Vol. 22, No. 3, August 1997
Printed in U.S.A.

ON BARVINOK'S ALGORITHM FOR COUNTING LATTICE POINTS IN FIXED DIMENSION

MARTIN DYER AND RAVI KANNAN

We describe a simplification of a recent polynomial-time algorithm of A. I. Barvinok for counting the number of lattice points in a polyhedron in fixed dimension. In particular, we show that only very elementary properties of exponential sums are needed to develop a polynomial-time algorithm.

1. Introduction. Barvinok (1994) gives the first polynomial time algorithm for counting the number of lattice points in a convex polyhedron in any fixed dimension d. This is a significant achievement, improving dramatically on the previously known cases for $d \leq 4$ (see Dyer 1991). In fact, Barvinok's algorithm counts the number of lattice points in a simplex with integer vertices, since it is known (see, for example, Dyer 1991) that the general problem can be reduced to this case. To do this, the method employs *exponential sums*. For a given polyhedron $P \subseteq \mathbf{R}^d$ and vector $c \in \mathbf{R}^d$ this is an expression of the form

$$\sigma(P, c) = \sum_{x \in P \cap \mathbf{Z}^d} e^{-c.x}.$$

(Note that we have made a sign change from the notation of Barvinok 1994.) In particular, if K is a pointed polyhedral cone generated by the vectors u_i $(i = 1, \ldots, k)$, the exponential sum converges provided $c.u_i > 0$ for $i = 1, \ldots, k$. Barvinok's solution uses two deeper properties of these sums. The first property is that the sum (regarded as a function of $c \in \mathbf{C}^d$) can be continued to define a meromorphic function on $\mathbf{C}^d$. The second is an identity of Brion (1992) which relates the exponential sum over a polytope to the sums over the cones generated by the edges at each vertex. The analytic continuation is crucial here, since it is impossible to find a single c for which all the required sums converge. This introduces an element of symbolic computation, in order to avoid the complication caused by poles of the sums.

The remainder of Barvinok's procedure uses an inclusion-exclusion method to replace a sum over an arbitrary cone with a sum over a polynomial (in the size of the data) number of *primitive* cones. The sum over a primitive cone can be evaluated explicitly. We discuss this in more detail below.

The purpose of this note is to indicate that the nonelementary properties of exponential sums invoked in Barvinok's algorithm are unnecessary to obtain a polynomial time algorithm for this problem. We give an algorithm which uses only the reduction to primitive cones, replacing the symbolic computation with arithmetic computation. This results from the fact that, in our algorithm, we can compute a c for which all the sums involved converge. We should emphasize, however, that our method still relies heavily on Barvinok's ideas.

Received April 1, 1994; revised December 3, 1996.
AMS 1991 subject classification. Primary: 52B05.
OR/MS Index 1978 subject classification. Primary Mathematics/Polyhedra.
Key words. Lattice points, polytopes, counting problems, fixed dimension.

0364-765X/97/2203/0545/$05.00

2. Definitions and notation. The notation we use mainly follows Barvinok (1994), and the reader may seek further information there on some of what follows.

Throughout, $K \subseteq \mathbf{R}^d$ will be a cone pointed at the origin with linearly independent integral generators u_i $(i = 1, \ldots, k)$. Then u_{ij} will denote the jth component of u_i. Different cones will be indicated by superscripts. Note that if $C = K + v$ is a cone pointed at an integer point v, then $\sigma(C, c) = e^{-c \cdot v}\sigma(K, c)$.

A *primitive* cone K is a cone having a particular unique minimal set of generators such that $x \in \mathbf{Z}^d \cap K$ if and only if x can be expressed as a linear combination of these u_i with nonnegative *integer* weights. It follows that, if K is primitive,

$$\sigma(K, c) = \prod_{i=1}^{k} \frac{1}{1 - e^{-c \cdot u_i}}.$$

For given cone K, the *index* $\operatorname{ind} K$ of K can be defined in several equivalent ways (see Barvinok 1994). We will use a computationally useful characterization of $\operatorname{ind} K$, as follows. Let U be the $d \times k$ matrix $[u_1 u_2 \cdots u_k]$ formed by the generators of K. From the Hermite normal form construction (see Schrijver 1986), there exists a $d \times d$ unimodular matrix T such that

