$

To compute $e_j(\Delta)$ we use our algorithm summarized in Theorem 1.2. We note that the volume of a face of Δ can be computed in polynomial time and that we have 2^{d+1} faces, including the empty face. The complexity of the algorithm from Lemma 3.4 is dominated by the term $(d \cdot \operatorname{size} \Delta)^{O(d)}$ for integer programming (see, for example, [7]). Thus the complexity of the algorithm from Theorem 3.5 is dominated by $(d \cdot \operatorname{size} \Delta)^{O(d)}$ too, because of the estimates on the number of iterations. Summarizing, we conclude that our algorithm for counting integral points in a simplex has $(d \cdot \operatorname{size} \Delta)^{O(d)}$ complexity. This is probably the best-known estimate so far.

Acknowledgment

I am grateful to Robert Morelli for many useful conversations.

References

1. A. Barvinok, Computing the Ehrhart polynomial of a convex lattice polytope, Preprint, TRITA/MAT-92-0036, Royal Institute of Technology, Stockholm, 1992.
2. A. I. Barvinok, A polynomial-time algorithm for counting integral points in polyhedra when the dimension is fixed, *Proceedings of 34th Symposium on the Foundations of Cc¨puter Science* (*FOCS '93*), IEEE Computer Society Press, New York, 1993, pp. 566–572.
3. W. Cook, M. Hartmann, R. Kannan, and C. McDiarmid, On integer points in polyhedra, *Combinatorica*, **12** (1992), 27–37.
4. M. Dyer and A. M. Frieze, On the complexity of computing the volume of a polyhedron, *SIAM J. Comput.*, **17**(5) (1988), 967–974.
5. W. Fulton, *Introduction to Toric Varieties*, Annals of Mathematics Studies, Vol. 131, Princeton University Press, Princeton, NJ, 1993.
6. M. Grötschel, L. Lovasz, and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Algorithms and Combinatorics, Vol. 2, Springer-Verlag, Berlin, 1988.
7. R. Kannan, Minkowski's convex body theorem and integer programming, *Math. Oper. Res.*, **12** (1987), 415–440.
8. J. Lawrence, Polytope volume computation, *Math. Comp.*, **57**(195) (1991), 259–271.
9. I. G. Macdonald, Polynomials associated with finite cell complexes, *J. London Math. Soc.* (*2*), **4** (1971), 181–192.
10. R. Morelli, Pick's theorem and the Todd class of a toric variety, *Adv. in Math.*, **100**(2) (1993), 183–231.
11. J. E. Pommersheim, Toric varieties, lattice points and Dedekind sums, *Math. Ann.*, **295** (1993), 1–24.
12. R. P. Stanley, *Enumerative Combinatorics*, Vol. 1, Wadsworth & Brooks/Cole, Monterey, CA, 1986.

Received November 3, 1992, and in revised form September 8, 1993.

Discrete Comput Geom 12:49–63 (1994)

Discrete & Computation
Geome
© 1994 Springer-Verlag New Yo

Free Arrangements and Relation Spaces*

K. A. Brandt[1] and H. Terao[2]

[1] Department of Mathematics, University of Kansas,
Lawrence, KS 66045, USA
brandt@math.ukans.edu

[2] Department of Mathematics, University of Wisconsin–Madison,
Madison, WI 53706, USA
terao@math.wisc.edu

Communicated by Louis Billera

Abstract. Yuzvinsky [7] has shown that free arrangements are formal. In tl we define a more general class of arrangements which we call k-formal, and v that free arrangements are k-formal. We close with an example which distir k-formal arrangements from formal arrangements.

1. Introduction

Let $\mathbb{K}$ be a field and let V be an l-dimensional vector space over $\mathbb{K}$. A h in V is a codimension 1 subspace of V. An *arrangement* $\mathcal{A}$ in V is a fi hyperplanes.

Let $\{x_1, \ldots, x_l\}$ be a basis for the dual V^* and let S be the symmet of V^* which is isomorphic to the polynomial algebra $\mathbb{K}[x_1, \ldots, x_l]$. T hyperplane H in V has a defining form

$$\alpha_H = a_1 x_1 + \cdots + a_l x_l$$

with $\ker(\alpha_H) = H$, unique up to a constant multiple. Thus an arrangem

* The first author was supported in part by a U.S. Department of Education Fel second author was supported in part by the National Science Foundation.