The Complexity of Resolvent Resolved *

Giovanni Gallo
Universitá di Catania
Italy

Bhubaneswar Mishra
Courant Institute, NYU
USA

Abstract

The concept of a resolvent *of a* prime ideal *was originally introduced by J.F. Ritt along with the notion of a characteristic set. The motivation for studying* resolvents *comes from its connections with the birational isomorphisms that describe structures of irreducible algebraic varieties by means of an equivalent hypersurface and a one-to-one rational map. As a result, these ideas have a wide range of applications in such areas as solid modeling, computer-aided design and manufacturing. An algorithm to compute the resolvent by means of characteristic sets was first proposed by Ritt. This and some related algorithms have resurfaced as interest in resolvent structures have grown, spurred by its applicability.*

Unfortunately, the algebraic complexity of the resolvent and the computational complexity of the associated algorithms have never been explicitly explored. In this paper, we give single exponential upper and lower bounds for the degrees of the resolvent and its associated parametrizing polynomials. We also show that the resolvent can be computed deterministically in single exponential sequential and polynomial parallel time complexity. All previous algorithms for resolvent had relied on a random choice of certain extraneous parameters.

*Supported by an Italian grant Italian MURST 40% Calcolo Algebraico e Simbolico 1993 and an NSF grant:#: CCR-9002819.

1 Introduction

The concept of a *resolvent* for a system of algebraic equations in n unknowns and over an algebraically closed field k of characteristic zero was originally introduced by J.F. Ritt. Ritt describes this theory in his books ([14, 15]) both for systems of purely algebraic and of differential algebraic equations and we follow his approach closely.

The motivation for studying *resolvents* comes from its connections with the birational isomorphisms that describe structures of irreducible algebraic varieties by means of an equivalent hypersurface and a one-to-one rational map. Furthermore, the structure provided by resolvents can also be fruitfully exploited in many applications involving description of and operations on algebraic surfaces.

Definition 1.1
(Rational Maps and Birational Isomorphisms)
A *rational map* $\phi : X \to Y \subseteq A^n$ is a collection of n rational functions $\phi_1, \ldots, \phi_n \in k(X)$, the field of rational functions over the variety X, such that $(\phi_1(x), \ldots, \phi_n(x)) \in Y$ for every

point $x \in X$ at which all the functions ϕ_i are regular.

A rational map $\phi : X \to Y$ is called a *birational isomorphism* if there is a rational map $\psi : Y \to X$ such that ψ is the inverse of ϕ. In this case X and Y are birationally isomorphic or equivalent. □

A birational map between varieties is, set-theoretically, a one-to-one correspondence between open sets (in the sense of Zariski topology) of one variety with another.

This definition leads naturally to a classification, modulo birational maps, of all the irreducible varieties: Two varieties are in the same class if they are birationally equivalent. Such classification is quite rough. For example, it does not preserve the singularities of a variety, while instead it preserves the genus and the dimension of a variety. In fact it is a fundamental problem in algebraic geometry to look, inside a birational class of varieties, for representatives (also called *models*) with some special properties, for example *smoothness* (see [17] pp. 105–108, for a summary of the known results about the existence of non-singular models).

It is sometimes important for applications in graphics and solid modeling to find a birational model of a given variety that can be described with a minimal number of indeterminates. This model may be easier to parametrize; its points may be easier to construct, thus allowing it to be used, together with the rational map that gives the birational equivalence, in investigating the original variety or at least some open subsets of it. The existence of such a rational model is a consequence of the following basic theorem of algebraic geometry:

Theorem 1.1 *Every irreducible closed set X is birationally isomorphic to a hypersurface in some affine space A^n (see [17] pp. 29).* □

The resolvent construction due to Ritt (but probably known to Kronecker for the algebraic case), gives another constructive proof of this result. Ritt, moreover, generalized the above theorem to algebraic systems of differential equations and it is one of the main tools in the investigation of such systems.

The resolvent computation relies on an elimination procedure: Ritt used his 'characteristic sets,' but it is easily seen that other techniques, for example Gröbner bases[2, 3, 12, 13], can be used as well. Here we will use characteristic sets, and the bounds on their complexity in [6] and [7], to get bounds on the complexity of the resolvent.

The current interest in applications of resolvents for parametrization has been spurred by the work of Gao and Chou [9], who first presented a probabilistic algorithm for resolvent without a complexity analysis. Certain complexity results related to the resolvent may be inferred from the work of Giusti and Heinz [10] and Alonso et. al. [1]. Here, we present tight upper and lower bounds for resolvent computation without relying on randomization.

2 The Resolvent

Through out this paper, $I = (f_1, \ldots, f_m)$ denotes a *prime ideal* generated by the polynomials $f_1, \ldots, f_m$ in the ring of $k[x_1, \ldots, x_n]$, where k is an *algebraically closed field of characteristic zero*.

Let $u_1, \ldots, u_q$ be a maximal set of algebraically independent variables, with respect to I, and let the other $p = (n-q)$ variables be renamed as $y_1, \ldots, y_p$. It is possible to compute such a maximal set of independent variables using $O(m^{O(1)} d^{O(n^2)})$ time on a sequential computer or $O(n^4 \log^2(m+d+1))$ time on a parallel computer ([4, 11]). Following Ritt, we shall call this maximal set of algebraically independent variables a *parametric set*, since, in fact, they allow a rational parametrization of the variety, as shown below.

Consider the following ordering on the variables:

$$u_1 < u_2 < \cdots < u_q \ < y_1 < y_2 < \cdots < y_p,$$

and a characteristic set for I, with respect to this ordering:

$$g_1, \ldots, g_p, \quad g_i \in k[u_1, \ldots, u_q, y_1, \ldots, y_i].$$

Since I is prime, $I = (g_1, \ldots, g_p)$. For the definition of characteristic sets and algorithms to compute them the reader may refer to [7, 8, 12, 14] or [18]. (Also, see appendix.)