$$TU = \begin{pmatrix} R \\ 0 \end{pmatrix},$$

where R is a nonsingular upper triangular matrix. Then $\operatorname{ind} K = |\det R|$. These computations can be carried out in polynomial time (see Schrijver 1986). It follows easily that K is primitive if and only if $\operatorname{ind} K = 1$ and that, if K' is any face of K, $\operatorname{ind} K' \leq \operatorname{ind} K$. Following Barvinok (1994), for integers ϵ_m and polyhedra $P^m (m \in M)$, we will write

$$P = \sum_{m \in M} \epsilon_m P^m$$

to mean the corresponding identity on the characteristic functions of the polyhedra, where the addition and scalar multiplication of functions is pointwise. Let us call the right-hand side expression a *composition* of the polyhedra. Note that these do not correspond to the usual operations of addition and scalar multiplication of convex sets. In general, a composition of convex sets would not necessarily be a characteristic function, let alone that of a convex set. However, this will always be the case here.

3. The algorithm. We will first show that an integral simplex $S \subseteq \mathbf{R}^{d-1}$ with vertices $v_1, \ldots, v_d$ can be expressed as a composition of cones pointed at the vertices, such that all cones lie in the interior of some half-space. We will assume without loss that S is contained in the nonnegative orthant of $\mathbf{R}^{d-1}$. This can always be arranged with a suitable translation. We wish to determine N, the number of integer points in S. Note that, if $\gamma_1 = 1 + \max_{i,j} v_{ij}$, then $N < \gamma_1^d$.

While we could work directly in $\mathbf{R}^{d-1}$, it is easier for exposition to embed the proof in $\mathbf{R}^d$. (This is why we choose to start from a simplex in $\mathbf{R}^{d-1}$.) Thus we consider the cone $K^* \subseteq \mathbf{R}^d$ with generators $u_i^* = (1, v_i)$ $(i = 1, \ldots, d)$. Then, in an obvious notation, $(1, S) = K^* \cap H_1$, where $H_1 = \{x : x_1 = 1\}$.

Let us call $K \subseteq \mathbf{R}^d$ a *standard* cone if its generators satisfy $u_{11} = 1$ and $u_{i1} = 0$ $(i = 2, \ldots, k)$, and each of the vectors u_i is lexicographically positive. Note that, if K is a standard cone, and $(1, C) = K \cap H_1$ then C is a cone with vertex v where $(1, v) = u_1$.

LEMMA 1. *The cone K^* is a composition of standard cones K^m $(m \in M)$ with $|M| \leq 3^{d-1}$, $\epsilon_m = \pm 1$ and* ind $K^m \leq$ ind K $(m \in M)$. *Moreover, the required composition can be determined in polynomial time.*

PROOF. We will prove the lemma by induction on r, for a cone K with k generators satisfying $u_{i1} = 1$ $(i = 1, \ldots, r)$, $u_{i1} = 0$ $(i = r+1, \ldots, k)$ where $1 \leq r \leq k \leq d$. (We require the case $r = k = d$.) The basis for the induction is $r = 1$, when there is nothing to prove.

Assume the truth of the lemma for $(r-1)$ and suppose $r \geq 2$. We assume without loss that the generators of K are in lexicographically decreasing order. Let $w = u_1 - u_2$, so w is lexicographically positive and $w_1 = 0$. We now use the "inclusion-exclusion" method, as in Dyer (1991) and Barvinok (1994), to "insert" the vector w. Now $K' = K \cup K''$, where K' has generators $w, u_2, \ldots, u_k$ and K'' has generators $u_1, w, \ldots, u_k$. Let $K''' = K \cap K''$ be the $(k-1)$-dimensional cone with generators $u_1, u_3, \ldots, u_k$. Then clearly

$$K' = K + K'' - K''', \quad \text{i.e., } K = K' - K'' + K'''.$$

Thus K is a composition of three cones, each with only $(r-1)$ generators having nonzero first component. Note that ind K' = ind K'' = ind K, since they all generate the same lattice, and ind $K''' \leq$ ind K, since the generators of K''' are a subset of those of K. Applying the inductive hypothesis gives the lemma. The proof clearly indicates a polynomial time algorithm. □

