On Barvinok's Algorithm for Counting Lattice Points in Fixed Dimension

Martin Dyer*
School of Computer Studies
University of Leeds, Leeds, UK

Ravi Kannan
School of Computer Science
Carnegie-Mellon University and
Department of Computer Science
Yale University, New Haven CT, USA

16 October, 1993

Abstract

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.

*Supported in part by Esprit Working Group RAND.

1 Introduction

In [1], Barvinok 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 $d \leq 4$ [3]. In fact, Barvinok's algorithm counts the number of lattice points in a simplex with integer vertices, since it is known [3] that the general problem can be reduced to this case. To do this, Barvinok 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

"the method" changed to Barvinok

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

(Note that we have made a sign change from the notation of [1].) 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 a define a meromorphic function on $\mathbf{C}^d$. The second is an identity of Brion [2] 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, 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 two non-elementary 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.

next sentence deleted. We have already stressed this

2 Definitions and Notation

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 $\sigma(C, c) = e^{-c.v}\sigma(K, c)$.

For given cone K, the *index* $\operatorname{ind} K$ of K can be defined in several equivalent ways (see [1]). We will use a computationally useful characterizarion 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 consruction [4], 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 [4].

If $\operatorname{ind} K = 1$, then we say that K is *primitive*.

It is easily seen that a cone is primitive iff it has a 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, then $\sigma(K, c)$ can be computed by the following simple formula :

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

Another simple fact we need is that if K' is any face of K, $\operatorname{ind} K' \leq \operatorname{ind} K$.

Following [1], if S is a subset of $\mathbf{R}^d$, we use S also to denote the charecteristic function of S (which is 1 on S and 0 outside). If P^m are polyhedra and ϵ_m are integers (positive, negative or zero), we call the function

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

Last senetence deleted. We do not want to sound like the reader must first read [1]

next couple of paragraphs swapped and some more rearrangement done

several modifications for readability in this para

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, of any set, let alone that of a convex set. However, this will always be the case here.

3 The algorithm

It suffices to count the number of lattice points in a simplex with integer vertices. Let S be a simplex in $\mathbf{R}^{d-1}$ with integer vertices $v_1, \ldots, v_d$. We embed S into a cone K^* in $\mathbf{R}^d$ in a natural fashion, namely, let $K^* \subseteq \mathbf{R}^d$ be the cone with generators $u_i^* = (1, v_i)$ $(i = 1, \ldots, d)$. Then, in an obvious notation, $(1, S) = K^* \cap H_1$, where $H_1 = \{x : x_1 = 1\}$.

For any positive integer t, let

$$p(t) = |K^* \cap \mathbf{Z}^d \cap \{x : x_1 = t\}|.$$

Then clearly, $p(1) = |S \cap \mathbf{Z}^{d-1}|$. Also, it is well-known that $p(t)$ is a polynomial of degree $d-1$ [???], so we may write

$$p(t) = \sum_{i=0}^{d-1} p_i t^i.$$

If now c_1 is any strictly positive real number, then it is easy to see that

$$\sum_{x \in K^* \cap \mathbf{Z}^d} e^{-c_1 x_1} = 1 + \sum_{t=1}^{\infty} p(t) e^{-c_1 t}$$

converges. Furthermore, the above sum is

$$1 + \sum_{i=0}^{d-1} p_i \sum_t t^i e^{-c_1 t}.$$

The inner sum can be evaluated in closed form. So if we find $\sum_{x \in K^* \cap \mathbf{Z}^d} e^{-c_1 x_1}$ for d different positive values of c_1, then we can find all the p_i by solving the

resulting equations (which are lineraly independent as a tedious, but standard proof shows.)

Let us call $K \subseteq \mathbf{R}^d$ a *standard* cone if its generators $u_1, u_2, \ldots u_k$ satisfy $u_{11} = 1$ and $u_{i1} = 0$ $(i = 2, \ldots, k)$, and each of the vectors u_i is lexicographically positive (i.e., for the least j such that $u_{ij} \neq 0$, we have $u_{ij} > 0$.) 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 $\operatorname{ind} K^m \leq \operatorname{ind} K$ $(m \in M)$. 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 [3, 1], 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

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

Thus K is a composition of three cones, each with only $(r-1)$ generators having nonzero first component. Note that $\operatorname{ind} K' = \operatorname{ind} K'' = \operatorname{ind} K$, since they all generate the same lattice, and $\operatorname{ind} K''' \leq \operatorname{ind} K$, 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. $\square$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 $\operatorname{ind} K > 1$, determine the matrix R as in section 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 [4] followed by enumeration. By Minkowski's theorem (see e.g. [4, p 71]),

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

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 $(\mathrm{ind}\, K)^{-1/k}$ in absolute value. We may clearly insist that w is lexicographically positive. We now, using inclusion-exclusion, we 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 [1] 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

$$\begin{pmatrix} R_i \\ 0 \end{pmatrix} = T_iU_i = T_iU\Lambda_i = T_iT^{-1}\begin{pmatrix} R\Lambda_i \\ 0 \end{pmatrix},$$

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

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

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

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

. □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

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

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 $N < \gamma^d$. □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 $\alpha \leq \frac{1}{4}$, and since

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

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

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

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 $0 \leq \alpha \leq \delta$, $\delta \leq \beta_i \leq \frac{1}{2}\sqrt{\delta}$. 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 will be at most $2^d\delta/(2d+3)! < \delta \leq 1/(8\tau)$. 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.

References

[1] A. I. Barvinok, A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed, to appear in FOCS'93.

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

[3] M. E. Dyer, On counting lattice points in polyhedra, *SIAM Journal on Computing* **20** (1991), 695–707.

[4] A. Schrijver, *Theory of linear and integer programming,* John Wiley, Chichester, 1986.