The resolvent computation requires existence (but not direct construction) of an open subset (in the sense of Zariski topology) of the variety defined by I where there is a one-to-one correspondence between the values taken by the parameters and the values of some linear function in the y_i's. The existence of such an open set is proved in the following lemma (also, see [14] pp. 26–31) and is defined by $h \neq 0$.

Lemma 2.1 *Let I be a prime ideal with a characteristic set $(g_1, \ldots, g_p)$ as above. Then there exist a polynomial h only in the u_i's and a polynomial $c = a_1y_1 + a_2y_2 + \cdots + a_py_p$, with a_j's constant, such that if*

$$(\overline{u_1}, \ldots, \overline{u_q}, y'_1, \ldots, y'_p) \quad \textit{and} \quad (\overline{u_1}, \ldots, \overline{u_q}, y''_1, \ldots, y''_p)$$

are two points of the variety defined by I then

$$h(\overline{u_1}, \ldots, \overline{u_q}) \neq 0 \quad \textit{and} \quad (y'_1, \ldots, y'_p) \neq (y''_1, \ldots, y''_p)$$

implies that

$$c(\overline{u_1}, \ldots, \overline{u_q}, y'_1, \ldots, y'_p) \neq c(\overline{u_1}, \ldots, \overline{u_q}, y''_1, \ldots, y''_p).$$

PROOF.
Introduce new variables $z_1, \ldots, z_p$ and consider the polynomials $s_1, \ldots, s_p$ obtained by substituting the y_i's with corresponding z_i's in the polynomials $g_1, \ldots, g_p$. Now, consider the variety V defined in a $q + 2p$ dimensional affine space by the ideal J generated by $(g_1, \ldots, g_p, s_1, \ldots, s_p)$.

It is then easy to verify that V has still dimension q and that $u_1, \ldots, u_q$ form a maximal set of algebraically independent variables with respect to J. Let

$$V = V_1 \cup V_2 \cup \cdots \cup V_t$$

be an irreducible decomposition of V. For each irreducible component V_i of V, one of the following three cases holds:

(A) *V_i is of dimension lower than q.* Thus, the prime ideal associated with this component in the irreducible decomposition of J must contain a polynomial only in the u_i's. Call this polynomial h_i.

(B) *V_i is of dimension q* and it is contained in the q-dimensional linear subspace determined by the equations

$$z_1 = y_1, \ \ z_2 = y_2, \ \ \ldots, \ \ z_p = y_p.$$

In this case, put $h'_i = 1$.

(C) *V_i is of dimension q* and it is not contained in the q-dimensional linear subspace determined by the equations

$$z_1 = y_1, \ \ z_2 = y_2, \ \ \ldots, \ \ z_p = y_p.$$

In this case V_i will not be contained in the hyperplane $z_j = y_j$ for some index j. Hence, the ideal generated by the prime ideal associated with V_i and by the polynomial $z_j - y_j$ is of dimension $< q$ and thus, must contain a polynomial only in the u_i's. Call this polynomial h'_i.

Let now $\overline{c}$ be the hyperplane of the linear equation

$$a_1(y_1 - z_1) + a_2(y_2 - z_2) + \cdots + a_p(y_p - z_p).$$

For a generic choice of a_i's, $\overline{c}$ intersects each irreducible component of V of dimension q in a lower dimensional variety, if the component is not completely contained in the diagonal

$$z_1 = y_1, \;\; z_2 = y_2, \;\; \ldots, \;\; z_p = y_p.$$

Now consider the ideal J_i generated by $\overline{c}$ and by one of the prime ideals associated with the irreducible component V_i of V. Such an ideal must have dimension at most $(q-1)$ and thus, contain a polynomial only in u_i's as they are dependent in J_i. Let $h_i'' \in J_i$ be the polynomial in u_i's.

Define h to be the product of all of the h_i's, the h_i''s and the h_i'''s. It is now simple to verify that the polynomials

$$c = a_1 y_1 + a_2 y_2 + \cdots + a_p y_p$$

and h, by construction, have the properties desired in the statement of the lemma; in fact, $\overline{c}$ is never zero in the open subset of V where $h \neq 0$. $\square$

Definition 2.1 (Resolvent) Let I be a prime ideal with a characteristic set $(g_1, \ldots, g_p)$ as above. Let w be a new variable and

$$w - c \;=\; w - a_1 y_1 - \cdots - a_p y_p,$$

a linear polynomial with the choices of a_i's as in the preceding lemma.

Let l, l_1, …, l_p be a characteristic set of $L \subseteq k[x_1, \ldots, x_n, w]$, generated by $(g_1, \ldots, g_p, w-c)$, computed with respect to the following ordering:

$$u_1 < u_2 < \ldots < u_q < w < y_1 < y_2 < \ldots < y_p.$$

The first polynomial (i.e. of the smallest rank) of the characteristic set, $l = l(u_1, u_2, \ldots, u_q, w)$, is called a *resolvent* of I. $\square$

The following theorem is the main result for the theory of the resolvent:

Theorem 2.2 *Let I be a prime ideal with a characteristic set, g_1, …, g_p, as in the preceding definition. Let w be a new indeterminate and let h and c be two polynomials satisfying the properties of lemma 2.1.*

Consider the ideal $L \subseteq k[x_1, \ldots, x_n, w]$,

$$L = (g_1, \ldots, g_p, w - c).$$

1. L is prime.

2. Let l, l_1, …, l_p be a characteristic set of L, computed as in the preceding definition. Then l = resolvent of I is only in the variables u_i's and in w, and each l_i is of degree 1 in y_i, i.e. is of the form

$$l_i = l_{i1} y_i + l_{i2},$$

where l_{ik}'s are polynomials free from y_j's.

PROOF.

