A PRIMAL BARVINOK ALGORITHM BASED ON IRRATIONAL DECOMPOSITIONS

MATTHIAS KÖPPE

Abstract. We introduce a variant of Barvinok's algorithm for counting lattice points in polyhedra. The new algorithm is based on irrational signed decomposition in the primal space and the construction of rational generating functions for cones with low index.

1. Introduction

Twelve years have passed since Alexander Barvinok's amazing algorithm for counting lattice points in polyhedra was published. In the mean time, efficient implementations (De Loera et al., 2004c, Verdoolaege et al., 2005) were designed, which helped to make Barvinok's algorithm a practical tool in many applications in discrete mathematics. The implications of Barvinok's technique, of course, reach far beyond the domain of combinatorial counting problems: For example, De Loera et al. (2004a) pointed out applications in Integer Linear Programming, and De Loera et al. (2004b, 2006) obtained an FPTAS for optimizing arbitrary polynomial functions over the mixed-integer points in polytopes of fixed dimension.

Barvinok's algorithm first triangulates the supporting cones of all vertices of a polytope, to obtain simplicial cones. Then, the simplicial cones are recursively decomposed into unimodular cones. It is essential that one uses *signed decomposition* here; triangulating these cones is not good enough to give a polynomiality result.

Moreover, the polynomiality result on Barvinok's algorithm and also the practical implementations rely on Brion's "polarization trick" (see Barvinok and Pommersheim, 1999, Remark 4.3) to avoid dealing with the exponentially many lower-dimensional cones that can arise from the intersecting faces of the subcones in an inclusion-exclusion formula: The computations with rational generating functions are invariant with respect to the contribution of non-pointed cones (cones with a non-trivial linear subspace). By operating in the dual space, i.e., by computing with the polars of all cones, lower-dimensional can be safely discarded, because this is equivalent to discarding non-pointed cones in the primal space.

Date: Revision: 1.4 – Date: 2006/03/06 03:54:08 .

This work was supported by a Feodor Lynen Research Fellowship from the Alexander von Humboldt Foundation. The author also acknowledges the hospitality of Jesús de Loera and the Department of Mathematics of the University of California, Davis.

In practical implementations of Barvinok's algorithm, one observes that in the hierarchy of cone decompositions, the index of the decomposed cones quickly descends from large numbers to fairly low numbers. The "last mile," i.e., decomposing many cones with fairly low index, creates extremely many unimodular cones and thus is the bottleneck of the whole computation in many instances.

The idea of this paper is to stop the decomposition when the index of a cone is small enough, and to compute with generating functions for the integer points in cones of small index rather than unimodular cones. The major difficulty here is that polarizing back a cone of small index can create a cone of very large index, because determinants of $d \times d$ matrices are homogeneous of order d.

To address this difficulty, we avoid polarization altogether and perform the signed decomposition in the primal space instead. To avoid having to deal with exponentially many lower-dimension subcones, we use the concept of *irrational decompositions* of rational polyhedra. Beck and Sottile (2005) introduced this notion to give astonishingly simple proofs for three theorems of Stanley on generating functions for the integer points in rational polyhedral cones. Using the same technique, Beck et al. (2005) gave simplified proofs of theorems of Brion and Lawrence−Varchenko. An irrational decomposition of a polyhedron is a decomposition into polyhedra whose intersections do not contain any lattice points. Counting formulae for lattice points based on irrational decompositions therefore do not need to take any inclusion-exclusion principle into account.

We give an explicit construction of a *uniform irrational shifting vector* $\mathbf{s}$ for a cone $\mathbf{v} + K$ with apex $\mathbf{v}$ such that the shifted cone $(\mathbf{v} + \mathbf{s}) + K$ has the same lattice points and contains no lattice points on its proper faces. More strongly, we prove that *all cones* appearing in the signed decompositions of $(\mathbf{v} + \mathbf{s}) + K$ in Barvinok's algorithm contain no lattice points on their proper faces. Therefore, discarding lower-dimensional cones is safe. Despite its name, the vector $\mathbf{s}$ only has rational coordinates, so after shifting the cone by $\mathbf{s}$, existing implementations of Barvinok's algorithm can be used to compute the irrational primal decompositions without a change.

2. Construction of a uniform irrational shifting vector

We shall first describe the *stability region* of a cone $\mathbf{v} + K$ with apex at $\mathbf{v}$, i.e., the set of apex points $\tilde{\mathbf{v}}$ such that $\tilde{\mathbf{v}} + K$ contains the same lattice points as $\mathbf{v} + K$.

