TORIC GENERALIZED CHARACTERISTIC POLYNOMIALS

J. MAURICE ROJAS

ABSTRACT. We illustrate an efficient new method for handling polynomial systems with degenerate solution sets. In particular, a corollary of our techniques is a new algorithm to find an isolated point in every excess component of the zero set (over an algebraically closed field) of any n by n system of polynomial equations. Since we use the sparse resultant, we thus obtain complexity bounds (for converting any input polynomial system into a multilinear factorization problem) which are close to cubic in the degree of the underlying variety — significantly better than previous bounds which were pseudo-polynomial in the classical Bézout bound. By carefully taking into account the underlying toric geometry, we are also able to improve the reliability of certain sparse resultant based algorithms for polynomial system solving.

1. INTRODUCTION

The rebirth of resultants, especially through the **toric**[1] resultant [GKZ94], has begun to provide a much needed alternative to Gröbner basis methods for solving polynomial systems. Continuing this philosophy, we will present a new, fast and reliable, resultant-based method for handling certain degenerate polynomial systems. Simply put, we refine and generalize the **generalized characteristic polynomial** (GCP) [Can90, Shu93] to take **sparsity** into account. Furthermore, we introduce the concept of a **twisted Chow form** in order to completely avoid any degeneracies within our algorithm.

The importance of dealing with degenerate polynomial systems has been observed in earlier work on quantifier elimination over algebraically closed fields [CG84, Ren87, Can88]: Many reasonable algorithms fail catastrophically when presented with an n by n system having positive-dimensional zero set. When such is the case, it is of considerable benefit to the user to at least be given some sort of description of the zero-dimensional part of the zero set. This was a benefit of Canny's original GCP, but he remarked [Can90, pg. 242] "For large, dense problems however, the resultant and GCP methods should be faster [than Gröbner algorithms]." Our construction,

Date: February 10, 1997.

This research was completed at MIT and was partially funded by an N.S.F. Mathematical Sciences Postdoctoral Fellowship. Research at MSRI is supported in part by NSF grant DMS-9022140.

[1]Other commonly used prefixes for this more modern generalization include: sparse, mixed, $\mathcal{A}$-, and $(\mathcal{A}_1, \ldots, \mathcal{A}_k)$-.

the **toric GCP**, promises to be much more competitive when applied to **sparse** systems in such a comparison.

Remark 1. *It should be emphasized that perturbation methods for degenerate systems (such as the toric GCP) are of the greatest importance when working with* **exact** *arithmetic. However, floating point polynomial system solving also benefits from a complete and rigourous understanding of the potential degeneracies within exact arithmetic, e.g.,* [Sma87]. *In any case, it is frequently the case in many applications that "real life" happens to land in a measure* 0 *exception which breaks an algorithm.*

In what follows, we will frequently use multi-index notation in order to precisely control which monomial terms are allowed to appear in our polynomial systems.[2] This notation, and in particular, **supports** and **Newton polytopes**, are amply detailed in earlier works of Emiris [Emi94], Huber [Hub96], Gelfand et. al. [GKZ90, GKZ94], Rojas [Roj94, Roj97b], Sturmfels [Stu93], and Verschelde [Ver96], to mention but a few authors and references.

Since what we will present is at heart a perturbation method, we will first need the following definition to construct certain polynomial systems in "general position."

Definition 1. [Roj94, RW96] *Given n-tuples $D:=(D_1,\ldots,D_n)$ and $E:=(E_1,\ldots,E_n)$ of nonempty finite subsets of $\mathbb{Z}^n$, we say that D* **fills** *E iff (0) $D_i\subseteq E_i$ for all $i\in[n]$ and (1) $\mathcal{M}(D)=\mathcal{M}(E)$. An* **irreducible** *fill is then simply a fill which is minimal with respect to n-tuple containment. If D or E is instead an n-tuple of polytopes in $\mathbb{R}^n$, then we will use the same definition.*

In the above, $\mathcal{M}(E)$ denotes the **mixed volume** [BZ88, Sch94, EC95, DGH96] of the convex hulls of the E_i, and we use $[j]$ for the set of integers $\{1,\ldots,j\}$.

Our construction is summarized in the following definition and main result. (Henceforth, all of our polynomials and roots are to be considered over an algebraically closed field K.)

Definition 2. *Suppose F is an $n\times n$ polynomial system with support contained in E and $g(x):=\sum_{e\in A} u_e x^e$, where the u_e are algebraically independent indeterminates and $A\subset\mathbb{Z}^n$ is nonempty and finite. Assume further that $\mathcal{M}(E)>0$ and A has at least two elements. Letting D be an irreducible fill of E, $F^*:=(\sum_{e\in D_i} x^e \mid i\in[n])$, and $u:=(u_e\mid e\in A)$, define $\mathbf{Ch}_A(u):=\mathrm{Res}_{(E,A)}(F,g)$ and $\boldsymbol{\mathcal{H}}(u;s):=\mathrm{Res}_{(E,A)}(F-sF^*,g)$, where s is a new indeterminate. We call $\mathcal{H}$ a* **toric generalized characteristic polynomial for $(\mathbf{F},\mathbf{A})$.**

In the above, $\mathrm{Res}_\star(\cdot)$ denotes the toric resultant. Recall also that to any n-dimensional rational polytope $P\subset\mathbb{R}^n$ one can associate its corresponding **toric variety** $\mathcal{T}_P$ [Dan78, KSZ92, Ful93, Roj97b].

[2]This is what we mean by sparsity, as opposed to working solely in terms of polynomial degrees. Note that our notion overlaps the case of having very few monomial terms.