(1) Assume to the contrary, that is L is not prime. Consider two polynomials, f and g, such that $f\,g \in L$ while neither f nor g belongs to L. Next, observe that $L \cap k[x_1, \ldots, x_n] = I$ and that using the polynomial $w - c$, it is possible to eliminate w from a polynomial f to obtain a polynomial $\widehat{f} \in k[x_1, \ldots, x_n]$ such that $f \in L$ if and only if $\widehat{f} \in I$. Now, using the polynomials $\widehat{f}$ and $\widehat{g}$, resulting from the elimination process, it is easily seen that

$$\widehat{f} \notin I, \;\; \widehat{g} \notin I, \quad \text{but} \quad \widehat{f}\,\widehat{g} \in I.$$

But this contradicts our original assumption that I is prime.

(2) Since L is prime it is easy to verify that the dimension of the variety it determines is still q and that its characteristic sets contain $p+1$ polynomials. Since the assumed ordering is

$$u_1 < \cdots < u_q \; < w < \; y_1 < \cdots < y_p,$$

l, the polynomial of the lowest rank is free from y_j's. Moreover it has to be irreducible as L is prime.

Algorithm RESOLVENT: (Algorithm 1)

- **Input:** A set of generators for the prime ideal I: $f_1, f_2, \ldots, f_m$.
- **Output:** Resolvent, l and a rational parametrization defined by: $l_1, l_2, \ldots, l_p$.

1. Compute a maximal set of independent variables u_1, …, u_q with respect to I. Rename the other variables as y_1, …, y_p.

2. forever repeat the following steps

step1. Choose at random a_1, …, a_p elements in k.

step2. Compute a characteristic set l, l_1, …, l_p for the ideal generated by f_1, …, f_m, $w - a_1 y_1 - \cdots - a_p y_p$ with respect to the ordering

$$u_1 < \ldots < u_q < w < y_1 < \ldots < y_p.$$

step3. If the polynomials l_1, …, l_p are linear in the variables $y_1, \ldots, y_p$
then output l as the resolvent and the l_i's as a rational parametrization of an open set of the original variety and terminate.

end{RESOLVENT.}

Figure 1: **Algorithm 1: A probabilistic algorithm to compute a resolvent.**

To prove that each l_i is of degree 1 in y_i, we begin by showing that l_1 is linear in y_1. Suppose the contrary holds and let $(\overline{u}, \overline{w})$ be a solution to the resolvent equation $l = 0$.

Then $l_1(\overline{u}, \overline{w}, y_1)$ has the same degree in y_1 as the polynomial $l_1(u, w, y_1)$, since l does not divide the initials of any of the l_i's. If $l_1(\overline{u}, \overline{w}, y_1)$ is of degree more than one, then the system of equations defining L has at least two distinct solutions, $(\overline{u}, \overline{w}, \overline{y})$ and $(\overline{u}, \overline{w}, \overline{y}')$ with $\overline{y} \neq \overline{y}'$. The polynomial h (as in lemma 2.1) is not in L, because the u_i's are algebraically independent with respect to L. Hence, $h(\overline{u}) \neq 0$. But, then as a direct consequence of the lemma 2.1, we have

$$c(\overline{y}) \neq c(\overline{y}'),$$

and that not both $\overline{w} - c(\overline{y}) = 0$ and $\overline{w} - c(\overline{y}') = 0$. But then this contradicts our initial assumption that the system of equations defining L has at least two distinct solutions and that l_1 is of degree more than 1.

Since the polynomial l_1 is linear in y_1 it can be used to eliminate y_1 from l_2, …, l_p. And the arguments of the earlier paragraph can be repeatedly used to show that l_2 and the successive polynomials are all linear in the corresponding y_i's. $\square$

Note that the resolvent defines a hypersurface H in the $q+1$-dimensional space which is birational to the variety V defined by I. The equations of the rational map from H to V are obtained by resolving the polynomials l_1, …, l_p for the y_i's.

$$y_1 = \frac{l_{11}(u_1, \ldots, u_q, w)}{l_{12}(u_1, \ldots, u_q, w)}, \quad \ldots, \quad y_p = \frac{l_{p1}(u_1, \ldots, u_q, w)}{l_{p2}(u_1, \ldots, u_q, w)},$$

where $(u_1, \ldots, u_q, w) \in H$ ranges over the solutions of the resolvent $l(u_1, \ldots, u_q, w)$. As a result, we shall also say that the equations l_1, ..., l_p provide a *parametrization* of the variety V defined by I.

Example 2.2 *[9]*

Consider the space curve defined by the polynomial equations

$$\begin{aligned} f_1 &= z^2 + y^3 - y^2 - 1 = 0 \\ f_2 &= z^2 - y^2 - x^2 = 0. \end{aligned}$$

A characteristic set of $\{f_1,\, f_2,\, w - y - z\}$ with respect to

$$x < w < y < z$$

is

$$l = w^6 - 3x^2w^4 + 8(X^2 - 1)w^3 + 3x^4w^2 - x^6$$

$$\begin{aligned} l_1 &= 2wy - (w^2 - x^2) \\ l_2 &= 2wz - (w^2 + x^2) \end{aligned}$$

Thus birational mapping $\phi : V(f_1, f_2) \to V(l)$ is

$$\phi : (x, y, z) \mapsto (x, w) = (x, y + z)$$

and its inverse is $\psi : V(l) \to V(f_1, f_2)$ is

$$\psi : (x, w) \mapsto \left(x, \left(\frac{w^2 - x^2}{2w}\right), \left(\frac{w^2 + x^2}{2w}\right)\right). \qquad \square$$

The above results lead to a very straightforward algorithm to compute the resolvent of an irreducible variety defined by a prime ideal I via characteristic set computations. However, a direct implementation of the constructions given in the proof leads to the computation of characteristic sets twice and consequently, fails to provide a tight upper bound for the degree of the resolvent and the parametrization. While this source of inefficiency can be easily eliminated, the choice of the parameters a_i's still results in a probabilistic algorithm. The probabilistic algorithm is shown in figure 1.

