SOME NEW APPLICATIONS OF TORIC GEOMETRY

J. MAURICE ROJAS

Abstract. This paper reexamines univariate reduction from a toric geometric point of view. We begin by constructing a binomial variant of the u-resultant and then retailor the generalized characteristic polynomial to fully exploit sparsity in the monomial structure of any given polynomial system. We thus obtain a fast new algorithm for univariate reduction and a better understanding of the underlying projections. As a corollary, we show that a refinement of Hilbert's Tenth Problem is decidable within single-exponential time. We also show how certain multisymmetric functions of the roots of polynomial systems can be calculated with sparse resultants.

1. Introduction

We give a new approach for combatting degeneracy problems which occur when reducing large polynomial systems to univariate polynomials. Taking a positive attitude, we will actually make use of these degeneracies to better understand polynomial system solving. We do this by applying new observations involving toric varieties to establish faster, more reliable algorithms for univariate reduction. Our techniques provide an intrinsic geometric setting for such reductions and fully exploit the sparsity of any polynomial system specified by its monomial term structure.

Algebraically reducing problems involving polynomial systems to simpler questions involving a single univariate polynomial is a technique which has been known for over a century, and has been applied with increasing efficiency in computational algebra over the last two decades. (For example, see [Laz81, KL92, PK95, GHMP95] and the references therein.) However, there are difficulties with this method which *still* have not been completely addressed. Three such problems are the following:

A: Since univariate reduction corresponds to projecting the solution space onto a projective line, the fiber over a point with finite coordinate might contain roots at infinity.

Date: February 10, 1997.

This research was partially funded by N.S.F. grant DMS-9022140 and an N.S.F. Mathematical Sciences Postdoctoral Fellowship.

Revision of an earlier version which appeared in Foundations of Computational Mathematics, selected papers of a conference, held at IMPA in Rio de Janeiro, January 1997, Felipe Cucker and Mike Shub (eds.), Springer-Verlag.

B: The univariate polynomial one reduces to might be identically zero, due to (1) degeneracies in the underlying projection, or (2) the presence of infinitely many roots.

C: Univariate reduction is still too slow for many problems of interest.

We circumvent A by the technique of *toric laminations*. By constructing a generalization of Canny's *generalized characteristic polynomial* (GCP) [Can90, Shu93] — the *toric* (or *sparse*) GCP — we can dispose of B_2. Our toric geometric approach also helps us better understand B_1. These two new techniques are contained in theorems 1–3 below.

Although problem B_2 was solved earlier in [Ren87, Can90], the toric GCP greatly improves the complexity bounds given there. In particular, we address problem C by using the *sparse resultant* [GKZ90, EC95] throughout our development. Fast methods for polynomial system solving were derived via the *sparse u-resultant* in [Emi94, EC95] but problems A and B were not addressed there. Our approach to univariate reduction thus unifies the GCP with the the sparse u-resultant. Furthermore, we generalize both techniques to certain *toric varieties* [KKMS73, Ful93, Stu95].

One advantage of a toric variety setting is reducing the problem of *exact* root counting for polynomial systems, almost completely, to convex geometry. Generically sharp *upper bounds* on the number of (complex) isolated roots, in terms of mixed volume, first appeared just over two decades ago [Kus75]. These bounds have since been generalized to algebraically closed fields [Dan78, Roj97a] and to various subsets of affine space (other than the algebraic torus) [Kho78, HS96, Roj97a]. However, the following algorithm appears to be the first example of a convex geometric approach to counting the exact number of roots. (We will assume henceforth that all our polynomials and roots are considered over an algebraically closed ground field K.)

Theorem 1. *Let $F(x_1,\ldots,x_n)$ be an $n\times n$ polynomial system with support $E:=(E_1,\ldots,E_n)$ such that $\mathcal{M}(E)>0$. Also let P_E be the sum of the convex hulls of the E_i, and pick $a\in\mathbb{Z}^n\setminus\{\mathbf{O}\}$ such that the segment $[\mathbf{O},a]$ is not parallel to any facet of P_E. Define $\pi_a(u_+,u_-):=\mathrm{Res}_{E_a}(F,u_++u_-x^a)$ where $\{u_\pm\}$ is a pair of algebraically independent indeterminates and $E_a:=(E,\{\mathbf{O},a\})$. Finally, let $\varepsilon_\pm$ be the lowest exponent of $u_\pm$ occurring in any monomial of π_a. Then F has* exactly *$\mathcal{N}:=\mathcal{M}(E)-\varepsilon_+-\varepsilon_-$ isolated roots (counting multiplicities) in $(K^*)^n$, provided $\mathcal{N}<\infty$.*

In the above, $\mathrm{Res}_\star(\cdot)$ and $\mathcal{M}(\cdot)$ respectively denote the sparse resultant and mixed volume [EC95, DGH96, Roj97a]. The key contributions of the above theorem are (a) fibering the solution space by maps more general than coordinate projections, and (b) making explicit use of roots at *toric* infinity when doing univariate reduction.

We may also calculate the number of *distinct* roots in a similar way.

Corollary 1. *Following the notation and assumptions of theorem 1, let $\pi'_a(u_+,u_-)$ be the square-free part of $\pi_a(u_+,u_-)$. Also let $\varepsilon'_\pm$ be the lowest exponent of $u_\pm$ occuring* *in* π'_a*. Then* F *has* exactly $\mathcal{N}' := \deg(\pi'_a) - \varepsilon'_+ - \varepsilon'_-$ *roots in* $(K^*)^n$*, provided* $\mathcal{N}' < \infty$ and *the projection of roots* $\{\zeta \in (K^*)^n \mid F(\zeta) = 0\} \longrightarrow \{\zeta^a\}$ *is injective.*

This corollary is proved alongside theorem 1 in section 5.

By instead calculating a particular *coefficient* of π_a, we can actually compute certain multisymmetric functions of the roots of F and thus do more than just count the number of isolated roots. Admittedly, such a computation can be rather difficult, but recent advances in interpolation techniques, e.g., [Zip93], are making this approach increasingly feasible. So let us at least give explicit formulae for the coefficients of π_a in terms of multisymmetric functions.