Main Theorem. *Following the notation of definition 2, consider $\mathcal{H}$ as a polynomial in s with coefficients in $K[u]$ and let $\boldsymbol{\mathcal{F}}_A(u)$ be the coefficient of the lowest degree term of $\mathcal{H}$. Also let $P := \sum_{i=1}^n \mathrm{Conv}(E_i)$, $\widetilde{P} := P + \mathrm{Conv}(A)$, and $\varphi : \mathcal{T}_{\widetilde{P}} \longrightarrow \mathbb{P}_K^{|A|-1}$ the natural morphism defined by $x \mapsto [x^e \mid e \in A]$ (cf. section 4). Then $\mathcal{F}_A$ is a homogeneous polynomial, of degree $\mathcal{M}(E)$, with the following properties:*

0. *The constant term of $\mathcal{H}(s)$ is precisely Ch_A. In particular, letting Z be the zero set of F in $\mathcal{T}_{\widetilde{P}}$, $\mathrm{Ch}_A \equiv 0 \iff \varphi(Z)$ is positive-dimensional.*
1. *If $\zeta \in \mathcal{T}_{\widetilde{P}}$ is an isolated root of F then $\mathcal{F}_A$ is divisible by $\sum_{e\in A} c_e u_e$, where $[c_e \mid e \in A] = \varphi(\zeta)$.*
2. *If a nonzero linear form $\sum_{e\in A} c_e u_e$ divides $\mathcal{F}_A$ then $[c_e \mid e\in A] = \varphi(\zeta)$ for* **some** *root $\zeta \in \mathcal{T}_{\widetilde{P}}$ of F.*
3. *$\mathcal{F}_A$ splits completely into linear factors. In particular, under the correspondence of (2), we can explicitly find at least one root of F within every positive-dimensional irreducible component of the zero set of F in $\mathcal{T}_{\widetilde{P}}$.*

We call $\mathcal{F}_A$ a **toric perturbation** *of Ch_A.*

A complete criterion for finding fills is given in theorem 1 of section 3 and some simple examples of filling (and our Main Theorem) appear in section 2. Compatibility is defined in section 4. There we also detail what is meant by the zero set of F in a toric variety.

Remark 2. *Alternatively, if one wants to avoid filling, one can substitute for F^* any polynomial system (with support contained in E)* **known** *to have exactly $\mathcal{M}(E)$ roots (counting multiplicities) in $(K^*)^n$. So one can also view filling as a deterministic way of explicitly constructing a "generic" polynomial system.*

So how does one actually use the above theorem? One simple example is the **sparse u-resultant** [Emi94], which is simply a variant of the classical u-resultant [Van50]. It can be defined simply as $\mathrm{Ch}_A(u)$ where A is the vertex set of the standard n-simplex in $\mathbb{R}^n$. One useful (and easily verified) property of the sparse u-resultant is that F has a root $\zeta := (\zeta_1, \ldots, \zeta_n) \in (K^*)^n \implies u_0 + \zeta_1 u_1 + \cdots + \zeta_n u_n$ divides $\mathrm{Ch}_A(u)$. So, assuming $\mathrm{Ch}_A(u)$ is not identically 0 (and that one has good software for toric resultants and multivariate factoring), one can find the isolated roots of F simply by factoring $\mathrm{Ch}_A(u)$. Thus the degenerate instances $\mathrm{Ch}_A(u) \equiv 0$ obstruct this reduction to factoring and our Main Theorem allows us to avoid this problem: Simply use $\mathcal{F}_A(u)$ instead of $\mathrm{Ch}_A(u)$.

Remark 3. *An interesting "failure" for the classical u-resultant is the case where F has only finitely many roots in affine space, while having infinitely many in projective space. This is where the classical GCP is especially handy. For the toric GCP, the toric variety $\mathcal{T}_P$ plays the role of projective space. This is part of the philosophy of sparse elimination theory: working in a well chosen toric compactification (depending on F) leads to better algorithms than if one were to work only in projective space.*

In particular, **lifting** *to $\mathcal{T}_{\tilde{P}}$ helps us detect precisely when the sparse u-resultant is identicaly* 0.

However, there is a stickier subtlety which occurs with the sparse u-resultant: It is possible for F to have only finitely many roots within $\mathcal{T}_P$ with $\mathrm{Ch}_A(u)$ **still** vanishing identically (cf. section 2.3). This is the motivation for **twisted Chow forms**, which are defined below, and pursued at much greater length in [Roj97c].

Corollary and Definition 3 (cf. section 4)**.** *Following the notation of our Main Theorem, pick A to be the vertices of a product of simplices with which P is compatible. We then call* $\mathrm{Ch}_A(u)$ *the* **twisted Chow form** *of the zero set of F* **with respect to** *A. Furthermore, a twisted Chow form does* **not** *vanish identically if F has only finitely many roots in $\mathcal{T}_P$.* □

In particular, since our last construction implies that $\mathcal{T}_{\mathrm{Conv}(A)}$ is a product of **twisted** projective spaces [Ful93], the coefficients of a twisted Chow form are actually multisymmetric functions [DS95, Roj97a] of projections (by φ) of roots of F (in $\mathcal{T}_P$) onto this product. So twisted Chow forms generalize the u-resultant, the sparse u-resultant, and (suitably extended [Roj97c]) the Chow form of a projective variety [DS95]. Moreover, when combined with the **Smith normal form** [Ili89, HM91, HS95] and the toric GCP, twisted Chow forms give a considerably more reliable method for solving polynomial systems than the sparse u-resultant [Roj97c].

An important difference to note is that our present toric GCP is primarily suited for finding roots in $(K^*)^n$, 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** [Roj97b] instead of filling, we can actually recover Canny's GCP in the dense case.