Lemma 1 (The stability region)**.** *Let $\mathbf{v} + B\mathbf{R}^d$ be a simplicial full-dimensional cone with apex at $\mathbf{v} \in \mathbf{Q}^d$, whose basis is given by the columns of the matrix $B \in \mathbf{Z}^{d\times d}$. Let $\boldsymbol{\lambda} = -B^{-1}\mathbf{v}$. Let $D = |\det B|$. Then, for every $\tilde{\boldsymbol{\lambda}}$ such that*

$$\tilde{\lambda}_i \in \left[\frac{1}{D}\left\lfloor D \cdot \lambda_i \right\rfloor, \frac{1}{D}\left\lceil D \cdot \lambda_i \right\rceil\right), \tag{1}$$

the cone $\tilde{\mathbf{v}} + B\mathbf{R}^d$ *with* $\tilde{\mathbf{v}} = -B\tilde{\boldsymbol{\lambda}}$ *contains the same integer points as the cone* $\mathbf{v} + B\mathbf{R}^d$*. Moreover, if each* $\tilde{\lambda}_i$ *is picked from the open interval, the cone* $\tilde{\mathbf{v}} + B\mathbf{R}^d$ *does not have integer points on its proper faces.*

Lemma 2 (A bound on the norm of the dual basis)**.** *Let* $B^* = -(B^{-1})^\top$ *be the basis of the polar cone. Then, for every column vector* $\mathbf{b}_i^*$ *of* B^* *we have the estimate*

$$\|\mathbf{b}_i^*\|_\infty \leq |\det B|^d . \tag{2}$$

Proof. From $\prod_{i=1}^d \|\mathbf{b}_i^*\|_2 \leq |\det B^*| = |\det B|^{-1}$ and $\|\mathbf{b}_j^*\|_2 \geq |\det B|^{-1}$ we obtain $\|\mathbf{b}_i^*\|_\infty \leq \|\mathbf{b}_i^*\|_2 \leq |\det B|^d$. □

Lemma 3 (The irrational lemma)**.** *Let* $M \in \mathbf{Z}_+$ *be an integer. Let*

$$\mathbf{q} = \left(\frac{1}{2M}, \frac{1}{(2M)^2}, \dots, \frac{1}{(2M)^d} \right). \tag{3}$$

Then $\langle \mathbf{z}, \mathbf{q} \rangle \notin \mathbf{Z}$ *for every* $\mathbf{z} \in \mathbf{Z}^d \setminus \{\mathbf{0}\}$ *with* $\|\mathbf{z}\|_\infty < M$*.*

Proof. Follows from the principle of representations of rational numbers in a positional system of base $2M$. □

Theorem 4. *Let* $\mathbf{v} + B\mathbf{R}^d$ *be a simplicial full-dimensional cone with apex at* $\mathbf{v} \in \mathbf{Q}^d$*, whose basis is given by the columns of the matrix* $B \in \mathbf{Z}^{d\times d}$*. Let* $D = |\det B|$*, let* $\boldsymbol{\lambda} = -B^{-1}\mathbf{v}$ *and let* $\hat{\boldsymbol{\lambda}} \in \mathbf{Q}^d$ *be defined by*

$$\hat{\lambda}_i = \frac{1}{D}\left(\lfloor D \cdot \lambda_i \rfloor + \frac{1}{2} \right) \quad \text{for } i = 1, \dots, d. \tag{4}$$

Let $\hat{\mathbf{v}} = -B\hat{\boldsymbol{\lambda}}$*. Using*

$$M = 2D^{d+1} \quad \text{and} \quad \gamma := \frac{1}{2},$$

define

$$\mathbf{s} = \gamma \cdot \left(\frac{1}{2M}, \frac{1}{(2M)^2}, \dots, \frac{1}{(2M)^d} \right).$$

Finally let $\tilde{\mathbf{v}} = -B\hat{\boldsymbol{\lambda}} + \mathbf{s}$.

(i) *We have* $(\tilde{\mathbf{v}} + B\mathbf{R}^d) \cap \mathbf{Z}^d = (\mathbf{v} + B\mathbf{R}^d) \cap \mathbf{Z}^d$*, i.e., the shifted cone has the same set of integer points as the original cone.*
(ii) *The shifted cone* $\tilde{\mathbf{v}} + B\mathbf{R}^d$ *contains no lattice points on its proper faces.*
(iii) *More strongly,* all cones *appearing in the signed decompositions of the shifted cone* $\tilde{\mathbf{v}} + B\mathbf{R}^d$ *in Barvinok's algorithm contain no lattice points on their proper faces.*

Proof. Part (i). Let $\boldsymbol{\mu} = -B^{-1}\mathbf{s}$, thus $\mu_i = \langle \mathbf{b}_i^*, \mathbf{s} \rangle$. Using Lemma 2, we have

$$|\mu_i| \leq \|\mathbf{b}_i^*\|_\infty \cdot \gamma \sum_{j=1}^d \frac{1}{(2M)^j} \leq D^d \cdot \gamma \frac{1}{M} = \frac{1}{4D}.$$

Thus
$$\hat{\lambda}_i + \mu_i \in \left(\frac{1}{D} \lfloor D \cdot \lambda_i \rfloor , \frac{1}{D} \lceil D \cdot \lambda_i \rceil \right),$$
so (i) follows from Lemma 1, since $\tilde{\mathbf{v}} = -B(\hat{\boldsymbol{\lambda}} + \boldsymbol{\mu})$.