Definition 1. *For any* $w \in \mathbb{R}^n \setminus \{\mathbf{O}\}$*, let* E^w_i *be the set of points of* E_i *having* minimal *inner product with* w*. Also, let* $E^w := (E^w_1, \ldots, E^w_n)$ *and, when* $w \in \mathbb{Q}^n \setminus \{\mathbf{O}\}$*, let* $p_w \in \mathbb{Z}^n$ *be the first lattice point not equal to the origin encountered along the ray generated by* w*. Finally, let* $L(E,a)$*, the* ambiguity locus*, be the subvariety of* $\mathcal{T}_{P_E} \setminus (K^*)^n$ *corresponding to the union of all faces of* P_E *having an inner normal perpendicular to the segment* $[\mathbf{O}, a]$*.*

Remark 1. *The toric variety (over* K*),* $\mathcal{T}_P$*, corresponding to a polytope* P *is detailed in* [KSZ92, Ful93, GKZ94, Stu95, Roj97a]*. Polynomial roots in a toric compactification are described (in a manner closest to our present framework) in* [Roj97a]*.*

Corollary 2. *Following the notation of theorem 1, assume instead that* a *is* any *point in* $\mathbb{Z}^n \setminus \{\mathbf{O}\}$ *and* $\varepsilon_+, \varepsilon_- < \infty$*. Then* π_a *is a homogeneous polynomial of degree* $\mathcal{M}(E)$ *and, for any* $d \in \{0, \ldots, \mathcal{M}(E) - \varepsilon_+ - \varepsilon_-\}$*, the coefficient of* $u_-^{d+\varepsilon_-} u_+^{\mathcal{M}(E)-d-\varepsilon_+}$ *in* π_a *is precisely*

$$C \sum \prod_{j=1}^{d} \zeta(j)^a,$$

where $C \in K^*$ *is independent of* d*, the sum ranges over all cardinality* d *multisets* $\{\zeta(1), \ldots, \zeta(d)\} \subseteq Z_F$*, and* Z_F *is the multiset of roots of* F *in* $(K^*)^n \cup L(E,a)$*. Furthermore, if* $\varepsilon_+ = \varepsilon_- = 0$ *then* C *is precisely*

$$(-1)^n \left(\prod_w \mathrm{Res}_{E^w}(F)^{-p_w \cdot a} \right),$$

where the product ranges over all inner facet directions of P_E *having negative inner product with* a*.* ■

Multisets are simply sets where repeated elements are allowed, and whose subsets have repetitions appropriately restricted [GKP94]. For example, if Z_F contains -1 as a root of multiplicity 5, then no subset of Z_F can have more than five -1's. So in essence, the coefficients of π_a (when suitably normalized) are just elementary symmetric functions of a-monomials of certain roots of F.

The above corollary follows easily from theorem 1 and the Pedersen-Sturmfels product formula [PS93].[1] Moreover, since the sparse resultant is invariant under muliplication of the individual polynomials by a monomial, we can compare the coefficients of π_a and π_{-a} to obtain the following beautiful identity.[2]

Corollary 3. *Following the notation and assumptions of corollary 2,* $\varepsilon_+ = \varepsilon_- = 0 \Longrightarrow$
$$\prod_{\zeta \in Z_F} (\zeta^a) = \prod_w \mathrm{Res}_{E^w}(F)^{p_w \cdot a}$$
where the product ranges over all *inner facet directions of* P_E. ■

Recall that a *ridge* is a polytope face of codimension 2 [Zie95]. Although the "bad" case of theorem 1 ($\mathcal{N} = \infty$) is an annoyance, it is a small annoyance and can actually be made use of in certain cases.

Theorem 2. *Following the notation and assumptions of theorem 1,* $\mathcal{N} = \infty \Longleftrightarrow F$ *has a root lying in* $L(E, a)$ or *infinitely many roots in* $(K^*)^n$*. Also, within the space of all systems with support contained in* E*, the* F *with* $\mathcal{N} = \infty$ *form a subvariety of codimension* ≥ 2.

Thus, if the roots of F avoid the ambiguity locus, F has infinitely many roots in $(K^*)^n \Longleftrightarrow \mathcal{N} = \infty$. In particular, it follows directly from the definition of $L(E, a)$ that $\mathrm{codim} L(E, a) = 2$, under the assumptions of theorem 2. (Since $L(E, a)$ then corresponds to a finite set of ridges [Ful93, Roj97a].)

We can completely avoid amiguity loci by replacing the binomial $u_+ + u_- x^a$ in our preceding results with another specially chosen indeterminate polynomial. This is detailed further in [Roj97c] and, to a certain extent, in the result we quote below. However it is worth noting that the roots of F *always* avoid $L(E, a)$ when $n < 3$ and E is the support of F (cf. lemma 1).

Remark 2. *The existence of infinitely many roots of* F *at toric infinity and the existence of a root of* F *within the ambiguity locus are independent in general (cf. section 3). Thus it is worthwhile to know something about* $L(E, a)$.

Remark 3. *A correspondence useful for visualizing theorems 1 and 2 is to identify toric infinity* ($\mathcal{T}_P \backslash (K^*)^n$) *with the boundary of the polytope* P *(cf. definition 2). Computing* π_a *then amounts to splitting* ∂P_E *into two signed halves, much like cracking an egg-shell. In particular, the half with sign* $\pm$ *consists precisely of those faces of* P_E *having an inner normal with* $\pm$ *inner product with* a*. The ambiguity locus is then precisely the common boundary of these two halves. We will see later that* π_a *can be*

[1] We also need the fact that the Pedersen-Sturmfels formula, originally stated only over $\mathbb{C}$, remains true over a general algebraically closed field. This is proved in [Roj97d].

[2] Alicia Dickenstein pointed out the $K = \mathbb{C}$ of the above formula (due to Cattani, Dickenstein and Sturmfels) to the author at the conference where this paper was presented. Shortly after, the author realized that this formula could also follow easily from corollary 2.

viewed as a coordinatization of a particular rational map $\mathcal{T}_{P_E} \dashrightarrow \mathbb{P}^1_K$. Thus, provided no roots lie in the ambiguity locus, $\varepsilon_\pm$ is the sum of the intersection numbers of the roots of F which lie in the $\pm$ half.

A general way to deal with the existence of *infinitely* many roots of F within a given toric compactification is the following result announced below.