We close this introduction with a word on the computational complexity of computing the toric GCP. Neglecting preprocessing (finding an irreducible fill and finding a mixed subdivision in order to set up the toric resultant matrices [EC95]), recent work of Emiris, Morrain, and Pan [EP97, MP97] suggests that it is possible to find the perturbation $\mathcal{F}_A$ within a number of arithmetic steps[3] which is close to **cubic** in $\mathcal{M}(E)$. (Indeed, Canny has pointed out [Can90] that the original GCP can be computed in time close to cubic in the Bézout bound, which would be a special case of time cubic in $\mathcal{M}(E)$.) Since $\mathcal{M}(E)$ is much smaller than the Bézout number for most polynomial systems [Roj94, Roj97b], these preliminary results suggest that the toric GCP has considerable potential for practical applications.

Let us now illustrate some of our theory.

[3]Although the possibility of "near-quadratic" algorithms for polynomial system solving is discussed in [EP97, MP97], neither paper discusses the case where the zero set of F is positive-dimensional, which is our main concern here.

2. Examples

We begin with two small examples of filling. We then see applications of the toric GCP to some degenerate 2×2 and 3×3 polynomial systems. Finally, we see a brief comparison of the toric GCP to the original GCP.

2.1. **Filling Squares and Cubes.** For our first example, consider the pair of rectangles $\mathcal{P}:=([0,a]\times[0,b],[0,c]\times[0,d])$ where a, b, c, and d are positive integers. Then it is easily verified (via theorem 1 of section 3) that the pair

$$D:=(\{(0,0),(a,b)\},\{(0,d),(c,0)\})$$

fills $\mathcal{P}$. In this case, the mixed area of both pairs is easily checked to be $ad+bc$. Note also that D is a pair of oppositely slanting diagonals of our initial pair of rectangles (modulo taking convex hulls). Finally, it is easily checked that D is indeed irreducible, since the removal of any point of D results in a mixed area of 0.

For our second example, let $\mathcal{P}$ instead be a triple of standard cubes (so that the vertex set of each cube is simply $\{0,1\}^3$). Then, using the criterion from theorem 1 once again, it is easily verified that the triple

$$D:=(\{(0,0,0),(1,1,1)\},\{(1,0,0),(0,1,0),(0,0,1)\},\{(1,1,0),(1,0,1),(0,1,1)\})$$

fills $\mathcal{P}$. Also, it is easily checked that the mixed volume of both triples is 6. Note that the triple D consists of a body diagonal and two oppositely oriented (but parallel) sub-triangles of the unit cube, modulo taking convex hulls. Finally, note that this D is irreducible as well by theorem 1. (This is also easily checked by one of the publically available software packages for mixed volume by Emiris, Huber, or Verschelde.)

2.2. **A Degenerate 2×2 System.** Consider the bivariate polynomial system $F:=(1+2x-2x^2y-5xy+x^2+3x^3y, 2+6x-6x^2y-11xy+4x^2+5x^3y)$. Letting E be the support of F, the reader can easily verify that $\mathcal{M}(E)=4$, and that the only roots of F are the points $\{(1,1),(\frac{1}{7},\frac{7}{4})\}$ and the line $\{-1\}\times K$ (assuming $\mathrm{char} K\neq 2$).[4] So it would appear that the u-resultant (and even the sparse u-resultant) will vanish identically and not give us any useful information about any of these roots. Let us see if perturbing the sparse u-resultant helps...

Note that by theorem 1, $D:=(\{\mathbf{O},(3,1)\},\{(1,1),(2,0)\})$ is an irreducible fill of E. So applying our Main Theorem with this D (and $A:=\{(0,0),(1,0),(0,1)\}$) one can compute with the use of `Maple` that $\mathcal{H}(u;s)$ is precisely

$$(u_2^4-u_0^4+u_1^4+6u_1^2u_2^2-4u_1u_2^3-4u_1^3u_2)\mathbf{s^8}$$

$$+(-20u_2u_0^3-20u_2^3u_0-4u_1u_0^3+36u_1^2u_2^2-19u_0^4-24u_2^4+6u_0^2u_1u_2$$

$$+36u_1u_2^3+36u_1^4-12u_0u_1^2u_2-9u_1^2u_0^2+3u_2^2u_0^2+36u_0u_1u_2^2-4u_0u_1^3-84u_1^3u_2)\mathbf{s^7}$$

$$+(-170u_2u_0^3-394u_1^3u_2-98u_1u_0^3-98u_0^2u_1u_2-20u_0^4+220u_2^4+370u_2^3u_0$$

[4] When $\mathrm{char} K=2$, the second isolated root becomes an isolated root lying on the x-axis.

$$+14u_0u_1u_2^2 - 110u_0u_1^3 - 226u_1^2u_0^2 - 354u_1^2u_2^2 + 454u_1^4 - 274u_0u_1^2u_2 + 74u_1u_2^3)\mathbf{s^6}$$

$$+(-1612u_0^2u_1u_2 + 1008u_2u_0^3 + 903u_0^4 - 624u_1u_0^3 - 2632u_2^3u_0 - 2104u_0u_1^2u_2 - 970u_2^4$$

$$-1010u_1u_2^3 + 418u_1^3u_2 - 2104u_0u_1u_2^2 - 642u_1^2u_2^2 - 1547u_1^2u_0^2 - 936u_0u_1^3 - 1557u_2^2u_0^2 + 2204u_1^4)\mathbf{s^5}$$

$$+(538u_0^2u_1u_2 + 1271u_0^4 + 12253u_2^2u_0^2 + 6972u_2u_0^3 + 1929u_1^4 - 3075u_1^2u_2^2 + 654u_0u_1u_2^2$$

$$+50u_1u_0^3 + 2156u_2^4 - 960u_1^2u_0^2 - 2290u_0u_1^3 + 132u_1u_2^3 - 5344u_0u_1^2u_2 - 1142u_1^3u_2 + 8708u_2^3u_0)\mathbf{s^4}$$

$$+(4384u_1u_0^3 - 24988u_2^2u_0^2 - 1582u_1^3u_2 - 6756u_0^4 + 10884u_0u_1u_2^2 + 3802u_1u_2^3 + 15438u_0u_1^2u_2$$