Note that the probability that the condition in step 3 of the algorithm 1 (Figure 1) will be satisfied approaches 1 if the choice of the a_i is done over a sufficiently large subset of k. To prove this observe that, if one treats the a_i's as variables in the computation of Step 4 each polynomial l_i is of the form $l_{i1}(a, u, w)y_i + l_{i2}(a, u, w)$, where l_{ij} is a polynomial in u_i's and a_j's whose degree can be bounded a priori, knowing the degree of the f_k's. The 'good' a_j's hence should not be such that they make the l_{i1}'s identically zeros. We shall show how a clever analysis of the degree bounds for the resolvent as well as the parametrizing polynomials, and a technique using a generalization of Schwartz's probabilistic method [16] leads to a deterministic version of the algorithm (Figure 2) for resolvent computation without any additional complexity penalty.

3 Complexity and Degree Bounds

In this section we will present upper and lower bounds on the degree of the resolvent for a prime ideal $I \subseteq k[x_1, \ldots, x_n]$ generated by m polynomials $f_1, \ldots, f_m$ each of degree at most d in the x_i's.

3.1 Lower bound

Example 3.1 In the ring of polynomials $k[u_1, \ldots, u_n, y_1, \ldots, y_n]$ consider the ideal I generated by the polynomials

$$y_1^d - u_1,\ y_2^d - u_2,\ \ldots,\ y_n^d - u_n.$$

I is prime. The variables $u_1, \ldots, u_n$ are independent with respect to I. Thus the variety V defined by I in a $2n$-dimensional affine space is irreducible and of dimension n.

The above set of generators is a characteristic set for I with respect to the ordering

$$u_1 < u_2 < \cdots < u_n < y_1 < y_2 < \cdots < y_n.$$

Algorithm RESOLVENT: (Algorithm 2)

- **Input:** A set of generators for the prime ideal I: $f_1, f_2, \ldots, f_m$.
- **Output:** Resolvent, l and a rational parametrization defined by: $l_1, l_2, \ldots, l_p$.

1. Compute a maximal set of independent variables u_1, …, u_q with respect to I. Rename the other variables as y_1, …, y_p.

2. Let $S = \{c_1,\ c_2,\ \ldots,\ c_N\}$, $c_i \in k$, c_i's distinct. For instance, we may choose $S = \{1, 2, \ldots, N\}$. Where N is chosen to be

$$|S| = N = 8(m+1)p(18p)^{4p}d(d+1)^{16p^2}$$

3. foreach $a_1 \in S$, …, $a_p \in S$

repeat the following steps:

step1. Compute a characteristic set l, l_1, …, l_p for the ideal generated by f_1, …, f_m, $w - a_1y_1 - \cdots - a_py_p$ with respect to the ordering

$$u_1 < \ldots < u_q < w < y_1 < \ldots < y_p.$$

step2. If the polynomials l_1, …, l_p are linear in the variables $y_1, \ldots, y_p$

then output l as the resolvent and the l_i's as a rational parametrization of an open set of the original variety and terminate.

end{RESOLVENT.}

Figure 2: **Algorithm 2: A deterministic algorithm to compute a resolvent.**

From the results in the previous section, V is birational to a hypersurface in a $n+1$-dimensional affine space. This is equivalent to saying that the field of rational functions over V, $k(V)$, obtained by taking the quotient field of $k[u_1, \ldots, u_n, y_1, \ldots, y_n]/I$ is isomorphic to the field of rational functions $k(u_1, u_2, \ldots, u_n, \overline{w})$ where u_i's are algebraically independent over k and $\overline{w}$ is algebraic over $k(u_1,\ u_2,\ \ldots,\ u_n)$.

It is clear, then, that the degree in w of the resolvent cannot be less than the degree of the minimal polynomial g for $\overline{w}$ over $k(u_1, u_2, \ldots, u_n)$. From field theory the degree of g is equal to the dimension of $k(u_1, u_2, \ldots, u_n, \overline{w})$ as a vector space over $k(u_1,\ u_2,\ \ldots,\ u_n)$. This is of course equal to the dimension of $k(V)$ as a vector space over $k(u_1,\ u_2,\ \ldots,\ u_n)$. Now it is easy to observe that $k(V)$ is generated, as a vector space over $k(u_1,\ u_2,\ \ldots,\ u_n)$ by the monomials in y_i's with degree in each y_i less than d. Since there are d^n of such monomials the degree of the resolvent must be at least of degree d^n. □

Observe that the degree of the resolvent depends on the particular ordering chosen for the variables. In fact V is a rational variety and with the choice of y_i's as parameters, it is immediately seen that V is birational to a hyperplane in the $n+1$-dimensional affine space. This phenomenon was already known to Ritt (see [14] pp. 44).

In the example above we were concerned only with the degree of the resolvent. The following (rather classical) example shows that the degree of the expressions involved in the rational map from the variety to its birationally equivalent surface may necessarily be of high degree also.

Example 3.2 In the ring $k[u, y_1, \ldots, y_{n-1}]$, consider the ideal I generated by the polynomials

$$y_1 - y_2^d,\ y_2 - y_3^d,\ \ldots,\ y_{n-1} - u^d.$$

The variety V described by I is irreducible and it is a rational curve, parametrized by u. The resolvent is then $w = 0$. However, the parametric equations for the curve are

$$y_1 - u^{d^n},\ y_2 - u^{d^{n-1}},\ \ldots,\ y_{n-1} - u^d. \quad \square$$

3.2 Upper bound

We begin by looking at the degree bounds for the resolvent and its associated parametrizing polynomials (i.e. l_i's). For a polynomial $f \in k[u_1, \ldots, u_q, w, y_1, \ldots, y_p]$, we define $\deg_{u_i}(f)$ (degree of f with respect to u_i) as the maximum degree of the variable u_i appearing in f. We define $\deg_w(f)$ and $\deg_{y_i}(f)$ analogously. We also use the notations $\deg_U(f)$ and $\deg_Y(f)$ to imply

$$\deg_U(f) = \sum_{i=1}^{q} \deg_{u_i}(f), \quad \text{and} \quad \deg_Y(f) = \sum_{i=1}^{p} \deg_{y_i}(f).$$

Finally, we write $\deg(f)$ to mean

$$\deg(f) = \deg_U(f) + \deg_w(f) + \deg_Y(f).$$

The following theorem follows from the bounds on the degrees of the polynomials of a characteristic set given in [7].