Theorem 3. [Roj97c] *Following the notation of theorem 1, suppose $g(x) := \sum_{e\in A} u_e x^e$ where the u_e are algebraically independent indeterminates and $A \subset \mathbb{Z}^n$ is nonempty and finite. Suppose further that $\mathcal{P} := (P_1, \ldots, P_n)$ is an n-tuple of integral polytopes in $\mathbb{R}^n$ containing the support of F, and let D be an irreducible fill of $\mathcal{P}$. Setting $F^* := (\sum_{e\in D_i} x^e \mid i \in [1..n])$, define $\mathcal{H}(s;u) := \mathrm{Res}_{(E,A)}(F - sF^*, g)$, where s is a new indeterminate. Finally, considering $\mathcal{H}$ as a polynomial in s with coefficients in $K[u]$, let $\mathcal{F}_A(u)$ be the coefficient of the lowest power term of $\mathcal{H}$. Then $\mathcal{F}_A$ is a homogeneous polynomial with the following properties:*

1. *$\mathcal{F}_A$ is divisible by $g(\zeta)$, for any root $\zeta \in (K^*)^n$ of F.*
2. *If $\mathcal{P}$ is compatible with $\mathrm{Conv}(A)$, then $\mathcal{F}_A$ has degree $\mathcal{M}(\mathcal{P})$ and to every irreducible factor of $\mathcal{F}_A$ there naturally corresponds a root of F in $\mathcal{T}_P$, where $P := \sum P_i$.*

We call $\mathcal{H}$ a toric *(or* sparse*)* generalized characteristic polynomial for (F, A). ■

The combinatorial portion of the above theorem can be explained as follows: We say that D *fills* $\mathcal{P}$ iff $D := (D_1, \ldots, D_n)$ satisfies $D_i \subseteq P_i$ for all $i \in [1..n]$ and $\mathcal{M}(D) = \mathcal{M}(\mathcal{P})$ [Roj94, RW96]. An *irreducible* fill is then simply a fill which is minimal with respect to n-tuple containment. Finding such a D amounts to a combinatorial preprocessing step which need only be done once for a given set of problems, provided E is fixed. Compatibility is defined in section 5 and the toric GCP is briefly compared to the original GCP in section 6. Combined with the toric variety version of Bernshtein's theorem [Roj97a], we see that the above theorem gives us a resultant-based method to work with the isolated roots of a sparse polynomial system, even in the presence of infinitely many roots. Furthermore, the roots defined by $\mathcal{F}_A$ which do *not* correspond to any isolated root of F can be usefully interpreted as contributions from the excess components.

We apply our main theorems to some simple examples in section 3. Our results are also very useful for root counting over $\mathbb{R}$, $\mathbb{Q}$, and even $\mathbb{Z}$. For example, one can combine standard univariate techniques such as Sturm sequences [GLRR94, Roy95] with our preceding results to quickly count the number of real roots [Roj97b]. Better still, we can go to an even smaller ring: In section 4 we will give a short proof (under some mild hypotheses) of the following refinement of Hilbert's Tenth Problem [Mat93].

Theorem 4. [Roj97d] *Consider, for any nonnegative integer d, the following collection of Diophantine systems:*

Hilb(d): *Multivariate polynomial systems with integer coefficients and d-dimensional* **complex** *solution set.*
Then there is an algorithm which, given any instance of **Hilb**(0)*, finds all integer solutions, or certifies that there are none, within single-exponential time.* ■

All of the above results stem from an observation on the vanishing of the sparse resultant. In particular, one basic property of the sparse resultant is that

$$(\star) \qquad (F, f_{n+1}) \text{ has a root in } (K^*)^n \Longrightarrow \mathrm{Res}_{\bar{E}}(F, f_{n+1}) = 0$$

(provided $\bar{E} = (E, E_{n+1})$ and f_{n+1} is a polynomial over K with support contained in $E_{n+1} \subset \mathbb{Z}^n$). However, the converse assertion is **not** always true. (The polynomial system $(x+y+1, x+y+2, x+y+3)$ with $\bar{E} = \{\mathbf{O}, \hat{e}_1, \hat{e}_2\}^3$ gives a simple counterexample reducing to the vanishing of a 3×3 determinant.) The correct statement in which *both* implications hold seems to be known only folklorically, while the *unmixed* case $E_1 = \cdots = E_{n+1} = \mathcal{A}$ (over $\mathbb{C}$) is contained in various recent works, e.g., [KSZ92, GKZ94]. So we will make use of the following more general result.

Vanishing Theorem for Resultants. [Roj97d] *Suppose f_i is a polynomial over K with support* contained in $E_i \subset \mathbb{Z}^n$ *for all $i \in [1..n+1]$. Then, provided*

$$\mathcal{M}(E_1, \ldots, \widehat{E_i}, \ldots, E_{n+1}) > 0$$

for some $i \in [1..n]$,

$$\mathrm{Res}_{\bar{E}}(f_1, \ldots, f_{n+1}) = 0 \Longleftrightarrow \bigcap_{i=1}^{n+1} \mathcal{D}_{P_{\bar{E}}}(f_i, \mathrm{Conv}(E_i)) \neq \emptyset,$$

where $\bar{E} := (E_1, \ldots, E_{n+1})$ and $P_{\bar{E}} := \sum_{i=1}^{n+1} \mathrm{Conv}(E_i)$. ■

In the above, $\mathcal{D}_P(f_i, P_i)$ is the *toric effective divisor* of $\mathcal{T}_P$ corresponding to (f_i, P_i) (cf. definition 2). This result provides a geometric analogue, over a *general* algebraically closed field, of the product formula for the sparse resultant [PS93].

We close this introduction with an important note:

In addition to the applications we have presented, our approach to univariate reduction provides a first step toward an intrinsic method for root finding in the algebraic torus $(K^*)^n$. Although one could in principle reduce to various coordinate subspaces to perform "sparse" elimination theory in K^n, such an approach runs into complications with intersection multiplicities on the coordinate hyperplanes and is really *not* intrinsic to K^n. We propose a more intrinsic (and efficient) approach to *affine elimination theory* by defining a new resultant operator — the *affine* sparse resultant — in [Roj97e]. Following this route, *all* of our main theorems generalize easily to root finding in affine space minus an arbitrary union of coordinate hyperplanes. This is pursued in greater depth in [Roj97a, Roj97e] and the complexity bound of theorem 4 is further refined in the latter work.

2. Related Work

We point out a few important recent approaches to elimination theory which can profit from our results.

From an applied angle, our observations on degeneracies and handling polynomial systems with infinitely many roots nicely complement the work of Emiris and Canny [EC95]. In particular, their sparse resultant based algorithms for polynomial system solving can now be made to work even when problem B occurs. Also, an added benefit of working torically (as opposed to the classical approach of working in projective space) is the increased efficiency of the sparse resultant: the resulting matrix calculations (for polynomial system solving) are much smaller and faster. In particular, whereas it was remarked in [Can90] that Gröbner basis methods are likely to be faster than the GCP for sparse polynomial systems, the toric GCP appears to be far more competitive in such a comparison.

