MATHEMATICS OF OPERATIONS RESEARCH
Vol. 19, No. 4, November 1994
Printed in U.S.A.

A POLYNOMIAL TIME ALGORITHM FOR COUNTING INTEGRAL POINTS IN POLYHEDRA WHEN THE DIMENSION IS FIXED

ALEXANDER I. BARVINOK

We prove that for any dimension d there exists a polynomial time algorithm for counting integral points in polyhedra in the d-dimensional Euclidean space. Previously such algorithms were known for dimensions $d = 1, 2, 3$, and 4 only.

1. Introduction. We present a polynomial time algorithm for counting integral points in polyhedra if the dimension of a polyhedron is fixed. Previously such algorithms were known for dimensions 1, 2, 3, and 4 only. Generally, a convex polyhedron is supposed to be given by linear inequalities or by the coordinates of its vertices. However, it can be shown that the problem of counting integral points in a rational polyhedron can be reduced in polynomial time to counting integral points in an integral simplex assuming that the dimension is fixed (see Cook et al. 1992 and Dyer 1991). Let $\mathbb{Z}^d \subset \mathbb{R}^d$ denote the standard integral lattice in the d-dimensional Euclidean space $\mathbb{R}^d$. We consider the following problem:

(1.1) Counting integral points in dimension d. Given $k+1$ integral vectors $v_1, \ldots, v_{k+1} \in \mathbb{Z}^d$, such that their convex hull $\Delta = \operatorname{conv}\{v_1, \ldots, v_{k+1}\}$ is a k-dimensional simplex, compute the number of integral points $\#(\Delta \cap \mathbb{Z}^d)$ in the simplex Δ.

For $d = 1$ a polynomial time algorithm in Problem 1.1 obviously exists. The case $d = 2$ also is relatively simple. A polynomial time algorithm is given by Pick's formula. For the cases $d = 3, 4$ polynomial time algorithms were designed by M. Dyer (1991). They essentially use some properties of Dedekind Sums. The paper by Dyer (1991) also contains a polynomial reduction of the case of even dimension $d = 2 \cdot m$ to the case of the preceding odd dimension $d = 2 \cdot m - 1$. In the paper by Cook et al. (1992) for each fixed d an algorithm was designed which for any given $\epsilon > 0$ solves Problem 1.1 with relative error less than ϵ in time which is polynomial in the size of the input and ϵ^{-1}. We also note that for any fixed dimension there is a polynomial algorithm which checks whether the polyhedron contains any integral point (see Lenstra 1983 and §6.7 of Grötschel 1988). Here we prove the following result.

(1.2) THEOREM. *Let us fix $d \in \mathbb{N}$. Then there exists a polynomial time algorithm which solves Problem* 1.1.

Therefore, by Cook et al (1992) and Dyer (1991) we conclude that for each dimension d there exists a polynomial algorithm for counting integral points in d-dimensional polyhedra.

The main idea of the algorithm is to use a remarkable identity discovered by M. Brion (1988, 1992) for exponential sums over polytopes. We discuss these

Received July 29, 1993; revised November 3, 1993.
AMS 1991 subject classification. Primary: 52C07; Secondary: 52B55, 90C10.
OR/MS Index 1978 subject classification. Primary: 439 sets/Polyhedra, Secondary: 627 Programming/Integer.
Key words. Integral points, rational polyhedra, integer programming

0364-765X/94/1904/0769/$01.25

identities in §2. In §3 we present a general outline of the algorithm. In §4–5 we describe important subroutines of the algorithm. Finally, §6 contains a description of the algorithm.

2. Preliminaries. Exponential sums over polyhedra. In this section we summarize some facts about exponential sums over polyhedra. Let $\mathbb{R}^d$ be the d-dimensional Euclidean space equipped with the standard inner product $\langle \cdot, \cdot \rangle$. The main tool of our algorithm is the following expression

$$\sum_{x \in P \cap \mathbb{Z}^d} \exp\{\langle c, x \rangle\}, \tag{2.1}$$

where $P \subset \mathbb{R}^d$ is a polyhedron and $c \in \mathbb{R}^d$ is a vector. Such an object usually appears in literature in a different form (see, for example, Chapter 4 of Stanley 1986). Namely, for each point $x = (x_1, \ldots, x_d) \in \mathbb{Z}^d$ the Laurent monomial $a^x = a_1^{x_1} \cdots a_d^{x_d}$ in d variables $a_1, \ldots, a_d$ is assigned. Instead of (2.1) the Laurent series

$$\sum_{x \in P \cap \mathbb{Z}^d} a^x \tag{2.2}$$

is considered. If in (2.2) we substitute formally $a_i = \exp\{c_i\}$ for $i = 1, \ldots, d$ then we get the expression (2.1) with $c = (c_1, \ldots, c_d)$. In what follows we translate some known statements about (2.2) into the corresponding statements about (2.1). We also note that all the necessary facts in the desired form are contained in the author's paper (Barvinok 1993).

