# Recent Progress in Characteristic Set Computation: Complexity & Open Problems

G. Gallo & B. Mishra
Courant Institute, New York University

*In this note, we will survey some recent progress made in completely settling the computational complexity of computing a characteristic set of an ideal in a ring of polynomials over a field. The concept of a characteristic set of an ideal was originally introduced by J.F. Ritt, in the late forties, and later, independently rediscovered by Wu Wen-Tsün, in the late seventies. Since then Wu-Ritt Characteristic Sets have found wide applications in Symbolic Computational Algebra, Automated Theorem Proving in Elementary Geometries and Computer Vision. We also list some related open problems and some open conjectures to which these results have interesting implications.*

## 1. Introduction

The concept of a characteristic set was discovered in the late forties by J.F. Ritt (see his now classic book *Differential Algebra* [13]) in the setting of differential algebra. Interests in these concepts were revived recently, when the Chinese mathematician Wu Wen-Tsün [16, 15, 17] exhibited their power in the case where Ritt's techniques are specialized to commutative algebra. In particular, he demonstrated its effectiveness (largely through empirical evidence) as a powerful tool for Mechanical Theorem proving; his system has come to be widely known as *the China Prover*. Surprisingly, until very recently, the constructivity of Ritt's characteristic set had not been explicitly demonstrated [6]; the original WU-RITT PROCESS, first devised by Ritt [13], subsequently modified by Wu [16, 15, 17], computes only an *extended* characteristic set. Unfortunately, the WU-RITT PROCESS has a non-elementary worst-case time complexity and thus, infeasible (see [7]).

However, many questions regarding the computational complexity of characteristic sets have now been settled (see [6, 7]). In this brief note we survey these new developments.

[0]Supported by NSF Grant #CDA-90-18673, #CCR-9002819, ONR Grant #N00014-89-J3042 and an Italian CNR fellowship.

## 2. Preliminaries

Let $k[x_1, \ldots, x_n]$ denote the ring of polynomials in $n$ indeterminates, with coefficients in a field $k$. Consider a fixed ordering on the set of indeterminates;

$$x_1 \prec x_2 \prec \cdots \prec x_n.$$

Let $f \in k[x_1, \ldots, x_n]$ be a multivariate polynomial with coefficients in $k$. 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 indeterminate $x_j$ in $f$. The *degree of $f$* is defined to be $\deg(f) = \sum_{j=1}^{n} \deg_{x_j}(f)$.

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 indeterminate $x_j$ is effectively present in $f$*, then, $\mathrm{class}(f) = 0$ and $\mathrm{cdeg}(f) = 0$; otherwise,

(2) If *$x_j$ is effectively present in $f$, and no $x_i \succ x_j$ is effectively present in $f$* then $\mathrm{class}(f) = j$ and $\mathrm{cdeg}(f) = \deg_{x_j}(f)$.

Given a polynomial $f$ of class $j$ and class degree $d$, its *initial polynomial*, $\mathrm{in}(f)$, is defined to be the polynomial $I_d(x_1, \ldots, x_{j-1})$ in the following expression:

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

**Pseudo-Division**

**1.** Consider two polynomials $f$ and $g \in k[x_1, \ldots x_n]$, with $\mathrm{class}(f) = j$. Then there exist two polynomials $q$ and $r$, and an integer $\alpha$ such that the following equation holds:

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

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

If $\alpha$ is assumed to be the smallest possible power satisfying equation (2) then $q$ and $r$ are uniquely determined. A polynomial $g$ is *reduced* with respect to $f$ if $g = \mathrm{prem}(g, f)$.

**2.** In order to generalize the pseudo-remainder concept, 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 there exists a sequence of polynomials (called a *pseudo-remainder sequence*), $g_0, g_1, \ldots, g_r = g$, such that for each $1 \leq i \leq r$, the following equation holds,

$$(\exists!\, q_i')\, (\exists!\, \alpha_i)\, \left[\mathrm{in}(f_i)^{\alpha_i} g_i = q_i' f_i + g_{i-1}\right]$$

where $g_{i-1}$ is reduced with respect to $f_i$ and $\alpha_i$ assumes the smallest possible power, achievable. Thus, the pseudo-remainder sequence is uniquely determined.