From a more theoretical point of view, our focus on univariate reduction is a useful addition to Sturmfels' foundational work on sparse elimination theory in the large [Stu93]. (We also point out that [Stu93] provides a wonderfully clear introduction to some of the toric variety techniques we refer to.)

Going further into the intersection of algebraic geometry and complexity theory, there is a beautiful new approach to elimination theory founded by the school of Heintz, et. al. [PK95, GHMP95]. Our results fill in some toric geometry missing from their more algebraic framework. In particular, we propose that toric laminations, i.e., "fibering" $\mathcal{T}_{P_E}$ by *toric* projections (instead of fibering $(K^*)^n$ by coordinate projections), can enhance their methods. For example, although their formulation in terms of straight-line programs is extremely general, it appears that their complexity bounds can be significantly improved with our techniques in the case of polynomial systems which are "sparse" in the specified supports sense we use here. This is explored further in [Roj97d].

3. Examples

We will give a 2×2 example of our first two theorems.

3.1. Root Counting with Sparse Resultants.

Let $n=2$ and consider the bivariate polynomial system $F:=(x^3+y^4-1, x^4+y^5-1)$. Also let E_1 and E_2 respectively be the supports $\{\mathbf{O},(3,0),(0,4)\}$ and $\{\mathbf{O},(4,0),(0,5)\}$. Clearly then the Newton polygons are two triangles and the segment $[\mathbf{O},(1,1)]$ is not parallel to any edge of the quadrilateral $P_E := \mathrm{Conv}(\mathbf{O},(7,0),(0,9),(4,4))$. So we can set $a:=(1,1)$ and apply theorem 1 to count the roots of F.

We are now ready to compute the sparse resultant $\mathrm{Res}_{E_a}(F, u_+ + u_- xy)$, where $E_a := (E_1, E_2, \{\mathbf{O},(1,1)\})$ and the coefficients of F have been replaced by algebraically independent indeterminates.[3] To do this, we can use `Maple` to calculate the Sylvester (2×1) resultants of the pairs $(f_2, u_+ + u_-xy)$ and $(f_1, u_+ + u_-xy)$, eliminating the variable y. Let us respectively call these resultants f_{-1} and f_{-2}. Using the Sylvester resultant one last time on (f_{-1}, f_{-2}) to eliminate x, we arrive at a *multiple* of the sparse resultant we are looking for. (This fact follows easily from the characterization of the sparse resultant as the (nonzero) polynomial of lowest total degree satisfying property $(\star)$ from the introduction [Stu93, Roj97d].)

The preceding computations, modulo typing, takes only fractions of a second on a Sun 4m Computeserver. From [Stu94] we know that the sparse resultant itself should have degree $\mathcal{M}(E_1, E_2) + \mathcal{M}(E_1, \{\mathbf{O}, a\}) + \mathcal{M}(E_2, \{\mathbf{O}, a\}) = 16 + 7 + 9 = 32$. (This calculation is easily done by hand via the general formula $\mathcal{M}(E_1, E_2) = \mathrm{Area}(\mathrm{Conv}(E_1 + E_2)) - \mathrm{Area}(\mathrm{Conv}(E_1)) - \mathrm{Area}(\mathrm{Conv}(E_2))$ [Sch94, DGH96].) So by factoring with `Maple` (which takes just under 2 seconds) we can isolate the sparse resultant and specialize coefficients to obtain

$$\pi_{(1,1)}(u_+, u_-) = \mathrm{Res}_{E_a}(x^3 + y^4 - 1, x^4 + y^5 - 1, u_+ + u_-xy) =$$

$$20u_-^9u_+^7 + 31u_-^8u_+^8 + 12u_-^7u_+^9 + 14u_-^5u_+^{11} + 14u_-^4u_+^{12} + 7u_-^3u_+^{13} - 9u_-^2u_+^{14} + u_-u_+^{15} + u_+^{16}$$

So $\varepsilon_+ = 7$, $\varepsilon_- = 0$, and theorem 1 tells us that F has exactly $16 - 7 = 9$ roots, counting multiplicities, in $(\mathbb{C}^*)^2$. Furthermore, a one-line `Maple` calculation shows that $\pi_{(1,1)}$ is irreducible over $\mathbb{Q}$. So corollary 1 (and basic Galois theory) tells us that the multiplicity of every root of F in $(\mathbb{C}^*)^2$ is 1.

The roots of F can also be counted via Gröbner basis methods but the toric geometry in this example is rather nice to observe. In particular, the coordinate cross $\{xy=0\}$ is naturally embedded in $\mathcal{T}_{P_E}$ and corresponds precisely to the two lower-left edges of P_E (cf. remark 3 and definition 2). Furthermore, the ambiguity locus consists of two distinct points which, due to the fact that π_a is not identically 0 (cf. theorem 2), the roots of F have luckily avoided. Also $\varepsilon_+ = 7 \Longrightarrow F$ has precisely 7 roots, counting multiplicities, on the coordinate cross. The latter fact can also be easily checked with a little commutative algebra.

We have included timing information solely for illustrative purposes. In particular, our calculations can be sped up tremendously with suitably specialized code.

4. A Refinement of Hilbert's Tenth Problem

We will present a concise proof of theorem 4 under the following three hypotheses:

1. The instances of **Hilb**(0) considered are $n \times n$ polynomial systems.
2. The complex roots of an instance must have all coordinates nonzero.

[3]The published version of this paper contains an erroneous computation (due to a software error) of this resultant. This was observed by John Dalbec at the conference where this paper was presented, and the calculation below is due to him. The author is deeply indebted to Professor Dalbec's astute observation.

3. No instance can have a complex root at toric infinity.

Note that (1) and (2) are of a combinatorial nature: they restrict the number and dimensions of the supports, as well as their intersections with the coordinate subspaces. On the other hand, (3) is of a more algebraic nature and, when the supports are fixed, is easily shown to fail only on a codimension 1 subvariety of polynomial systems, e.g., [Roj97a, Main Theorem 2].

The above hypotheses are present mainly for technical reasons and are removed in [Roj97d]. They may also be removed with other recent techniques [BPR94, PK95, GHMP95], but through our toric techniques it is possible to obtain a general complexity bound with near *quadratic* dependence on the mixed volume [Roj97c]. This would be the best asymptotic bound to date for solving Diophantine systems.