We remark that this type of decomposition is well known. For example, it is the starting point in Varchenko (1987) and it is mentioned there as a "folklore result." It also leads to an elementary proof of the Brion's identity in the spirit of Khovanskii and Puhlikov (1992). Now, we follow Barvinok's method to express each of the cones K^m from Lemma 1 as a composition of primitive cones. This is done in the following way. For a given cone K with ind $K > 1$, determine the matrix R as in §2 using a Hermite normal form algorithm. Compute the shortest nonzero vector λ, in l_∞ norm, in the lattice generated by the columns of R^{-1}. This can be done in polynomial time, in fixed dimension, using the basis reduction algorithm (see Schrijver 1986) followed by enumeration. By Minkowski's theorem (see, e.g., Schrijver 1986, p. 71),

$$\|\lambda\|_\infty \leq |\det R^{-1}|^{1/k} = |\det R|^{-1/k} = (\text{ind } K)^{-1/k}.$$

Now $\lambda = R^{-1}z$, for some integral z so $z = R\lambda$ and hence

$$w = T^{-1}\begin{pmatrix} z \\ 0 \end{pmatrix} = T^{-1}\begin{pmatrix} R \\ 0 \end{pmatrix}\lambda = U\lambda,$$

is a nonzero integer vector which is a linear combination of the generators of K with weights at most $(\text{ind } K)^{-1/k}$ in absolute value. We may clearly insist that w is lexicographically positive. We now, using inclusion-exclusion, can express K as a composition of faces of the cones K^i with generators $u_1, \ldots, u_{i-1}, w, u_{i+1}, \ldots, u_k$. See Barvinok (1994) for details. There are at most $k2^k$ cones of this form. Suppose U_i is the matrix of generators of K^i. Note that $w = U\lambda$. Let Λ_i be the matrix which is a $k \times k$ identity, except that the ith column is λ. Then $U_i = U\Lambda_i$. Let T_i, T be the unimodular matrices which reduce U_i, U, respectively, to Hermite normal form, then

$$\begin{pmatrix} R_i \\ 0 \end{pmatrix} = T_i U_i = T_i U \Lambda_i = T_i T^{-1}\begin{pmatrix} R\Lambda_i \\ 0 \end{pmatrix},$$

from which it follows that $|\det R_i| = |\det(R\Lambda_i)|$. Hence

$$\operatorname{ind} K^i = \lambda_i \operatorname{ind} K \leq (\operatorname{ind} K)^{-1/k} \operatorname{ind} K = (\operatorname{ind} K)^{(k-1)/k}.$$

From this it follows that iterating this $O(\log\log \operatorname{ind} K)$ times we obtain cones with $\operatorname{ind} K = 1$, i.e., primitive cones. The total number of cones generated is then only polynomial in $\log \operatorname{ind} K$, for fixed k.

At the end of this process, we have expressed the simplex S as a composition of a polynomial number of primitive cones, such that all cones have vertex in the nonnegative orthant and all cone generators are lexicographically positive. We now show that there is a polynomial-sized $c > 0$ such that $c.u_i > 0$ for all generators of all cones.

LEMMA 2. *Let $u_r \in \mathbf{R}^d$ $(r = 1, 2, \ldots)$ be any collection of lexicographically positive integer vectors such that $\gamma_2 = 1 + \max_{r,j}|u_{r,j}|$ is bounded. Then the vector $c_0 = (\gamma_2^{d-1}, \gamma_2^{d-2}, \ldots, \gamma_2, 1)$ satisfies $c_0.u_r \geq 1$ $(\forall r)$.*

PROOF. Suppose $u_{r,s} \geq 1$ is the first nonzero element of u_r. Then

$$c_0.u_r \geq \gamma_2^{d-s} - \sum_{j=0}^{d-s-1} (\gamma_2 - 1).\gamma_2^j = 1. \quad \square$$

Thus there exists a c_0 such that for any $c = \delta c_0 (0 < \delta \leq 1)$, $\sigma(S, c)$ can be expressed as a sum of τ terms of the form

$$\pm \frac{e^{-c.v}}{\prod_{i=1}^{d}(1 - e^{-c.u_i})}, \tag{1}$$

where $c.v > 0$ and $c.u_i > 0$ for $i = 1, \ldots, d$ and τ is bounded by a polynomial in the size of the description of S. We now show that we find a suitable δ such that $\sigma(S, c)$ approximates N closely enough. Let $\gamma = \max\{\gamma_1, \gamma_2\}$.