First, we introduce some notation. By $\operatorname{conv} S$ we denote the convex hull of a set $S \subset \mathbb{R}^d$. By $\operatorname{co} S$ we denote the (convex) conic hull of a set $S \subset \mathbb{R}^d$, i.e.,

$$\operatorname{co} S = \left\{ x = \sum_i \lambda_i \cdot y_i : \lambda_i \geq 0 \text{ and } y_i \in S \text{ for all } i \right\}.$$

By $\operatorname{Lin} S$ we denote the linear hull of a set $S \subset \mathbb{R}^d$. A *lattice* is a discrete additive subgroup in Euclidean space. Thus, $\mathbb{Z}^d$ is a lattice in $\mathbb{R}^d$. Each lattice $\Lambda \subset \mathbb{R}^d$ has a *basis*, i.e., a set of linearly independent vectors $u_1, \ldots, u_k$ such that

$$\Lambda = \left\{ \sum_{i=1}^{k} \lambda_i \cdot u_i : \lambda_i \in \mathbb{Z} \text{ for } i = 1, \ldots, k \right\}.$$

Let us consider first the exponential sum (2.1) over a polyhedral cone.

(2.3) DEFINITION. A convex cone $K \subset \mathbb{R}^d$ is called *rational* if it is the conic hull of finitely many integral vectors:

$$K = \operatorname{co}\{u_1, \ldots, u_k\} : u_i \in \mathbb{Z}^d \quad \text{for } i = 1, \ldots, k.$$

Then we say that $u_1, \ldots, u_k$ are the generators of the cone K. A cone K is called *simple* if it can be generated by linearly independent vectors.

With each rational cone one can associate a certain meromorphic function.

(2.4) PROPOSITION (SEE, FOR EXAMPLE, THEOREM 4.6.11 OF STANLEY 1986 OR BARVINOK 1993). *Let $K \subset \mathbb{R}^d$ be a simple rational cone. Let $c \in \mathbb{R}^d$ be a vector such*

that the linear function $\langle c, \cdot \rangle$ *decreases along the extreme rays of* K. *Then the series*

$$\sum_{x \in K \cap \mathbb{Z}^d} \exp\{\langle c, x \rangle\}$$

converges and defines a meromorphic function in $c \in \mathbb{C}^d$ (*we denote this function* $\sigma(K;c)$). *If* $u_1, \ldots, u_k \in \mathbb{Z}^d$ *are linearly independent generators of* K *then for all* $c = (c_1, \ldots, c_d) \in \mathbb{C}^d$,

$$\sigma(K;c) = p_K(\exp\{c_1\}, \ldots, \exp\{c_d\}) \cdot \prod_{i=1}^{k} \frac{1}{1-\exp\{\langle c, u_i \rangle\}},$$

where p_K *is a Laurent polynomial in* d *variables. Thus the set of real singular points of* $\sigma(K;c)$ *is the union of hyperplanes*

$$H_j = \{c \in \mathbb{R}^d : \langle c, u_j \rangle = 0\}, \quad j = 1, \ldots, k. \quad \square$$

(2.5) REMARK. We give the idea of the standard proof which also displays the structure of the polynomial p_K in Proposition 2.4.

Let us consider the following "semi-open" parallelopiped Π:

$$\Pi = \left\{ x = \sum_{i=1}^{k} \alpha_i \cdot u_i : 0 \le \alpha_i < 1 \right\}.$$

It can be checked that for each point $x \in K \cap \mathbb{Z}^d$ there exists a unique representation

$$x = a + \sum_{i=1}^{k} m_i \cdot u_i,$$

where $a \in \Pi \cap \mathbb{Z}^d$ and m_i are nonnegative integers for $i = 1, \ldots, k$. Using the summation formula for a geometric series we conclude that

$$\sigma(K;c) = \left(\sum_{x \in \Pi \cap \mathbb{Z}^d} \exp\{\langle c, x \rangle\} \right) \cdot \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}}.$$

Now we consider the exponential sum (2.1) taken over a convex polytope.

