J. Symbolic Computation (1990) **9**, 241–250

Generalised Characteristic Polynomials

JOHN CANNY*

543 Evans Hall, Computer Science Division, University of California, Berkeley

(*Received* 5 *October* 1987)

Multipolynomial resultants provide the most efficient methods known (in terms as asymptotic complexity) for solving certain systems of polynomial equations or eliminating variables (Bajaj *et al.*, 1988). The resultant of $f_1, \ldots, f_n$ in $K[x_1, \ldots, x_m]$ will be a polynomial in $m-n+1$ variables which is zero when the system $f_i = 0$ has a solution in $\bar{K}^m$ ($\bar{K}$ the algebraic closure of K). Thus the resultant defines a projection operator from $\bar{K}^m$ to $\bar{K}^{(m-n+1)}$. However, resultants are only exact conditions for homogeneous systems, and in the affine case just mentioned, the resultant may be zero even if the system has no affine solution. This is most serious when the solution set of the system of polynomials has "excess components" (components of dimension $>m-n$), which may not even be affine, since these cause the resultant to vanish identically. In this paper we describe a projection operator which is not identically zero, but which is guaranteed to vanish on all the proper (dimension $= m-n$) components of the system $f_i = 0$. Thus it fills the role of a general affine projection operator or variable elimination "black box" which can be used for arbitrary polynomial systems. The construction is based on a generalisation of the characteristic polynomial of a linear system to polynomial systems. As a corollary, we give a single-exponential time method for finding all the isolated solution points of a system of polynomials, even in the presence of infinitely many solutions at infinity or elsewhere.

1. Introduction

Our experience with linear algebra suggests that if we have n *polynomial* equations $f_i = 0$ in $K[x_1, \ldots, x_m]$, we should be able to successively eliminate variables and arrive at a single polynomial in $m-n+1$ variables which is zero when the original system has a solution. In fact successive elimination is an extremely inefficient way to arrive at such a condition, and it is possible to compute a much smaller polynomial whose vanishing is necessary and sufficient for the system $f_i = 0$ to have a solution. This polynomial is called the *resultant* or *eliminant* and can be thought of as a projection operator, since it defines an algebraic set which is the projection of the set defined by the system $f_i = 0$. This projection operator is a fundamental "black box" in algebraic computation with a variety of applications (Bajaj *et al.*, 1988). It can also be computed quite efficiently (Canny, 1987).

Unfortunately, although resultants are defined for homogeneous systems, they cannot readily be used for non-homogeneous systems. While the vanishing of the resultant is necessary and sufficient for a solution in projective space, in affine space we only get a necessary condition, i.e. the resultant as described in the last paragraph may vanish even if there is no affine solution, because of the presence of solution components "at infinity" (in a certain projective closure of the affine space). If these components are of excess ($>m-n$) dimension, the resultant will vanish identically, and provide no information about the

*Supported by a David and Lucile Packard Foundation Fellowship and by NSF Presidential Young Investigator Grant IRI-8958577.

0747-7171/90/030241+10 $03.00/0

solution set. In this paper we describe a projection operator that cannot vanish identically, and which is equal to the (homogeneous) resultant if the resultant is not identically zero.

The operator is based on a generalisation of the characteristic polynomial of a system of linear equations to systems of multivariate polynomial equations. The generalisation is natural in the sense that it reduces to the usual definition when all the polynomials are linear. Whereas the constant coefficient of the characteristic polynomial of a linear system is the determinant, the constant coefficient of the generalised characteristic polynomial (henceforth GCP) is the *resultant* of the system. More generally, the *lowest degree non-identically zero coefficient* of the GCP is the projection operator we are looking for. It has the property that it is zero on the projection of any *proper* (dimension $= m-n$) component of the algebraic set defined by the system $f_i = 0$.

The GCP projection operator has the following limitation: although it vanishes on the projection of all proper components, it may also vanish on the projection of certain proper algebraic sets that are contained in excess components. So if the lowest-degree coefficient of the GCP vanishes at a point, no information is given as to whether that point is the projection of a point in an excess or proper component. However, this information has not been needed in the applications of the GCP operator to date (Canny, 1987; Renegar, 1989; Ierardi, 1989).