Theorem 3.1
(Resolvent Upper Bound Theorem)
Let $I = (f_1, \ldots, f_m)$ be a prime ideal in $k[x_1, \ldots, x_n]$ (k is a field of characteristic zero) and $\deg(f_i) \le d$. Assume that $x_1 = u_1, \ldots, x_q = u_q$ are the independent variables with respect to I and the remaining $p = n - q$ variables, $x_{q+1} = y_1, \ldots, x_n = y_p$, are dependent. Let w be the new variable introduced as in the definition of the resolvent.

Let l be the resolvent of I and $l_1, \ldots, l_p$, its associated parametrizing polynomials. Then

$$\begin{aligned} \deg(l) &= O\Big(m\, d^{O(p^2)}\Big), \quad \textit{and} \\ \deg(l_i) &= O\Big(m\, d^{O(p^2)}\Big), \quad \textit{for all } i = 1, \ldots, p. \end{aligned}$$

PROOF.
The proof follows from the GENERAL UPPER BOUND THEOREM of [7] and the algorithm for Resolvent as in the Figure 1. $\square$

In fact a careful examination of the proof of the GENERAL UPPER BOUND THEOREM of [7] reveals more.

$$\begin{aligned} \deg_U(l) &\le 4(m+1)(18p)^{4p} d(d+1)^{16p^2}, \\ \deg_w(l) &\le 2(d+1)^{2p+2}, \\ \deg_Y(l) &= 0, \quad \text{and} \end{aligned}$$

$$\begin{aligned} \deg_U(l_i) &\le 4(m+1)(18p)^{4p} d(d+1)^{16p^2}, \\ \deg_w(l_i) &\le 2(d+1)^{2p+2}, \\ \deg_Y(l) &= 1, \quad \text{for all } i = 1, \ldots, p. \end{aligned}$$

Furthermore, l and each of the l_i's can be expressed as a linear combination of the f_j's and $w - c = w - a_1 y_1 - \cdots - a_p y_p$ as follows

$$\begin{aligned} l &= b_0(w - c) + \sum_{j=1}^{m} b_j f_j, \\ l_i &= a_{i0}(w - c) + \sum_{j=1}^{m} a_{ij} f_j, \end{aligned}$$

where b's and a's are polynomials in $k[u_1, \ldots, u_q, w, y_1, \ldots, y_p]$ and

$$\left.\begin{array}{c}\deg(b_0),\\ \deg(b_j f_j)\end{array}\right\} \leq 11(m+1)(18p)^{4p} d(d+1)^{16p^2}, \quad \text{and}$$

$$\left.\begin{array}{c}\deg(a_{i0}),\\ \deg(a_{ij} f_j)\end{array}\right\} \leq 11(m+1)(18p)^{4p} d(d+1)^{16p^2}.$$

These bounds lead to straightforward algorithms to compute the resolvent and correspondingly, a single exponential sequential time bound and a polynomial parallel time bound. (See [7].)

Theorem 3.2
(Randomized Complexity of Resolvent)
Let $I = (f_1, \ldots, f_m)$ be a prime ideal in $k[x_1, \ldots, x_n]$ (k is a field of characteristic zero) and $\deg(f_i) \leq d$. Assume that $x_1 = u_1, \ldots, x_q = u_q$ are the independent variables with respect to I and the remaining $p = n - q$ variables, $x_{q+1} = y_1, \ldots, x_n = y_p$, are dependent.

Then assuming a suitable choice of the a_i's, one can compute the resolvent of I and its associated parametrizing polynomials, in $O\Big(m^{O(n)}(d+1)^{O(n^3)}\Big)$ sequential time or $O(n^7 \log^2(m+d+1)$ parallel time. $\square$

Since a random choice of a_i's satisfies the requirements with probability 1, the above theorem gives a probabilistic complexity analysis for our Resolvent algorithm in Figure 1.

However, the algorithm can be made deterministic since it is possible to search for appropriate a_i's over large subsets of k, where the search process is guaranteed to succeed. This leads to the final Resolvent algorithm in Figure 2.

Let

$$K = \{c_1, c_2, c_3, \ldots\} \subseteq k$$

be a countably infinite subset of k. For instance, we could have chosen

$$K = \{1, 2, 3, \ldots\}$$

where

$$1 = 1, \quad 2 = 1 + 1, \quad 3 = 1 + 1 + 1, \quad \text{etc.}$$

Our a_i's will be chosen from some large but finite subsets $S_i \subset K$.

Let $f(a_1, \ldots, a_p) \in k[a_1, \ldots, a_p]$ be a nontrivial multivariate polynomial, i.e.

$$f(a_1, \ldots, a_p) \not\equiv 0.$$

We would like to count the number of elements of $S_1 \times S_2 \times \cdots \times S_p \subset K^p$ where f vanishes, i.e. the cardinality of the set

$$Z(f) = \Big\{(\overline{a_1}, \ldots, \overline{a_p}) \ : \ \overline{a_1} \in S_1, \ldots, \overline{a_p} \in S_p \ \& f(\overline{a_1}, \ldots, \overline{a_p}) = 0\Big\}.$$

Let $d_1 = \deg_{a_1}(f), \ldots, d_p = \deg_{a_p}(f)$.

$$f = f_{d_1}(a_2, \ldots, a_p) a_1^{d_1} + \cdots + f_0(a_2, \ldots, a_p).$$

At a point $(\overline{a_1}, \ldots, \overline{a_p})$, $f(\overline{a_1}, \ldots, \overline{a_p})$ can vanish for one of two reasons:

1. $\overline{a_1}$ is a root of the univariate polynomial in a_1 with coefficients $f_j(\overline{a_2}, \ldots, \overline{a_p})$,
2. for each j $(0 \leq j \leq d_1)$, $f_j(\overline{a_2}, \ldots, \overline{a_p}) = 0$.

