AFFINE ELIMINATION THEORY

J. MAURICE ROJAS

We propose a new resultant operator, providing a geometrically and computationally more intrinsic setting for elimination theory. The **affine** resultant extends the benefits the sparse resultant provides (for algebraic geometry in the algebraic torus) to affine space minus an arbitrary union of coordinate hyperplanes. As an application of the affine resultant, we give an explicit formula for the degree of a zero-dimensional intersection of n algebraic hypersurfaces in K^n, for any algebraically closed field K. The latter formula refines and generalizes the celebrated mixed volume formula of David N. Bernshtein [Ber75], as well as its many extensions [DK87, Roj94, LW96, RW96, HS97, Roj99, Roj97, EV97, GLW98]. In particular, we can compute the **exact** number of roots of a polynomial system in various regions — not just its generic number of roots. Also, our formula is valid in arbitrary characteristic. An example of our formula appears at the end of this brief note.

Although one could try to use multiple sparse resultants in various coordinate subspaces to analyze affine roots, it is desirable (and more efficient) to instead perform a single, more intrinsic, resultant computation. This is one motivation for the affine resultant, defined below. In order to set the stage for this kind of intrinsic elimination theory, we will first show how to correctly combine multiple sparse resultants to get a single affine resultant operator. A more direct definition of the affine resultant, independent of sparse resultants, will appear in the full paper corresponding to this abstract [Roj98b].

We will use the following notation: Let $E_1, \ldots, E_{n+1}$ be nonempty finite subsets of $(\mathbb{N} \cup \{0\})^n$. For any $e = (e_1, \ldots, e_n) \in (\mathbb{N} \cup \{0\})^n$ let x^e denote the monomial $x_1^{e_1} \cdots x_n^{e_n}$. In this way we will let $f_1, \ldots, f_{n+1}$ be polynomials in the variables $\{x_1, \ldots, x_n\}$ with (algebraically independent) indeterminate coefficients, such that the set of exponent vectors occuring in f_i is precisely E_i. The set E_i is called the **support** of f_i and this representation specifies exactly which monomials can appear in f_i. Our resultants will make maximal use of this monomial term information — not just the degrees of the f_i. A convenient short-hand will be the following: Let $\bar{E} := (E_1, \ldots, E_{n+1})$ and $\bar{F} := (f_1, \ldots, f_{n+1})$. Then $\bar{E}$ is the **support** of $\bar{F}$ and we call $\bar{F}$ an $\boldsymbol{(n+1) \times n}$ **indeterminate polynomial system**. In general, regardless of constant or indeterminate coefficients, we write $\mathbf{Supp}(\bar{\boldsymbol{F}}) = \bar{\boldsymbol{E}}$ (resp. $\mathbf{Supp}(\bar{\boldsymbol{F}}) \subseteq \bar{\boldsymbol{E}}$) when the $(n+1)$-tuple of sets of exponent vectors of $\bar{F}$ is precisely (resp. $(n+1)$-tuple-wise contained in) $\bar{E}$. The preceding terminology extends naturally to $k \times n$ systems.

It will also be helpful to describe certain subspaces concisely.

Definition 1. *Let $|\cdot|$ denote set cardinality and let $[n]$ be the set of integers $\{1, \ldots, n\}$. For any $I \subseteq [n]$, define $\mathrm{Lin}(I) \subseteq \mathbb{R}^n$ to be the coordinate subspace generated by the subset $\{\hat{e}_j \mid j \in I\}$ of the standard basis. Finally, let $\mathbf{O}$ denote the origin in whatever module we work in. In particular, $\mathrm{Lin}(\emptyset) = \mathbf{O}$.*

Our foundational definition for the affine resultant will be recursive, building up from **cornered** or lower dimensional cases. So we first give the definition of cornering, and a special case of our general affine resultant definition.