As an application, we describe an efficient algorithm for solving systems of polynomial equations over the complex numbers which works even in the presence of infinitely many solutions "at infinity". The methods of Lazard (1981), Renegar (1987) and Canny (1987) all give single-exponential time bounds for the problem of solving polynomial systems. But these methods are all based on the u-resultant (van der Waerden, 1950) and are only applicable to systems to homogeneous polynomials having finitely many solutions. As we shall see in section 4 of this paper, the presence of an infinite number of solutions causes all the u-resultant based methods to fail. Using the GCP projection operator allows these methods to run in single-exponential time and to succeed even in the presence of an infinity of solutions. It does not matter whether these solutions are at infinity or elsewhere, and we obtain all the isolated points in the solution set.

When considering new equation solving and elimination problems, it is natural to contrast them with Gröbner basis algorithms (Buchberger, 1985). A lexicographic-ordered Gröbner basis can be very easily used to compute solutions of a polynomial system, and for variable elimination. However, it cannot be computed as efficiently as the GCP. The differences are most marked when the dimension of the set of solutions of the polynomial system is greater than one. Here the running time of the Gröbner basis algorithm may be double exponential (time $d^{2^{O(n)}}$) in the number of variables n, and there are examples of polynomials systems which attain this bound (Mayr & Meyer, 1982) (d is the maximum degree of the input polynomials). If the dimension of the set of solutions is zero, then much better bounds apply, and the basis algorithm will run in $d^{O(n^2)}$ time (Caniglia *et al.*, 1989). The example due to Brownawell (1987) suggests that this bound is tight. The method described in section 3 of this paper on the other hand, can find a point in every proper component of an algebraic set in time $d^{O(n)}$. If the input polynomials are densely represented, this bound is low order polynomial (about $O(N^4)$) in the input size for every fixed n. The Gröbner basis bound by contrast, even for dimension zero ($d^{O(n^2)}$), is super-polynomial for n fixed.

On sparse systems, Gröbner algorithms seem to do much better than the worst case bounds. For large, dense problems however, the resultant and GCP methods should be faster. Currently, the best resultant algorithm takes time $O(N^{2+\varepsilon})$ with dense input and

fixed n (Canny *et al.*, 1989), and a good research topic is to reduce this to a pseudo-linear bound $O(N^{1+\varepsilon})$ for fixed n. Right now, there is a pseudo-linear algorithm only in the case $n = 2$. Resultant algorithms can be adapted to GCP calculation with an increase by a factor of N in the complexity. In fact GCP algorithms are not new. The methods of Renegar (1987) and Canny (1987) for resultant computation actually compute a GCP (or something very close to it) as a side effect. So it comes essentially free with these methods.

The paper is structured as follows. We give a definition of the generalised characteristic polynomial in section 2, and briefly sketch an algorithm for it. In section 3 we prove that the GCP has the desired properties, using some basic results about dimension of algebraic sets. We show that while the resultant may vanish identically in the presence of solutions of excess dimension, the lowest degree coefficient of the GCP still contains information about the components of proper dimension. Finally, in section 4 we apply these results to the equation solving problem. Using the u-resultant construction and the GCP we obtain a single exponential time algorithm which recovers all isolated solutions to a system of homogeneous polynomials even if the system has solutions of excess dimension.

2. Computation of Generalised Characteristic Polynomials

In this section we give the construction of the generalised characteristic polynomial $C(s)$ for a system of homogeneous polynomials f_i. It is a natural generalisation of the characteristic polynomial of a linear system and it equals the latter in the special case where all the f_i are linear. The constant coefficient of $C(s)$ is the (multipolynomial) resultant of the f_i. This property is analogous to the fact that the constant coefficient of the characteristic polynomial of a linear system is the determinant. Our construction is based on Macaulay's (1902) formula for the general resultant. Macaulay shows that the resultant equals the quotient of the determinant of a certain matrix A whose entries are coefficients of the polynomials, and a subdeterminant of A.

Suppose we are given n homogeneous polynomials f_i in n variables x_j, and that f_i has degree d_i. We need some notation for monomials of f_i. Let α be an n-tuple of integers, we write x^α for the monomial $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$.