$$+1024u_0u_1^3 + 8324u_1^2u_0^2 - 12826u_2^3u_0 + 11270u_0^2u_1u_2 - 6976u_1^4 + 7164u_1^2u_2^2 - 21326u_2u_0^3 - 2408u_2^4)\mathbf{s^3}$$

$$+(3436u_1^3u_2 + 3800u_0u_1^3 + 7756u_2^3u_0 - 3886u_1u_2^3 + 1225u_2^4 + 17059u_2^2u_0^2 - 5984u_1^2u_0^2$$

$$+15708u_2u_0^3 - 12232u_0u_1u_2^2 + 5180u_0^4 - 2091u_1^2u_2^2 - 6828u_0u_1^2u_2 + 1316u_1^4 - 12700u_0^2u_1u_2 - 4312u_1u_0^3)\mathbf{s^2}$$

$$+(-196u_2^4 - 448u_0^4 - 768u_1^3u_2 + 512u_1^2u_0^2 - 1288u_2^3u_0$$

$$-2436u_2^2u_0^2 + 1920u_0u_1u_2^2 + 1536u_0^2u_1u_2 + 1024u_0u_1^2u_2$$

$$+384u_1u_0^3 - 1792u_2u_0^3 - 384u_0u_1^3 + 768u_1u_2^3 + 260u_1^2u_2^2 - 64u_1^4)\underline{\mathbf{s}}.$$

(Sparse resultants of this size are quite amenable with the aid of `Maple`, following the technique of a similar computation in [Roj97a].) So our $\mathcal{F}_A$ is just the coefficient of s or s^2 in this polynomial, according as $\mathrm{char} K \neq 2$ or $\mathrm{char} K = 2$. To simplify our discussion, let us henceforth assume the former possibility.

Factoring with `Maple`, we obtain that $\mathcal{F}_A$ can be written as follows:

$$-4(u_0 + u_1 + u_2)(28u_0 + 4u_1 + 49u_2)(u_0 - u_1 + u_2)(4u_0 - 4u_1 + u_2)$$

In particular, given any factor above, the ratio of the coefficients of u_i and u_0 is precisely the $i^{\underline{\text{th}}}$ coordinate of a corresponding root of F. Thus the first two factors correspond precisely to the two isolated roots we already know. As for the last two factors, note that they both give isolated points lying on the aforementioned line $\{-1\} \times K$. This can be interpreted as assigning an **excess intersection multiplicity** of 2 to the line, so that the sum of all intersection numbers (of the irreducible components of the zero set of F in $\mathcal{T}_{\tilde{P}}$) is 4.

Note that the original GCP could have been used above but would have resulted in a u-form of degree 16 (the product of the degrees of f_1 and f_2). Also, the corresponding version of $\mathcal{H}(\cdot)$ is significantly larger, having 672 terms, compared to 110 for our above toric GCP.

2.3. **Stranger Degeneracies.** Here we give two examples showing how the sparse u-resultant can fail to find roots in $\mathcal{T}_P$, even with the benefit of the toric GCP, unless some other construction (such as a twisted Chow form) is used.

First consider the parameterized bivariate system $F := (a_1 y + a_2 x + a_3 xy, b_1 y + b_2 x + b_3 xy)$. Note that the mixed volume bound for this system is 1. The sparse u-resultant for this system is also easily found (using the same techniques as in our last example) to be:

$$\begin{aligned} & (a_3^2 b_2 b_1 + b_3^2 a_2 a_1 - b_3 a_2 a_3 b_1 - b_3 a_3 b_2 a_1) u_0 \\ + \quad & (b_1^2 a_2 a_3 - b_1 b_3 a_2 a_1 - b_2 a_1 a_3 b_1 + b_2 b_3 a_1^2) u_1 \\ + \quad & (b_1 b_3 a_2^2 - b_2 a_2 a_3 b_1 + b_2^2 a_3 a_1 - b_2 b_3 a_2 a_1) u_2 \end{aligned}$$

In particular, we see that when

$$(a_1, a_2, a_3, b_1, b_2, b_3) = (0, 1, 2, 0, 1, 3).$$

the sparse u-resultant vanishes identically. For this specialization, it is also easy to see that F has only **one** root in $\mathcal{T}_P$, and this root lies at the point of $\mathcal{T}_P$ corresponding to the vertex $(0,1)$ of P (cf. lemma 1 from section 4), following the notation of our Main Theorem. In fact, for this P, $\mathcal{T}_P \cong \mathbb{P}^2_K$ and the vertex $(0,1)$ corresponds precisely to the point $[x : y : z] = [1 : 0 : 0]$ in this particular copy of $\mathbb{P}^2_K$ (z denoting an extra variable for homogenizing).

There are two ways of viewing this degeneracy ($\mathrm{Ch}_A(u) \equiv 0$ while F has only finitely many roots in $\mathcal{T}_P$) of the sparse u-resultant. The first is pragmatic: One should not count this as a deficiency of the sparse u-resultant because we've cheated and set two of the coefficients of F to 0, thus changing the supports. (Our next example avoids this trick.) The second point of view is more geometric: By our Main Theorem, this particular sparse resultant **must** vanish due to the fact that our specialization of F results in the existence of infinitely many roots of F in $\mathcal{T}_{\widetilde{P}}$. In fact, F vanishes on the 1-dimensional subvariety of $\mathcal{T}_{\widetilde{P}}$ corresponding to the left-hand vertical edge of the hexagon $\widetilde{P}$ (cf. section 4).

Going one dimension higher, consider instead the 3×3 system G, consisting of the following polynomials:

$$\begin{gathered} a_1 yz + a_2 xz + a_3 xy + a_4 xyz \\ b_1 yz + b_2 xz + b_3 xy + b_4 xyz \\ c_1 yz + c_2 xz + c_3 xy + c_4 xyz \end{gathered}$$

Note that the mixed volume bound for this system is again 1.