Definition 2. *Call a k-tuple $C := (C_1, \ldots, C_k)$ of nonempty subsets of $\mathbb{R}^n$* **cornered** *iff C_i lies in the nonnegative orthant and $C_i \cap \{(y_1, \ldots, y_n) \in \mathbb{R}^n \mid y_j = 0\} \neq \emptyset$ for all $i \in [k]$ and $j \in [n]$. Also, for any $a_1, \ldots, a_k \in \mathbb{R}^n$, define $a \cup C$ to be the k-tuple $(\{a_1\} \cup C_1, \ldots, \{a_k\} \cup C_k)$. Finally, if $\bar{E}$ is cornered, define the* **affine resultant of $\bar{\boldsymbol{F}}$ with respect to $\bar{\boldsymbol{E}}$, $\mathbf{AffRes}_{\bar{\boldsymbol{E}}}(\bar{\boldsymbol{F}})$**, *to be $\mathrm{Res}_{\mathbf{O} \cup \bar{E}}(\bar{F})$ — the sparse resultant of $\bar{F}$ with respect to the support $\mathbf{O} \cup \bar{E}$.*

Date: September 1, 1997.

Extended abstract submitted to a conference in honor of David A. Buchsbaum. This research was completed at MIT and partially funded by an NSF Mathematical Sciences Postdoctoral Research Fellowship.

Remark 1. *For further details on the definition of the sparse*[1] *resultant, as well as instructive examples, we refer the reader to* [KSZ92, Stu93, PS93, SZ94, Stu94, GKZ94, EC95, Stu98, Roj97, Roj98a]. *In particular, under certain degenerate instances (which can be completely described by the combinatorics of $\bar{E}$), the sparse resultant can be identically* 0 *or* 1. *We also point out that the above notation is closest to that in* [Roj99, Section 6.3].

The most general definition of the affine resultant, for the purposes of our present discussion, is the following:

Main Definition. *Suppose $\bar{F}$ is an $(n+1)\times n$ indeterminate polynomial system with support $\bar{E}$. For all $i\in[n+1]$ and $j\in[n]$, define $m_{ij}:=\min\{y_j \mid (y_1,\ldots,y_n)\in E_i\}$ and $m_i:=(m_{i1},\ldots,m_{in})$. Then the* **affine resultant of $\bar{F}$ with respect to $\bar{E}$** *is precisely*

$$\mathbf{AffRes}_{\bar{E}}(\bar{F}):=\prod_{J\subseteq[n+1]}\ \prod_{\rho:J^c\hookrightarrow[n]}\left(\mathrm{AffRes}_{\bar{E}_{(J,\rho)}}(\bar{F}_{(J,\rho)})\uparrow\prod_{j\in J^c} m_{j\rho(j)}\right),$$

where $(\cdot)^c$ denotes set-theoretic complement, $\uparrow$ denotes exponentiation,

$$\bar{E}_{(J,\rho)}:=((E_i-m_i)\cap \mathrm{Lin}(\rho(J^c)^c)\mid i\in J),$$

and $\bar{F}_{(J,\rho)}$ is the polynomial system obtained by setting the variables $\{x_j \mid j\in\rho(J^c)\}$ to 0 in the $|J|$-tuple

$$(x_1^{-m_{i1}}\cdots x_n^{-m_{in}}f_i \mid i\in J).$$

$\square$

Remark 2. *Although not obvious from the above definition,* $\mathrm{AffRes}_\star(\cdot)$ *can actually be computed much more quickly than the corresponding product of sparse resultants implied by our last two definitions* [Roj98b]. *Also, in order to avoid normalization problems (cf. example 1), our exponent lattices* [PS93] *will* **always** *be of the form $L\cap\mathbb{Z}^n$, for some coordinate subspace $L\subseteq\mathbb{R}^n$.*

With a very slight modification of our Main Definition, we can also obtain resultant operators which are tailored to computation in affine space minus an arbitrary union of coordinate hyperplanes, thus giving a common generalization of $\mathrm{Res}_\star(\cdot)$ and $\mathrm{AffRes}_\star(\cdot)$ [Roj98b]. However, for the sake of brevity, we will only deal with affine space.