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

The polynomial $g_0 \in k[x_1, \ldots, x_n]$ is said to be the (*generalized*) *pseudo-remainder* (of $g$ with respect to the ascending set $\mathcal{F}$), $g_0 = \text{prem}(g, \mathcal{F})$. We say a polynomial $g$ is *reduced with respect to an ascending set* $\mathcal{F}$ if $g = \text{prem}(g, \mathcal{F})$.

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 (i) $\text{class}(f_1) < \text{class}(f_2)$, or (ii) $\text{class}(f_1) = \text{class}(f_2)$ and $\text{cdeg}(f_1) < \text{cdeg}(f_2)$.

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*, $f_1 \sim f_2$.

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 $0 < \text{class}(f_1) < \text{class}(f_2) < \cdots < \text{class}(f_r) \le n$, and each $f_i$ is reduced with respect to the preceding $f_j$'s $(1 \le j < i)$.
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 $(n - r)$.

Given two ascending sets $\mathcal{F} = \langle f_1, \ldots, f_r\rangle$ and $\mathcal{G} = \langle g_1, \ldots, g_s\rangle$, 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 $i \le \min\{r, s\}$ such that
$(\forall\, 1 \le j < i)\ f_j \sim g_j$, and $f_i \prec g_i$;
(2) $r > s$ and $(\forall\, 1 \le j \le s)\ f_j \sim g_j$.
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 $(\forall\, 1 \le j \le s)\ f_j \sim g_j$, and $\mathcal{F}$ and $\mathcal{G}$ are said to be of the *same rank*, $\mathcal{F} \sim \mathcal{G}$.

**Definition 2.1 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 $I$,

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

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 $I$. □

We note that if $\mathcal{G}$ is a characteristic set of $I$ then $n \ge |\mathcal{G}| \ge n - \dim I$. Also, observe that, for a given ordering of the indeterminates, characteristic set of an ideal is not necessarily unique. However, any two characteristic sets of an ideal must be of the same rank.

## 3. Pseudo-Remainder and Wu's Approach

Let us consider the following triangulation process, due to J.F. Ritt and Wu Wen-Tsün, which computes a so-called *extended characteristic set* of an ideal by repeated applications of the generalized pseudo-division.

The following well-known proposition provides an algebraic characterization of a characteristic set, and motivates the concept of an extended characteristic set.

**Proposition 3.1** *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* $(\forall\, f \in I)$ $[\mathrm{prem}(f, \mathcal{G}) = 0]$. ■

The extended characteristic set, computed as below, satisfies a much weaker condition: while it cannot guarantee that every polynomial *in the ideal* reduces to zero, it does guarantee that every polynomial in a given basis reduces to zero.

```
Wu-Ritt Process:
  𝒢 := ∅;   R := ∅;
  loop
      F := F ∪ R;   F' := F;   R := ∅;
      while F' ≠ ∅ loop
          Choose a polynomial f ∈ F' of minimal rank;
          F' := F' \ {g: class(g) = class(f) and g is not reduced with respect to f};
          𝒢 := 𝒢 ∪ {f};
      for all f ∈ F \ 𝒢 loop
          if r := prem(f, 𝒢) ≠ 0  then R := R ∪ {r};
  until R = ∅;
  return 𝒢.  ■
```

**Definition 3.2 Ritt's Principle.**
*Let $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ be a finite nonempty set of polynomials, and $I = (F)$ be the ideal generated by $F$. The* Wu-Ritt Process *described above obtains an ascending set $\mathcal{G}$ such that* either
*(1)* $\mathcal{G}$ *consists of a polynomial in $k \cap I$,* or
*(2)* $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$ *with* $\mathrm{class}(g_1) > 0$ *and such that*

$$\begin{aligned} g_i &\in I, &&\text{for all } i = 1, \ldots, r, \\ \mathrm{prem}(f_j, \mathcal{G}) &= 0, &&\text{for all } j = 1, \ldots, s. \end{aligned}$$

*Ascending chain $\mathcal{G}$ is called an* extended characteristic set *of $F$.* □

