COUNTING LATTICE POINTS IN POLYHEDRA

ANDREW CRITES, MICHAEL GOFF, MATT KORSON, LEE PATROLIA, LUKE WOLCOTT

Abstract. We present Barvinok's 1994 and 1999 algorithms for counting lattice points in polyhedra.

1. The 1994 algorithm

In [2], Barvinok presents an algorithm that, for a fixed dimension d, calculates the number of integer points in a rational polyhedron. It is shown in [6] and [7] that the question can be reduced to counting the number of integer points in a k-dimensional simplex with integer vertices $v_1, \dots, v_{k+1}$ in $\mathbb{Z}^d$. We discuss an algorithm for solving the latter problem, also for a fixed d.

Problem 1.1. *Consider a simplex P in $\mathbb{Z}^d$ with integer vertices $v_1, \dots, v_{k+1}$ in $\mathbb{Z}^d$. Determine how many integer points lie in P.*

An important tool in the algorithm is the exponential sum. Let $\{c, x\}$ be the standard inner product on $c = (c_1, \dots, c_d)$ and $x = (x_1, \dots, x_d)$. The formal sum $\sum_{P \cap \mathbb{Z}^d} \exp\{\langle c, x\rangle\}$ is attained by substituting $a_i = \exp(c_i)$ into the Laurent series $\sum_{x \in P \cap \mathbb{Z}^d} a^x$.

Definition 1.2. *Let $P \subset \mathbb{R}^d$ be a polyhedron and v be a vertex of P. Suppose that $P = \{\mathbf{x} \in \mathbb{R}^d : A\mathbf{x} \leq \mathbf{b}\}$ and $A'\mathbf{x} = \mathbf{b}'$ is the subsystem held at equality at v. Then the supporting or tangent cone* $\operatorname{cone}(P, v)$ *of P at v is defined by*

$$\operatorname{cone}(P, v) := \{\mathbf{x} \in \mathbb{R}^d : A'\mathbf{x} \leq \mathbf{b}'\}.$$

The algorithm uses the following theorem of Brion ([4], [5]).

Theorem 1.3. *Let P be an integral polytope. Then*

$$\sum_{x \in P \cap \mathbb{Z}^d} \exp\{\langle c, x\rangle\} = \sum_{v \in \mathrm{Vert}\,(P)} \left(\exp\{\langle c, v\rangle\} \sum_{x \in \operatorname{cone}(P,v) \cap \mathbb{Z}^d} \exp\{\langle c, x\rangle\} \right)$$

Substituting $c = 0$ seems to give the number of integer points in P, but $c = 0$ is a singular point on the right hand side. Instead, the algorithm calculates the constant term of the Taylor series about $t = 0$ of the functions

$$\exp\{t\langle c, v\rangle\} \sum_{x \in \operatorname{cone}(P,v) \cap \mathbb{Z}^d} \exp\{t\langle c, x\rangle\}. \tag{1}$$

Define $\operatorname{Lin} K$ to be the linear span of a cone K. We define a cone to be *simple* if it can be generated by linearly independent vectors. A simple rational cone is *unimodular* with *primitive generators* $\{u_1, \dots, u_k\}$ if $u_1, \dots, u_k$ is a basis of the lattice

Date: April 5, 2008.

$\mathbb{Z}^d \cap \operatorname{Lin} K$. There is an explicit formula for (1) when $\operatorname{cone}(P, v)$ is a unimodular cone. The following is proven in [2].

Theorem 1.4. *If the dimension d is fixed, then given a rational polyhedral cone $K \subset \mathbb{R}^d$, there exists a polynomial time algorithm that computes unimodular cones K_i and numbers $\epsilon_i \in \{-1, 1\}$ such that*

$$[K] = \sum_{i \in I} \epsilon_i [K_i].$$

Proof: (Sketch) First, we may assume that K is the conic hull $K = \operatorname{co}\{u_1, ..., u_d\}$ for some linearly independent integer vectors $u_1, ..., u_d$ in $\mathbb{Z}^d$. The reduction to this assumption can be made using triangulation on the cone, however, in practice, to insure polynomial time, we must use signed decompositions.