(2.6) DEFINITION. Let $P \subset \mathbb{R}^d$ be a convex polytope. For a vertex v of P we define the supporting cone K_v of P at v as follows:

$$K_v = \{u \in \mathbb{R}^d : v + \delta \cdot u \in P \text{ for all sufficiently small } \delta > 0\}.$$

Thus, the cone K_v is generated by the vectors $w - v$ where w ranges over the set of all vertices of P such that $[v, w]$ is an edge of P.

A convex polytope $P \subset \mathbb{R}^d$ is called *integral* if its vertices belong to the lattice $\mathbb{Z}^d$. The set of vertices of P we denote by Vert P. The following proposition is crucial for our considerations.

(2.7) PROPOSITION (BRION 1988, 1992). *Let* P *be an integral polytope. Then*

$$\sum_{x \in P \cap \mathbb{Z}^d} \exp\{\langle c, x \rangle\} = \sum_{v \in \operatorname{Vert} P} \exp\{\langle c, v \rangle\} \cdot \sigma(K_v; c),$$

for all $c \in \mathbb{R}^d$ *which are not singular points of any function* $\sigma(K_v; c)$. $\square$

For an elementary proof of Proposition 2.7 see Barvinok (1993) or Khovanskii and Puhlikov (1992).

EXAMPLE. Let $d = 1$ and P be an interval, $P = [0, n]$: $n \in \mathbb{N}$. Then Vert $P = \{0, n\}$. Thus we have $K_0 = [0, +\infty)$ and $\sigma(K_0; c) = 1/(1 - \exp\{c\})$ whereas $K_n = (-\infty, 0]$ and $\sigma(K_n; c) = 1/(1 - \exp\{-c\})$. Finally we get the formula:

$$\sum_{x=0}^{n} \exp\{c \cdot x\} = \frac{\exp\{c \cdot (n+1)\} - 1}{\exp\{c\} - 1}$$

$$= \exp\{c \cdot 0\} \cdot \sigma(K_0; c) + \exp\{c \cdot n\} \cdot \sigma(K_n; c).$$

3. An outline of the algorithm. A straightforward idea for how to solve Problem 1.1 would be to substitute $c = 0$ in the formula of Proposition 2.7 for $P = \Delta$. However, the point $c = 0$ is singular for all the functions $\sigma(K_v; c)$. To overcome this difficulty, let us introduce a parameter $t \in \mathbb{R}$. Let c be a "generic" point in $\mathbb{R}^d$, so that c is a regular point for all the functions $\sigma(K_v; c)$, $v \in \text{Vert } \Delta$. We want to compute the constant term of the Taylor expansion of the function

$$\sum_{x \in \mathbb{Z}^d \cap \Delta} \exp\{t \cdot \langle c, x \rangle\}$$

in a neighborhood of the point $t = 0$. Now by Proposition 2.7 we can reduce our problem to the computation of the constant terms $R(K_v, v, c)$ of the Laurent expansions of the functions

$$\exp\{t \cdot \langle c, v \rangle\} \cdot \sigma(K_v; t \cdot c)$$

for all vertices v of Δ. We define a class of cones for which the last value can be computed relatively easily.

(3.1) DEFINITION. A simple rational cone K is called *primitive* if

$$K = \text{co}\{u_1, \ldots, u_k\},$$

where $u_1, \ldots, u_k$ is a basis of the lattice $\Lambda = \mathbb{Z}^d \cap \text{Lin} K$. The vectors $u_1, \ldots, u_k$ are called *primitive generators* of K.

It turns out that for a primitive cone K_v there exists an explicit formula for this constant term $R(K_v, v, c)$. This formula is based on the observation that for a primitive cone K the function $\sigma(K; c)$ looks very simple, namely the polynomial p_K in Proposition 2.4 is identically 1 (see §4.)

Finally, we represent an arbitrary simple rational cone K as a "linear combination" of primitive cones. It turns out that if the dimension d is fixed, then this can be done in polynomial time and the number of such primitive cones is bounded by a polynomial in the input size (§5). Such a decomposition immediately leads to a polynomial algorithm for the computation of the constant term $R(K, v, c)$ for an arbitrary simple rational cone $K \subset \mathbb{R}^d$ and for an arbitrary vector $v \in \mathbb{Z}^d$ when d is fixed. Thus the decomposition described in §5 constitutes the core of the algorithm.