It is not hard to see that the algorithm terminates; but the bound on the running time requires some involved computation and has been shown to be nonelementary (see [7]). In particular, it is possible to construct an example which consists of $s$ polynomials in $n$ variables with degrees (in each variable) bounded by $d$ and each of class $= n$ and cdeg $= d$ such that the above process may require, in the worst case, following number of arithmetic steps:

$$T_n(d) = c \cdot \underbrace{d(1+\sqrt{2})^{d(1+\sqrt{2})^{\cdot^{\cdot^{\cdot^{d(1+\sqrt{2})^d}}}}}}_{n}.$$

## 4. Complexity of Characteristic Sets[1]

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal generated by a set of $s$ generators, $f_1$, $\ldots$, $f_s$, in the ring of polynomials in $n$ indeterminates over the field $k$. Further, assume that each of the polynomial $f_i$ in the given set of generators has its degree bounded by $d$: $(\forall\, 1 \leq i \leq s)\ [\deg(f_i) \leq d]$. Let $\mathcal{G} = \langle g_1, \ldots, g_r\rangle$ be a characteristic set of the ideal, and let $D = \max\{\deg(g_i) : 1 \leq i \leq r\}$ be the degree of this characteristic set. Next, we shall give upper and lower bounds for $D$, as function of $s$, $d$ and $n$, for a large class of orderings on the indeterminates.

**Theorem 4.2** *Let $k$ be an algebraically closed field, and let $I$ be an ideal in $k[x_1, \ldots, x_n]$, generated by the following $n$ polynomials, $F = \{f_1, \ldots, f_n\}$, each of degree $d$:*

$$f_1 = x_1 - x_n^d,\ \ f_2 = x_2 - x_1^d,\ \ \ldots,\ \ f_{n-1} = x_{n-1} - x_{n-2}^d,\ \ f_n = x_n - x_{n-1}^d.$$

*Then, independent of the ordering on the indeterminates,*
*(1) Every characteristic set of $F$ is of degree $D \geq d^n$;*
*(2) Every extended characteristic set of $F$ is of degree $D \geq d^n$.* ■

We note that the ideal $I$ of theorem 4.2 is a zero-dimensional ideal; the previous example can be modified to show that, in general, the degree of a characteristic set is $\Omega(d^{(n-\dim I)})$.

Now, we are ready to derive an upper bound that matches quite closely the lower bound of the Theorem 4.2. We proceed as follows: First, we show that every zero dimensional ideal $I$ contains a univariate polynomial $h_j(x_j)$, in each variable $x_j$, with the additional property that $\deg(h_j) \leq 2(d+1)^{2n}$. This follows from an effective version of *Hilbert's Nullstellensatz*, originally due to D. Brownawell [2] and later sharpened by J. Kollár [8]. Since the sequence $\langle h_1, \ldots, h_n\rangle$ is clearly an ascending set in $\mathbf{S}_I$, we get a similar bound on the class degrees of the polynomials in a characteristic set of $I$. This leads to a degree bound of $2n(d+1)^{2n}$ for a characteristic set of $I$. In particular the following theorem holds:

**Theorem 4.3** *Let $I = (f_1, \ldots, f_s)$ be a zero-dimensional ideal in $k[x_1, \ldots, x_n]$, where $k$ is an arbitrary field, and $\deg(f_i) \leq d$, $1 \leq i \leq s$. Then $I$ has a characteristic set $\mathcal{G} = \langle g_1, \ldots, g_n\rangle$ with respect to the ordering,*

$$x_1 \prec x_2 \prec \cdots \prec x_n,$$

*where for all $1 \leq j \leq n$,*

*1.* $\mathrm{class}(g_j) = j$ *and* $\deg(g_j) \leq 2n(d+1)^{2n} = O\left(d^{O(n)}\right)$.

[1] The results in this section are largely based on the paper [6]; more details may be found therein.