Let $\operatorname{ind}(K)$ denote the volume of the parallelepiped spanned by $u_1, ...u_d$. Now, our goal is to rewrite $[K]$ as a linear combination of indicator functions $[K_i]$ such that the K_i are rational cones with $\operatorname{ind}(K_i) \leq \operatorname{ind}(\mathrm{K})$ for all i. We repeat the process until we have a decomposition of K into unimodular cones, each with index no larger than that of K.

To begin, consider the parallelepiped given by

$$P = \{a_1 u_1 + ... + a_d u_d : |a_j| \leq (\operatorname{ind}(K))^{-1/d} \, for \, j = 1, ..., d\}$$

The Minkowski convex body theorem implies that there is a nonzero integer point $z \in P$ [8]. Then for each j, define a cone

$$K_j = \operatorname{co}\{u_1, ..., u_{j-1}, z, u_{j+1}, ..., u_d\}.$$

Each integer point in P can be written as a linear combination of the u_i, thus we have $z = a_1 u_1 + ... + a_d u_d$ for some a_i. This yields the inequality

$$\operatorname{ind}(K_j) = |a_j| \operatorname{ind}(K) \leq (\operatorname{ind}(K))^{(d-1)/d}$$

and the decomposition

$$[K] = \sum_{j \in J} \epsilon_j [K_j] + \sum_F \epsilon_F [F]$$

where the second sum is taken over lower dimensional faces of K_j and $\epsilon_j, \epsilon_F \in \{-1, 1\}$ for all j and F. To complete the decomposition, we iterate this procedure and observe that the resulting number of cones is bounded by a polynomial in $\log(\operatorname{ind}(K))$. □

2. The 1999 algorithm

The algebra of polyhedra $\mathcal{P}(\mathbb{R}^d)$ is the vector space (over $\mathbb{Q}$) spanned by the indicator functions $[P]$ of all polyhedra $P \subset \mathbb{R}^d$. This is closed under pointwise multiplication of functions (since $P \cap Q$ is a polyhedron for any polyhedra P and Q.) Thus $\mathcal{P}(\mathbb{R}^d)$ is a commutative algebra. We may also consider the subalgebras $\mathcal{P}_c(\mathbb{R}^d)$ spanned by indicator functions of polytopes and $\mathcal{P}_K(\mathbb{R}^d)$ spanned by the indicator functions of finitely generated cones. We call $\mathcal{P}_c(\mathbb{R}^d)$ the algebra of polytopes and $\mathcal{P}_K(\mathbb{R}^d)$ the algebra of cones. A final important subalgebra is $\mathcal{P}(\mathbb{Q}^d)$ spanned by indicator functions of of rational polyhedra.

Definition 2.1. *A linear transformation*

$$\Phi\colon \mathcal{P}(\mathbb{R}^d) \to V$$

is called a valuation. A linear map defined on any of the subalgebras above is also called a valuation.

Valuations are important because they satisfy the inclusion-exclusion principle:

$$\Phi([P \cup Q]) + \Phi([P \cap Q]) = \Phi([P]) + \Phi([Q]).$$

We now wish to move the problem of counting integer points in polyhedra into a question involving the algebra of polyhedra. Following [3], we have Theorem 2.2 which states that assigning to each polyhedron the generating function of its integer points give a valuation on $\mathcal{P}(\mathbb{Q}^d)$.

Theorem 2.2. *There is a valuation $\mathfrak{F}\colon \mathcal{P}(\mathbb{Q}^d) \to \mathbb{Q}(\mathbf{x})$ which associates to each rational polyhedron $P \subset \mathbb{R}^d$ a rational function $\mathfrak{F}([P]) = f(P;\mathbf{x})$ with the following properties:*

(1) *For any $m \in \mathbb{Z}^d$, $f(m+P;\mathbf{x}) = \mathbf{x}^m f(P,\mathbf{x})$.*

(2)
$$f(P;\mathbf{x}) = \sum_{m \in P \cap \mathbb{Z}^d} \mathbf{x}^m$$
for all $\mathbf{x} \in \mathbb{C}^d$ such that this series converges absolutely.