We discuss the *input size* (see, for example, Grötschel et al. 1988) of our algorithms. For a vector $u = (u_1, \ldots, u_d) \in \mathbb{Z}^d$ we denote $|u| = \max\{|u_i|: i = 1, \ldots, d\}$. Thus size $u = O(d \cdot (\log(|u| + 1) + 1))$. We assume that a simple rational cone K is given by its integral linearly independent generators $u_1, \ldots, u_k$. Thus size $K = O(\text{size } u_1 + \cdots + \text{size } u_k)$.

4. Primitive cones. We start with an explicit formula for the function $\sigma(K; c)$ in case of a primitive cone K.

(4.1) PROPOSITION (SEE, FOR EXAMPLE, COROLLARY 4.6.8 IN STANLEY 1986 OR BARVINOK 1993). *Assume that $K \subset \mathbb{R}^d$ is a primitive cone with primitive generators $u_1, \ldots, u_k \in \mathbb{Z}^d$. Then*

$$\sigma(K; c) = \prod_{i=1}^{k} \frac{1}{1 - \exp\{\langle c, u_i \rangle\}}. \quad \square$$

We note that Proposition 4.1 follows from Remark 2.5 since the parallelopiped Π in the case of a primitive cone K contains exactly one integral point, namely, the origin.

(4.2) COROLLARY. *For any $k \in \mathbb{Z}_+$ there exists a polynomial $Q_k(x_1, \ldots, x_k; y)$ of degree not more than k with rational coefficients such that for any primitive k-dimensional cone $K \subset \mathbb{R}^d$ with primitive generators $u_1, \ldots, u_k \in \mathbb{Z}^d$, for any $v \in \mathbb{Z}^d$, and for any $c \in \mathbb{R}^d$ such that c is a regular point of the function $\sigma(K; c)$ the constant term $R(K, v, c)$ of the Laurent expansion of the function*

$$\exp\{t \cdot \langle c, v \rangle\} \cdot \sigma(K; t \cdot c)$$

in a neighbourhood of $t = 0$ is equal to the value of

$$Q_k(x_1, \ldots, x_k; y) \cdot \prod_{i=1}^{k} x_i^{-1}$$

for $y = \langle c, v \rangle$ and $x_i = \langle c, u_i \rangle$: $i = 1, \ldots, k$.

PROOF. Let us consider a function F_k in $k + 2$ variables $x_1, \ldots, x_k, y, t$:

$$F_k(x_1, \ldots, x_k; y, t) = \exp\{t \cdot y\} \cdot \prod_{i=1}^{k} \frac{t \cdot x_i}{1 - \exp\{t \cdot x_i\}}.$$

Then F_k is an analytic function in a neighbourhood of the point $x_1 = \cdots = x_k = y = t = 0$ and there its Taylor expansion exists in this neighbourhood. Moreover, we observe that the coefficients of this expansion are rational (since the Taylor expansion of exp contains rational coefficients only.) Let us group together all the terms which have degree k in t. We get the term $t^k \cdot Q_k(x_1, \ldots, x_k; y)$ where Q_k is a polynomial of degree not more than k with rational coefficients. By Proposition 4.1 we conclude that Q_k is the desired polynomial. $\square$

(4.3) LEMMA. *Let us fix d. There exists a polynomial algorithm, which for any primitive cone $K \subset \mathbb{R}^d$, given by its primitive generators, for any given integral vector $v \in \mathbb{Z}^d$, and for any given rational vector $c \in \mathbb{Q}^d$ such that c is a regular point of the function $\sigma(K; c)$ computes the value of the constant term $R(K, v, c)$.*

PROOF. Our algorithm is the following. Let $u_1, \ldots, u_k$ be the given primitive generators of the cone K. We compute $y = \langle c, v \rangle$, $x_i = \langle c, u_i \rangle$ for $i = 1, \ldots, k$ and substitute these values into the formula of Corollary 4.2. Since d is fixed and $k \le d$ our algorithm has polynomial complexity.

Note that we compute the polynomials Q_k: $k = 0, \ldots, d$ before starting the algorithm. $\square$

5. Decomposition of rational cones.

(5.1) DEFINITION. Let $K \subset \mathbb{R}^d$ be a rational simple cone, given by linearly independent generators $u_1, \ldots, u_k \in \mathbb{Z}^d$. Let us denote by Π the "semi-open" parallelopiped (see also Remark 2.5)

$$\Pi = \left\{ x = \sum_{i=1}^{k} \alpha_i \cdot u_i : 0 \le \alpha_i < 1 \right\}.$$

The number $\#(\Pi \cap \mathbb{Z}^d)$ of integral points in Π will be called *the index* of the given cone K and denoted by $\operatorname{Ind} K$.