The affine resultant satisfies many properties analogous to those of the sparse resultant. These are addressed in [Roj98b], so let us instead leap into an application of the affine resultant.

Definition 3. *Let F be an $n\times n$ polynomial system with constant coefficients and* $\mathrm{Supp}(F)=E$. *Following the notation of our Main Definition, assume further that $\prod_{j\in J^c} m_{j\rho(j)}>0 \Longrightarrow E_{(J,\rho)}$ is not null for $\mathrm{Lin}(\rho(J^c)^c)$, for all $J\subseteq[\boldsymbol{n}]$ and $\rho:J^c\hookrightarrow[n]$ (cf. remark 3). Call a facet of a polytope in $\mathbb{R}^n$* **bad** *iff it has an inner normal* **outside** *the nonnegative orthant. Finally, suppose $A\subset(\mathbb{N}\cup\{0\})^n$ satisfies the following properties:*

1. $\mathbf{O}\in A$
2. $|A|\geq n+1$
3. *The convex hull* $\mathrm{Conv}(A)$ *is such that the cone generated by the edges emanating from the vertex* $\mathbf{O}$ *is precisely the nonnegative orthant in* $\mathbb{R}^n$.
4. *Every bad facet of* $\mathrm{Conv}(A)$ *is parallel to some facet of the Minkowski sum* $P:=\sum_{i=1}^n \mathrm{Conv}(E_i)$.

We then call the polynomial $\mathrm{Ch}_A(u):=\mathrm{AffRes}_{(E,A)}(F,\sum_{e\in A}u_e x^e)$ *an* **(affine) twisted Chow form** *of F.*

[1] Other equivalent prefixes used for this modern version of the resultant are the following: $\mathcal{A}$-, $(\mathcal{A}_1,\ldots,\mathcal{A}_k)$-, mixed, sparse mixed, GKZ, Newton, and toric.

A less restricted version of the above construction is given in [Roj98a] and applied to polynomial system solving. Note that the above definition generalizes the classical u-resultant [Can86]. Also note that when $A=\{\mathbf{O}, d_1\hat{e}_1, \ldots, d_n\hat{e}_n\}$, with $d_1, \ldots, d_n \in \mathbb{N}$, the toric variety $\mathcal{T}_A$ corresponding to the point set A [GKZ94] is a twisted projective space containing a naturally embedded copy of K^n, hence our terminology.

Remark 3. *The "non-nullity" condition (which borrows terminology from* [Roj99, Section 4.3]*) simply requires that E be such that certain $F_{(J,\rho)}$ generically have positively many roots.*[2] *This assumption is precisely what is required to avoid dealing with those F which, up to a monomial change of variables, have an overdetermined subsystem* [Roj98b]. *Twisted Chow forms for overdetermined systems require a theory of sparse resultant* **ideals**, *which has yet to be developed. So we will address the overdetermined case in future work.*

We are now ready to state our formula for affine root counting.

Main Theorem. [Roj98b] *Following the notation of our last two definitions...*

1. *If $\mathrm{Ch}_A(u)$ is not identically zero, then the number of roots of F in K^n, counting multiplicities, is precisely the degree of $\mathrm{Ch}_A(u)$ as a polynomial in $u_{\mathbf{O}}$.*
2. *Let $\mathrm{Ch}'_A(u)$ be the square-free part of $\mathrm{Ch}_A(u)$. Then if $\mathrm{Ch}'_A(u)$ is not identically zero, the number of distinct roots of F in K^n is at least the degree of $\mathrm{Ch}'_A(u)$ as a polynomial in $u_{\mathbf{O}}$.*
3. *Suppose further that E is fixed so that a generic F with $\mathrm{Supp}(F)\subseteq E$ has only finitely many roots in K^n. Then the F for which $\mathrm{Ch}_A(u)$ vanishes identically form a subvariety of codimension ≥ 2.*
4. *Suppose further that $n=2$. Then $\mathrm{Ch}_A(u)$ vanishes identically $\Longleftrightarrow$ F has infinitely many roots in K^2.*

