Wu-Ritt Characteristic Sets and Their Complexity

G. Gallo & B. Mishra

Courant Institute, New York University

Based on a talk presented by B. Mishra at the Algebra and Geometry Workshop, Discrete Mathematics and Computer Science Center (DIMACS), Rutgers University, New Jersey. May 22, 1990.

Abstract

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. In this paper, we survey the original Wu-Ritt process, and its applications: particularly, in geometry. We also present optimal algorithms for computing a characteristic set with simple-exponential sequential and polynomial parallel time complexities. These algorithms were first devised by the present authors by using an effective version of Hilbert's Nullstellensatz, due to D. Brownawell and J. Kollár.

Supported by NSF Grant #CDA-90-18673, #CCR-9002819, ONR Grant #N00014-89-J3042 and an Italian CNR fellowship.
Authors' Address: Courant Institute, New York University, 251 Mercer Street, New York, NY 10012.
Last Updated: July 8, 1995.

1. Introduction

The history of the origin and subsequent developments of *Wu-Ritt Characteristic Sets* is somewhat peculiar. The concept of a characteristic set was discovered in the late forties by J.F. Ritt (see his now classic book *Differential Algebra* [34]) in an effort to extend some of the constructive algebraic methods to differential algebra. However, these concepts languished in near oblivion until the last decade when the Chinese mathematician Wu Wen-Tsün [36, 35, 37] realized its power in the case where Ritt's techniques are specialized to commutative algebra. In particular, he exhibited its effectiveness (largely through empirical evidence) as a powerful tool for Mechanical Theorem proving. This proved to be a turning point; a renewed interest in the subject has contributed to a better understanding of the power and complexity of the Ritt's techniques.

For a system of algebraic or differential equations, its characteristic set is a certain effectively-constructible triangular set of equations that preserves many of the interesting geometric properties of the original system [10, 18, 17, 25, 34]. However, until very recently, the constructivity of Ritt's characteristic set had not been explicitly demonstrated [18]; the original Wu-Ritt Process, first devised by Ritt [34], subsequently modified by Wu [36, 35, 37] and widely implemented [10], computes only an *extended* characteristic set. Furthermore, the Wu-Ritt Process, as it is, has a non-elementary[1] worst-case time complexity and thus, in principle, infeasible.

It has been speculated that the reason Wu-Ritt process has failed to receive its deserving place in constructive algebra was largely because it has been eclipsed by the spectacular success of Buchberger's "Gröbner Bases Algorithm." A lively debate about the respective power of these two algorithms has sprung up. Considerable amounts of experimental data are available, comparing the time-complexity of various implementations of Wu-Ritt Process with Gröbner Bases algorithms [7, 10, 9, 27, 30, 31]. However, while the worst-case complexity of Gröbner Bases algorithms are fairly well-understood at this point [2, 3, 4, 15, 16, 19, 23, 28, 29, 32, 38], the computational complexity of Wu-Ritt Characteristic Sets had remained open until very recently [18].

In this paper, we survey the original Wu-Ritt process, and its applications: particularly, in geometry. We also present optimal algorithms for computing a characteristic set with simple-exponential sequential and polynomial parallel time complexities. These algorithms were first devised by the present authors by using an effective version of Hilbert's Nullstellensatz, due to D. Brownawell and J. Kollár [6, 26].

[1]For a discussion of the nonelementary computational problems, see pp. 419–423 of the algorithms text by Aho, Hopcroft and Ullman [1]. Roughly, a problem is said to have a nonelementary complexity, if its complexity cannot be bounded by a function that involves only a fixed number of iterations of the exponential function.

2. Characteristic Sets

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; without loss of generality, we may assume that the given ordering is the following:

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

Definition 2.1 Class and Class Degree. Let $f \in k[x_1, \ldots, x_n]$ be a multivariate polynomial with coefficients in k. An indeterminate 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 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, (i.e., $f \in k$) then, by convention, $\mathrm{class}(f) = 0$ 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 (i.e., $f \in k[x_1, \ldots, x_j] \setminus k[x_1, \ldots, x_{j-1}]$) then $\mathrm{class}(f) = j$ and $\mathrm{cdeg}(f) = \deg_{x_j}(f)$.

Thus, with each polynomial $f \in k[x_1, \ldots, x_n]$, we can associate a pair of integers, its *type*:

$$\begin{aligned} \mathrm{type} &: k[x_1, \ldots, x_n] \to \mathbb{N} \times \mathbb{N} \\ &: f \mapsto \langle \mathrm{class}(f), \mathrm{cdeg}(f) \rangle. \end{aligned}$$

□

Definition 2.2 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 (i) $\mathrm{class}(f_1) < \mathrm{class}(f_2)$, or (ii) $\mathrm{class}(f_1) = \mathrm{class}(f_2)$ and $\mathrm{cdeg}(f_1) < \mathrm{cdeg}(f_2)$. This is equivalent to saying that the polynomials are ordered according to the lexicographic order on their types:

$$f_1 \prec f_2 \quad \textit{if and only if} \quad \mathrm{type}(f_1) <_{\mathrm{lex}} \mathrm{type}(f_2).$$