Thus K is a primitive cone given by its primitive generators if and only if $\operatorname{Ind} K = 1$. Generally, $\operatorname{Ind} K$ is a natural number which measures the "deviation" of the cone K and its generators $u_1, \ldots, u_k$ from being primitive. At the same time $\operatorname{Ind} K$ measures the "complexity" of the polynomial p_K in Proposition 2.4. As is well known, the index of the cone K can also be described as follows. Let $\dim K = k$. Let us define a k-dimensional lattice $\Lambda = \operatorname{Lin} K \cap \mathbb{Z}^d$. The *determinant* of Λ is the volume of a k-dimensional parallelopiped spanned by a basis of Λ. Then

$$\operatorname{Ind} K = |u_1 \wedge \cdots \wedge u_k| / \det \Lambda.$$

Here we use the standard notation for the volume of the parallelopiped Π spanned by $u_1, \ldots, u_k$. In other words, $\operatorname{Ind} K$ is the index of the subgroup generated by $u_1, \ldots, u_k$ in the group Λ. In particular, we conclude that the index of a cone is polynomially computable and that $\log(\operatorname{Ind} K)$ is bounded by a polynomial in the input size (see, for example, §5.4 of Grötschel et al 1988). It follows by Definition 5.1 that the index of a face of a simple rational cone given by a subset of the set of generators does not exceed the index of the cone.

Let $S \subset \mathbb{R}^d$ be a set. By χ_S we denote the characteristic function of S. Thus

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

For a finite family of cones $K, K_i \subset \mathbb{R}^d$: $i \in I$ and integral numbers ϵ_i: $i \in I$ we write

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

if

$$\chi_K(x) = \sum_{i \in I} \epsilon_i \cdot \chi_{K_i}(x)$$

for all $x \in \mathbb{R}^d$. We are going to design a polynomial time algorithm for decomposing a nonprimitive rational cone K into a linear combination of rational cones with smaller indices. Iterating this procedure, we finally obtain a decomposition of the cone into a linear combination of primitive cones. If the dimension d is fixed, this algorithm turns out to have polynomial complexity since the number of iterations grows as $\log\log(\operatorname{Ind} K)$ whereas the number of cones in the decomposition grows singly exponentially in the number of iterations. The following lemma provides the key argument for such an algorithm.

(5.2) LEMMA. *Fix $d \in \mathbb{N}$. Then there exists a polynomial algorithm which for any given k linearly independent vectors $u_1, \ldots, u_k \in \mathbb{Z}^d$ constructs a nonzero vector $w \in$*

$\mathrm{Lin}\{u_1, \ldots, u_k\} \cap \mathbb{Z}^d$ *such that*

(a) *the vectors* $w, u_1 \ldots u_k$ *belong to a certain open halfspace in* $\mathbb{R}^d$;

(b) *if* $K_j = \mathrm{co}\{u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots, u_k\}$ *is a* k*-dimensional cone then*

$$\mathrm{Ind}\, K_j \le (\mathrm{Ind}\, K)^{(d-1)/d};$$

(c) $|w| \le |u_1| + \cdots + |u_k|$.

PROOF. Let us denote $\Lambda = \mathrm{Lin}\{u_1, \ldots, u_k\} \cap \mathbb{Z}^d$. Thus Λ is a k-dimensional lattice and $\mathrm{Ind}\, K = |u_1 \wedge \cdots \wedge u_k|/\det \Lambda$. Let us consider the following parallelopiped Ψ:

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

So, Ψ is a k-dimensional centrally symmetric convex body and its volume is equal to $2^k \cdot \det \Lambda$. Therefore by Minkowski's Theorem (see, for example, §5.3 of Grötschel et al. 1988) it contains a nonzero vector $w \in \Lambda \cap \Psi$. Then for all j such that $u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots, u_k$ are linearly independent we get

$$\begin{aligned} \mathrm{Ind}\, K_j &= |u_1 \wedge \cdots \wedge u_{j-1} \wedge w \wedge u_{j+1} \wedge \cdots \wedge u_k|/\det \Lambda \\ &\le (\mathrm{Ind}\, K)^{-1/k} \cdot |u_1 \wedge \cdots \wedge u_{j-1} \wedge u_j \wedge u_{j-1} \wedge \cdots \wedge u_k|/\det \Lambda \\ &= (\mathrm{Ind}\, K)^{(k-1)/k} \le (\mathrm{Ind}\, K)^{(d-1)/d} \end{aligned}$$

and (b) holds. Moreover, if $w \in \Psi \cap \Lambda$ then $-w \in \Psi \cap \Lambda$ and for one of these vectors (a) holds too. We note that (c) is obvious.