Clearly, $\frac{1}{xyz} G$ is a linear system in $\{\frac{1}{x}, \frac{1}{y}, \frac{1}{z}\}$. So by Cramer's rule, we can express x, y, and z as ratios of 3×3 determinants in the coefficients. Combining this with the product formula for toric resultants [PS93] (and clearing denominators) we obtain that the sparse u-resultant of G is precisely[5]

$$[423][143][124]u_0 + [123][143][124]u_1 + [123][423][124]u_2 + [123][423][143]u_3$$

where the **bracket** $[ijk]$ [DS95] is the 3×3 subdeterminant

$$\begin{vmatrix} a_i & a_j & a_k \\ b_i & b_j & b_k \\ c_i & c_j & c_k \end{vmatrix}$$

of the coefficient matrix of G. This compactly expressed resultant can be thought of as a **semi-mixed** Chow form — a toric resultant of a semi-mixed system [HS95], compressed in terms of suitable brackets.

Now consider the specialization of G to

$$\begin{aligned} yz + xz + 2xy + 3xyz \\ yz + xz + 4xy + 9xyz \\ yz + xz + 8xy + 27xyz \end{aligned}$$

It is then easily verified that G has exactly one root in $\mathcal{T}_P \cong \mathbb{P}^3_K$:

$$[x : y : z : w] = [1 : -1 : 0 : 0]$$

(w denoting an extra variable for homogenizing).[6] More to the point, the sparse u-resultant vanishes identically for this specialization of G, even though G has no zero coefficients. Furthermore, one can easily check that the correspondence of (2) (from our Main Theorem) does **not** give us the root of G in $\mathcal{T}_P$. (Using $D := (\{(0,1,1),(1,1,1)\}, \{(1,0,1),(1,1,1)\}, \{(1,1,0),(1,1,1)\})$, the coefficients of the u_i in $\mathcal{F}_A$ suggest the nonsensical root $[0 : 0 : 5 : 21]$.)

To remedy this, we can use the twisted Chow form $\mathrm{Ch}_{A'}(u)$ with

$$A' := \{(0,1,1),(1,0,1),(1,1,0),(1,1,1)\}.$$

In particular, when the coefficients of G are unspecialized,

$$\mathrm{Ch}_{A'}(u) = \begin{vmatrix} a_1 & a_2 & a_3 & a_4 \\ b_1 & b_2 & b_3 & b_4 \\ c_1 & c_2 & c_3 & c_4 \\ u_{(0,1,1)} & u_{(1,0,1)} & u_{(1,1,0)} & u_{(1,1,1)} \end{vmatrix}$$

[5]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].

[6]If $\mathrm{char} K \in \{2,3\}$ then G will actually have infinitely many roots in $\mathcal{T}_P$. So let us assume henceforth that $\mathrm{char} K \notin \{2,3\}$. (It is easy to construct similar examples when $\mathrm{char} K \in \{2,3\}$ as well.)

So under our last specialization, this becomes $12u_{(1,0,1)} - 12u_{(0,1,1)}$. Thus the coordinates of the sole root of G in $\mathcal{T}_{\mathrm{Conv}(A')} \cong \mathbb{P}^3_K$ are precisely $[1 : -1 : 0 : 0]$. To conclude, by virtue of our (compatible) choice of A', the natural embeddings of $(K^*)^3$ into $\mathcal{T}_P$ and $\mathcal{T}_{\mathrm{Conv}(A')}$ are identical. This is how we've recovered our root in $\mathcal{T}_P$.

In closing, note that in practice we would never actually compute $\mathcal{H}(u; s)$ — we would instead recover $\mathcal{F}_A$ via rapid and sophisticated interpolation techniques, e.g., [Zip93]. In particular, our calculations can be sped up tremendously with suitably specialized code.

2.4. **The "Dense" Case.** Our last example illustrates a simple fundamental case.

Suppose E is the n-tuple $(d_1\Delta, \ldots, d_n\Delta)$ where $\Delta \subset \mathbb{R}^n$ is the vertex set of the standard n-simplex in $\mathbb{R}^n$ 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 E (cf. theorem 1). Letting $A = \Delta$, we see that our polynomial $\mathcal{H}$ is a variant (over a general algebraically closed field) of the original GCP applied to an $n \times n$ system of polynomials with degrees $d_1, \ldots, d_n$ [Can90]. In particular, our $F - sF^*$ has $2n$ s-monomials, compared to the 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.

3. Filling

Here we briefly recount filling and some related concepts. Some of the material below is covered at greater length in [Roj94]. The paper [Stu94] is also a useful reference but deals more with the sparse resultant than with filling. The results below form the basis for our combinatorial approach to perturbing degenerate polynomial systems.

Let $\mathcal{S}^{n-1} \subset \mathbb{R}^n$ denote the unit $(n-1)$-sphere centered at the origin. For any compact $B \subset \mathbb{R}^n$ and any $w \in \mathbb{R}^n$, define B^w to be the set of $x \in B$ where the inner-product $x \cdot w$ is minimized. (Thus B^w is the intersection of B with its supporting hyperplane in the direction w.) We then define $E^w := (E_1^w, \ldots, E_n^w)$ and $D \cap E^w := (D_1 \cap E_1^w, \ldots, D_n \cap E_n^w)$.

Recall that the **dimension** of any $B \subseteq \mathbb{R}^n$, $\dim B$, is the dimension of the smallest subspace of $\mathbb{R}^n$ containing a translate of B. The following definition is fundamental to our development.