Note that there are distinct polynomials f_1 and f_2 that are not comparable under the preceding order. In this case, $\mathrm{type}(f_1) = \mathrm{type}(f_2)$, and f_1 and f_2 are said to be of the *same rank*, $f_1 \sim f_2$. □

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

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

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

Definition 2.3 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). □

Lemma 2.1 Pseudo-Division Lemma.
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 α such that the following equation holds:*

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

where $\deg_{x_j}(r) < \deg_{x_j}(f)$ *and* $\alpha \leq \deg_{x_j}(g) - \deg_{x_j}(f) + 1$.
If α is assumed to be the smallest possible power satisfying equation (2) then q and r are uniquely determined. In this case, the polynomial r is said to be the pseudo-remainder *of g with respect to f, and denoted by,* $\mathrm{prem}(g, f)$. *We say a polynomial g is* reduced *with respect to f if* $g = \mathrm{prem}(g, f)$.
■

Definition 2.4 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 $(n - r)$. □

Thus, with each ascending set $\mathcal{F}$ we can associate an $(n+1)$-vector, its *type*,

$$\text{type: Family of Ascending Sets } \to (\mathbb{N} \cup \{\infty\})^{n+1},$$

where ∞ is assumed to be greater than any integer. For all $0 \leq i \leq n$, the i^{th} component of the vector is

$$\mathrm{type}\,(\mathcal{F})\,[i] = \begin{cases} \mathrm{cdeg}(g), & \text{if } (\exists!\, g \in \mathcal{F})\ \mathrm{class}(g) = i; \\ \infty, & \text{otherwise.} \end{cases}$$

Definition 2.5 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

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

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

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 $(\forall\, 1 \leq j \leq s)\ f_j \sim g_j$, and $\mathcal{F}$ and $\mathcal{G}$ are said to be of the *same rank*, $\mathcal{F} \sim \mathcal{G}$. □

Hence,

$$\mathcal{F} \prec \mathcal{G} \quad \textit{if and only if} \quad \text{type}(\mathcal{F}) <_{\text{lex}} \text{type}(\mathcal{G}).$$

Thus the map, *type*, is a partially ordered homomorphism from the family of ascending sets to $(\mathbb{N} \cup \{\infty\})^{n+1}$, where $(\mathbb{N} \cup \{\infty\})^{n+1}$ is ordered by the lexicographic order. Hence, the family of ascending sets endowed with the ordering '$\prec$' is a well ordered set.

Definition 2.6 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 remark that if $\mathcal{G}$ is a characteristic set of I then

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

Since $\mathcal{G}$ is an ascending set, by definition, $n \ge |\mathcal{G}|$. The other inequality can be shown as follows: Consider some arbitrary ordering of variables and assume that $|\mathcal{G}| = k$ and the class variables are $v_k, \ldots, v_1$. Let the remaining variables be called $u_1, \ldots, u_l$. We claim that u's must all be independent. Then $n - k = l \le \dim I$ and $|\mathcal{G}| = k \ge n - \dim I$.

The proof of the claim: Suppose that the claim is false. Then I must contain a polynomial $f(u_1, \ldots, u_l)$ which is of class say u_j. Also, f is reduced with respect to those polynomials of $\mathcal{G}$ with lower ranks. Then one can add f to $\mathcal{G}$ to get an ascending set of lower rank, which is impossible, by the definition of characteristic set.

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.

The following technical lemma, concerning a system of univariate polynomials, will have further applications in obtaining degree and complexity bounds; for a direct (but lengthy) proof[2] see [18].

Lemma 2.2 *Let $H = \{h_1, h_2, \ldots, h_n\} \subseteq k[x_1, x_2, \ldots, x_n]$ be a set of univariate monic polynomials, one in each variable:*

$$h_j(x_j) \in k[x_j] \setminus k, \quad \textit{and} \quad \text{in}(h_j) = 1.$$

Then $\mathcal{H} = \langle h_1, h_2, \ldots, h_n \rangle$ is a characteristic set of (H) with respect to the following ordering of the indeterminates:

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

■

[2] A somewhat indirect proof of the above lemma may be obtained by first observing that H is a Gröbner basis of the ideal (H) (with respect to any admissible ordering), which immediately implies that

$$\Big(\forall\, g \in (H)\Big) \; \Big(\forall\, 1 \le j \le n\Big) \; \Big[\deg_{x_j}(g) \ge \text{cdeg}(h_j)\Big].$$

Since, $\text{class}(h_j) = j$, and since it has the minimal possible class degree, indeed, $\mathcal{H}$ is a characteristic set of (H).