LEMMA 3. *Let $\delta = \min\{1/(4d\gamma^{2d}), 1/(8\tau)\}$ and $c = \delta c_0$, then*

$$\sigma(S, c) \leq N < \sigma(S, c) + \tfrac{1}{4}.$$

PROOF. For any $x \in S$ we have

$$c.x \leq \delta\left(d\gamma_2^{d-1}\right)\gamma_1 < \tfrac{1}{4}\gamma^{-d}.$$

Hence $1 - \frac{1}{4}\gamma^{-d} < 1 - c.x \leq e^{-c.x} \leq 1$, and thus

$$N - \tfrac{1}{4} < \sum_{x \in S} e^{-c.x} \leq N,$$

since $N < \gamma^d$. $\square$

Clearly the c determined in Lemma 3 is a rational vector of polynomial size in the data. We now determine an approximation $\hat{\sigma}(S, c)$ to $\sigma(S, c)$ such that $|\hat{\sigma}(S, c) - \sigma(S, c)| \leq \frac{1}{4}$. Then

$$\hat{\sigma}(S, c) - \tfrac{1}{4} \leq N < \hat{\sigma}(S, c) + \tfrac{1}{2},$$

and thus N is $\hat{\sigma}(S, c)$ rounded to the nearest integer. Thus it suffices to determine each term (1) to within $1/(4\tau)$.

Let $c.v = \alpha$, $c.u_i = \beta_i$. Then $\alpha \le \frac{1}{4}$, and since

$$1 \le c_0.u_i \le \sum_{j=0}^{d-1} (\gamma_2 - 1)\gamma_2^j < \gamma_2^d,$$

and $\delta < \frac{1}{4}$, we have

$$\delta \le \beta_i \le \delta\gamma_2^d < \delta(4\,d\delta)^{-1} \le \tfrac{1}{2}\sqrt{\delta} < \tfrac{1}{4}.$$

Now let $a(y)$ be the approximation to e^{-y} using the first $(2d + 3)$ terms of its series expansion. This series is alternating and we have $0 \le \alpha \le \delta$, $\delta \le \beta_i \le \frac{1}{2}\sqrt{\delta}$. It follows that $a(\alpha)$ approximates $e^{-\alpha}$, and $(1 - a(\beta_i))$ approximates $(1 - e^{-\beta_i})$ with relative error less than $\frac{1}{2}\delta^{d+1}/(2d + 3)!$. Thus using the approximation $a(y)$ in (1) leads to an approximation with relative error less than $(d + 1)\delta^{d+1}/(2d + 3)!$. Now the term (1) is at most $(2/\delta)^d$. Hence the absolute error due to approximating (1) in this manner will be at most $2^d\delta/(2d + 3)! < \delta \le 1/(8\tau)$. Thus it suffices to replace each exponential by the fixed polynomial $a(x)$ of degree $2(d + 1)$. It now follows that we can compute the required $\hat{\sigma}(S, c)$ in polynomial time.

Acknowledgments. We are grateful to Alexander Barvinok for helpful comments. The work of Martin Dyer was supported in part by Esprit Working Group RAND.

References

Barvinok, A. I. (1994). A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Math. Oper. Res.* **19** 769–779.

Brion, M. (1992). Polyèdres et réseaux. *L'enseignement Mathématique* **38** 71–78.

Dyer, M. E. (1991). On counting lattice points in polyhedra. *SIAM J. Computing* **20** 695–707.

Khovanskii, A. G., A. V. Puhlikov (1992). A Riemann-Roch theorem for integrals and sums of quasipolynomials on virtual polytopes (Russian). *Algebra i analiz*, **4** 188–216. Translated in *St. Petersburg Math. J.* **4** 789–812.

Schrijver, A. (1986). *Theory of Linear and Integer Programming*, John Wiley, Chichester.

Varchenko, A. N. (1987), Combinatorics and topology of the disposition of affine hyperplanes in real space (Russian). *Funktsional. Anal. i Prilozhen.* **21** N 1, 11–22. Translated in *Funct. Anal. Appl.* **21** 9–19.

M. E. Dyer: School of Computer Studies, University of Leeds, Leeds LS2 9JT, United Kingdom; e-mail: dyer@scs.leeds.ac.uk

R. Kannan: Department of Computer Science, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213-3890; e-mail: ravindran.kannan@theory.cs.cmu.edu