Definition 4. *Suppose $C := (C_1, \ldots, C_n)$ is an n-tuple of polytopes in $\mathbb{R}^n$* **or** *an n-tuple of finite subsets of $\mathbb{R}^n$. We will allow any C_i to be empty and say that a nonempty subset $J \subseteq [n]$ is* **essential** *for C (or C* **has essential subset** *J) $\Longleftrightarrow$ (0) $\mathrm{Supp}(C) \supseteq J$, (1) $\dim(\sum_{j \in J} C_j) = |J| - 1$, and (2) $\dim(\sum_{j \in J'} C_j) \geq |J'|$ for all nonempty* **proper** *$J' \subsetneq J$.*

Equivalently, J is essential for $C \iff$ the $|J|$-dimensional mixed volume of $(C_j \mid j \in J)$ is 0 and no smaller subset of J has this property. Figure 1 below shows some simple examples of essential subsets for C, for various C in the case $n=2$.

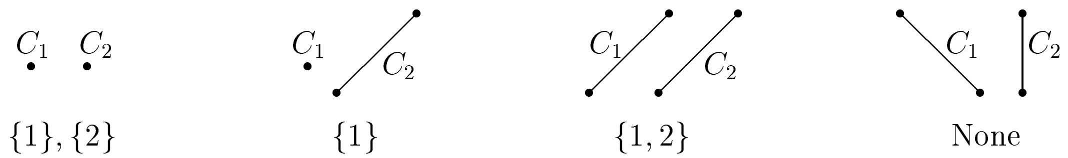

FIGURE 1. The essential subsets for 4 different pairs of plane polygons. (The segments in the third pair are meant to be parallel.)

A basic fact about mixed volumes is that $\mathcal{M}(E)=0 \iff E$ has an essential subset, whenever $\mathrm{Supp}(E)=[n]$. However, there is an even deeper connection between filling and essentiality:

Theorem 1. [Roj94, sec. 2.5] *Suppose D and E are n-tuples of finite subsets of $\mathbb{Z}^n$ such that $\mathcal{M}(E)>0$. Then D fills $E \iff$ for all $w \in \mathcal{S}^{n-1}$, $\mathrm{Supp}(D \cap E^w)$ contains a subset essential for E^w.* □

Remark 4. *One certainly need not check infinitely many w. In fact, we need only check one w (just pick any inner normal) for each face of the polytope $\sum_{i=1}^n \mathrm{Conv}(E_i)$.*

Filling is closely related to root counting for sparse polynomial systems, and this aspect is explored much further in [Roj94, RW96, Roj97b]. We also point out that the computational complexity of finding an irreducible fill is an open question. However, for $n \leq 3$, finding irreducible fills is quite simple and no harder (asymptotically) than finding a convex hull. (Using theorem 1, this follows as a simple geometric exercise.) In any event, 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 an irreducible fill is too hard, this step of our toric GCP construction 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 remains fixed once and for all, and the coefficients may vary many thousands of times, actually occurs frequently in many practical contexts such as robot control or computational geometry.

4. Toric Geometry and the Proof of Our Main Theorem

Our notation is a slight variation of that used in [Ful93], and is described at greater length in [Roj97b]. We will assume the reader to be familiar with normal fans of polytopes and the construction of a toric variety from a fan or a finite point set [Ful93, GKZ94]. However, we will at least list our cast of main characters:

Definition 5. [Roj97b] *Given any $w\in\mathbb{R}^n$, we will use the following notation:*

$$
\begin{aligned}
T &= \textit{The algebraic torus } (K^*)^n\\
P^w &= \textit{The face of } P \textit{ with inner normal } w\\
\sigma_w &= \textit{The closure of the cone generated by the inner normals of } P^w\\
U_w &= \textit{The affine chart of } \mathcal{T}_P \textit{ corresponding to the cone } \sigma_w \textit{ of } \mathrm{Fan}(P)\\
L_w &= \textit{The } \dim(P^w)\textit{-dimensional subspace of } \mathbb{R}^n \textit{ parallel to } P^w\\
x_w &= \textit{The point in } U_w \textit{ corresponding to the semigroup homomorphism } \sigma_w^\vee\cap\mathbb{Z}^n \longrightarrow\\
&\quad\ \{0,1\} \textit{ mapping } p\mapsto\delta_{w\cdot p,0}, \textit{ where } \delta_{ij} \textit{ denotes the Kronecker delta}\\
O_w &= \textit{The } T\textit{-orbit of } x_w = \textit{The } T\textit{-orbit corresponding to } \mathrm{RelInt}P^w\\
\mathcal{E}_P(Q) &= \textit{The } T\textit{-invariant Weil divisor of } \mathcal{T}_P \textit{ corresponding to a polytope } Q.\\
\mathrm{Div}(f) &= \textit{The Weil divisor of } \mathcal{T}_P \textit{ defined by a rational function } f \textit{ on } (K^*)^n\\
\mathcal{D}_P(f,Q) &= \mathrm{Div}(f)+\mathcal{E}_P(Q) = \textit{The toric effective divisor of } \mathcal{T}_P \textit{ corresponding to } (f,Q)\\
\mathcal{D}_P(F,\mathcal{P}) &= \textit{The (nonnegative) cycle in the Chow ring of } \mathcal{T}_P \textit{ defined by } \textstyle\bigcap_{i=1}^k \mathcal{D}_P(f_i,P_i), \textit{ when-}\\
&\quad\ \textit{ever } \mathcal{P}=(P_1,\ldots,P_k)
\end{aligned}
$$

We will say that a polytope P is **compatible** with Q iff every cone of $\mathrm{Fan}(Q)$ is a union of cones of $\mathrm{Fan}(P)$ [Kho77, Ful93, Roj97b]. In particular, whenever F is an $k\times n$ polynomial system with support contained in E, we will define the **zero set of F in $\mathcal{T}_\mathbf{P}$** to be the toric cycle $\mathcal{D}_P(F,\mathcal{P})$, where $\mathcal{P}:=(\mathrm{Conv}(E_1),\ldots,\mathrm{Conv}(E_k))$.

The following result will provide some necessary geometric intuition for specializing resultants.