2. $(\exists\, a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n])\ \left[g_j = \sum_{i=1}^{s} a_{j,i} f_i,\right]$,
*and* $\deg(a_{j,i} f_i) \leq 8n(d+1)^{2n} = O\left(d^{O(n)}\right), 1 \leq i \leq s$. ∎

The results on the bounds for a characteristic set of a zero-dimensional ideal can be extended to the more general classes of ideals, by the following 'lifting' process: Let $I = (f_1, \ldots, f_s)$ be an ideal in the ring, $k[x_1, \ldots, x_n]$, where $k$ is an arbitrary field, $\deg(f_i) \leq d$. Assume that the indeterminates, $x_{\pi(1)} = u_1, \ldots, x_{\pi(l)} = u_l$, are the *independent* variables with respect to $I$. Thus, $\dim(I) = l > 0$. The remaining $r = (n-l)$ indeterminates, $x_{\pi(l+1)} = v_1, \ldots, x_{\pi(n)} = v_r$, form the set of *dependent* variables. We write $k[u_1, \ldots, u_l, v_1, \ldots, v_r]$ for the ring of polynomials, $k[x_1, \ldots, x_n]$.

The ordering on the indeterminates is assumed to be so chosen that

$$(\forall\, 1 \leq i \leq l)\ (\forall\, 1 \leq j \leq r)\ [u_i \prec v_j].$$

For a polynomial $f \in k[u_1, \ldots, u_l, v_1, \ldots, v_r]$, we shall use the notations, $\deg_U(f)$ and $\deg_V(f)$, to imply

$$\deg_U(f) = \sum_{i=1}^{l} \deg_{u_i}(f) \quad \text{and} \quad \deg_V(f) = \sum_{j=1}^{r} \deg_{v_j}(f).$$

Let $I'$ be the *extended ideal* of $I$ in the ring $k(u_1, \ldots, u_l)[v_1, \ldots, v_r]$, i.e.

$$I' = I\Big\{k(u_1, \ldots, u_l)[v_1, \ldots, v_r]\Big\}.$$

Then $I'$ is a zero-dimensional ideal in $k(u_1, \ldots, u_l)[v_1, \ldots, v_r]$, and by the results of the previous subsection, $I'$ has a characteristic set $\mathcal{G}' = \langle g'_1, \ldots, g'_r \rangle$, where

$$\text{class}(g'_j) = \pi(l+j), \quad \text{and} \quad g'_j = \sum_{i=1}^{s} a'_{j,i} f_i, \tag{4}$$
$$\text{where} \quad \deg_V(g'_j) \leq 2r(d+1)^{2r}, \quad \text{and} \quad \deg_V(a'_{j,i} f_i) \leq 8r(d+1)^{2r}.$$

Thus the system of linear equations, defined by (4) consists of at most

$$\Gamma = \binom{8r(d+1)^{2r} + r}{r}$$

equations in at most $(s+1)\Gamma$ unknowns, where the known coefficients are polynomials of degree at most $d$ in $k[u_1, \ldots, u_l]$. Now, the left and right hand sides of the equation (4) can be multiplied by an appropriate polynomial, $m \in k[u_1, \ldots, u_l]$, to clear out the denominators and yield the equation, $g_j = \sum_{i=1}^{s} a_{j,i} f_i$. Using simple bounds from linear algebra, we can obtain the appropriate bounds for $m$, $g_j$ and $a_{j,i} f_i$, as follows:

$$\begin{aligned}
\deg_U(m) &\leq d(s+1)\Gamma^2, \\
\deg_U(g_j) &\leq d\Gamma + d(s+1)\Gamma^2, \quad \text{and} \\
\deg_U(a_{j,i} f_i) &\leq d + d\Gamma + d(s+1)\Gamma^2.
\end{aligned}$$

Since it can be easily seen that $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$ is, in fact, a characteristic set of the ideal $I$, we obtain the following general upper bound result:

**Theorem 4.4** *Let $I = (f_1, \ldots, f_s)$ be an ideal in $k[x_1, \ldots, x_n]$, where $k$ is an arbitrary field, and $\deg(f_i) \le d$, $1 \le i \le s$. Assume that $x_1, \ldots, x_l$ are the independent variables with respect to $I$. Let $r = n - \dim I = n - l$. Then $I$ has a characteristic set $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$ with respect to the ordering*

$$x_1 \prec x_2 \prec \cdots \prec x_n,$$

*where for all $1 \le j \le r$,*

1. $\mathrm{class}(g_j) = j + l$ *and* $\deg(g_j) \le 4(s+1)(9r)^{2r} d(d+1)^{4r^2} = O\left(s\, d^{O(r^2)}\right)$.
2. $(\exists\, a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n])$ $[g_j = \sum_{i=1}^{s} a_{j,i} f_i,]$, *and* $\deg(a_{j,i} f_i) \le 11(s+1)(9r)^{2r} d(d+1)^{4r^2} = O\left(s\, d^{O(r^2)}\right)$, $1 \le i \le s$. ■

## 5. Algorithms

Now, we can describe a simple procedure to compute a characteristic set of an ideal, by using the degree bounds of the previous section and fairly simple ideas from linear algebra. In particular, we need, as subroutines, fast sequential and parallel algorithms for computing the *rank* and *determinants* of a matrices of order $N$ over arbitrary field. For this purpose, we assume that the sequential algorithms have time complexity $O(N^{2.376})$ [3] and that the parallel algorithms have time complexity $O(\log^2 N)$, (and polynomial size) [4, 11]. Our complexity model assumes an $O(1)$-complexity cost for all field operations over $k$.

Let $I$ be an ideal given by a set of generators $\{f_1, \ldots, f_s\} \in k[x_1, \ldots, x_n]$, where $k$ is an arbitrary field, $\deg(f_i) \le d$. Assume that after some reordering of the indeterminates, the indeterminates $x_1, \ldots, x_n$ are so arranged that the first $l$ of them are *independent* with respect to $I$, and the remaining $r = (n - l)$ variables, *dependent*. These conditions can be verified in $O(s^7 d^{O(n^2)})$ sequential time, or equivalently, in $O(n^4 \log^2(sd))$ parallel time by an algorithm of Dickenstein et. al. [5].

Assume, inductively, that the first $(j-1)$ elements $g_1, \ldots, g_{j-1}$, of a characteristic set, $\mathcal{G}$, of $I$ have been computed, and we wish to compute the $j^{\text{th}}$ element $g_j$ of $\mathcal{G}$. By the theorem 4.4, we know that $\mathrm{class}(g_1) = (l+1), \ldots, \mathrm{class}(g_{j-1}) = (l+j-1)$ and $\mathrm{class}(g_j) = (l+j)$. Let

$$\mathrm{cdeg}(g_1) = d_{l+1}, \ldots, \mathrm{cdeg}(g_{j-1}) = d_{l+j-1}.$$

Thus, the polynomial $g_j$, sought, must be a nonzero polynomial of least degree in $x_{l+j}$, in $I \cap k[x_1, \ldots, x_{l+j}]$ such that

$$\deg_{x_{l+1}}(g_1) < d_{l+1}, \ldots, \deg_{x_{l+j-1}} < d_{l+j-1}.$$

Furthermore, we know that in the following equation

$$\left(\exists\, a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n]\right)\ \left[g_j = \sum_{i=1}^{s} a_{j,i} f_i,\right], \tag{5}$$

we have upper bounds for $\deg(g_j)$ and $\deg(a_{j,i} f_i)$. Thus $g_j$ satisfying all the properties can be determined by solving an appropriate system of linear equations, involving $O\left(s^{O(n)}(d+1)^{O(n^3)}\right)$-many linear equations and with sequential and parallel complexities of $O(s^{O(n)}(d+1)^{O(n^3)})$ and $O(n^6 \log^2(s+d+1))$, respectively.

Thus, a characteristic set of the given ideal $I$, can be computed by at most $n$-many iterations in $O(s^{O(n)}(d+1)^{O(n^3)})$ sequential time and $O(n^7 \log^2(s+d+1))$ parallel time. If the ideal is zero-dimensional, then the arguments in this section can be specialized to yield better bounds (see [6]).