Proof of Theorem 4: First we outline our algorithm:

Step 1: Following the notation of theorem 3, let A be the vertices of a standard n-simplex in $\mathbb{R}^n$ and $\mathcal{P}$ the n-tuple of Newton polytopes of F. Form the polynomial $\mathcal{F}_A$.

Step 2: Using the Lenstra-Lenstra-Lovasz algorithm [LLL82], factor $\mathcal{F}_A$ over $\mathbb{Z}$.

Step 3: Any integral root $(z_1, \ldots, z_n) \in \mathbb{Z}^n$ of F corresponds precisely to an integral factor of $\mathcal{F}_A$ of the form $u_{\mathbf{O}} + z_1 u_{\hat{e}_1} + \cdots + z_n u_{\hat{e}_n}$.

Step 1 runs in time polynomial in the mixed volume, applying hypotheses (1) and (3), and the results of [Stu93, Emi96]. In fact, we are merely computing a "sparse" variant of the u-resultant in Step 1. To prove this (and the fact that this sparse u-resultant is not identically 0) one uses slightly more general versions of theorems 1 and 2 [Roj97d]. One also needs the fact that hypotheses (1) and (3) together imply that the complex zero set of F in $(K^*)^n$ is zero-dimensional, but this is an immediate consequence of [Roj97a, Corollary 3]. We also point out that working more generally in terms of $\mathcal{F}_A$ aids in later removing hypothesis (3) [Roj97d].

To see that Step 2 runs within time single-exponential in the input size, one need only observe that (a) the coefficient growth in the sparse u-resultant calculation can be reasonably bounded, and (b) the LLL-algorithm runs within time single-exponential in n and polynomial in the bit-sizes of the coefficients of F. Part (a) is detailed in [Roj97d], and part (b) follows easily from the univariate case covered in [LLL82].

That we can terminate as described in Step 3 follows immediately from hypothesis (2) and the Vanishing Theorem for Resultants. ■

We conclude this section with some brief notes on related work.

First, we point out the rather surprising fact that restructuring Hilbert's Tenth Problem as the union $\bigcup_{d=0}^{\infty} \mathbf{Hilb}(d)$ seems to be new. (In particular, Hilbert's Tenth Problem was originally stated as deciding the existence of a *single* integral root for *one* polynomial in several variables.) Although the results of [Jon82] imply that $\mathbf{Hilb}(8)$ is undecidable, nothing seems to be known about $\mathbf{Hilb}(d)$ for $0 < d < 8$. We find this shocking, considering the vast effort within arithmetic geometry to use complex geometric invariants in Diophantine problems, e.g., Falting's theorem and the deep conjectures of Lang and Vojta [CS86].

We also point out that **Hilb**(0) being a single-exponential problem may not be so new: Teresa Krick and Luis-Miguel Pardo-Vasallo have pointed out to the author that theorem 4 can also be readily derived from [PK95, GHMP95]. (Indeed, such an argument could have also been derived directly from [LLL82] and [Ren87] in 1987.) Pardo-Vasallo has also pointed out that Marie-Françoise Roy lectured in 1995 on a similar result, presumably derived from [BPR94]. Nevertheless, optimal bounds are open territory; not to mention the 6-long gap in the status of **Hilb**(d).

5. Toric Varieties and Sparse Resultants

Our notation is a slight variation of that used in [Ful93], and is described at greater length in [Roj97a]. We will assume the reader to be familiar with normal fans of polytopes and the construction of a toric variety from a fan [Ful93, GKZ94]. However, we will at least list our cast of main characters:

Definition 2. [Roj97a] *Given any $w \in \mathbb{R}^n$, we will use the following notation:*

$T =$ *The algebraic torus* $(K^*)^n$

$P^w =$ *The face of P with inner normal w*

$\sigma_w =$ *The closure of the cone generated by the inner normals of P^w*

$U_w =$ *The affine chart of $\mathcal{T}_P$ corresponding to the cone σ_w of* $\mathrm{Fan}(P)$

$L_w =$ *The* $\dim(P^w)$*-dimensional subspace of $\mathbb{R}^n$ parallel to P^w*

$x_w =$ *The point in U_w corresponding to the semigroup homomorphism $\sigma_w^\vee \cap \mathbb{Z}^n \longrightarrow \{0,1\}$ mapping $p \mapsto \delta_{w\cdot p,0}$, where δ_{ij} denotes the Kronecker delta*

$O_w =$ *The T-orbit of $x_w =$ The T-orbit corresponding to* $\mathrm{RelInt} P^w$

$\mathcal{E}_P(Q) =$ *The T-invariant Weil divisor of $\mathcal{T}_P$ corresponding to a polytope Q with which P is compatible*

$\mathrm{Div}(f) =$ *The Weil divisor of $\mathcal{T}_P$ defined by a rational function f on $(K^*)^n$*

$\mathcal{D}_P(f,Q) = \mathrm{Div}(f) + \mathcal{E}_P(Q) =$ *The toric effective divisor of $\mathcal{T}_P$ corresponding to (f,Q)*

$\mathcal{D}_P(F,\mathcal{P}) =$ *The (nonnegative) cycle in the Chow ring of $\mathcal{T}_P$ defined by $\bigcap_{i=1}^n \mathcal{D}_P(f_i,P_i)$*

We will say that a polytope P (resp. an n-tuple $\mathcal{P}$) is *compatible* with Q iff every cone of $\mathrm{Fan}(Q)$ is a union of cones of $\mathrm{Fan}(P)$ (resp. a union of cones of $\mathrm{Fan}(P_i)$ for each i) [Kho77, Roj97a]. We will also make frequent use of the natural correspondence between the face interiors $\{\mathrm{RelInt} P^w\}$ and the T-orbits $\{O_w\}$ [KSZ92, Ful93, GKZ94]. The following lemma gives a more explicit algebraic analogy between the vertices of P and the maximal affine charts of $\mathcal{T}_P$.