Lemma 2.3 Generalized Pseudo-Division 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 there exists a sequence of polynomials (called a* pseudo-remainder sequence*),* g_0, g_1, $\ldots$, $g_r = g$, *such that for each* $1 \le i \le r$, *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* α_i *assumes the smallest possible power, achievable. Thus, the pseudo-remainder sequence 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*)* pseudo-remainder of g with respect to the ascending set $\mathcal{F}$, $g_0 = \mathrm{prem}\,(g, \mathcal{F})$. *By the earlier observations,* 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* $g = \mathrm{prem}\,(g, \mathcal{F})$. ∎

For an ascending set $\mathcal{F}$, we describe the set of all polynomials that are *pseudo-divisible* by $\mathcal{F}$, by the following notation:

$$\mathcal{M}(\mathcal{F}) = \Big\{g \in k[x_1, \ldots, x_n]: \mathrm{prem}(g, \mathcal{F}) = 0\Big\}.$$

Proposition 2.4 *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*

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

∎

3. Properties of Characteristic Sets

The main properties of characteristic sets are summarized in the next theorem. First, we need some additional notations.

For any set of polynomials $F = \{f_1, \ldots, f_r\} \subseteq k[x_1, \ldots, x_n]$, we write $\mathcal{Z}(F)$, to denote its *zero set*:

$$\mathcal{Z}(F) = \Big\{\langle p_1, \ldots, p_n\rangle \in k^n: \Big(\forall\ f \in F\Big)\ f(p_1, \ldots, p_n) = 0\Big\}.$$

By F^∞, we shall denote the set of all *finite products* of

$$\mathrm{in}(f_1), \ldots, \mathrm{in}(f_r),$$

and, for any ideal I in $k[x_1, \ldots, x_n]$, we use the notation $I{:}\,F^\infty$ for

$$\Big\{h : \Big(\exists\ f \in F^\infty\Big)\ [hf \in I]\Big\}.$$

It is easily seen that $I{:}\,F^\infty$ is itself an ideal. Note that, for an ascending set $\mathcal{F} = \langle f_1, \ldots, f_r\rangle$,

$$\mathrm{prem}(h, \mathcal{F}) = 0 \quad\Rightarrow\quad h \in (\mathcal{F}){:}\,\mathcal{F}^\infty.$$

Theorem 3.5 *Let I be an ideal in $k[x_1, \ldots, x_n]$ generated by $F = \{f_1, \ldots, f_s\}$. Let $\mathcal{G} = \langle g_1, \ldots, g_r\rangle$ be a characteristic set of I, and let $J = (g_1, \ldots, g_r) \subseteq I$ be the ideal generated by the elements of $\mathcal{G}$. Then*

1. $J \subseteq I \subseteq J : \mathcal{G}^\infty$.
2. $\mathcal{Z}(\mathcal{G}) \setminus \left(\bigcup_{i=1}^r \mathcal{Z}\Big(\mathrm{in}(g_i)\Big)\right) \subseteq \mathcal{Z}(I) \subseteq \mathcal{Z}(\mathcal{G})$.
3. $I =$ *prime ideal* $\quad \Rightarrow \quad I \cap \mathcal{G}^\infty = \emptyset$ *&* $I = J : \mathcal{G}^\infty$.

PROOF.
First, make the following two observations:

1. $J = (g_1, \ldots, g_r) \subseteq I$, $\qquad [\because g_i \in I$ by definition.$]$
2. $\mathrm{in}(g_i) \notin I$, $\qquad [\because \mathrm{prem}(\mathrm{in}(g_i), \mathcal{G}) = \mathrm{in}(g_i) \neq 0.]$

The assertion (1) follows from the first observation and the fact that

$$(\forall\, f \in I)\ \Big[\mathrm{prem}(f, \mathcal{G}) = 0\Big];$$

thus, for some element $\mathrm{in}(g_r)^{\alpha_r}\mathrm{in}(g_{r-1})^{\alpha_{r-1}} \cdots \mathrm{in}(g_1)^{\alpha_1} = g \in \mathcal{G}^\infty$,

$$gf = \sum_{i=1}^r q_i g_i \in J.$$

The assertion (2) follows from the previous assertion and the elementary properties of the zero sets of polynomials. Thus,

$$\mathcal{Z}(I) \subseteq \mathcal{Z}(J) = \mathcal{Z}(\mathcal{G}).$$

Hence, it suffices to prove that

$$\mathcal{Z}(\mathcal{G}) \setminus \left(\bigcup_{i=1}^r \mathcal{Z}\Big(\mathrm{in}(g_i)\Big)\right) \subseteq \mathcal{Z}(I).$$

Let $p \in k^n$ be a point in the zero set $\mathcal{Z}(\mathcal{G}) \setminus \left(\bigcup_{i=1}^r \mathcal{Z}\Big(\mathrm{in}(g_i)\Big)\right)$. Let $f \in I$. Then there exists a $g = \prod_{i=1}^r \mathrm{in}(g_i)^{\alpha_i} \in \mathcal{G}^\infty$ such that $gf \in J$. Thus, $g(p)\, f(p) = 0$. But by assumption, $g(p) \neq 0$. Then $f(p) = 0$, as is to be shown.