## 6. Open Problems

We have seen that the degrees of a characteristic set of an ideal is bounded from both above and below by a simple-exponential function in the number of variables. Also, if the ideal is zero-dimensional, this is true, irrespective of the ordering on the indeterminates that may be chosen. However, for the general ideals, the upper-bound is true, only for certain special orderings on the indeterminates; such orderings are abundant ($O(2^{O(n \log n)})$), and can be selected efficiently (i.e., simple exponential sequential, or polynomial parallel time). Thus, in all practical applications, this will not be a cause of a problem. However, the question of finding optimal degree bounds for any particular ordering of indeterminates, remains an intriguing and important open problem. We conjecture that our simple exponential upper bound holds, in general, *independent of the ordering chosen.*

Recently, Li and Swanson (see [10]) have used the Wu-Ritt characteristic set criteria to attack the Jacobian conjecture [1, 14]. Let $F: k[x_1, \ldots, x_n] \to k[x_1, \ldots, x_n]$ be a $k$-endomorphism, where $F$ may be written as $F = (f_1, \ldots, f_n)$ (where $f_i \in k[x_1, \ldots, x_n]$). The Jacobian conjecture states that $F$ is invertible, only if $J(F) = \det\left(\dfrac{\partial f_i}{\partial x_j}\right)$ is a nonzero element in the field $k$. Li and Swanson have shown that $F$ is invertible with inverse $G = (g_1, \ldots, g_n)$ if and only if

$$\mathcal{G} = \{x_1 - g_1(y_1, \ldots, y_n),\ \ldots,\ x_n - g_n(y_1, \ldots, y_n)\}$$

is a characteristic set of the ideal

$$I = (y_1 - f_1(x_1, \ldots, x_n),\ \ldots,\ y_n - f_n(x_1, \ldots, x_n))k[y_1, \ldots, y_n, x_1, \ldots, x_n].$$

From the main theorem of our paper, one can also obtain a degree bound for the the inverse, which is $O(nd^{O(n^2)})$. However, Gabber[1] has already proven a simpler bound of $d^{n-1}$. It is thus interesting to ask if our proof techniques can be modified to provide a simpler proof of Gabber's bound for this particular case.

Recently, D. Richardson has uses the Wu-Ritt process to give an elementary proof of Kovanskii Finiteness Theorem ([12, 9], which provides an upper bound on the number of connected components of the intersection of an algebraic set with a pfaffian manifold in $\mathbb{R}^k$.

A differentiable manifold $M$ in $\mathbb{R}^k$ is a pfaffian manifold if there exist sequences $M_0, M_1, \ldots, M_k$ of differentable manifolds, and $V_1, \ldots, V_k$ of polynomial vector fields such that

(1) $M_i$ is contained, with codimension 1 in $M_{i-1}$, for $i = 1, \ldots, k$;

(2) $M_0 = \mathbb{R}^k$ and $M_k = M$;

(3) $M_i$ does not contain any singular point of the vector field $V_i$ (considered as a vector field on $M_{i-1}$, for $i = 1, \ldots, k$);

(4) $M_i$ is orthogonal to $V_i$ in $M_{i-1}$ for $i = 1, \ldots, k$, i.e., for any path $p(t)$ on $M_i$, $p'(t) \cdot V_i = 0$. Moreover $M_i$ is the maximal differentiable manifold satisfying this property.

The sequences of the $M_i$'s and $V_i$'s are called the construction of the pfaffian manifold $M$.

Examples of pfaffian manifolds are the graph of the function $y = exp(x)$ in $\mathbb{R}^2$, or the set of zeroes in $\mathbb{R}^k$ of a polynomial in the variables $x_1, \ldots, x_n$ and in $exp(x_1), \ldots, exp(x_n)$.

We will call *Gamma condition* a finite set of polynomial equalities $PS = \{f_1 = 0, \ldots, f_m = 0\}$ and one polynomial inequality $J \neq 0$, together with a construction for a pfaffian manifold. The polynomial equations of a Gamma condition are called its *algebraic part*.