(3) *If P contains a straight line, $f(P,\mathbf{x}) = 0$.*

We may compute this in the case of a simple cone. For $k \le d$, choose k linearly independent integer vectors $v_1, \dots, v_k$. Let K be the cone generated by these:

$$K = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : \lambda_i \ge 0\}.$$

Let Z be the half-open parallelepiped spanned by $v_1, \dots, v_k$:

$$Z = \{\lambda_1 v_1 + \cdots + \lambda_k v_k : 0 \le \lambda_i < 1\}.$$

It is well-known that each integer point $m \in K \cap \mathbb{Z}^d$ has a unique expression of the form

$$m = n + a_1 v_1 + \cdots + a_k v_k$$

where $n \in Z \cap \mathbb{Z}^d$ and $a_1, \dots, a_k \in \mathbb{Z}_{\ge 0}$. Define $U_K \subset \mathbb{C}^d$ by

$$U_K = \{\mathbf{x} \in \mathbb{C}^d : |\mathbf{x}^{v_i}| < 1, i = 1, \dots, k\}.$$

Then U_K is a nonempty open set and

$$\sum_{m \in K \cap \mathbb{Z}^d} \mathbf{x}^m = \left(\sum_{n \in Z \cap \mathbb{Z}^d} \mathbf{x}^n \right) \prod_{i=1}^k \frac{1}{1 - \mathbf{x}^{v_i}}$$

converges absolutely for $\mathbf{x} \in U_K$. Then by (2), we have

$$f(K;\mathbf{x}) = \left(\sum_{n \in Z \cap \mathbb{Z}^d} \mathbf{x}^n \right) \prod_{i=1}^k \frac{1}{1 - \mathbf{x}^{v_i}}.$$

A particularly nice case of this is when $Z \cap \mathbb{Z}^d = \{\mathbf{0}\}$. This occurs when $v_1, \dots, v_k$ is a Hilbert basis for K, and we call K a unimodular cone. Then we have

$$f(K;\mathbf{x}) = \prod_{i=1}^k \frac{1}{1 - \mathbf{x}^{v_i}}.$$

Proof of Theorem 2.2: (Sketch) The above shows that the theorem holds for a simple cone K. If P is any pointed cone, it may be triangulated in to finitely many simple cones K_i. Then using the principle of inclusion-exclusion, $f(P;\mathbf{x})$ is a linear combination of $f(K_i;\mathbf{x})$, and the generating function converges on some open set containing $\mathbf{0}$.

To extend this to rational polyhedra P containing no straight lines, embed P in $\mathbb{R}^{d+1}$ by $x \mapsto (x,1)$, and let K be the cone spanned by P. Then K is a pointed rational cone, so $f(K;\mathbf{x},t)$ is a rational function. Then we have

$$f(P;\mathbf{x}) = \left.\frac{\partial f(K;\mathbf{x},t)}{\partial t}\right|_{t=0}.$$

This defines $\mathfrak{F}$ on $[P]$ where P is a polyhedron containing no straight lines such that (1) and (2) are satisfied. Linearity is also satisfied for any $P_1,\dots,P_k$ such that all the series defining $f(P_i;\mathbf{x})$ converge absolutely on a common set.

Now suppose P is any rational polyhedron. Write P as the union $P_1 \cup \cdots \cup P_k$ for polyhedra P_i containing no straight lines. For $I \subset \{1,\dots,k\}$, let $P_I = \bigcup_{i\in I} P_i$. Then by inclusion-exclusion, $[P]$ is a linear combination of the $[P_I]$ and each P_I contains no straight lines. Thus we may define $f(P;\mathbf{x})$ by linearity. We need only check that $f(P;\mathbf{x})$ is well-defined when P contains no straight lines. This will be true because there is a nonempty open set where all the series defining $f(P;\mathbf{x})$ and $f(P_I;\mathbf{x})$ converge absolutely. So we have defined the linear map $\mathfrak{F}$ which satisfies (1) and (2). Then (3) follows because if P contains a line, then there is an m such that $P+m=P$, so $f(P;\mathbf{x}) = \mathbf{x}^m f(P;\mathbf{x})$, so $f(P;\mathbf{x}) = 0$. □

Theorem 2.3. *Let P be a rational polyhedron. Then*

$$f(P;\mathbf{x}) = \sum_v f(\operatorname{cone}(P,v);\mathbf{x})$$

where the sum is taken over all vertices v of P.

This was originally proved by Brion [4] using algebraic geometry before Theorem 2.2 had a proof. Later elementary proofs were given by Lawrence [9], Pukhlikov and Khovanskii [10], and Barvinok [1]. Here, we follow the exposition in [3].