Proceeding as in [16], we have

$$|Z(f)| \leq d_1 \prod_{j=2}^{p} |S_j| + |Z(f_{d_1})|\,|S_1|,$$

since, for a fixed value of $a_2, \ldots, a_p$, there are d_1 zeros of f and each a_j can assume only $|S_j|$ values; therefore, there are at most $d_1 \prod_{j=1}^{p} |S_j|$

zeros of the first kind. The total number of zeros of the second kind are obviously bounded by the number of zeros of $f_{d_1}(a_2, \ldots, a_p)$.

Thus

$$\begin{aligned} \frac{|Z(f)|}{\prod_{j=1}^{p}|S_j|} &\leq \frac{d_1}{|S_1|} + \frac{|Z(f_{d_1})|}{\prod_{j=2}^{p}|S_j|} \\ &\leq \sum_{j=1}^{p} \frac{d_j}{|S_j|} \\ &\leq \frac{\sum_{j=1}^{p} d_j}{\min|S_j|} = \frac{\deg(f)}{\min|S_j|}. \end{aligned}$$

Now choosing

$$S_1 = S_2 = \cdots = S_p = S \subset K, \quad \text{and} \quad |S| = 2\deg(f),$$

we are guaranteed to have at least one elment in S^p at which f assumes a nonzero value. Actually, f does not vanish for at least half the points of S^p; that is, if we choose a point uniformly randomly from S^p then, after two draws on the average, we would have found a point where f does not vanish.

Now going back to our original problem, let us perform our resolvent computation with a_i's as symbolic variables. (In the ordering of the variables, a_i's are assumed to occur before all other variables.) Then our parametrizing polynomials are of the following form:

$$\begin{aligned} l_1 &= l_{11}(a_1, \ldots, a_p, u_1, \ldots, u_q, w) y_1 \\ &\quad + l_{12}(a_1, \ldots, a_p, u_1, \ldots, u_q, w) \\ &\vdots \\ l_p &= l_{p1}(a_1, \ldots, a_p, u_1, \ldots, u_q, w) y_p \\ &\quad + l_{p2}(a_1, \ldots, a_p, u_1, \ldots, u_q, w). \end{aligned}$$

Now, we would like to choose $(\overline{a_1}, \ldots, \overline{a_p})$ such that

$$\begin{aligned} l_{11}(\overline{a_1}, \ldots, \overline{a_p}, u_1, \ldots, u_q, w) &\not\equiv 0, \\ &\vdots \\ l_{p1}(\overline{a_1}, \ldots, \overline{a_p}, u_1, \ldots, u_q, w) &\not\equiv 0. \end{aligned}$$

Equivalently, if

$$\begin{aligned} &L(a_1, \ldots, a_p, u_1, \ldots, u_q, w) \\ &\quad = \prod_{j=1}^{p} l_{j1}(a_1, \ldots, a_p, u_1, \ldots, u_q, w), \end{aligned}$$

our choice of $(\overline{a_1}, \ldots, \overline{a_p})$ must satisfy

$$L(\overline{a_1}, \ldots, \overline{a_p}, u_1, \ldots, u_q, w) \not\equiv 0.$$

Now, using the general upper bound theorem of [7], we see that for all j $(1 \leq j \leq p)$,

$$\deg_A(l_{j1}) \leq 4(m+1)(18p)^{4p} d(d+1)^{16p^2},$$

and

$$\deg_A(L) \leq 4(m+1)p(18p)^{4p} d(d+1)^{16p^2}.$$

Thus, if we choose an $I \subset K$ such that

$$|S| = 8(m+1)p(18p)^{4p} d(d+1)^{16p^2}$$

then there is an $(\overline{a_1}, \ldots, \overline{a_p}) \in S^p$ for which the resolvent algorithm is guaranteed to produce appropriate parametrizing polynomials. Since we need to search only over a space of cardinality

$$|S^p| = O\Big(m^{O(p)} d^{O(p^3)}\Big),$$

the time complexities of our algorithms (both under sequential as well as parallel models) remain unaffected.

Thus, in summary, we have the following:

Theorem 3.3 (Complexity of Resolvent) *Let $I = (f_1, \ldots, f_m)$ be a prime ideal in $k[x_1, \ldots, x_n]$ (k is a field of characteristic zero) and $\deg(f_i) \leq d$. Assume that $x_1 = u_1, \ldots, x_q = u_q$ are the independent variables with respect to I and the remaining $p = n - q$ variables, $x_{q+1} = y_1, \ldots, x_n = y_p$, are dependent.*

Then one can compute the resolvent of I and its associated parametrizing polynomials, deterministically in $O\Big(m^{O(n)}(d+1)^{O(n^3)}\Big)$ sequential time or $O(n^7 \log^2(m+d+1)$ parallel time. □

References

[1] M.E. Alonso, T. Mora and M. Raimondo. "*Local Decomposition Algorithms,*" In *Proceedings of Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, AAECC-9*, Tokyo, LNCS 508, pp. 208-221, Springer-Verlag, New York, 1990.

[2] B. Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D. thesis, University of Innsbruck, Austria, 1965.

[3] Thomas Becker and Volker Weispfenning. *Gröbner Bases: A Computational Approach to Commutative Algebra,*" Graduate Texts in Mathematics, Springer-Verlag, New York, 1993.

[4] A. Dickenstein, N. Fitchas, M. Giusti and C. Sessa. "*The Membership Problem for Unmixed Polynomial Ideals Is Solvable in Subexponential Time,*" In *Proceedings of Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, AAECC-7*, Toulouse, 1989.

