JOURNAL OF ALGEBRA 177, 612–616 (1995)

Minimal Resultant Systems

Gennady Lyubeznik

Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

Communicated by Melvin Hochster

Received July 19, 1994

Let k be an algebraically closed field and let $f_1, f_2, \ldots, f_s$ be a family of s forms in two homogeneous variables x and y with indeterminate coefficients and of fixed degrees $\deg f_1, \ldots, \deg f_s$. By letting the coefficients take values in k we get families of forms with coefficients in k. We can think of each such family as a closed point of A_k^n, the affine n-space over k, where $n = \sum_{i=1}^{i=s}(1 + \deg f_i)$ is the number of coefficients. The set of all such families that have a common nontrivial zero in k is known to be an algebraic subvariety of A_k^n [W, XI, 80] which we call the resultant variety of $f_1, \ldots, f_s$. In other words, there exists a set of polynomials in the coefficients of $f_1, \ldots, f_s$ such that they all vanish precisely when $f_1, \ldots, f_s$ have a common nontrivial zero in k. We call such a set of polynomials a resultant system. If $s = 2$, there exists a resultant system consisting of just one polynomial (the usual resultant of f_1 and f_2). This raises a natural question: What is the minimum possible number of polynomials in a resultant system if $s \geq 3$? It is not hard to see that the resultant variety has codimension $s - 1$ in A_k^n, so every resultant system contains at least $s - 1$ polynomials. Here we prove the following much stronger result.

THEOREM 1. *Assume* $\deg f_1 \geq \deg f_2 \geq \cdots \geq \deg f_s$ *and* $\deg f_1 \neq \deg f_3$.

(a) *Every resultant system contains at least*

$$N_s = 1 + \sum_{t=3}^{t=s} (1 + \deg f_t)$$

polynomials.

(b) *If* $s = 3$, *there exists a resultant system consisting of precisely* N_3 *polynomials.*

0021-8693/95 $12.00

The following question is still open.

QUESTION 1.

(a) *Is it true that every resultant system contains at least N_s polynomials even if* $\deg f_1 = \deg f_3$?

(b) *Is it true that there exists a resultant system containing precisely N_s polynomials even when* $s \geq 4$?

Remark 1. The answer to 1(b) is positive if $\deg f_i = 1$ for all i. Indeed, in this case the resultant variety is defined by the 2×2 minors of a $2 \times s$ matrix, so we are done by [BF, 5.21].

Now, let $g_1, \ldots, g_s$ be a family of s polynomials in one variable z of fixed degrees $\deg g_1, \ldots, \deg g_s$ with the top coefficient of g_1 equal to 1 and all other coefficients of $g_1, \ldots, g_s$ indeterminate. Again, by letting the coefficients take values in k, we get families of polynomials with coefficients in k and we can think of each such family as a closed point in A_k^n, where n is the number of indeterminate coefficients. The set of all such families that have a common root in k is again algebraic [W, XI, 77], so there exists a set of polynomials in the coefficients of $g_1, \ldots, g_s$ such that they all vanish if and only if $g_1, \ldots, g_s$ all have a common root. As before, we call such a set of polynomials a resultant system. If $s = 2$, the usual resultant provides a resultant system consisting of just one polynomial. What is the minimum number of polynomials in a resultant system if $s \geq 3$? The codimension of the resultant variety is still $s - 1$, so every resultant system contains at least $s - 1$ polynomials. We give a much stronger lower bound in Theorem 2 below.

Since g_1 is monic, for all $i \geq 2$ we can write

$$g_i = g_1 q_i + g_i', \qquad (\deg g_i' < \deg g_1)$$

and $g_1, g_2, \ldots, g_s$ have a common zero if and only if $g_1, g_2', \ldots, g_s'$ have a common zero. So, there is no loss of generality in assuming that $\deg g_1 > \deg g_i$ for all i. Clearly, we can also assume without loss of generality that $\deg g_2 \geq \deg g_3 \geq \cdots \geq \deg g_s$.

THEOREM 2. *Assume that* $\deg g_1 > \deg g_2 \geq \cdots \geq \deg g_s$.

(a) *Every resultant system consists of at least*

$$N_s = 1 + \sum_{t=3}^{t=s} (1 + \deg g_t)$$

polynomials.

(b) *If* $s = 3$, *or if* $\deg g_i = \deg g_1 - 1$ *for all* $i \neq 1$, *there exists a resultant system consisting of precisely N_s polynomials.*

The following question is still open.