Proof: (Sketch) Let $\mathcal{L}$ be the subspace spanned by indicator functions of polyhedra containing straight lines. By (3) of Theorem 2.2, $\mathcal{L}$ is contained in the kernel of $\mathfrak{F}$, so we may work modulo this subspace. It will suffice to show that

$$[P] \equiv \sum_v [\operatorname{cone}(P,v)] \pmod{\mathcal{L}}.$$

We may decompose P as $P = Q+K+L$, where Q is a polytope, K is a pointed cone, and L is a subspace of $\mathbb{R}^d$. If $L \neq \{0\}$, then $f(P;\mathbf{x}) = 0$ and P has no vertices, so the theorem holds. Now it will suffice to prove the theorem for polytopes, because if

$$[Q] \equiv \sum_v [\operatorname{cone}(Q,v)] \pmod{\mathcal{L}},$$

then

$$[P] = [Q+K] \equiv \sum_v [\operatorname{cone}(Q,v)+K] \pmod{\mathcal{L}}.$$

Every vertex v of P is a vertex of Q, and $\operatorname{cone}(P,v) = \operatorname{cone}(Q,v)+K$. A vertex v of Q is a vertex of P if and only if $\operatorname{cone}(Q,v)+K$ contains no straight lines. So $[P]$ has the desired form.

To prove this for polytopes, first assume $Q = \Delta$ is a full-dimensional simplex. Then Δ is the intersection of $d+1$ half-spaces such that the intersection of any d of these half-spaces is the tangent cone at a vertex of Δ. Further, the intersection of fewer than d half-spaces contains a line, so by inclusion-exclusion

$$[\Delta] \equiv \sum_v [\text{cone}(\Delta, v)] \pmod{\mathcal{L}}.$$

We extend this to all polytopes by taking triangulations. □

Let $P \subset \mathbb{R}^n$ be a rational polyhedron. We have observed that the number of integer points in P can be computed by evaluating its generating function $f(P;x)$ at the point $x = (1,1,1,...,1)$. This leads us to our main theorem. In order to prove that there is a polynomial time algorithm for counting the number of integer points in P, we must first prove that we can compute the generating function for P in a simple form and that this computation can be done in polynomial time. With this in mind, we have the following result:

Theorem 2.4. *If the dimension d is fixed, then given a rational polyhedron $P \subset \mathbb{R}^d$, there exists a polynomial time algorithm that computes the generating function $f(P;x)$ for P in the form*

$$f(P;x) = \sum_{i \in I} \frac{\epsilon_i x^{a_i}}{(1-x^{b_{i1}})...(1-x^{b_{id}})}.$$

The algorithm is based on the idea that a rational polyhedron can be broken down into a rational cone at each vertex, which can in turn be broken down into unimodular cones. We then simply use the result that unimodular cones have easily computed generating functions and that the generating function of a general polyhedron can be written as a sum of the generating functions of the cones at its vertices. Before proving Theorem 2.4, we begin with the correspoding result in the case of a cone.

The proof given for Theorem 2.4 follow Barvinok and Pommersheim [3].

In addition, by applying the above algorithm to the dual K^* of a given cone K and discarding lower dimensional cones at each step, the computational complexity may be further reduced. This technique results in a decomposition into full dimensional unimodular cones of the form

$$[K] = \sum_{i \in I} \epsilon_i [K_i^*] \text{ modulo cones containing straight lines.}$$

We now sketch the algorithm for Theorem 2.4.

Proof of Theorem 2.4: (Sketch) We begin by breaking the polyhedron into cones at each vertex. For each vertex v, define I_v to be the set of inequalities that are active at v:

$$I_v = \{i \in I : \langle c_i, v \rangle = \beta_i\}.$$

Let $\text{N}(P,v)$ be the cone generated by the vectors c_i. Then for the cone of P at vertex v, we have

$$\text{cone}(P,v) = -\text{N}^*(P,v) + v.$$

Using Theorem 1.4 (applied to the dual cone), we can decompose $[\text{N}(P,v)]$ into a linear combination of characteristic functions of full dimensional unimodular cones, say

$$[\mathrm{N}(P,v)] = \sum_{j \in J_v} \epsilon_{v,j}[K_{v,j}].$$

The result is that

$$[\mathrm{cone}(P,v)] = [v - \mathrm{N}^*(P,v)] = \sum_{j \in J_v} \epsilon_{v,j}[v - K^*_{v,j}] \text{ modulo cones containing straight lines.}$$