The rows and columns of the matrix A are indexed by the set of monomials in $x_1, \ldots, x_n$ of degree d where

$$d = 1 + \sum_{i=1,\ldots,n} (d_i - 1) \tag{1}$$

and letting X^d denote the set of monomials of degree d, the cardinality of X^d is

$$N = |X^d| = \binom{d+n-1}{d} \tag{2}$$

DEFINITION. A polynomial is said to be *reduced* in x_i if its degree (the maximum degree of its monomials) in x_i is less than d_i. A polynomial that is reduced in all variables but one is said simply to be reduced.

Now consider the polynomial

$$F = C_1 f_1 + C_2 f_2 + \ldots + C_n f_n \tag{3}$$

where each C_i is a homogeneous polynomial of degree $d - d_i$ with symbolic coefficients,

which is reduced in $x_1, \ldots, x_{i-1}$ for $2 \leq i \leq n$. F is a homogeneous polynomial of degree d, and so has N coefficients. There are also, in total, exactly N coefficients in the C_i. To see this, imagine for the moment that each f_i equals $x_i^{d_i}$. Then every monomial in F is a multiple of a monomial from exactly one of the C_is. For the monomial cx^α, let j be the smallest index i such that x^α is not reduced in x_i. Then cx^α is a multiple of a monomial from C_j and from no other C_i.

Since the coefficients of F are linear functions of the coefficients of the C_i via (3), this determines a linear map A from coefficients of the C_i to coefficients of F. Each non-zero entry in the matrix A is a coefficient of some f_i. This defines the matrix A that we mentioned earlier.

More concretely, if we index rows and columns of A by elements of X^d, then the column corresponding to x^α represents the polynomial

$$\frac{x^\alpha}{x_i^{d_i}} f_i \tag{4}$$

where i is the smallest j such that x^α has degree at least d_j in x_j.

The determinant of A vanishes if the f_i have a common zero, and it is therefore a multiple of the resultant R of the system (Macaulay, 1902). We can write $\det(A) = MR$, where M is an additional factor which we would like to remove. Macaulay shows that M is the determinant of a certain submatrix of A, in fact the submatrix of elements whose row and column indices are not reduced. Thus he obtains the simple formula $R = \det(A)/\det(M)$.

Having given a brief sketch of what a multipolynomial resultant is, we can now give the construction of generalised characteristic polynomials.

DEFINITION. The *generalised characteristic polynomial* (or GCP), $C(s)$ of a system of homogeneous polynomials $f_1, \ldots, f_n$ in $x_1, \ldots, x_n$ is the resultant of $\hat{f}_1, \ldots, \hat{f}_n$, where $\hat{f}_i = f_i - s x_i^{d_i}$.

We do not claim this to be a novel construction. But what has not previously been observed is that it is both inexpensive to compute, and that it can be used to recover all the isolated zeros of a system of polynomials, as shown in the next section.

Inspection of the matrices A and M shows that the coefficients of $x_i^{d_i}$ in f_i always appear on the leading diagonals. So the determinant of the matrix $\hat{A}$ for the new system $\hat{f}_i$ is actually the characteristic polynomial (in the usual sense) of A, i.e. $\det(\hat{A}) = \det(A - sI) = \text{CharPoly}(A)(s)$, where $\text{CharPoly}(A)(s)$ denotes the characteristic polynomial of A in the variable s. The same holds true for M, so that the *generalised* characteristic polynomial of the f_i is given as

$$C(s) = \frac{\text{CharPoly}(A)(s)}{\text{CharPoly}(M)(s)} \tag{5}$$

Now A is an $N \times N$ matrix, while M has $N - D$ rows and columns, where

$$D = \sum_i \prod_{j \neq i} d_j \tag{6}$$

is the number of reduced rows (or columns). This follows because a reduced monomial is reduced in all variables but one, say the i^{th}, and its degree in every other x_j is in the range $0, \ldots, d_j - 1$, i.e. d_j values. This implies that $\text{CharPoly}(A)(s)$ has degree N and

CharPoly(M)(s) has degree $N-D$, so that the GCP $C(s)$ has degree D. To compute a characteristic polynomial using Newton's identity (Csanky, 1976) takes $O(N^4)$ arithmetic operations. For large problems, N is much larger than D, and so it seems that computation of all N coefficients of CharPoly(A)(s) in (5) is wasteful. But we can use the fact that if the quotient of two polynomials has degree D, then that quotient depends only on the D most significant coefficients of those polynomials. So it is possible to compute $C(s)$ by computing only the first D coefficients of CharPoly(A)(s) and CharPoly(M)(s). Using the Newton identity, this can be done with $O(N^3D)$ operations.