Now we show that one can construct such a vector $w \in \Psi \cap \Lambda$ in polynomial time. To do that, we reduce our problem to a problem of integer programming in dimension d.

Let us compute in polynomial time linearly independent rational vectors u_i^*: $i = 1, \ldots, d$ such that

$$\langle u_i, u_j^* \rangle = \begin{cases} \delta_{ij}, & \text{if } j \le k; \\ 0, & \text{otherwise.} \end{cases}$$

Let us compute a rational number L which approximates $(\mathrm{Ind}\, K)^{-1/k}$ with error less than $1/D$ where D is the least common denominator of the coordinates of vectors u_i^*, $i = 1, \ldots, d$. This can also be done in polynomial time. For $m = 1, \ldots, d$ let us consider the following problem of integer programming in fixed dimension d:

Find $w = (w_1, \ldots, w_d) \in \mathbb{Z}^d$

Such that: $-L \le \langle w, u_i^* \rangle \le L$ *for* $i = 1, \ldots, k$ *and* $\langle w, u_i^* \rangle = 0$ *for* $i = k+1, \ldots, d$;

and $w_m \ge 1$.

For some m the program has a solution which gives us a nonzero vector $w \in \Psi \cap \mathbb{Z}^d$. Since d is fixed, this solution can be found in polynomial time (see Lenstra 1983 and §5.4 of Grötschel et al 1988 for more recent developments of integer programming). Now we can check in polynomial time which vector w or $-w$ satisfies the condition (a). □

(5.3) LEMMA. *Let us fix $d \in \mathbb{N}$. Then there exists a polynomial algorithm which for any given simple rational cone $K \subset \mathbb{R}^d$ constructs not more than 2^d simple rational cones $K_i \subset \mathbb{R}^d$: $i \in I$ and computes integral number $\epsilon_i \in \{-1, 1\}$: $i \in I$ such that*

(a) $\operatorname{Ind} K_i \leq (\operatorname{Ind} K)^{(d-1)/d}$ *for all* $i \in I$;

(b)

$$K = \sum_{i \in I} \epsilon_i \cdot K_i \quad \text{and} \quad \sigma(K; c) = \sum_{i \in I} \epsilon_i \cdot \sigma(K_i; c);$$

(c) *size* $K_i \leq$ *size* $K + O(d^2)$.

PROOF. Let us denote by $u_1, \ldots, u_k$ the given generators of K. Then we construct the vector w as in Lemma 5.2.

Let us put $J = \{j \in \{1, \ldots, k\}$: the vectors $u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots, u_k$ are linearly independent$\}$. For each $j \in J$ let us put

$$K_j = \operatorname{co}\{u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots, u_k\}.$$

By Lemma 5.2, $\operatorname{Ind} K_j \leq (\operatorname{Ind} K)^{d-1/d}$.

We are going to represent the cone K as a linear combination of faces K_i of the cones K_j. To do that we follow Lemma 2 from Dyer (1991).

Let us put $J_- = \{j \in J$: the bases $(u_1, \ldots, u_{j-1}, w, u_{j+1}, \ldots, u_k)$ and $(u_1, \ldots, u_{j-1}, u_j, u_{j+1}, \ldots, u_k)$ have the same orientation$\}$ and $J_+ = J \setminus J_-$. Since the cones $\{K_j$: $j \in J_-\}$ constitute a triangulation of the cone $C = \operatorname{co}\{u_1, \ldots, u_k, w\}$, using inclusion-exclusion formula we get a decomposition

$$C = \sum_{i \in I_1} \epsilon_i \cdot K_i, \tag{5.3.1}$$

where K_i: $i \in I_1$ is a common face of some cones K_j: $j \in J_-$ and $\epsilon_i \in \{-1, 1\}$. Thus the number of terms in the decomposition (5.3.1) does not exceed 2^p, where $p \leq d$ is the cardinality of J_-. Since d is fixed, decomposition (5.3.1) can be computed in polynomial time. For each $j \in J_-$ the intersection $\Gamma_j = K_j \cap K$ is the common facet of K_j and K. Let us put $\tilde{K}_j = K_j \setminus \Gamma_j$. Since the cones $\{\tilde{K}_j$: $j \in J_-\}$ constitute a triangulation of $C \setminus K$, using inclusion-exclusion formula we can compute in polynomial time a decomposition