Thus we have

$$f(\mathrm{cone}(P,v);x) = \sum_{j \in J_v} \epsilon_{v,j} f(v - K^*_{v,j};x).$$

Each of the cones $v - K^*_{v,j}$ is unimodular with vertex v, and since the generating function of a unimodular cone can be computed easily, this allows us to compute the generating function of P (see the computation following Theorem 2.2). □

Now that we can produce the generating function of a given polyhedron, there is one final step required to actually count the number of integer points. As we observed earlier, the number of integer points is encoded in the generating function as the value at $x = (1,...1)$. However, Theorem A gives us the generating function in the form

$$f(P;x) = \sum_{i \in I} \frac{\epsilon_i x^{a_i}}{(1 - x^{b_{i1}})...(1 - x^{b_{id}})}.$$

which has the point $(1,...1)$ as a pole. Thus evaluating at this point will require residue theory.

Given $f(P;x)$ in the form above, the idea is to construct an integer vector $w \in \mathbb{Z}^d$ with the property that $\langle w, b_{ij} \rangle \neq 0$ for each b_{ij} (this is accomplished by choosing w from among specific values of the curve $g : \mathbb{R} \to \mathbb{R}^d$ given by $g(t) = (1, t, t^2, ..., t^{(d-1)}))$. We use w to write

$$|P \cap \mathbb{Z}^d| = \lim_{x \to (1,...,1)} f(P,x) = \lim_{t \to 0} \sum_{i \in I} \epsilon_i \frac{\exp(t \langle w, a_i \rangle)}{(1 - \exp(t \langle w, b_{i1} \rangle))...(1 - \exp(t \langle w, b_{id} \rangle))}.$$

Finally, we use Taylor series to compute

$$|P \cap \mathbb{Z}^d| = \sum_{i \in I} \frac{\epsilon_i}{\zeta_{i1}...\zeta_{id}} \sum_{k=0}^{d} \frac{\eta_i^k}{k!} td_{d-k}(\zeta_{i1}, ..., \zeta_{id})$$

where $\zeta_{ij} = \langle w, b_{ij} \rangle$ and $\eta_i = \langle w, a_i \rangle$, yielding the desired polynomial time computation of the number of integer points in P.

References

[1] A.I. Barvinok, "Computing the volume, counting integral points, and exponential sums", *Discrete Comput. Geom.* **10**:2 (1993), 123–141.

[2] A. Barvinok, "A polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed", Math. Oper. Res. 19 (1994), 769-779.

[3] A. Barvinok and J.E. Pommersheim, "An algorithmic theory of lattice points in polyhedra, New Perspectives in Algebraic Combinatorics" (Berkeley, CA, 1996–97), Math. Sci. Res. Inst. Publ., vol. 38, Cambridge Univ. Press, Cambridge, 1999, pp. 91–147.

[4] M. Brion, "Points entiers dans Polyèdres Convexes". Ann. Sci. Ècole, Norm. Sup. (4) 21 653-663.

[5] M. Brion, "Polyèdres et Rèseaux". L. Enseignement Mathèmatique 38, 71-88.

[6] W. Cook, M. Hartmann, R. Kannan, C. McDiarmid, "On integer points in polyhedra", Combinatorica 12, 27-37.

[7] M.E. Dyer, "On counting lattice points in polyhedra", SIAM J. Comput., 20, 695-707.

[8] J.C. Lagarias, “Point Lattices”, pp. 919–966 in *Handbook of Combinitorics*, vol. 1, edited by E. by R.L. Graham et al., Elsevier, Amsterdam, 1995.

[9] J. Lawrence, “Rational-function-valued valuations on polyhedra”, pp. 199–208 in *Discrete and computational geometry* (New Brunswick, NJ, 1989/1990), edited by R.P. Jacob, E. Goodman, and W. Steiger, DIMACS Ser. Discrete Math. Theoret. Comput. Sci. **6**, Amer. Math. Soc., Providence, RI, 1991.

[10] A.V. Pukhlikov and A.G. Khovanskii, “The Riemann-Roch theorem for integrals and sums of quasipolynomials on virtual polytopes”, *Algebra i Analiz* **4**:4 (1992), 188–216. In Russian; translation in *St. Petersburg Mathematical Journal*, **4**:4 (1993), 789–812.