3. Main Properties

We next prove our main result, that the GCP $C(s)$ contains all the information needed to recover the proper components of the zeros set of the f_i. This result gives as an immediate corollary, a method for finding all the zeros of a system of n non-homogeneous polynomials in n variables, even if such a system has infinitely many solutions "at infinity". The method is based on the u-resultant (van der Waerden, 1950), but unlike previous methods (Lazard, 1981; Reneger, 1987; Canny, 1987) does not require that there be only finitely many solutions at infinity. As noted previously, the GCP must be used with some care because it will also provide proper components within excess components, but does not distinguish these from the true proper components.

To begin, we give some definitions and basic results on dimension of algebraic sets. We will not define the dimension of an algebraic set, but detailed definitions are given in Mumford (1976) chapter 1, page 6. In what follows, we assume that variable values range over the complex numbers $\mathbb{C}$.

DEFINITION. The set of common zeros of a system of polynomials $f_1, \ldots, f_n$ in $x_1, \ldots, x_m$ is called an *algebraic set* and is denoted $V(f_1, \ldots, f_n) \subset \mathbb{C}^m$. An algebraic set $V(f)$ defined by a single polynomial (which is not identically zero) is called a *hypersurface*. If f is linear, then $V(f)$ is called a *hyperplane*.

If all the f_i are homogenous, it is more convenient to work with the projective space $\mathbb{P}^{m-1}$, formed by identifying points in $\mathbb{C}^m$ which are scalar multiples of each other. That is, a "point" in $\mathbb{P}^{m-1}$ corresponds to all points in $\mathbb{C}^m$ of the form $\lambda(p_1, \ldots, p_m)$, where the $p \in \mathbb{C}^m$ is a non-zero constant vector, and λ ranges over all non-zero complex values. Points in $\mathbb{P}^{m-1}$ are sometimes called solution "rays" for this reason. $\mathbb{P}^{m-1}$ has dimension $m-1$ and is compact. We use the same notation, $V(f_1, \ldots, f_n) \subset \mathbb{P}^{m-1}$ for an algebraic set defined by homogenous polynomials f_i.

DEFINITION. An algebraic set is said to be *reducible* if it can be expressed as a finite union of proper subsets which are algebraic. An algebraic set which is not reducible is *irreducible*.

Any algebraic set can always be expressed as a finite union of irreducible algebraic subsets called *components*. Many results in algebraic geometry apply only to irreducible algebraic sets, and in much of what follows, we work with the individual components of an algebraic set.

DEFINITION. Let Z be the intersection of m hypersurfaces in n-dimensional affine or projective space. A component W of Z is said to be *proper* if it has dimension $n-m$. A component of dimension greater than $n-m$ is said to be an *excess* component.

And in fact all components of an intersection must be either proper or excess by the following lemma:

LEMMA 3.1. *If f_i are m non-honogeneous polynomials in n variables, (or homogeneous in $n+1$ variables), then every component of $V(f_1, \ldots, f_m)$ has dimension at least $n-m$.*

For a proof, see for example Mumford (1976) corollary 3.14. Our main result is that if $C(s)$ is arranged in powers of s, then its lowest degree coefficient vanishes on the projection of all proper components of the intersection. We start with n polynomials $f_i(u_1, \ldots, u_m, x_1, \ldots, x_n)$, which are homogeneous in the x_j. Then:

THEOREM 3.2. *Let $Z = V(f_1, \ldots, f_n) \subset \mathbb{C}^m \times \mathbb{P}^{n-1}$, and let W be a proper component of Z, so that the dimension of W is $m-1$. Let $C(u_1, \ldots, u_m)(s)$ be the generalised characteristic polynomial of the f_i, as polynomials in the x_j. Arranging the GCP in powers of s, let $C_k(u_1, \ldots, u_m)$ be its coefficient of lowest degree. If $\pi_u : \mathbb{C}^m \times \mathbb{P}^{n-1} \to \mathbb{C}^m$ denotes projection on u_i-coordinates, then $C_k(\pi_u(p)) = 0$ for all $p \in W$.*

PROOF. The GCP is the resultant of the polynomials $\hat{f}_i = f_i - sx_i^{d_i}$. With the addition of the complex variable s, the zeros set of the $\hat{f}_i$, call it Z', lies in $\mathbb{C}^m \times \mathbb{P}^{n-1} \times \mathbb{C}$. Since $\hat{f}_i$ and f_i are identical when $s = 0$, the intersection of Z' and the hypersurface $s = 0$ is exactly $Z \times \{0\}$. So for every component W of Z, we have $W \times \{0\} \subset Z'$. If W is a *proper* component it has dimension $m-1$, but by the dimension lemma, every component of Z' has dimension at least m. So $W \times \{0\}$ must be contained in some component W' of dimension m.

Because every point of W' has an m-dimensional neighbourhood, and because the intersection of this neighbourhood with the hypersurface $s = 0$ is $(m-1)$-dimensional, it follows that for every point $p \in W \times \{0\}$, there is a sequence of points (p_j) in $W' - W \times \{0\}$ which converges to p. Writing $C(u_1, \ldots, u_m)(s)$ now for the GCP of the f_i, or equivalently the resultant of the $\hat{f}_i$, then $C(\pi_u(q))(\pi_s(q)) = 0$ for any point q in Z', where π_s denotes projection on the s-coordinate. In particular $C(\pi_u(p_j))(\pi_s(p_j)) = 0$ for all j. Dividing this polynomial through by $\pi_s(p_j)^k$ (which is non-zero), and letting C_i denote the coefficient of s^i in the GCP, we obtain

$$C_k(\pi_u(p_j)) + \sum_{i=k+1,\ldots,D} (\pi_s(p_j))^{i-k} C_i(\pi_u(p_j)) = 0 \tag{7}$$

for all p_j, where C_k is the lowest degree non-vanishing coefficient of $C(s)$, and D is the degree of $C(s)$. This expression is a polynomial in the coordinates of the p_j, and is therefore a continuous function of the coordinates. Since it is zero for all $p_j \to p$, it must be zero at p. But the point p has s-coordinate zero, so the summation over i vanishes, and we conclude that $C_k(\pi_u(p))$ must equal zero. □

We can restate the theorem succinctly as:

$$\pi_u(\cup W_i) \subset V(C_k) \subset \pi_u(V(f_1, \ldots, f_n)) \tag{8}$$

The second containment follows because $\pi_u(V(f_1, \ldots, f_n)) = V(C_0)$, where C_0 is the resultant of the f_i. If $k = 0$ it is trivially true, whereas $k > 0$ implies $C_0 = 0$, so that $V(C_0) = \mathbb{C}^m$.

CONJECTURE. We conjecture that if Z_i is *any* component of $V(f_1, \ldots, f_n)$, then it contains a component that intersects the closure of the perturbed system for $s \neq 0$, i.e. there exists a

non-empty algebraic set U such that

$$Z_i \supset U \subset \overline{(V(\hat{f}_i, \ldots, \hat{f}_n) - V(s))} \tag{9}$$

To prove the conjecture, one needs to show that if Z is an excess component, for small enough ε, $V(\hat{f}_i, \ldots, \hat{f}_n) \cap V(s = \varepsilon)$ has a proper component "near" to Z. The intuition behind this is that if just one of the coefficients of $x_i^{d_i}$ in f_i is changed slightly, it causes each component of the intersection to either "move" slightly, or to be cut into components of lower dimension, which are all contained within that component. In either case, every point of the new intersection is close to some point of the old intersection. Applying this inductively to each f_i, we eventually obtain a new intersection with only proper components, such that each of its components is near to one of the original components.