Lemma 1. [Roj97a] *Suppose F is a $k \times n$ polynomial system over K with support contained in a k-tuple of integral polytopes $\mathcal{P} := (P_1, \ldots, P_k)$ in $\mathbb{R}^n$. Assume further that P is a rational polytope in $\mathbb{R}^n$ compatible with $\mathcal{P}$. Then the defining ideal in $K[x^e \mid e \in \sigma_w^\vee \cap \mathbb{Z}^n]$ of $U_w \cap \mathcal{D}_P(F,\mathcal{P})$ is $\langle x^{b_1} f_1, \ldots, x^{b_k} f_k \rangle$, for any $b_1, \ldots, b_k \in \mathbb{Z}^n$ such that $b_i + P_i^w \subseteq L_w$ for all $i \in [1..k]$.* ■

Theorems 1 and 2 will follow easily from the Vanishing Theorem for Resultants via following two lemmata below.

Lemma 2. *Following the notation of theorem 1, define*

$$\mathcal{P}_E := (\mathrm{Conv}(E_1), \ldots, \mathrm{Conv}(E_n)).$$

Then the map $x \mapsto x^a$ extends to a proper morphism $\phi_a : \mathcal{T}_{P_E} \backslash L(E,a) \longrightarrow \mathbb{P}^1_K$. Also, if $\mathcal{D}_{P_E}(F, \mathcal{P}_E)$ has zero-dimensional intersection with $(K^*)^n$ and avoids the ambiguity locus, then π_a is, up to a nonzero constant multiple, the Chow form of the subvariety $\phi_a(\mathcal{D}_{P_E}(F, \mathcal{P}_E))$ of $\mathbb{P}^1_K$. ■

Lemma 3. *Following the notation of theorem 1, pick points $a(1), \ldots, a(n-1) \in \mathbb{Z}^n$ which together generate a hyperplane in $\mathbb{R}^n$ which is not parallel to any facet of P_E. Then F has infinitely many roots in $(K^*)^n \Longrightarrow$ the polynomial $p(u_+, u_-) := \prod_{i=1}^{n-1} \pi_{a(i)}$ is identically 0.* ■

Sufficiently armed, let us now prove theorem 2.

Proof of Theorem 2: Suppose that F has no roots within $L(E,a)$ and only finitely many roots within $(K^*)^n$. Then it follows from lemma 2 that u_+ (resp. u_-) divides π_a iff F has a root in some torus orbit O_w with $w \cdot a > 0$ (resp. $w \cdot a < 0$). More to the point, if $c \in K^*$ then it follows similarly that $u_+ + cu_-$ divides π_a iff some root of F lies in the closure of the hypersurface $\{x^a = c\}$ in $\mathcal{T}_{P_E}$. Furthermore, lemma 1 immediately implies that any two (distinct) hypersurfaces of this form must intersect precisely on the ambiguity locus. Thus π_a can not be identically 0 and we obtain that $\mathcal{N}$ is finite.

Now assume that F has a root in the ambiguity locus. Then, by the Vanishing Theorem for Resultants and what we've just learned about the hypersurface $\{x^a = c\}$, π_a must be divisible by infinitely many distinct binomials of the form $u_+ + cu_-$. So the existence of a root of F within the ambiguity locus implies that $\mathcal{N} = \infty$. Similarly, the existence of infinitely many roots of F within $(K^*)^n$ implies that $\mathcal{N} = \infty$ as well. Thus we are done with the first portion of the theorem.

As for the codimension of the space of "degenerate" F being ≥ 2, first consider the F which have a root on the ambiguity locus. These F actually form a codimension 2 subvariety. To see this, first note that F has a root in $O_w \Longleftrightarrow$ the initial term system $\mathrm{in}_w(F)$ has a root in $(K^*)^n$ [Roj97a, corollary 2]. By the definition of $L(E,a)$, we can then conclude via theorem 1.3 of [Stu94]. (Although the results of [Stu94] are stated over the complex numbers, this is only a minor technicality: in this case, the results of [Roj97a] immediately imply that we can apply theorem 1.3 over *any* algebraically closed field.)

As for the F with infinitely many roots in $(K^*)^n$, assume temporarily that the coefficients of F are algebraically independent indeterminates. That the F with infinitely many roots in $(K^*)^n$ define a subvariety of codimension ≥ 2 must certainly be an old result. However, for completeness, we will give a quick proof: Following the notation of lemma 3, Hilbert's Irreducibility Theorem [Lan83] readily implies that we can choose $\alpha, \beta, \gamma, \delta \in K^*$ such that the polynomials $p(\alpha, \beta)$ and $p(\gamma, \delta)$ are relatively prime in $K[\mathcal{C}_E]$. So, by lemma 3, these F are indeed contained in a codimension 2 subvariety: $\{\mathcal{C}_E \mid p(\alpha,\beta)=q(\gamma,\delta)=0\}$. ■

So in summary, computing π_a amounts to laminating $\mathcal{T}_{P_E}$ with hypersurfaces of the form $\overline{\{c_+ x^a = c_-\}}$. These laminae all intersect at the ambiguity locus, and toric infinity is precisely the union of the two degenerate laminae corresponding to (cf. remark 3) the $\pm$ halves of ∂P_E.

Proof of Theorem 1 and Corollary 1: We need only state the preceding paragraph more algebraically. In particular, lemma 2 has already done this for us. We thus obtain that when $\mathcal{N} < \infty$, the multiplicity of a factor $c_+ u_+ + c_- u_-$ of π_a is precisely the sum of the intersection numbers of the components of $\mathcal{D}_{P_E}(F, \mathcal{P}_E)$ lying in the fiber $\bar{\varphi}^{-1}([c_- : c_+])$. So $\mathcal{N}$ (resp. $\mathcal{N}'$) is indeed the exact number of roots, counting multiplicities (resp. *not* counting multiplicities), of F in $(K^*)^n$. ■

Note that it is actually possible for a positive-dimensional component of $\mathcal{D}_{P_E}(F, \mathcal{P}_E)$ lying at toric infinity to make a positive (finite) contribution to $\mathcal{N}$ (or $\mathcal{N}'$). This can be interpreted as an alternative way of associating an intersection number to an excess component [Ful84].

6. Toric Generalized Characteristic Polynomials

We will first comment briefly on the combinatorial preprocessing step. The following example illustrates a simple fundamental case.