The nonvanishing of $\mathrm{Ch}_A(u)$ is a very weak assumption and still permits F to have infinitely many roots at toric infinity [Roj98b]. Assertion (3) thus tells us that our above root counting method will fail very rarely. (This also refines an analogous result for counting in $(K^*)^n$ from [Roj97].) Also, any nontrivial affine root counting problem will always result in an E satisfying the hypothesis of (3).[3]

This rarity of failure for elimination-theoretic root counting does **not** hold for the classical u-resultant [Roj98a], hence our need for twisted Chow forms. In fact, by applying the **toric GCP** [Roj98a], one can **always** efficiently and accurately count roots in K^n, even when Ch_A vanishes identically [Roj98b].

There are also analogous formulae for the number of roots lying in **any** affine chart (corresponding to a polytope vertex) of a toric variety corresponding to a polytope [Roj98b]. To close our brief discussion of the K^n case, we present the following example:

Example 1. *Let $n=2$ and consider the following bivariate polynomial system:*

$$\begin{aligned} f_1(x,y) &:= y^2+y^5+xy^6+x^3y^5 \\ f_2(x,y) &:= x+x^3+xy+x^5y+x^3y^2 \end{aligned}$$

To calculate the exact number of affine roots of $F:=(f_1,f_2)$, set $E:=\mathrm{Supp}(F)$ and $A:=\{(0,0),(2,0),(0,1)\}$. It is then easily verified that the hypotheses of definition 3 are satisfied, so let us set $\bar{E}:=(E,A)$ and calculate the corresponding affine resultant.

From our Main Definition, we obtain $m_1:=(0,2)$, $m_2:=(1,0)$, $m_3:=(0,0)$. So, letting u_0,u_1,u_2 respectively denote $u_{\mathbf{O}}, u_{(2,0)}, u_{(0,1)}$ for convenience, our recursive product of affine resultants becomes

---

[2] The non-nullity condition also implies that $\dim P=n$, so condition (4) is indeed well-defined.

[3] These particular E can also be completely characterized in combinatorial terms [Roj99].

the following:[4]

$$\mathrm{AffRes}_{\bar{E}}(F, u_0+u_1x^2+u_2y) :=$$

$$\mathrm{AffRes}_{\bar{E}_{([3],\cdot)}}(1+y^3+xy^4+x^3y^3, 1+x^2+y+x^4y+x^2y^2, u_0+u_1x^2+u_2y)$$

$$\times(\mathrm{AffRes}_{\bar{E}_{(\{2,3\},1\mapsto 1)}}(1+x^2, u_0+u_1x^2))^2 \mathrm{AffRes}_{\bar{E}_{(\{1,3\},2\mapsto 2)}}(1+y^3, u_0+u_2y)(\mathrm{AffRes}_{\bar{E}_{(\{3\},Id)}}(u_0))^2$$

Using definition 2, and after a few seconds of `Maple`*, the first affine resultant on the right hand side can be written explicitly as follows:*

$$(-u_2+u_1)^3(u_0-u_2)(\text{Polynomial of Degree 4 in } u_0, \text{ Irreducible Over } \mathbb{Q})$$

$$\times(\text{Larger Polynomial of Degree 8 in } u_0, \text{ Irreducible Over } \mathbb{Q})$$

Using definition 2 again, we can then compute[5] *the rest of our product expression for* $\mathrm{AffRes}_{\bar{E}}(\bar{F})$*:*

$$((u_0-u_1)^2)^2(u_0^3-u_2^3)u_0^2$$

So by our Main Theorem, we can thus conclude that F *has exactly* $(1+4+8)+4+3+2=$ **22** *roots in* K^2*, counting multiplicities. Better still, we also obtain that* F *has at least* $(1+4+8)+1+2+1=$ **17** *distinct roots in* $\mathbb{C}^2$*. (With a closer look at the affine resultants, one can actually improve this to* **exactly 18** *distinct roots in* $\mathbb{C}^2$ [Roj98b]*. We omit the case of distinct root counting in positive characteristic for lack of space.) On the other hand, the* **stable mixed volume bound** [HS97, EV97, GLW98] *would only tell us that* F *has* $\leq$**25** *isolated roots, counting multiplicities.*

The preceding computations (and techniques for performing them more efficiently) are described in greater detail in [Roj98b].