It is also reasonable to conjecture that the degree of vanishing of $C(u_1, \ldots, u_m)(s)$, at some point $u_i = p_i$ is a measure of the intersection multiplicity (in some appropriate sense) of the surfaces defined by the f_i. For example, we could consider the intersection multiplicity of the surfaces $f_i(p_1, \ldots, p_m, x_1, \ldots, x_n) = v_i$ in $\mathbb{C}^{2n}$.

4. Application to Equation Solving

The main theorem of the last section can be applied to the following problem: Given n non-homogeneous polynomials g_i in n variables, $x_1, \ldots, x_n$ find all the isolated solution points of the system $g_i = 0$. By isolated solution points, we mean those points that are not contained in some higher-dimensional component of the solution set. The system has an equal number of equations and variables, and so the proper components of $V(g_1, \ldots, g_n)$ are zero-dimensional, i.e. points.

Since the methods we will use apply to homogeneous polynomials, we must produce a homogeneous system from the g_i by introducing an additional variable x_0. For each polynomial g_i of degree d_i we produce a homogeneous polynomial f_i of degree d_i by multiplying terms of g_i of degree δ_i by $x_0^{(d_i - \delta_i)}$. Then if $(p_1, \ldots, p_n) \in \mathbb{C}^n$ is a solution of the original system, $\lambda(1, p_1, \ldots, p_n) \in \mathbb{P}^n$ is a solution ray of the homogeneous system.

In fact there is a one-to-one correspondence between solution points of the original system and solution rays of the homogeneous system which have $x_0 \neq 0$. However, there may be solutions of the homogeneous system which have $x_0 = 0$, called "solutions at infinity" which have no counterpart in the original system. There may in fact be excess components of the intersection at infinity, even if the original system has only proper solutions.

The presence of excess components at infinity causes the methods of Lazard (1981), Renegar (1987) and Canny (1987) to fail, and there is no easy way to ensure that the given system has only proper solutions at infinity. The methods just mentioned are the only polynomial equation-solving methods that have single exponential bounds. They are based on the u-resultant which we now describe. Using the GCP, we can give a u-resultant style method with single-exponential time bounds which succeeds even in the presence of excess solutions at infinity or elsewhere.

To a system of n homogeneous polynomials f_i in $n+1$ variables, we add the linear polynomial

$$u_0 x_0 + u_1 x_1 + \ldots + u_n x_n \tag{10}$$

where the coefficients $u_0, \ldots, u_n$ are indeterminates. We call this last polynomial the *u-form* and denote it $U(x_0, \ldots, x_n, u_0, \ldots, u_n)$. We now have a system of $n+1$ homogeneous

polynomials in $n+1$ variables, and the resultant of such a system is a polynomial $R(u_0, \ldots, u_n)$ called the u-resultant.

Suppose now that $\lambda(p_0, \ldots, p_n)$ is a solution ray of the system f_i. Then it will also satisfy the u-form U if and only if

$$p_0 u_0 + \ldots + p_n u_n = 0 \tag{11}$$

So the system as a whole has a solution, and therefore the resultant $R(u_0, \ldots, u_n)$ will vanish, whenever $p_0 u_0 + \ldots + p_n u_n = 0$. This implies that $(p_0 u_0 + \ldots + p_n u_n)$ *divides* $R(u_0, \ldots, u_n)$. Similarly, every other solution ray of the f_i leads to a corresponding linear factor of the u-resultant. By computing the u-resultant and factoring it over the complex numbers, we can obtain the coordinates of all the solution rays. This is the essence of the methods in Lazard (1981), Renegar (1987), and Canny (1987) although they differ in how the factorisation is computed.

But suppose now that $V(f_1, \ldots, f_n)$ has a component of dimension 1 (or higher). It is a standard result (Mumford, 1976, corollary 3.30), that two projective varieties in the same space always intersect if the sum of their dimensions is at least the dimension of the space. For any fixed set of values of the u_i, the equation $u_0 x_0 + \ldots + u_n x_n = 0$ defines a variety of dimension at least $n-1$ in $\mathbb{P}^n$, and this must always intersect an excess solution of the f_i, irrespective of the value of the u_i. So the polynomial $R(u_0, \ldots, u_n)$ must be zero for all values of the u_i, i.e. it is identically zero. This is why the u-resultant methods fail if there are excess components in the solution set.