QUESTION 2. *Is it true that there exists a resultant system consisting of precisely N_s polynomials even if $s \geq 4$ and* $\deg g_i < \deg g_1 - 1$ *for some* i?

The results of this paper were obtained in 1982–1983 and form part of my thesis [L1].

Proof of 2(a). Set $R = k$ [all coefficients of $g_1, \ldots, g_2$] and let $I \subset R$ be the defining ideal of the resultant variety. By Hilbert's Nullstellensatz all we have to prove is that I cannot be generated up to radical by fewer than N_s elements of R. Pick $\deg g_1$ pairwise distinct elements $v_1, \ldots, v_{\deg g_1}$ of k (which is possible since k is algebraically closed and therefore infinite). Set $g_1' = (x - v_1) \cdots (x - v_{\deg g_1})$ and $R' = k$ [all coefficients of $g_2, \ldots, g_s$]. Let φ: $R \to R'$ be the ring homomorphism that is the identity on k, sends all the coefficients of $g_2, \ldots, g_s$ to themselves, and sends each coefficient of g_1 to the corresponding coefficient of g_1'. Let I' be the image of I in R'. If I were generated up to radical by fewer than N_s elements, the images of these elements under φ would generate I' up to radical. So, it is enough to prove that I' cannot be generated up to radical by fewer than N_s elements of R'. The ideal I' defines the algebraic set in the space of coefficients of $g_2, \ldots, g_s$ under which $g_1', g_2, \ldots, g_s$ all have a common zero. But $g_1', g_2, \ldots, g_s$ have a common zero if and only if at least one v_i is a root of $g_2, \ldots, g_s$. The set of the coefficients of $g_2, \ldots, g_s$ under which v_i is a root of all of them is algebraic and is defined by the ideal $(g_2(v_i), \ldots, g_s(v_i))$. Therefore, I' defines the same algebraic set as the ideal

$$\mathscr{B} = \bigcap_{i=1}^{i=\deg g_1'} (g_2(v_i), \ldots, g_s(v_i)).$$

Clearly,

$$\mathscr{B} = \mathscr{A}_1 \cap \mathscr{A}_2 \cap \cdots \cap \mathscr{A}_{\deg g_2} \cap \mathscr{A}_{\deg g_2 + 1},$$

where

$$\mathscr{A}_i = (g_2(v_i), g_3(v_i), \ldots, g_s(v_i)) \qquad (1 \leq i \leq \deg g_2)$$

and

$$\mathscr{A}_{\deg g_2 + 1} = \bigcap_{i = \deg g_2 + 1}^{i = \deg g_1} (g_2(v_i), \ldots, g_s(v_i)).$$

If $t \leq \deg g_i + 1$, for some t and i, then $g_i(v_{j_1}), g_i(v_{j_2}), \ldots, g_i(v_{j_t})$ are linearly independent in the k-vector space spanned by the coefficients of

g_i, since $v_j \neq v_{j'}$ for all $j \neq j'$ and therefore the upper left $t \times t$ minor of the $t \times (\deg g_i + 1)$ matrix $(a_{pq} = v_{j_p}^{q-1})$ is nonzero. So, if $t \geq \deg g_i + 1$, then $g_i(v_{j_1}), g_i(v_{j_2}), \ldots, g_i(v_{j_t})$ span this vector space, since its dimension equals $\deg g_i + 1$. Therefore the sum of all $\mathscr{A}_i$ is m-primary, where m is the maximal ideal generated by all the coefficients of $g_2, \ldots, g_s$. At this point we quote the main theorem of [L2]:

Let (A, m) be an n-dimensional Cohen–Macaulay ring. Let $V = V_1 \cup V_2 \cup \cdots \cup V_k$ be the union of k closed subsets of Spec k *defined by (not necessarily radical) ideals $\mathscr{A}_i$: $V_i = V(\mathscr{A}_i)$. If the following conditions are satisfied,*

(i) $V_1 \cap V_2 \cap \cdots \cap V_k = \{m\}$,

(ii) *there exist k elements a_i $(1 \leq i \leq k)$ and an ideal $\mathscr{A}$ of A such that $a_1, a_2, \ldots, a_k$ is an $A/\mathscr{A}$-regular sequence and $\mathscr{A}_i' + \mathscr{A} \subset (a_i) + \mathscr{A}$ for all i,*

then V cannot be generated up to radical by fewer than $n - k + 1$ elements of A.

Now we set $A = R'_m$, we let $\mathscr{A}$ be the ideal generated by all the coefficients of $g_3, \ldots, g_s$, and we set $a_i = g_2(v_i)$ for $i \leq \deg g_2 + 1$. Then the above-quoted theorem applies with $n = \sum_{i=2}^{i=s}(1 + \deg g_i)$ and $k = 1 + \deg g_2$, so we are done.