[5] J. Dieudonné. *History of Algebraic Geometry*. Wadsworth, California 1985.

[6] G. Gallo. *Complexity Issues in Computational Algebra.* Ph.D. thesis, Courant Institute of Mathematical Sciences, New York University, New York, 1992.

[7] G. Gallo and B. Mishra. "*Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets,*" Volume 94 of *Progress in Mathematics, Effective Methods in Algebraic Geometry*, (edited by F. Mora and C. Traverso), pp. 119–142. Birkhäuser, Boston, 1991.

[8] G. Gallo and B. Mishra. "*Wu-Ritt Characteristic Sets and Their Complexity,*" Volume 6 of *Discrete and Computational Geometry: Papers from the DIMACS (Discrete Mathematics and Computer Science) Special Year,* (edited by J.E. Goodman, R. Pollack and W. Steiger), pp. 111–136. American Mathematical Society and Association of Computing Machinery, 1991.

[9] X-S. Gao and S-C. Chou. "*On the Parametrization of algebraic Curves.*" Technical report, Department of Computer Science, The University of Texas, Austin, Texas, 1991.

[10] M. Giusti and J. Heintz. "*Algorithmes-disons Rapides- puor la Decomposition d'une Variete Algebrique en Composantes Irriducibles et Equidimetionelles,*" Volume 94 of *Progress in Mathematics, Effective Methods in Algebraic Geometry*, MEGA '90, (edited by F. Mora and C. Traverso), pp. 169–194. Birkhäuser, Boston, 1991.

[11] A. Logar. "*A Computational Proof of the Noether Normalization Lemma,*" pp. 259–273, Lecture Notes in Computer Science, Springer-Verlag, 1989, AAECC-6 Conference.

[12] B. Mishra. *Algorithmic Algebra.* Texts and Monographs in Computer Science, Springer-Verlag, New York, 1993.

[13] B. Mishra and C. Yap. "*Notes on Gröbner Bases,*" *Information Sciences*, 48:219–252, 1989.

[14] J.F. Ritt. *Differential Equations from an Algebraic Standpoint*. AMS Colloquium Publications, volume XIV, New York 1932.

[15] J.F. Ritt. *Differential Algebra*. AMS Colloquium Publications, volume XXXII, New York 1950.

[16] J.T. Schwartz. "*Fast Probabilistic Algorithms for Verification of Polynomial Identities*," *Journal of Association for Computing Machinery*, 27:701–717, 1980.

[17] I.R. Shafarevich. *Basic Algebraic Geometry*, Springer-Verlag, New York, 1974.

[18] W.T. Wu, "*On the Decision Problem and Mechanization of Theorem Proving in Elementary Geometry*," *Scientia Sinica*, 21:157–179, 1978.

Appendix: Characteristic Set

Let $k[x_1, \ldots, x_n]$ denote the ring of polynomials in n variables, with coefficients in a field k. Consider a fixed ordering on the set of variables; without loss of generality, we may assume that the given ordering is the following:

$$x_1 < x_2 < \cdots < x_n.$$

Definition .3 (Class and Class Degree) Let $f \in k[x_1, \ldots, x_n]$ be a multivariate polynomial with coefficients in k. A variable x_j is said to be *effectively present in* f if some monomial in f with nonzero coefficient contains a (strictly) positive power of x_j.

For $1 \leq j \leq n$, *degree of f with respect to x_j*, $\deg_{x_j}(f)$, is defined to be the maximum degree of the variable x_j in f.

The *class* and the *class degree* (Cdeg) of a polynomial $f \in k[x_1, \ldots, x_n]$ with respect to a given ordering is defined as follows:

1. If *no variable x_j is effectively present in f*, (i.e., $f \in k$), then, by convention,

$$\mathrm{Class}(f) = 0 \quad \text{and} \quad \mathrm{Cdeg}(f) = 0.$$

2. Otherwise, if *x_j is effectively present in f, and no $x_i > x_j$ is effectively present in f* (i.e., $f \in k[x_1, \ldots, x_j] \setminus k[x_1, \ldots, x_{j-1}]$), then

$$\mathrm{Class}(f) = j \text{ and } \mathrm{Cdeg}(f) = \deg_{x_j}(f). \quad \square$$

Definition .4 (Ordering on the Polynomials) Given two polynomials f_1 and $f_2 \in k[x_1, \ldots, x_n]$, we say f_1 is of *lower rank than* f_2,

$$f_1 \prec f_2,$$

if either

1. $\mathrm{Class}(f_1) < \mathrm{Class}(f_2)$, or

2. $\mathrm{Class}(f_1) = \mathrm{Class}(f_2)$ and $\mathrm{Cdeg}(f_1) < \mathrm{Cdeg}(f_2)$.

Note that there are distinct polynomials f_1 and f_2 that are not comparable under the preceding order. In this case, f_1 and f_2 are said to be of the *same rank*, $f_1 \sim f_2$. $\square$

Thus, a polynomial f of class j and class degree d can be written as

$$\begin{aligned} f = {} & I_d(x_1, \ldots, x_{j-1})x_j^d \\ & + I_{d-1}(x_1, \ldots, x_{j-1})x_j^{d-1} \\ & + \cdots + I_0(x_1, \ldots, x_{j-1}), \end{aligned} \tag{1}$$

where $I_l(x_1, \ldots, x_{j-1}) \in k[x_1, \ldots, x_{j-1}]$ ($l = 0, 1, \ldots, d$).