To get around this problem, we use a slight variation of the GCP of the f_i and the u-form U. Normally in constructing the GCP we would subtract sx_n from the last polynomial, which is U. But x_n already has a symbolic coefficient (u_n) in U. We compute instead the resultant of $\hat{f}_i = f_i - sx_i^{d_i}$, for $i = 1, \ldots, n$ and the unchanged u-form, and this will still give us a non-vanishing resultant (since we could specialise $u_n = s$ which makes the resultant monic in s). Another way to compute this resultant is to compute the GCP of the f_i *and* U, and then to substitute $u_n + s$ for u_n in the GCP.

Let the resultant obtained by either method be denoted $R(s, u_0, \ldots, u_n)$, then we see that it is precisely the u-resultant of the system $\hat{f}_i = 0$. Now for almost all values of s, and in particular, all sufficiently small values of $s \neq 0$, the perturbed system $\hat{f}_i = 0$ will have a finite number of solution rays. This follows because the resultant is a non-identically vanishing polynomial in s, and is the u-resultant of the system $\hat{f}_i = 0$. The number of solutions will be $\prod d_i$ (counting multiplicity), by Bezout's theorem.

We can think of the zeros set $V(\hat{f}_1, \ldots, \hat{f}_n, U)$ as lying in the space $\mathbb{C}^{n+1} \times \mathbb{P}^n \times \mathbb{C}$ with coordinates $(u_0, \ldots, u_n, \lambda(x_0, \ldots, x_n), s)$. Taking a sequence $(s_k) \to 0$, each solution set $V(\hat{f}_1, \ldots, \hat{f}_n, U, s - s_k)$ consists of $\prod d_i$ n-dimensional planes, counting multiplicity, whose projections on u_i-coordinates are hyperplanes. Each of these hyperplanes must approach a limiting hyperplane (possibly via a subsequence) at $s = 0$. This follows because the Grassmanian of hyperplanes in $\mathbb{C}^{n+1}$ is compact (Mumford, 1976, p. 174).

If $C_k(u_0, \ldots, u_n)$ is the lowest degree non-vanishing coefficient of $R(s, u_0, \ldots, u_n)$ as a polynomial in s, then from the proof of the main theorem of the last section, C_k must vanish on the projection of all the limit points of $V(\hat{f}_1, \ldots, \hat{f}_n, U)$ as $s \to 0$. Thus it must vanish at all of the $\prod d_i$ limiting hyperplanes, and therefore factors completely into linear factors because the degree of C_k is also $\prod d_i$. To see this, recall that the degree of the resultant in the coefficients of each polynomial is the product of the degrees of the other polynomials. Since the u-form is independent of s, the degree of the resultant (and all its coefficients as a polynomial in s) in the u_is must be $\prod d_i$.

The equation solving methods of Renegar (1987) and Canny (1988) avoid explicit computation of $R(u_0, \ldots, u_n)$, since it has so many coefficients ($O(d^{n^2})$ if all polynomials have degree d). Instead, they compute certain specialisations of it. For example in Canny (1988) the solutions not at infinity can be found with the following specialisations: $R_0(v, t) = R(v, t, t^2, \ldots, t^n)$ and $R_i^+(v, t) = R(v, t, \ldots, t^i+1, \ldots, t^n)$ and $R_i^-(v, t) = R(v, t, \ldots, t^i-1, \ldots, t^n)$, for $i = 1, \ldots, n$. Making these specialisations *before* the resultant is computed means that all arithmetic is done on polynomials in two variables v and t, and so the number of coefficients is at most $O(d^{2n})$.

We can make the same specialisations of the u_is before making the perturbation. The arguments in Canny (1988) which show that the resultant is non-vanishing for the above specialisations also apply to the lowest degree coefficient of $R(s, u_0, \ldots, u_n)$. So it is impossible for example, that the lowest degree coefficient of the specialisation of $R(s, u_0, \ldots, u_n)$ could be some other coefficient than C_k. Since C_k factors completely into linear factors, the methods of Renegar (1987) and Canny (1988) for factorising the u-resultant from its specialisations still apply to C_k and its specialisations. So, to summarise, the isolated solution points of a system of polynomials can be found using Renegar (1987) or Canny (1988) by replacing each resultant with the lowest degree coefficient of a specialisation of $R(s, u_0, \ldots, u_n)$.