To see the last assertion, observe that if I is a prime ideal then

- If some $g \in \mathcal{G}^\infty$ belongs to I then so does one of the factors of g, say $\mathrm{in}(g_i)$. But this contradicts the second observation made in the beginning of this proof.
- Consider an $f \in J : \mathcal{G}^\infty$. By definition, there exists a $g \in \mathcal{G}^\infty$ such that

$$gf \in J \subseteq I \quad \& \quad g \notin I.$$

From the primality of I, conclude that $f \in I$. That is, $J : \mathcal{G}^\infty = I$. ∎

As an immediate consequence of the above statement, we have

$$\mathrm{prem}(f, \mathcal{G}) = 0 \quad \Leftrightarrow \quad f \in I,$$

provided that I is prime.

Remark 3.7

1. The inclusions in the assertion (2) of theorem 3.5 can be strict. Consider the ideal $I = (x^2+y^2-1, xy)$ and suppose $x \prec y$. A possible characteristic set for I is $\{xy, y^3-y\}$ whose zeroes are a set of higher dimension than the zeroes of I. Removing from it the zeroes of the initial of xy, i.e., the line of equation $y = 0$ one gets only two of the four original points in $\mathcal{Z}(I)$.

2. The hypothesis of primality for I in the assertion (4) of theorem 3.5 cannot be relaxed. Consider for example the ideal $I = (xy, y^2)$. The given set of generators is already a characteristic set for I, assuming $y \prec x$, but $\mathrm{in}((xy)^2) = y^2 \in I$. $\square$

One way to interpret the preceding theorem is to say that constructing characteristic sets helps only in answering geometrical questions, but not with general algebraic problems. Thus, while characteristic sets are capable of answering the *membership problem for a radical ideal*, they are not powerful enough to handle the more general *membership problem for an arbitrary ideal*.

4. Wu's Approach to the Construction of Characteristic Sets

In this section, we shall 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. Historically, this represents the first effort to effectively construct a triangular set corresponding to a system of differential equations. Here, we focus just on the algebraic analog.

Definition 4.8 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 below 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*

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

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

Wu-Ritt Process:
Input: $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$.
Output: $\mathcal{G}$, an extended characteristic set of F.

1. $\mathcal{G} := \emptyset$; $R := \emptyset$;
2. loop
3. $F := F \cup R$; $F' := F$; $R := \emptyset$;
4. while $F' \neq \emptyset$ loop
5. Choose a polynomial $f \in F'$ of *minimal rank*;
6. $F' := F' \setminus \{g\colon \mathrm{class}(g) = \mathrm{class}(f)$ and
7. g is not reduced with respect to $f\}$;
8. $\mathcal{G} := \mathcal{G} \cup \{f\}$;
9. end{loop };
10. for all $f \in F \setminus \mathcal{G}$ loop
11. if $r := \mathrm{prem}(f, \mathcal{G}) \neq 0$ then
12. $R := R \cup \{r\}$;
13. end{if };
14. end{loop };
15. until $R = \emptyset$;
16. return $\mathcal{G}$;

end{Wu-Ritt Process}. ■

It is trivial to see that when the algorithm terminates, it, in fact, returns an ascending set $\mathcal{G}$ that satisfies the conditions given in definition 4.8. The termination follows from the following observations:

Let $F \subseteq k[x_1, \ldots, x_n]$ be a (possibly, infinite) set of polynomials. Consider the family of all ascending sets, each of whose components is in F,

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

A minimal element in $\mathbf{S}_F$ (with respect to the $\prec$ order on ascending sets) is denoted as $\mathrm{MinASC}(F)$. The following easy proposition can be shown:

Proposition 4.6 *Let F be as above. Let g be a polynomial reduced with respect to* $\mathrm{MinASC}(F)$. *Then*

$$\mathrm{MinASC}(F \cup \{g\}) \prec \mathrm{MinASC}(F).$$

■

Now, let F_i be the set of polynomials obtained at the beginning of the i^{th} iteration of the loop [lines 2–15]. Starting from the set F_i, the algorithm constructs the ascending chain $\mathcal{G}_i = \mathrm{MinASC}(F_i)$ in the loop [lines 4–9]. Now, if R_i (constructed by the loop [lines 10–14]) is non-empty, then each element of R_i is reduced with respect to $\mathcal{G}_i$. Now, since

$$F_{i+1} = F_i \cup R_i,$$

we observe that

$$\mathrm{MinASC}(F_0) \succ \mathrm{MinASC}(F_1) \succ \cdots \succ \mathrm{MinASC}(F_i) \succ \cdots$$

Since the "$\prec$" is a well-ordering on the ascending sets, the above chain must be finite and the algorithm must terminate. However, the number of steps the algorithm may take in the worst case can be non-elementary in the parameters n (the number of variables) and d (the maximum degree of the polynomials). Assume the usual ordering on the indeterminates:

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

To understand the worst-case behavior of the algorithm, we need to consider 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 $= d$. After each iteration of the main loops, we can show that the largest degree in any variable is bounded by $T_2(k)$, where

$$\begin{aligned} T_2(0) &= d \\ T_2(1) &= 2d \\ T_2(k) &= 2\,T(k-1) + T(k-2), \quad k > 1. \end{aligned}$$

We observe that if after the $(i-1)$, $2 < i \le d+1$, iterations of the loops, we have a set of s polynomials consisting of

- f_1 of class $= n$, cdeg $= d - i + 2$ and deg $\le T_1(i-1)$,
- f_2 of class $= n$, cdeg $= d - i + 1$ and deg $\le T_2(i-1)$ and
- f_3, ..., f_s, each of class $= n$, cdeg $= d - i + 1$ and deg $\le T_3(i-1)$,

then, in the worst-case, we can obtain after i iterations, a set of s polynomials consisting of

- f_1' of class $= n$, cdeg $= d - i + 1$ and deg $\le T_2(i-1)$,
- f_2' of class $= n$, cdeg $= d - i$ and deg $\le 2T_2(i-1) + T_1(i-1)$ and
- f_3', ..., f_s', each of class $= n$, cdeg $= d - i$ and deg $\le T_2(i-1) + T_3(i-1)$.

The rest follows from the fact that the maximal value of the degrees is given by T_2.

The recurrence equation can be easily solved to get:

$$T_2(k) \le \frac{d}{2\sqrt{2}}(1+\sqrt{2})^{(k+1)}.$$

Now observe that the above process can be repeated for at most d iterations to yield a similar instance with class reduced by 1 but class degree enlarged to $c'd(1+\sqrt{2})^d$. Thus, a bound on the number of iterations can be given by the following recurrence equations:

$$\begin{aligned} T(0,d) &= 1, \\ T(n,d) &\le T\Big(n-1, c'(1+\sqrt{2})^d\Big) + d, \quad n \ge 1. \end{aligned}$$

A solution to the above equation leads to

$$T(n,d) \le c \cdot \underbrace{d(1+\sqrt{2})^{d(1+\sqrt{2})^{\cdot^{\cdot^{d(1+\sqrt{2})^d}}}}}_{n},$$

a non-elementary function in the input-size.

In general, an extended characteristic set of an ideal is not a characteristic set of the ideal. However, an extended characteristic set *does* satisfy the following property, in a manner similar to a characteristic set.

Theorem 4.7 *Let $F \subseteq k[x_1, \ldots, x_n]$ be a basis of an ideal I, with an extended characteristic set $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$. Then*

$$\mathcal{Z}(\mathcal{G}) \setminus \left(\bigcup_{i=1}^{r} \mathcal{Z}\Big(\mathrm{in}(g_i)\Big) \right) \subseteq \mathcal{Z}(I) \subseteq \mathcal{Z}(\mathcal{G}).$$

PROOF.
Let

$$\mathcal{M}(\mathcal{G}) = \Big\{ f \colon \mathrm{prem}(f, \mathcal{G}) = 0 \Big\}.$$

denote, as before, the set of all polynomials that are *pseudo-divisible* by $\mathcal{G}$. Thus, by the properties of an extended characteristic set,

$$(\mathcal{G}) \subseteq I \subseteq \Big(\mathcal{M}(\mathcal{G})\Big).$$

Using the elementary properties of the zero sets of polynomials, we get

$$\mathcal{Z}\Big(\mathcal{M}(\mathcal{G})\Big) \subseteq \mathcal{Z}(I) \subseteq \mathcal{Z}(\mathcal{G}).$$

Hence, it suffices to prove that

$$\mathcal{Z}(\mathcal{G}) \setminus \left(\bigcup_{i=1}^{r} \mathcal{Z}\Big(\mathrm{in}(g_i)\Big) \right) \subseteq \mathcal{Z}\Big(\mathcal{M}(\mathcal{G})\Big).$$

Let $p \in k^n$ be a point in the zero set $\mathcal{Z}(\mathcal{G}) \setminus \Big(\bigcup_{i=1}^{r} \mathcal{Z}\Big(\mathrm{in}(g_i)\Big) \Big)$. Let $f \in \mathcal{M}(\mathcal{G})$. Then there exists a $g = \prod_{i=1}^{r} \mathrm{in}(g_i)^{\alpha_i} \in \mathcal{G}^{\infty}$ such that $gf \in J$. Thus, $g(p)\, f(p) = 0$. But by assumption, $g(p) \neq 0$. Then $f(p) = 0$, as is to be shown. ■

5. Construction and Complexity of Characteristic Sets[3]

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:

$$\Big(\forall\ 1 \leq i \leq s\Big)\ \Big[\deg(f_i) \leq d\Big].$$

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. In the next two subsections, 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.

5.1 Lower Bounds

Theorem 5.8 Lower Bound Theorem.
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:

$$\begin{aligned} f_1 &= x_1 - x_n^d, \\ f_2 &= x_2 - x_1^d, \\ &\vdots \\ f_{n-1} &= x_{n-1} - x_{n-2}^d, \\ f_n &= x_n - x_{n-1}^d. \end{aligned}$$

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 $D \geq d^n$.