Example 3 (The "Dense" Case). *Suppose $\mathcal{P}$ is the n-tuple $(d_1\Delta, \ldots, d_n\Delta)$ where $\Delta \subset \mathbb{R}^n$ is the standard n-simplex and $d_i \in \mathbb{N}$ for all i. It is then easily verified that the n-tuple $D := (\{\mathbf{O}, d_1\hat{e}_1\}, \ldots, \{\mathbf{O}, d_n\hat{e}_n\})$ is an irreducible fill of $\mathcal{P}$* [Roj94, Sch94]. *Letting A be the vertices of Δ, theorem 3 then implies that $\mathcal{H}$ is a variant (over a general algebraically closed field) of the original GCP applied to an $n \times n$ system of equations with degrees $d_1, \ldots, d_n$* [Can90]. *In particular, our $F - sF^*$ has $2n$ s-monomials, compared to n s-monomials in Canny's $(f_1 - sx_1^{d_1}, \ldots, f_n - sx_n^{d_n})$. Note also that* $\mathrm{Conv}(A)$ *and P are homothetic and $\mathcal{T}_P \cong \mathbb{P}^n_K$. Neglecting the extra s-monomials, setting $d_i = 1$ for all i, and suitably specializing the coefficients of g, we can then recover the usual characteristic polynomial of a matrix.*

We point out that the computational complexity of finding an irreducible fill is an open question. However, the connection between fills and polynomial system solving (not to mention specialized resultants) appears to be new and, we hope, provides added incentive to investigate filling. Also, even if finding a fill is difficult, this step need only be done *once* for a given family of problems, provided E remains fixed. The situation where the monomial term structure of a polynomial system is fixed once and for all (and the coefficients may vary thousands of times) actually occurs frequently in many practical contexts, such as robot control or computational geometry.

In any event, the toric GCP is an algebraic perturbation method and irreducible fills provide a combinatorial means of inducing "general position" into the roots of $\mathcal{F}_A$. For example, the following lemma implies that F^* is sufficiently generic in a useful sense.

Lemma 4. *Following the notation and assumptions of theorem 3, for any point v lying in any D_i, there exists a $w \in \mathbb{R}^n \setminus \{\mathbf{O}\}$ such that $\{i\}$ is the unique essential subset of D^w and $D_i^w = \{v\}$. In particular, F^* has exactly $\mathcal{M}(\mathcal{P})$ roots (counting multiplicities) in $(K^*)^n$.* ■

This lemma follows easily from the techniques of [Roj94], particularly section 2.5.

Given that F^* thus has maximally many isolated roots (counting multiplicities) and *no* excess components in $(K^*)^n$, theorem 3 then follows easily from the Vanishing Theorem for Resultants and an algebraic homotopy argument. A similar homotopy technique appears in [RW96, Roj97a], and the dense case (with $K = \mathbb{C}$) is covered in [Can90, Shu93]. (However, toric variety language was not used in the last two works.) Thus, the usual GCP is (almost) the special case of the toric GCP where $\mathcal{T}_P$ is complex projective space.

In closing, an important difference to note is that our present toric GCP is primarily suited for $(K^*)^n$, while the original GCP is mainly suited (in a non-sparse way) for affine space. To *completely* generalize and improve the GCP in affine space, it is necessary to use the *affine* sparse resultant and this is pursued further in [Roj97e]. For instance, by replacing the sparse resultant with the affine sparse resultant, and using K^n*-counting* [Roj97a] instead of filling, we can actually recover Canny's GCP in the dense case.

7. Acknowledgements

The main results of this paper were presented during a visit of the author at City University of Hong Kong. The author thanks Steve Smale for his invitation, warm hospitality, and even warmer beach hikes. Special thanks go to John Dalbec for pointing on an error in an earlier version of section 3, and to Robert L. Williams for his encouragement and keen commentary. The author also thanks his former roommates Jean-Pierre Dedieu and Gregorio Malajovich for their input, but most of all for not getting too mad at him for not washing the dishes.

Work on this paper began at MSRI and concluded at MIT. The author thanks both institutions for their support, and especially Marsh Borg at MSRI for her kind assistance.

References

[BPR94] Basu, S., Pollack, R., and Roy, M.-F., *"On the Combinatorial and Algebraic Complexity of Quantifier Elimination,"* in Proc. IEEE Symp. Foundations of Comp. Sci., Santa Fe, New Mexico, 1994, to appear.

[Can90] Canny, John F., *"Generalised Characteristic Polynomials,"* J. Symbolic Computation (1990) 9, pp. 241–250.

[CS86] Cornell, Gary and Silverman, Joseph H., *Arithmetic Geometry,* with contributions by M. Artin, et. al., Springer-Verlag, 1986.

[Dan78] Danilov, V. I., *"The Geometry of Toric Varieties,"* Russian Mathematical Surveys, 33 (2), pp. 97–154, 1978.

[DGH96] Dyer, M., Gritzmann, P., and Hufnagel, A., *"On the Complexity of Computing Mixed Volumes,"* SIAM J. Comput., to appear (1996).

[DS95] Dalbec, John, and Sturmfels, Bernd, *"Introduction to Chow Forms,"* Invariant Methods in Discrete and Computational Geometry (Curaçao, 1994), pp. 37–58, Kluwer Academic Publishers, Dordrecht, 1995.

[EC95] Emiris, Ioannis Z. and Canny, John F., *"Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume,"* Journal of Symbolic Computation, vol. 20 (1995), pp. 117–149.

[Emi94] Emiris, Ioannis Z., *"Sparse Elimination and Applications in Kinematics,"* Ph.D. dissertation, Computer Science Division, U. C. Berkeley (December, 1994), available on-line at `http://www.inria.fr/safir/SAFIR/Ioannis.html`

[Emi96] ________, *"On the Complexity of Sparse Elimination,"* preprint, INRIA, March 1996, available on-line at `http://www.inria.fr/safir/SAFIR/Ioannis.html`

[Ful84] Fulton, William, *Intersection Theory,* Springer-Verlag, 1984.

[Ful93] ________, *Introduction to Toric Varieties*, Annals of Mathematics Studies, no. 131, Princeton University Press, Princeton, New Jersey, 1993.

[GHMP95] Giusti, M., Heintz, J., Morais, J. E., Pardo, L. M., *"When Polynomial Systems Can Be 'Solved' Fast?,"* Proc. $11^{\underline{\text{th}}}$ International Symposium, AAECC-11, Paris, France, July 17-22, 1995, G. Cohen, M. Giusti and T. Mora, eds., Springer LNCS 948 (1995) pp. 205–231.

[GKP94] Graham, R. L., Knuth, D. E., and Patashnik, O., *Concrete Mathematics: A Foundation for Computer Science*, $2^{\underline{\text{nd}}}$ edition, Addison-Wesley, 1994.

[GKZ90] Gel'fand, I. M., Kapranov, M. M., and Zelevinsky, A. V., *"Discriminants of Polynomials in Several Variables and Triangulations of Newton Polytopes,"* Algebra and Analysis (translated from Russian) 2, pp. 1–62, 1990.