$$C \setminus K = \sum_{i \in I_2} \delta_i \cdot \tilde{K}_i, \tag{5.3.2}$$

where $\tilde{K}_i$ is a common face of some cones $\tilde{K}_j$: $j \in J_-$ and $\delta_i \in \{-1, 1\}$. Thus the number of terms in the decomposition (5.3.2) does not exceed 2^m, where $m < d - 1$ is the cardinality of the set J_-. Now we observe that each cone $\tilde{K}_i$ can be represented as a difference of two faces of some K_j:

$$\tilde{K}_i = K_i - K_i \cap \Gamma_j, \tag{5.3.3}$$

where K_i is a face of K_j for some $j \in J_-$. Combining (5.3.1), (5.3.2) and (5.3.3) we get the first decomposition in (b), where each cone K_i is a face of a certain cone K_j: $j \in J$ (we allow repetitions of cones).

We note that there exists an open subset $W \subset \mathbb{R}^d$ such that for all $c \in W$ the series defining the functions $\sigma(K; c), \sigma(K_i; c)$ converge. Therefore, the second identity in

(b) also holds. Since the index of a face does not exceed the index of the cone, we get

$$\text{Ind } K_i \le \text{Ind } K_j \le (\text{Ind } K)^{(d-1)/d}. \quad \square$$

Finally, (c) follows by the inequality (c) of Lemma 5.2.

Now we can prove the main theorem of this section.

(5.4) THEOREM. *Let us fix $d \in \mathbb{N}$. Then there exists a polynomial algorithm which for any given simple rational cone K constructs a family $K_i \subset \mathbb{R}^d$: $i \in I$ of rational primitive cones and computes integral numbers ϵ_i: $i \in I$ such that*

$$K = \sum_{i \in I} \epsilon_i \cdot K_i \quad \text{and} \quad \sigma(K; c) = \sum_{i \in I} \epsilon_i \cdot \sigma(K_i; c)$$

for all $c \in \mathbb{P}^d$ which are regular points for the functions $\sigma(K; c), \sigma(K_i; c)$: $i \in I$.

PROOF. Let us choose the smallest integral T such that

$$T \ge \frac{-\text{loglog } 1.9 + \text{loglog}(\text{Ind } K)}{\log d - \log(d-1)}.$$

We apply the algorithm from Lemma 5.3 inductively, first to the cone K, then to the cones K_i and so on, altogether T iterations. Finally we get not more than $(2^d)^T$ cones K_i such that Ind $K_i \le 1.9$. Since Ind K_i is always an integer, we get that Ind $K_i = 1$. We apply the algorithm from Lemma 5.3 not more than $(2^d)^T$ times. By Lemma 5.3 it follows now that the complexity of the resulting algorithm is polynomial in the input size and linear in $(2^d)^T$. Now we see that the last number is bounded by a polynomial in the input size. Indeed, let us denote

$$C_1(d) = \exp\left\{\left(\frac{-\text{loglog } 1.9}{\log d - \log(d-1)} + 1\right) \cdot \log(2^d)\right\};$$

$$C_2(d) = \frac{\log(2^d)}{\log d - \log(d-1)}.$$

Thus C_1 and C_2 are constants for a fixed d. Then

$$(2^d)^T \le C_1(d) \cdot (\log(\text{Ind } K))^{C_2(d)}.$$

Since the value $\log(\text{Ind } K)$ is bounded by a polynomial in the input size, the last value (for a fixed d) is bounded by a polynomial as well. $\square$

6. The Algorithm. In this section we describe our algorithm for Problem 1.1. First, we need a simple result which states that a "generic" vector can be constructed in polynomial time.

(6.1) LEMMA. *There exists a polynomial time algorithm which for any given $d \in \mathbb{N}$, for any given $m \in \mathbb{N}$, and for any rational vectors $u_1, \dots, u_m \in \mathbb{Q}^d$ constructs a rational vector $c \in \mathbb{Q}^d$ such that $\langle c, u_i \rangle \ne 0$ for $i = 1, \dots, m$.*

PROOF. We look for a vector c of the form

$$c(t) = (1, t, \dots, t^{d-1}): t \in \mathbb{Q}.$$

Thus $p_i(t) = \langle c(t), u_i \rangle$: $i = 1, \ldots, m$ is a family of nonzero polynomials of degree $d - 1$. Therefore for some $t \in \{0, 1, \ldots, m \cdot (d-1)\}$ the vector $c(t)$ satisfies our condition. □