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 $i\in[n+1]$. Then, provided*

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

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

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

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

Remark 5. *This result provides a geometric analogue, over a* **general** *algebraically closed field, of the product formula for the sparse resultant* [PS93].

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 faces of P and the affine charts of $\mathcal{T}_P$.

Lemma 1. [Roj97b, Sections 4.2–5.1] *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 $\mathbb{R}^n$. 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 $\langle x^{b_i} f_i \mid$ for all $i \in [k]$ and $b_i \in \mathbb{Z}^n$ such that $b_i + P_i \subset \sigma_w^\vee \rangle$. □

Lifting (or projecting) from one toric variety to another is an important fundamental ideal we will also use. The following lemma follows directly from the development of [Ful93].

Lemma 2. *Suppose $P \subset \mathbb{R}^n$ is an n-dimensional rational polytope, and A is either a nonempty finite subset of $\mathbb{Z}^n$* **or** *a rational polytope in $\mathbb{R}^n$. Assume further that P is compatible with $\mathrm{Conv}(A)$. Then there is a natural (surjective) proper morphism $\varphi : \mathcal{T}_P \twoheadrightarrow \mathcal{T}_A$. In particular, following the notation of this section, $\varphi(\mathcal{D}_P(F,\mathcal{P})) = \mathcal{D}_A(F,\mathcal{P})$, where the latter cycle is the image of $\mathcal{D}_{\mathrm{Conv}(A)}(F,\mathcal{P})$ under the natural proper morphism from $\mathcal{T}_{\mathrm{Conv}(A)}$ to $\mathcal{T}_A$.*

Remark 6. *Recall that $\mathcal{T}_A$ can be defined as the image of of $\mathcal{T}_{\widetilde{P}}$ under the map φ from our Main Theorem. So, with this understanding, there is no ambiguity between our first and second φ.*

To conclude our background, we will need the following lemma implying that F^* is sufficiently generic in a useful sense.

Lemma 3. *Suppose D is an irreducible fill of some n-tuple E. Then 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, following the notation of our Main Theorem, 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.

4.1. **The Proof of Our Main Theorem.** We first note that the well known results on the degree of $\mathrm{Res}_{\bar{E}}(f_1, \ldots, f_{n+1})$ with respect to the coefficients of different f_i [Stu94] remain true over any algebraically closed field. This follows easily from the formulation of the resultant for a collection of invertible sheafs on a projective variety [GKZ94]. In particular, the degree of $\mathcal{H}$ as a polynomial in s should be

$$\sum_{i=1}^{n} \mathcal{M}(E_1, \ldots, E_{i-1}, E_{i+1}, \ldots, E_n, A).$$

Also each coefficient of $\mathcal{H}(s)$ should be a homogeneous polynomial (in the u_e) of degree $\mathcal{M}(E)$. These two assertions of course include the opening statement of our Main Theorem (on the degree and homogeneity of $\mathcal{F}_A$), but they will follow only upon showing that $\mathcal{H}$ is not identically 0.

To see this, note that lemma 1 and the Vanishing Theorem for Resultants readily imply that the coefficient of the **highest** power of s in $\mathcal{H}$ is precisely $\mathrm{Res}_{(E,A)}(F^*, g)$. (Simply check the zero set of $F - sF^*$ in $\mathcal{T}_{\widetilde{P}}$ at $s = \infty$.) By lemma 3, and the Vanishing

Theorem once more, we see that this polynomial in the u_e is not identically 0. So $\mathcal{H}\not\equiv 0$ and we've finished the simplest part of our proof.

Part (0) of our Main Theorem follows similarly: One need only consider the **unspecialized** resultant polynomial $\mathrm{Res}_{(E,A)}(F,g)$ and observe the terms of degree 0 in s as we specialize coefficients to obtain $F-sF^*$. The statement on the vanishing of Ch_A then follows easily from lemma 2 (since $\widetilde{P}$ is compatible with $\mathrm{Conv}(A)$) and the Vanishing Theorem: We obtain that $\varphi(Z)$ is positive-dimensional iff Ch_A has infinitely many distinct divisors of the form $\sum_{e\in A} c_e u_e$. In particular, corollary 3 follows as a special case of (0) since P compatible with $\mathrm{Conv}(A) \Longrightarrow \mathcal{T}_P = \mathcal{T}_{\widetilde{P}}$. Note that (1), (2), and (3) also follow almost trivially, **provided** Ch_A is not identically 0.

To properly handle the cases of (1), (2), and (3) where we are actually working with a non-trivial toric perturbation, let us first construct two important toric cycles: Let $\bar{Z}$ be the zero set of $F-sF^*$ in $\mathcal{T}_{\widetilde{P}}\times\mathbb{P}^1_K$ and $\bar{Z}^\vee_+$ the zero set of $\mathcal{H}(u;s)$ in $\mathbb{P}^{|A|-1}_K\times\mathbb{P}^1_K$. Then it is easily observed that $Z=\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{0\})$. Also, it can be shown [Roj97b, Section 5.1] that $\bar{Z}$ contains an algebraic curve C (possibly reducible), with surjective projection onto the second factor of $\mathcal{T}_{\widetilde{P}}\times\mathbb{P}^1_K$, obeying the following property: $C\cap(\mathcal{T}_{\widetilde{P}}\times\{0\})$ contains the zero-dimensional part of Z, and consists of exactly $\mathcal{M}(E)$ points (counting multiplicities). (In fact, $\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})=C\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})$ for almost all $s_0\in\mathbb{P}^1_K$.) Furthermore, by slightly modifying step (i) of the proof of the toric variety version of Bernshtein's theorem [Roj97b, Section 5.1], one can show that C intersects every positive-dimensional irreducible component of Z. (One also needs to use the definition of intersection multiplicity of an irreducible component W as the number of curve branches intersecting W in a 1-parameter deformation.)