References

[Ber75] Bernshtein, D. N., *"The Number of Roots of a System of Equations,"* Functional Analysis and its Applications (translated from Russian), Vol. 9, No. 2, (1975), pp. 183–185.

[Can86] Canny, John F., *"The Complexity of Robot Motion Planning Problems,"* ACM Doctoral Dissertation Award Series, ACM Press, 1986.

[DK87] Danilov, V. I., and Khovanskii, A., *"Newton Polyhedra and an Algorithm for Computing Hodge-Deligne Numbers,"* Math. USSR Ivzestiya, Vol. 29 (1987), No. 2.

[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.

[EV97] Emiris, Ioannis Z. and Verschelde, Jan, *"How to Count Efficiently All Affine Roots of a Polynomial System,"* Research Report No. 3212, July 1997, INRIA, Sophia-Antipolis.

[GLW98] Gao, T., Li, T. Y., and Wang, X., *"Finding Isolated Zeroes of Polynomial Systems in* $\mathbb{C}^n$ *via Stable Mixed Subdivisions,"*, Journal of Symbolic Computation, to appear.

[GKZ94] Gel'fand, I. M., Kapranov, M. M., and Zelevinsky, A. V., *Discriminants, Resultants and Multidimensional Determinants,* Birkhauser, Boston, 1994.

[HS97] Huber, Birk and Sturmfels, Bernd, *"Bernshtein's Theorem in Affine Space,"* Discrete and Computational Geometry, **17** (1997), pp. 137–141.

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

[LW96] Li, T. Y. and Wang, Xiaoshen, *"The BKK Root Count in* $\mathbb{C}^n$*,"* Mathematics of Computation, 65 (1996), no. 216, pp. 1477-1484.

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

[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.

[4]In reality, there are 3 more affine resultant powers in the product on the right hand side, but these reduce to 1 so we have omitted them.

[5]Had we not fixed our exponent lattices properly (as described in remark 2), the first product term below would have had the wrong exponent.

[Roj97] ________________, *"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).

[Roj98a] ________________, *"Solving Degenerate Sparse Polynomial Systems Faster,"* Journal of Symbolic Computation, special issue on elimination theory, to appear.

[Roj98b] ________________, *"The Geometry of Elimination II: Affine Elimination Theory and Better Nullstellensatze,"* preprint.

[Roj99] ________________, *"Toric Intersection Theory for Affine Root Counting,"* Journal of Pure and Applied Algebra, June, 1999.

[RW96] Rojas, J. Maurice, and Wang, Xiaoshen, *"Counting Affine Roots of Polynomial Systems Via Pointed Newton Polytopes,"* Journal of Complexity, vol. 12, June (1996), pp. 116–133.

[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.

[Stu98] ________________, *"Introduction to Resultants,"* Applications of Computational Algebraic Geometry (San Diego, CA, 1997), pp. 25–39, Proc. Sympos. Appl. Math., 53, Amer. Math. Soc., Providence, RI, 1998.

[SZ94] Sturmfels, B. and Zelevinsky, A., *"Multigraded Resultants of Sylvester Type,"* Journal of Algebra, 163(1): 115–127, 1994.

Department of Mathematics, City University of Hong Kong, 83 Tat Chee Avenue, Kowloon, HONG KONG

E-mail address: `rojas@math.mit.edu, Web-page: http://www-math.mit.edu/~rojas`