Kovanskii had shown, using arguments of Real Algebraic Geometry, that the set of solutions of a Gamma condition is a finite union of connected components. Richardson provided a simpler proof as outlined below: He begins by substituting the given Gamma condition with a set of *triangular* Gamma conditions using the, so called, *Zero structure theorem* which states that given a Gamma condition $\Gamma$ we can effectively find a finite list $\Gamma_i$'s of Gamma conditions whose algebraic part is triangular and such that the solution of the condition $\Gamma$ are given by the union of the solutions of the conditions $\Gamma_i$. The algorithm to get such decomposition uses a generalization of the Wu-Ritt process. The successive step in Richardson's construction is to refine the original system in order to get a zero-dimensional set of solutions with the property that each connected component of the original solution is represented at least by one 'sample' zero of the refined system. The cardinality of the 'sample' set is an upper bound for the number of connected components of the solutions of the original Gamma condition and it can be computed, in principle, from the bounds on the Wu-Ritt procedure and on the sampling technique used above.

It is an interesting open problem to understand better the relationship between the explicit bound given by Kovanskii and the bound provided with the construction sketched above. Another area of open problems related with pfaffian manifolds is to determine efficiently the topological relationships among the sets of solution of the triangular Gamma conditions $\Gamma_i$'s, obtained decomposing the original condition $\Gamma$.

# References


[1] H. Bass, E. Connell, and D. Wright. The Jacobian Conjecture: Reduction of Degree and Formal Expression of the Inverse. *Bull. Amer. Math. Soc.*, 7:287–300, 1982.

[2] D. Brownawell. Bounds for the Degree in the Nullstellensatz. *Annals of Mathematics, Second Series*, 126(3):577–591, 1987.

[3] Don Coppersmith and Shmuel Winograd. Matrix Multiplication via Arithmetic Progressions. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*, pages 1–6, New York City, New York, 25-27, May 1987.

[4] L. Csanky. Fast Parallel Matrix Inversion Algorithms. *SIAM Journal of Computing*, 5(4):618–623, December 1976.

[5] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The Membership Problem for Unmixed Polynomial Ideals is Solvable in Subexponential time. (Unpublished Manuscript), 1989.

[6] G. Gallo and B. Mishra. *Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets*, pages 119–142. Effective Methods in Algebraic Geometry. Birkhüser, 1991. Eds. T. Mora and C. Traverso.

[7] G. Gallo and B. Mishra. *Wu-Ritt Characteristic Sets and Their Complexity*, volume 6 of *DIMACS series in Discrete Mathematics and Theoretical Computer Science*, pages 111–136. Amarican Methematical Society and Association for Computing Machinery, 1991. Eds. J. Goodman and R. Pollack and W. Steiger.

[8] János Kollár. Sharp Effective Nullstellensatz. Unpublished Manuscript, 1988.

[9] A.G. Kovanskii. On a Class of Systems of Ftrascendental Equations. *Soviet Math. Dokl.*, 22(3):762–765, 1980.

[10] Wei Li and Steven Swanson. A Wu-Ritt Characteristic Set Criterion for the Invertibility of Polynomial Maps. Unpublished Manuscript, Purdue University, 1991.

[11] K. Mulmuley. A Fast Parallel Algorithm to Compute the Rank of a Matrix over an Arbitrary Field. *Combinatorica*, 7(1):101–104, 1987.

[12] D. Richardson. Wu's Method and the Kovanskii Finitess Theorem. *Journal of Symbolic Computation*, 12:127–141, 1991.

[13] J.F. Ritt. *Differential Algebra*. American Mathematical Society, New York, 1950.

[14] A. van den Essen. A Criterion to Determine if a Polynomial Map is Invertible and to Compute the Inverse. *Comm. Algebra*, 18:3183–3186, 1990.

[15] Wu Wen-Tsün. On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientia Sinica*, 21:157–179, 1978.

[16] Wu Wen-Tsün. Basic principles of mechanical theorem proving in geometries. *Journal of Sys. Sci. and Math. Sci.*, 4(3):207–235, 1984. Also in *Journal of Automated Reasoning*, 2(4):221–252, 1986.

[17] Wu Wen-Tsün. *Some Recent Advances in Mechanical Theorem-Proving of Geometries*, volume 29 of *Automated Theorem Proving: After 25 Years, Contemporary Mathematics*, pages 235–242. American Methematical Society, 1984.