5. Conclusions

We described a new construction called the generalised characteristic polynomial, which is a useful adjunct to the multipolynomial resultant. The GCP can be used in situations where resultant-based methods fail because of the presence of components of excess dimension in the solution set of a system of polynomials. It provides a means for systematically perturbing a polynomial system away from a "bad" or excess intersection, and for recovering the proper components of the intersection, which are robust with respect to this perturbation. While it is guaranteed to contain projections of all proper components, it may also contain the projections of proper components that lie inside excess components.

The GCP can be obtained naturally from certain resultant algorithms. We showed that it can be computed as a quotient of the characteristic polynomials of two square matrices. By judicious use of Newton's identity for characteristic polynomials, the quotient can be found by computing only some of the coefficients of the matrix characteristic polynomials. This provides a significant reduction in the cost of computing the GCP. But there is still much that can be done to improve the running time of both resultant and GCP algorithms. Our algorithm required $O(N^4)$ operations as a function of the matrix size, whereas in the special case of two homogeneous polynomials, the (Sylvester) resultant can be computed with $O(N \log^2 N)$ operations. It should be possible to improve the GCP bounds to quadratic or pseudo-linear.

References

Bajaj, C., Garrity, T., Warren, J. (1988). On the applications of multi-equational resultants, Computer Science Department Technical Report No. 826, Purdue University.

Brownawell, D. (1987). Bounds for the degrees in the Nullstellensatz. *Ann. Math.* 2nd series, **126**, 577–591.

Buchberger, B. (1985). Gröbner: An algorithmic method in polynomial ideal theory. *Multidimensional Systems Theory* (N. K. Bose, ed.), D. Reidel, Dordrecht, chapter 6.

Caniglia, L., Galligo, A., Heintz, J. (1989). Some new effectivity bounds in computational geometry. *Proc. 6th Int. Conf. on Applied Algebra and Error-correcting codes*, LNCS 357, Springer-Verlag, Berlin, 131–152.

Canny, J. F. (1987). A new algebraic method for motion planning and real geometry. *Proc. 28th IEEE Symp.* FOCS, Los Angeles, 39–48.

Canny, J. F. (1988). Some algebraic and geometric computations in PSPACE. *Proc. ACM STOC,* Chicago, 460–467.

Canny, J., Kaltofen, E, Yagati, L. (1989). Solving systems of non-linear polynomial equations faster. *Proc. ACM Int. Symp. on Symbolic and Algebraic Computation,* Portland OR, 121–128.

Csanky, L. (1976). Fast parallel matrix inversion algorithms. *SIAM J. Comp.* **5,** 618–623.

Ierardi, D. (1989). Quantifier elimination in the theory of an algebraically-closed field. *Proc. 21st ACM STOC,* Seattle WA, 138–147.

Lazard, D. (1981). Résolution des systèmes d'équations algébriques. *Theor. Comp. Sci.* **15,** 146–156.

Macaulay, F. S. (1902). Some formulae in elimination. *Proc. London Math. Soc.* (1) **35,** 3–27.

Mayr, E., Meyer, A. (1982). The complexity of the word problem for commutative semigroups and polynomial ideals. *Adv. Math.* **46,** 305–329.

Mumford, D. (1976). *Algebraic Geometry I, Complex Projective Varieties.* Springer-Verlag, Berlin.

Renegar, J. (1987). On the worst case arithmetic complexity of approximating zeros of systems of polynomials. Technical Report, School of Operations Research and Industrial Engineering, Cornell University.

Renegar, J. (1989). On the computational complexity and geometry of the first-order theory of the reals, Parts I, II, and III, Technical Reports, School of Operations Research and Industrial Engineering, Cornell University.

van der Waerden, B. L. (1950). *Modern Algebra* (3rd edn.) F. Ungar, New York.