PROOF.
Let $\pi \in S_n$ be a permutation of $[1..n]$, and the arbitrary but fixed ordering on the indeterminates be the following

$$x_i = x_{\pi(1)} \prec x_{\pi(2)} \prec \cdots \prec x_{\pi(n)}.$$

Note that $I \cap \Big(k[x_i] \setminus k\Big)$ contains a nonzero polynomial $x_i - x_i^{d^n}$ of *minimal possible degree*, d^n.
(1) Let $\mathcal{G} = \langle g_1, \ldots, g_r\rangle$ be a characteristic set of F, with respect to the chosen ordering. Since $\dim I = 0$,

$$|\mathcal{G}| = n, \quad \text{and} \quad g_1 \in I \cap \Big(k[x_i] \setminus k\Big).$$

Thus, $\quad D \geq \operatorname{cdeg}(g_1) = \min\Big\{\deg(f) \colon f \in I \cap (k[x_i] \setminus k)\Big\} = d^n.$
(2) Let $\mathcal{G}' = \langle g_1', \ldots, g_r'\rangle$ be an extended characteristic set of F, with respect to the chosen ordering. By an examination of the Wu-Ritt process, we see that $\operatorname{in}(g_j') = 1$, for all $1 \leq j \leq r$, and by Lemma 4.7,

$$\mathcal{Z}(\mathcal{G}') = \mathcal{Z}(I) = \text{a finite set}.$$

[3] The results in this section are largely based on the paper [18]; more details may be found therein.

Hence

$$|\mathcal{G}'| = n, \quad \text{and} \quad g_1 \in I \cap \Big(k[x_i] \setminus k\Big).$$

Thus, $D \geq \operatorname{cdeg}(g_1) = \min\Big\{\deg(f) \colon f \in I \cap (k[x_i] \setminus k)\Big\} \geq d^n.$ ■

In the subsequent discussion, we shall focus only on the characteristic sets of an ideal, since it is dubious whether an extended characteristic set improves the computational power of our algorithms. We remark that if we choose the following ordering on the indeterminates:

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

then a characteristic set of I of theorem 5.8 is given by,

$$\begin{array}{rrcl} \mathcal{G} = \Big\langle & g_1 & = & x_1 - x_1^{d^n}, \\ & g_2 & = & x_2 - x_1^{d}, \\ & & \vdots & \\ & g_{n-1} & = & x_{n-1} - x_1^{d^{n-2}}, \\ & g_n & = & x_n - x_1^{d^{n-1}} \Big\rangle. \end{array}$$

A slightly better bound of

$$\deg(f_1)\deg(f_2)\cdots\deg(f_n),$$

can be obtained, by a simple modification of the construction in theorem 5.8.

We note that the ideal I of theorem 5.8 is a zero-dimensional ideal; the previous example can be modified to show that, in general, the degree of a characteristic set is $\Omega(d^{(n-\dim I)})$. It is interesting to ask if a better lower bound can be constructed for more general cases.

5.2 Upper Bounds

We start by recalling the following version of *effective Hilbert's Nullstellensatz*, originally due to D. Brownawell [6] and later sharpened by J. Kollár [26].

Theorem 5.9 Effective Hilbert's Nullstellensatz.
Let $I = (f_1, \ldots, f_s)$ be an ideal in $k[x_1, \ldots, x_n]$, where k is an arbitrary field, and $\deg(f_i) \leq d$, $1 \leq i \leq s$. Let $h \in K[x_1, \ldots, x_n]$ be a polynomial with $\deg(h) = \delta$. Then

$$h \in \sqrt{I}$$

if and only if

$$\Big(\exists\, b_1, \ldots, b_s \in k[x_1, \ldots, x_n]\Big) \left[h^M = \sum_{i=1}^{s} b_i f_i,\right],$$

where $M \leq 2(d+1)^n$ and $\deg(b_i f_i) \leq 2(\delta+1)(d+1)^n, 1 \leq i \leq s.$ ■

Using this version of Nullstellensatz, we shall first derive a degree bound for a characteristic set of a zero-dimensional ideal, and then use a 'lifting' procedure to obtain a bound for the more general cases.

The following proposition shows that every zero dimensional ideal I contains a univariate polynomial $h_j(x_j)$, in each variable x_j, with the additional property that $\deg(h_j) \leq 2(d+1)^{2n}$. 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.

Lemma 5.10 *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 for every indeterminate x_j, there exists a univariate polynomial $h_j \in I \cap k[x_j]$ such that*

$$\Big(\exists\, b_{j,1}, \ldots, b_{j,s} \in k[x_1, \ldots, x_n]\Big) \left[h_j = \sum_{i=1}^{s} b_{j,i} f_i,\right],$$

where $\deg(h_j) \leq 2(d+1)^{2n}$, *and* $\deg(b_{j,i}f_i) \leq 4(d+1)^{2n}, 1 \leq i \leq s$.