Definition .5 (Initial Polynomial) Given a polynomial f of class j and class degree d, its *initial polynomial*, $\mathrm{In}(f)$, is defined to be the polynomial $I_d(x_1, \ldots, x_{j-1})$ as in equation (1). $\square$

Corollary .4 (Pseudodivision Lemma) *Consider two polynomials f and $g \in k[x_1, \ldots x_n]$, with $\mathrm{Class}(f) = j$. Then using the pseudo-division process, we can write*

$$\mathrm{In}(f)^\alpha g = qf + r, \tag{2}$$

where $\deg_{x_j}(r) < \deg_{x_j}(f)$ and $\alpha \leq \deg_{x_j}(g) - \deg_{x_j}(f) + 1$. $\square$

If α is assumed to be the smallest possible power satisfying equation (2), then the pseudo-quotient and the pseudoremainder are unique. Also, polynomial g is reduced with respect to f if $g = \mathrm{PRemainder}(g, f)$.

Definition .6 (Ascending Set) A sequence of polynomials $\mathcal{F} = \langle f_1, f_2, \ldots, f_r\rangle \subseteq k[x_1, \ldots, x_n]$ is said to be an *ascending set* (or *chain*), if one of the following two conditions holds:

1. $r = 1$ and f_1 is not identically zero;

2. $r > 1$, and $0 < \mathrm{Class}(f_1) < \mathrm{Class}(f_2) < \cdots < \mathrm{Class}(f_r) \leq n$,
and each f_i is reduced with respect to the preceding polynomials,
f_j's $(1 \leq j < i)$.

Every ascending set is finite and has at most n elements. The *dimension* of an ascending set $\mathcal{F} = \langle f_1, f_2, \ldots, f_r\rangle$, $\dim \mathcal{F}$, is defined to be $(n - r)$. $\square$

Definition .7 (Ordering on the Ascending Sets) Given two ascending sets

$$\mathcal{F} = \langle f_1, \ldots, f_r\rangle \quad \text{and} \quad \mathcal{G} = \langle g_1, \ldots, g_s\rangle,$$

we say $\mathcal{F}$ is of *lower rank* than $\mathcal{G}$, $\mathcal{F} \prec \mathcal{G}$, if one of the following two conditions is satisfied,

1. There exists an index $i \leq \min\{r, s\}$ such that

$$\Big(\forall\, 1 \leq j < i\Big) \Big[f_j \sim g_j\Big] \text{ and } \Big[f_i \prec g_i\Big];$$

2. $r > s$ and $\Big(\forall\, 1 \leq j \leq s\Big) \Big[f_j \sim g_j\Big]$.

Note that there are distinct ascending sets $\mathcal{F}$ and $\mathcal{G}$ that are not comparable under the preceding order. In this case $r = s$, and $(\forall\, 1 \leq j \leq s)\ [f_j \sim g_j]$, and $\mathcal{F}$ and $\mathcal{G}$ are said to be of the *same rank*, $\mathcal{F} \sim \mathcal{G}$. $\square$

Note that the family of ascending sets endowed with the ordering "$\prec$" is a well-ordered set.

Definition .8 (Characteristic Set) Let I be an ideal in $k[x_1, \ldots, x_n]$. Consider the family of all ascending sets, each of whose components is in I,

$$\mathbf{S}_I = \Big\{\mathcal{F} = \langle f_1, \ldots, f_r\rangle \ : \ \mathcal{F} \text{ is an ascending set and } f_i \in I, 1 \leq i \leq r\Big\}.$$

A minimal element in $\mathbf{S}_I$ (with respect to the $\prec$ order on ascending sets) is said to be a *characteristic set* of the ideal I. $\square$

We remark that if $\mathcal{G}$ is a characteristic set of I, then

$$n \;\geq\; |\mathcal{G}| \;\geq\; n - \dim I.$$

Also, observe that, for a given ordering of the variables, the characteristic set of an ideal is not necessarily unique. However, any two characteristic sets of an ideal must be of the same rank.

Corollary .5 (Successive Pseudodivision Lemma) *Consider an ascending set* $\mathcal{F} = \langle f_1,\, f_2,\, \ldots,\, f_r\rangle \subseteq k[x_1,\, \ldots,\, x_n]$, *and a polynomial* $g \in k[x_1,\, \ldots,\, x_n]$. *Then using the successive pseudodivision, we can find a sequence of polynomials (called a* pseudoremainder chain*),* $g_0,\, g_1,\, \ldots,\, g_r = g$, *such that for each* $1 \leq i \leq r$, *the following equation holds,*

$$\Big(\exists\, q_i'\Big)\ \Big(\exists\, \alpha_i\Big)\ \Big[\mathrm{In}(f_i)^{\alpha_i} g_i = q_i' f_i + g_{i-1}\Big]$$

where g_{i-1} *is reduced with respect to* f_i *and* α_i *assumes the smallest possible power, achievable. Thus, the pseudoremainder chain is uniquely determined. Moreover, each* g_{i-1} *is reduced with respect to* $f_i,\, f_{i+1},\, \ldots,\, f_r$.

$$\mathrm{In}(f_r)^{\alpha_r}\mathrm{In}(f_{r-1})^{\alpha_{r-1}} \cdots \mathrm{In}(f_1)^{\alpha_1} g = \sum_{i=1}^{r} q_i f_i + g_0. \tag{3}$$

The polynomial $g_0 \in k[x_1,\, \ldots,\, x_n]$ *is said to be the* (generalized) pseudoremainder of g with respect to the ascending set $\mathcal{F}$,

$$g_0 = \mathrm{PRemainder}\,(g, \mathcal{F})\,.$$

It is easily seen that g_0 *is uniquely determined, and reduced with respect to* $f_1,\, f_2,\, \ldots,\, f_r$. *We say a polynomial* g *is* reduced with respect to an ascending set $\mathcal{F}$ *if* $g = \mathrm{PRemainder}\,(g, \mathcal{F})$.
□

Theorem .6 *Let* I *be an ideal in* $k[x_1, \ldots, x_n]$. *Then the ascending set* $\mathcal{G} = \langle g_1,\, \ldots,\, g_r\rangle$ *is a characteristic set of* I *if and only if*

$$\Big(\forall\, f \in I\Big)\ \Big[\mathrm{PRemainder}(f, \mathcal{G}) = 0\Big]. \quad \square$$