Parts (ii) and (iii). Every cone appearing in the course of Barvinok's signed decomposition algorithm has the same apex $\tilde{\mathbf{v}}$ as the input cone and a basis $\bar{B} \in \mathbf{Z}^{d\times d}$ with $\left|\det \bar{B}\right| \leq D$. Let such a $\bar{B}$ be fixed and denote by $\bar{\mathbf{b}}_i^*$ the columns of the dual basis matrix $\bar{B}^* = -(\bar{B}^{-1})^\top$. Let $\mathbf{z} \in \mathbf{Z}^d$ be an aribtrary integer point. We shall show that $\mathbf{z}$ is not on any of the facets of the cone, i.e.,
$$\langle \bar{\mathbf{b}}_i^*, \mathbf{z} - \mathbf{v} \rangle \neq 0 \qquad \text{for } i = 1, \dots, d. \tag{5}$$
Let $i \in \{1, \dots, d\}$ arbitrary. We will show (5) by showing
$$\langle \det \bar{B} \cdot \bar{\mathbf{b}}_i^*, \tilde{\mathbf{v}} \rangle \notin \mathbf{Z}. \tag{6}$$
Clearly, if (6) holds, we have $\langle \bar{\mathbf{b}}_i^*, \tilde{\mathbf{v}} \rangle \notin (\det \bar{B})^{-1}\mathbf{Z}$. But since $\langle \bar{\mathbf{b}}_i^*, \mathbf{z} \rangle \in (\det \bar{B})^{-1}\mathbf{Z}$, we have $\langle \bar{\mathbf{b}}_i^*, \mathbf{z} - \tilde{\mathbf{v}} \rangle \notin \mathbf{Z}$; in particular it is nonzero, which proves (5).

To prove (6), let $M = 2D^{d+1}$. By Lemma 2, we have
$$\left\|\det \bar{B} \cdot \bar{\mathbf{b}}_i^*\right\|_\infty \leq \left|\det \bar{B}\right| \cdot \left|\det \bar{B}\right|^d \leq D^{d+1} < M. \tag{7}$$
Lemma 3 with $\mathbf{z} = \det \bar{B} \cdot \bar{\mathbf{b}}_i^*$ gives $\langle \mathbf{z}, \mathbf{s} \rangle \notin \frac{1}{2}\mathbf{Z}$. Observing that by the definition (4), we have
$$\langle \mathbf{z}, \hat{\mathbf{v}} \rangle = \langle \mathbf{z}, -B\hat{\boldsymbol{\lambda}} \rangle \in \frac{1}{2}\mathbf{Z}.$$
Therefore, we have $\langle \mathbf{z}, \tilde{\mathbf{v}} \rangle \notin \frac{1}{2}\mathbf{Z}$. This proves (6), and thus completes the proof. □

3. Computational experiments

... to be carried out...

References

Alexander I. Barvinok. Polynomial time algorithm for counting integral points in polyhedra when the dimension is fixed. *Mathematics of Operations Research*, 19:769–779, 1994.

Alexander I. Barvinok and James E. Pommersheim. An algorithmic theory of lattice points in polyhedra. In *New Perspectives in Algebraic Combinatorics*, volume 38 of *Math. Sci. Res. Inst. Publ.*, pages 91–147. Cambridge Univ. Press, Cambridge, 1999.

Matthias Beck, Christian Haase, and Frank Sottile. Theorems of Brion, Lawrence, and Varchenko on rational generating functions for cones, 2005. eprint arXiv:math.CO/0506466.

Matthias Beck and Frank Sottile. Irrational proofs for three theorems of Stanley, 2005. eprint arXiv:math.CO/0501359 v4.

Jesús A. De Loera, David Haws, Raymond Hemmecke, Peter Huggins, and Ruriko Yoshida. Three kinds of integer programming algorithms based on Barvinok's rational functions. In *Integer Programming and Combinatorial Optimization, 10th IPCO Proceedings*, volume 3064 of *Lecture Notes in Computer Science*, pages 244–255. Springer, 2004a.

Jesús A. De Loera, Raymond Hemmecke, Matthias Köppe, and Robert Weismantel. Integer polynomial optimization in fixed dimension. eprint arXiv: math.OC/0410111, to appear in Mathematics of Operations Research, 2004b.

Jesús A. De Loera, Raymond Hemmecke, Matthias Köppe, and Robert Weismantel. FPTAS for mixed-integer polynomial optimization with a fixed number of variables. In *Proceedings of the 17th Annual ACM-SIAM Symposium on Discrete Algorithms, Miami, FL, January 22–24, 2006*, pages 743–748, 2006.

Jesús A. De Loera, Raymond Hemmecke, Jeremiah Tauzer, and Ruriko Yoshida. Effective lattice point counting in rational convex polytopes. *Journal of Symbolic Computation*, 38(4):1273–1302, 2004c.

S. Verdoolaege, R. Seghir, K. Beyls, V. Loechner, and M. Bruynooghe. Counting integer points in parametric polytopes using Barvinok's rational functions, 2005. To appear in Algorithmica.

Otto-von-Guericke-Universität Magdeburg, Department of Mathematics/IMO, Universitätsplatz 2, 39106 Magdeburg, Germany

E-mail address: `mkoeppe@imo.math.uni-magdeburg.de`