Remark 2. Using an argument similar to the proof of the Theorem of [L3], one can show that the local cohomology module $H_{I'}^{N_s}(R') \neq 0$. This gives an alternative proof of 2(a). One can further show that $H_{I'}^{i}(R') = 0$ for all $i > N_s$. The fact that $H_{I'}^{N_s}(R') \neq 0$ implies that $H_I^{N_s}(R) \neq 0$. It follows from 2(b) that if $s = 3$, or if $\deg g_i = \deg g_1 - 1$ for all $i > 1$, then $H_I^i(R) = 0$ for all $i > N_s$. We do not know whether $H_I^i(R) = 0$ for all $i > N_s$ in all other cases as well.

Proof of 1(a). Set $z = x/y$, let f_1' be obtained from f_1 by setting the coefficient at the top power of x to be 1, and define polynomials $g_1, \ldots, g_s$ in z by $f_1' = x^{\deg f_1} g_1$ and $f_i = x^{\deg f_i} g_i$ for all $i \geq 2$. By setting the top coefficient of f_1 to be 1 in a given resultant system for $f_1, \ldots, f_s$ we get a resultant system for $g_1, \ldots, g_s$ consisting of the same number of polynomials. By 2(a) every resultant system of $g_1, \ldots, g_s$ consists of at least N_s polynomials, so we are done.

Proof of 1(b). Pick integers p and q so that f_1^p and f_2^q are of the same degree. Pick $N_3 - 1$ pairwise distinct elements $u_1, u_2, \ldots, u_{N_3 - 1}$ of k and consider the following $N_3 - 1$ forms:

$$F_i = f_1^p + u_i f_2^q \qquad (1 \leq i \leq N_3 - 1).$$

Put $R_i = R(F_i, f_3)$ if $1 \le i \le N_3 - 1$ and put $R_{N_3} = R(f_1, f_2)$, where we denote by $R(-,-)$ the ordinary resultant of two forms. The polynomials $R_1, R_2, \ldots, R_{N_3}$ form a desired resultant system. Indeed, if not all coefficients of f_3 are equal to zero, then f_3 has only $\deg f_3$ nontrivial zeros. If all $R_1, \ldots, R_{N_3}$ vanish, then every F_i has one nontrivial zero in common with f_3 and since there are $1 + \deg f_3$ forms F_i, some two of them, say, F_i and F_j, must have one and the same zero in common with f_3. Since $u_i \neq u_j$, both f_1 and f_2 have the same nontrivial zero in common with f_3, so we are done. And if all the coefficients of f_3 are equal to zero, then $R_{N_3} = 0$ implies that f_1 and f_2 (hence also f_3) have a common nontrivial zero.

Proof of 2(b). If $s = 3$, the result follows from 1(b). Assume $s \ge 4$ and $\deg g_i = \deg g_1 - 1$ for all $i > 1$. Pick N_s pairwise distinct nonzero elements $u_1, \ldots, u_{N_s}$ of k. Consider the following N_s polynomials in z:

$$G_i = \sum_{j=2}^{j=s} u_i^{j-1} g_j \qquad (1 \le i \le N_s)$$

and put

$$R_i = R(G_i, g_1) \qquad (1 \le i \le N_s).$$

The polynomials R_i form a desired resultant system. Indeed, if all the R_i are equal to zero, then every G_i has one root in common with g_1. Since g_1 has only $\deg g_1$ roots and there are $1 + (s-2)\deg g_1$ polynomials G_i, some $s - 1$ of them must have one and the same root in common with g_1. Since the determinant of the corresponding matrix consisting of powers of u_i is nonzero, all the g_i vanish when z equals this root, i.e., all the g_i have a root in common.

REFERENCES

[BF] W. Bruns and U. Vetter, "Determinantal Rings," Lecture Notes in Mathematics, Vol. 1327, Springer-Verlag, New York/Berlin, 1988.

[L1] G. Lyubeznik, "Set-Theoretic Intersections and Monomial Ideals," thesis, Columbia University, 1984.

[L2] G. Lyubeznik, On set-theoretic intersections, *J. Algebra* **87** (1984), 105–112.

[L3] G. Lyubeznik, Some algebraic sets of high local cohomological dimension in P_k^n, *Proc. Amer. Math. Soc.* **95** (1985), 9–10.

[W] B. L. van der Waerden, "Modern Algebra," Vol. 2, Ungar, New York, 1950.