PROOF OF THEOREM 1.2. Our algorithm is the following. For each vertex v of the simplex Δ let us compute integral generators $u_1(v), \ldots, u_k(v)$ of the supporting cone K_v of Δ at v. This can be done in polynomial time. Using theorem 5.4 let us represent each cone K_v as a linear combination of primitive cones K_i:

$$K_v = \sum_{i \in I_v} \epsilon_i \cdot K_i.$$

Using Lemma 6.1 let us construct a vector c which is not orthogonal to any of the generators of the cones $K_i, i \in \bigcup_v I_v$. Finally, using Lemma 4.3 let us compute for all v and $i \in I_v$ the constant term $R(K_i, v, c)$ of the function

$$\exp\{\langle t \cdot c, v \rangle\} \cdot \sigma(K_i; t \cdot c)$$

as $t \to 0$. By Proposition 2.7 we conclude that

$$\#(\Delta \cap \mathbb{Z}^d) = \sum_{v \in \mathrm{Vert}} \sum_{\Delta i \in I_v} \epsilon_i \cdot R(K_i, v, c).$$

Thus we compute the sum in the right-hand side. □

7. Some remarks. Our approach allows one to design a polynomial time algorithm for the computation of the sums

$$\sum_{x \in \Delta \cap \mathbb{Z}^d} \phi(x),$$

where ϕ: $\mathbb{R}^d \to \mathbb{R}$ is a given polynomial. To do that, we should use a version of Brion's identity with a polynomial density (see Barvinok 1993).

The complexity of our algorithm for solving Problem 1.1 is $\mathscr{L}^{O(d^2)}$, where $\mathscr{L}$ is the size of the input. There is a modification of the algorithm which allows us to achieve $\mathscr{L}^{O(d)}$ complexity. Instead of Brion's identity (Brion 1988, 1992) we should use then Morelli's identities (Morelli 1993) which express the number of integral points in an integral polytope in terms of the volumes of faces and certain additive measures on the supporting cones at these faces. Our algorithm implies polynomial computability of the *Ehrhart polynomial*, that is, of the polynomial

$$\#(m \cdot \Delta) = \sum_{k=0}^{d} e_k(\Delta) \cdot m^k : m \in \mathbb{N}$$

(see, for example, Chapter 4 of Stanley 1986) of a given integral simplex Δ of the fixed dimension d. Morelli's identities, however, allow one to compute in polynomial time any fixed number of the highest coefficients of the Ehrhart polynomial of a given simplex even if the dimension varies. These results will be described elsewhere.

Acknowledgements. I am grateful to Martin Dyer and Günter Ziegler for drawing my attention to this problem. I am indebted to Anders Björner and Shmuel Onn for valuable conversations and remarks. A preliminary version of this paper appeared in the Proceedings of FOCS'93. The author was supported by KTH, Stockholm. The

Paper was written while the author was visiting Department of Mathematics of the Royal Institute of Technology, Stockholm, Sweden.

References

Barvinok, A. I. (1993). Computing the Volume, Counting Integral Points, and Exponential sums. *Discrete Comput. Geom.* **10** 1–13.

Brion, M. (1988). Points entiers dans Polyèdres Convexes. *Ann. Sci. École, Norm. Sup.* (4) **21** 653–663.

——— (1992). Polyédres et Réseaux. *L' Enseignement Mathématique* **38** 71–88.

Cook, W., Hartmann, M., Kannan, R., and McDiarmid, C. (1992). On Integer Points in Polyhedra. *Combinatorica* **12** 27–37.

Dyer, M. E. (1991). On Counting Lattice Points in Polyhedra, *SIAM J. Comput.* **20** 695–707.

Grötschel, M., Lovász, L., and Schrijver, A. (1988). *Geometric Algorithms and Combinatorial Optimization* Springer-Verlag, *Algorithms and Combinatorics*, **2**.

Khovanskii, A. G., and Puhlikov, A. V. (1992). The Riemann-Roch Theorem for Integrals and Sums of Quasipolynomials on Virtual Polytopes (Russian). *Algebra i analiz* **4** 188–216. Translated in *St.-Petersburg Mathematical Journal*, **4** 789–812.

Lenstra Jr., H. W. (1983) Integer Programming with a Fixed Number of Variables. *Math. Oper. Res.* **8** 538–548.

Morelli, R. (1993). Pick's Theorem and the Todd Class of a Toric Variety. *Adv. Math.* **100** 183–231.

Stanley, R. P. (1986). *Enumerative Combinatorics*, Vol. I. Wadsworth and Brooks/Cole. Monterey, CA.

A. I. Barvinok: Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109-1003; e-mail: barvinok@math.lsa.umich.edu