The proof of the rest of our main theorem will reduce to establishing a precise correspondence between the factors of $\mathcal{F}_A$ and the points of $\varphi(C\cap(\mathcal{T}_{\widetilde{P}}\times\{0\}))$. To complete this connection, we need only observe that $\bar{Z}^\vee_+$ is a very special kind of hypersurface, closely related to $\bar{Z}$.

In particular, if k is the least power of s in $\mathcal{H}$, observe that $\bar{Z}^\vee_+$ and the zero set of $\frac{\mathcal{H}}{s^k}$ in $\mathbb{P}^{|A|-1}_K\times\mathbb{P}^1_K$ differ only by the presence of the hyperplane $\mathbb{P}^{|A|-1}_K\times\{0\}$. The second zero set does **not** contain this hyperplane, so let's call the second zero set $\bar{Z}^\vee$. Then by lemmata 1 and 2, and the Vanishing Theorem for Resultants, $\dim[\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})]=0$ implies the following equivalence: $\mathcal{H}(H_{\varphi(\zeta)};s_0)=0 \Longleftrightarrow \zeta\in\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})$, where H_p is the hyperplane dual to the point p.[7] Now $\dim[\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{\infty\})]=0$ by construction. Hence $\dim[\bar{Z}\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})]=0$ for almost all $s_0\in\mathbb{P}^1_K$, by Main Theorem 2 of [Roj97b]. So $\psi^\vee(C)$ is an open subset of $\bar{Z}^\vee$, where we define $\psi^\vee(C):=\{(y,s_0)\mid y\in H_{\varphi(\zeta)}\ ;\ \zeta\in C\cap(\mathcal{T}_{\widetilde{P}}\times\{s_0\})\ ;\ s_0\in\mathbb{P}^1_K\}$. Therefore, since φ is a proper map, $\frac{\mathcal{H}}{s^k}$ must vanish on

[7] So if $p:=[p_e\mid e\in A]\in\mathbb{P}^{|A|-1}_K$ then $H_p:=\{[y_e\mid e\in A]\in\mathbb{P}^{|A|-1}_K\mid\sum_{e\in A}p_e y_e=0\}$.

all of $\psi^\vee(C)$. In particular,

$$\mathcal{F}_A(u) = \alpha \cdot \prod_{\zeta \in C \cap (\mathcal{T}_{\tilde{P}} \times \{0\})} \left(\sum_{e \in A} c_{\zeta,e} u_e \right)$$

where $\alpha \in K^*$, $[c_{\zeta,e} \mid e \in A] := \varphi(\zeta)$, and the product counts intersection multiplicities.

Continuing our main proof, (1), (2), and (3) follow immediately from our last formula and our preceding observations. $\square$

Note that our algebraic proof avoids the use of limiting arguments that were present in [Can90]. Thus our result is equally valid when K has positive characteristic.

References

[BZ88] Burago, Yu. D. and Zalgaller, V. A., *Geometric Inequalities,* Grundlehren der mathematischen Wissenschaften 285, Springer-Verlag (1988).

[Can88] Canny, John F., *"Some Algebraic and Geometric Computations in PSPACE,"* Proc. $20^{\underline{\text{th}}}$ ACM Symp. Theory of Computing, Chicago (1988).

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

[CG84] Chistov, A. L., and Grigoriev, Dima Yu, *"Complexity of Quantifier Elimination in the Theory of Algebraically Closed Fields,"* Lect. Notes Comp. Sci. 176, Springer-Verlag (1984).

[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.

[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`

[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.

[EP97] Emiris, Ioannis Z. and Pan, Victor Y., *"The Structure of Sparse Resultant Matrices,"* preprint, 1997.

[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.

[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.

[HM91] Hafner, James L. and McCurley, Kevin S., *"Asymptotically Fast Triangularization of Matrices Over Rings,"* SIAM Journal on Computing, 20 (1991), no. 6, pp. 1068–1083.

[HS95] Huber, Birkett and Sturmfels, Bernd, *"A Polyhedral Method for Solving Sparse Polynomial Systems,"* Mathematics of Computation, 64, pp. 1541–1555, 1995.

[Hub96] Huber, Birk, *"Solving Sparse Polynomial Systems,"* Ph.D. Dissertation, Department of Mathematics, Cornell University (1996).

[Ili89] Iliopoulos, Costas S., *"Worst Case Complexity Bounds on Algorithms for Computing the Canonical Structure of Finite Abelian Groups and the Hermite and Smith Normal Forms of an Integer Matrix,"* SIAM Journal on Computing, 18 (1989), no. 4, pp. 658–669.

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

[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.

[MP97] Morrain, Bernard and Pan, Victor Y. *"Solving Special Polynomial Systems by Using Structured Matrices and Algebraic Residues,"* Foundations of Computational Mathematics, selected papers of a conference, held at IMPA in Rio de Janeiro, January 1997, Springer-Verlag (1997).

[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 Laminations, Sparse Generalized Characteristic Polynomials, and a Refinement of Hilbert's Tenth Problem,"* Foundations of Computational Mathematics, selected papers of a conference, held at IMPA in Rio de Janeiro, January 1997, Springer-Verlag (1997).

[Roj97b] ________________ *"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`.)

[Roj97c] ________________ *"Solving Polynomial Equations via Twisted Chow Forms,"* preprint, MIT (1997).

[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).

[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.

[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.

[Sma87] Smale, Steve, *"The Topology of Algorithms I,"* Journal of Complexity, **3** (1987), pp. 81–89.

[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.

[Van50] van der Waerden, B. L., *Modern Algebra,* 3rd edition, F. Ungar, New York.
[Ver96] Verschelde, Jan, *"Homotopy Continuation Methods for Solving Polynomial Systems,"* Doctoral Dissertation, Katholieke Universiteit Leuven, Leuven, Belgium, May 1996.
[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.