PROOF.
Suppose first that k is algebraically closed. Assume that the finite set of T zeroes of I are given by

$$\mathcal{Z}(I) = \Big\{P_i = \langle p_{i,1}, \ldots, p_{i,j}, \ldots, p_{i,n}\rangle \in k^n \colon 1 \leq i \leq T\Big\} \neq \emptyset.$$

By the Bezout's inequality of J. Heintz [20], we have $T \leq (d+1)^n$. Now consider the following monic polynomial $h'_j(x_j) \in k[x_j]$,

$$h'_j(x_j) = \prod_{i=1}^{t} (x_j - p_{i,j}),$$

where $p_{i,j}$ is the j^{th} coordinate of the i^{th} zero of I. As h'_j vanishes at all the zeros of I, by Hilbert's Nullstellensatz, it must be in the *radical* of I,

$$h'_j \in \sqrt{I}, \quad \text{that is,} \quad h_j = (h'_j)^M \in I.$$

But by construction h_j is a monic polynomial of degree TM, in $k[x_j]$. Moreover, by theorem 5.9, we see that $M \leq 2(d+1)^n$, and

$$\deg(h_j) \leq 2(d+1)^{2n}, \quad 1 \leq j \leq n.$$

The bound on the representation of h_j comes directly from theorem 5.9,

$$\deg(b_{j,i}f_i) \leq 2(T+1)(d+1)^n \leq 4(d+1)^{2n}.$$

If k is not algebraically closed the above construction can be done in its algebraic closure. Observe now that, since the degree of h_j is bounded, its coefficients are determined by a system of linear equations over k, and thus, $h_j \in k[x_j]$. ■

Corollary 5.11 *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 $\deg(f_i) \leq d$, $1 \leq i \leq s$. Let $g \in k[x_1, \ldots, x_n]$ be a polynomial with $\deg(g) = \Delta$. Then*

$$g \in I$$

if and only if

$$\Big(\exists\, a_1, \ldots, a_s \in k[x_1, \ldots, x_n]\Big) \left[g = \sum_{i=1}^{s} a_i f_i,\right],$$

where $\deg(a_i f_i) \leq \max\{d, \Delta\} + 6n(d+1)^{2n}, 1 \leq i \leq s$.

PROOF.

Assume that $g \in I$. Then, using the univariate, monic polynomials h_j's (obtained in lemma 5.10) as rewriting rules modulo $J = (h_1, \ldots, h_n) \subseteq I$, g may be expressed as follows:

$$g \;=\; h + \sum_{i=1}^{s} a'_i f_i,$$

$$\text{where} \qquad \deg(a'_i f_i) \;\leq\; \max_{1\leq i\leq s}\Big\{\deg(f_i)\Big\} + \sum_{j=1}^{n} \deg_{x_j}(h_j) \;\leq\; d + 2n(d+1)^{2n}, \qquad 1 \leq i \leq s.$$

Thus, we have

$$h = g - \sum_{i=1}^{s} a'_i f_i \in J, \quad \text{and} \quad \deg(h) \;\leq\; \max\Big\{\Delta, d + 2n(d+1)^{2n}\Big\}.$$

But, by Lemma 2.2, $\mathcal{H} = \langle h_1, \ldots, h_n\rangle$ is a characteristic set of J. Since $h \in J$, we see that $\mathrm{prem}(h, \mathcal{H}) = 0$. But since $\mathrm{in}(h_j) = 1$, for all $1 \leq j \leq n$, we have,

$$h = \sum_{j=1}^{n} q_j h_j = \sum_{i=1}^{s} \left(\sum_{j=1}^{n} q_j b_{j,i}\right) f_i = \sum_{i=1}^{s} a''_i f_i,$$

$$\begin{aligned} \text{where} \quad \deg(a''_i f_i) \;&\leq\; \max_{j}\Big\{\deg(q_j)\Big\} + \max_{i,j}\Big\{\deg(b_{j,i} f_i)\Big\} \\ &\leq\; \deg(h) + 4(d+1)^{2n} \;\leq\; \max\{d, \Delta\} + 6n(d+1)^{2n}, \quad 1 \leq i \leq s. \end{aligned}$$

Thus g may be expressed as

$$g = \sum_{i=1}^{s} \left(a''_i + a'_i\right) f_i = \sum_{i=1}^{s} a_i f_i,$$

where $\deg(a_i f_i) \leq \max_{1\leq i\leq s}\Big\{\deg(a''_i f_i), \deg(a'_i f_i)\Big\} \leq \max\{d, \Delta\} + 6n(d+1)^{2n}$. ■

Theorem 5.12 Zero-Dimensional Upper Bound Theorem.

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

2.

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

and $\deg(a_{j,i} f_i) \le 8n(d+1)^{2n} = O\left(d^{O(n)}\right), 1 \le i \le s$.