[GKZ94] ________, *Discriminants, Resultants and Multidimensional Determinants,* Birkhäuser, Boston, 1994.

[GLRR94] Gonzalez, L., Lombardi, H., Recio, T., Roy, M.-F., *"Sturm-Habicht Sequence, Determinants and Real Roots of Univariate Polynomials,"* Quantifier Elimination and Cylindrical Algebraic Decomposition, Texts and Monographs in Symbolic Computation, B. Caviness and J. Johnson, Eds., Springer-Verlag, Wien, New York, 1994, to appear.

[HS96] Huber, Birkett and Sturmfels, Bernd, *"Bernshtein's Theorem in Affine Space,"* Discrete and Computational Geometry, to appear, 1996.

[Jon82] Jones, James P., *"Universal Diophantine Equation,"* Journal of Symbolic Logic, 47 (3):549–571.

[Kho77] Khovanskii, A. G., *"Newton Polyhedra and Toroidal Varieties,"* Functional Anal. Appl., 11 (1977), pp. 289–296.

[Kho78] ________, *"Newton Polyhedra and the Genus of Complete Intersections,"* Functional Analysis (translated from Russian), Vol. 12, No. 1, January–March (1978), pp. 51–61.

[KL92] Kapur, Deepak and Lakshman, Yagati N., *"Elimination Methods: an Introduction,"* Symbolic and Numerical Computation for Artificial Intelligence, B. Donald et. al. (eds.), Academic Press, 1992.

[KKMS73] Kempf, G., Knudsen, F., Mumford, D., Saint-Donat, B., *Toroidal Embeddings I*, Lecture Notes in Mathematics 339, Springer-Verlag, 1973.

[KSZ92] Kapranov, M. M., Sturmfels, B., and Zelevinsky, A. V., *"Chow Polytopes and General Resultants,"* Duke Mathematical Journal, Vol. 67, No. 1, July, 1992, pp. 189–218.

[Kus75] Kushnirenko, A. G., *"A Newton Polytope and the Number of Solutions of a System of k Equations in k Unknowns,"* Usp. Matem. Nauk., 30, No. 2, pp. 266–267 (1975).

[Lan83] Lang, Serge, *Fundamentals of Diophantine Geometry,* Springer-Verlag, 1983.

[Laz81] Lazard, D. *"Résolution des Systèmes d'équations Algébriques,"* Theor. Comp. Sci. 15, pp. 146–156.

[LLL82] Lenstra, A. K., Lenstra, H. W., and Lovász, L. *"Factoring Polynomials with Rational Coefficients,"* Math. Ann. **261** (1982), pp. 515-534.

[Mat93] Matiyasevich, Yuri V., *Hilbert's Tenth Problem,* MIT Press, MIT, Cambridge, Massachusetts, 1993.

[PK95] Pardo-Vasallo, Luis-Miguel and Krick, Teresa, *"A Computational Method for Diophantine Approximation,"* to appear in Proc. MEGA '94, Birkhäuser, Progress in Math. (1995).

[PS93] Pedersen, P. and Sturmfels, B., *"Product Formulas for Sparse Resultants and Chow Forms,"* Mathematische Zeitschrift, 214: 377–396, 1993.

[Ren87] Renegar, Jim, *"On the Worst Case Arithmetic Complexity of Approximating Zeros of Systems of Polynomials,"* Technical Report, School of Operations Research and Industrial Engineering, Cornell University.

[Roj94] Rojas, J. Maurice, *"A Convex Geometric Approach to Counting the Roots of a Polynomial System,"* Theoretical Computer Science (1994), vol. 133 (1), pp. 105–140.

[Roj97a] ________________, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, to appear. (Also available on-line at `http://www-math.mit.edu/~rojas` .)

[Roj97b] ________________, *"A New Approach to Counting Nash Equilibria,"* Proceedings of the Conference on Computational Intelligence for Financial Engineering, Manhattan, New York, March 23–25, 1997, to appear.

[Roj97c] ________________, *"Toric Generalized Characteristic Polyomials,"* submitted to the Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation. (Also available on-line at `http://www-math.mit.edu/~rojas`.)

[Roj97d] ________________, *"When do Resultants Really Vanish? Applications to Diophantine Complexity,"* preprint, MIT (1997).

[Roj97e] ________________, *"Affine Elimination Theory and Solving Certain Diophantine Systems Quickly,"* preprint, MIT (1997).

[Roy95] Roy, Marie-Françoise *"Basic Algorithms in Real Algebraic Geometry and their Complexity: from Sturm Theorem to the Existential Theory of Reals,"* preprint, IRMAR, Rennes, France, 1995.

[RW96] Rojas, J. M., and Wang, Xiaoshen, *"Counting Affine Roots of Polynomial Systems Via Pointed Newton Polytopes,"* Journal of Complexity, vol. 12, June (1996), pp. 116–133, also available on-line at `http://www-math.mit.edu/~rojas`.

[Sch94] Schneider, Rolf, *Convex Bodies: The Brunn-Minkowski Theory,* Encyclopedia of Mathematics and its Applications, v. 44, Cambridge University Press, 1994.

[Shu93] Shub, Mike, *"Some Remarks on Bézout's Theorem and Complexity Theory,* From Topology to Computation: Proceedings of the Smalefest, pp. 443–455, Springer-Verlag, 1993.

[Stu93] Sturmfels, Bernd, *"Sparse Elimination Theory,"* In D. Eisenbud and L. Robbiano, editors, Proc. Computat. Algebraic Geom. and Commut. Algebra 1991, pages 377–396, Cortona, Italy, 1993, Cambridge Univ. Press.

[Stu94] ______________, *"On the Newton Polytope of the Resultant,"* Journal of Algebraic Combinatorics, 3: 207–236, 1994.
[Stu95] ______________, *Gröbner Bases and Convex Polytopes,* Lectures presented at the Holiday Symposium at New Mexico State University, December 27–31, 1994.
[Zie95] Ziegler, Gunter M., *Lectures on Polytopes,* Graduate Texts in Mathematics 152, Springer-Verlag, New York, 1995.
[Zip93] Zippel, R., *Effective Polynomial Computation,* Kluwer Academic Publishers, Boston, 1993.

Massachusetts Institute of Technology, Mathematics Department, 77 Mass. Ave., Cambridge, MA 02139, U.S.A.