PROOF.
Note that $\mathcal{H} = \langle h_1, \ldots, h_n \rangle$ of lemma 5.10, is an ascending set in $\mathbf{S}_I$. The first condition follows from the facts that, for all $1 \le j \le n$,
1. $\text{class}(g_j) = \text{class}(h_j) = j$, and $\text{cdeg}(g_j) \le \text{cdeg}(h_j) \le \deg(h_j) \le 2(d+1)^{2n}$.
2. For all $1 \le i < j$, $\deg_{x_i}(g_j) < \deg_{x_i}(g_i)$, as g_j is reduced with respect to the preceding g_i's. Thus

$$\deg(g_j) \le \left(\sum_{i=1}^{j} \text{cdeg}(g_i)\right) - j + 1 \;\le\; 2j(d+1)^{2n} - j + 1 \;\le\; 2n(d+1)^{2n}.$$

Since each g_j is in I, the condition (3) is an immediate consequence of the corollary 5.11. ∎

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. However, in this case, we need to restrict the class of orderings on the indeterminates that may be chosen.

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, $\deg(f_i) \le d$. Assume that the indeterminates, $x_{\pi(1)} = u_1, \ldots, x_{\pi(l)} = u_l$, are the *independent* variables with respect to I. That is, these independent variables form the largest subset of $\{x_1, \ldots, x_n\}$ such that

$$I \cap k[u_1, \ldots, u_l] = (0).$$

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

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

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

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

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

$$\mathrm{class}(g_j') = \pi(l+j), \quad \text{and} \quad \deg_V(g_j') \leq 2r(d+1)^{2r}.$$

Additionally, by the results of the previous section, each g_j' can be expressed as

$$g_j' = \sum_{i=1}^{s} a_{j,i}' f_i, \quad \text{where} \quad \deg_V(a_{j,i}' f_i) \leq 8r(d+1)^{2r}. \tag{4}$$

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 $k[u_1, \ldots, u_l]$. Note that there is one equation per each power-product in r variables of degree $\leq 8r(d+1)^{2r}$, and one unknown per coefficient of the polynomials g_j' and $a_{j,i}'$'s. Thus the coefficients of g_j' and $a_{i,j}'$'s are rational functions in $k(u_1, \ldots, u_d)$, with the numerators and denominators being determined by determinants of polynomial matrices of order $\leq \Gamma$ and with entries of degree $\leq d$ in $k[u_1, \ldots, u_l]$. Hence, these numerators and denominators, themselves, have their degrees bounded by $d\Gamma$.

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 following equation,

$$g_j = \sum_{i=1}^{s} a_{j,i} f_i, \tag{5}$$

where all the coefficients are in $k[u_1, \ldots, u_l]$. Note that m can be chosen to be the *least common multiplier* of all the denominators, and since there are at most $(s+1)\Gamma$ such denominators, we have

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

In the following theorem, we show that $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$ is, in fact, a characteristic set of the ideal I.

Theorem 5.13 General Upper Bound Theorem.
Let $I = (f_1, \ldots, f_s)$ be an ideal in $k[x_1, \ldots, x_n]$, where k is an arbitrary field, and $\deg(f_i) \leq d$, $1 \leq i \leq s$. 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 $1 \leq j \leq r$,

1. $\text{class}(g_j) = j + l$ *and* $\deg(g_j) \leq 4(s+1)(9r)^{2r} d(d+1)^{4r^2} = O\left(s\ d^{O(r^2)}\right)$.

2.

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

and $\deg(a_{j,i} f_i) \leq 11(s+1)(9r)^{2r} d(d+1)^{4r^2} = O\left(s\ d^{O(r^2)}\right), 1 \leq i \leq s$.

PROOF.
As before, let us assume that the independent variables with respect to I are $u_1 = x_1$, …, and $u_l = x_l$, and we write $k[u_1, \ldots, u_l, v_1, \ldots, v_r]$ for the ring $k[x_1, \ldots, x_n]$. Let $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$ be the sequence of polynomials defined in the preceding paragraph. As g_j's were derived from an ascending set $\mathcal{G}'$ of $\mathbf{S}_{I'}$ in $k(u_1, \ldots, u_l)[v_1, \ldots, v_r]$, by multiplication with a polynomial in $k[u_1, \ldots, u_l]$, and since $g_j \in I$ (by construction), clearly $\mathcal{G}$ is an ascending set in $\mathbf{S}_I$.

Furthermore, $\mathcal{G}$ is a minimal set in $\mathbf{S}_I$, since, if there were another ascending set $\mathcal{H} \prec \mathcal{G}$ in $\mathbf{S}_I$, then $\mathcal{H}$ itself would be an ascending set in $\mathbf{S}_{I'}$ and of smaller rank than $\mathcal{G}'$, when the polynomials in $\mathcal{H}$ are treated as polynomials in $k(u_1, \ldots, u_l)[v_1, \ldots, v_r]$; this, however, would contradict the assumption that $\mathcal{G}'$ is a characteristic set of the extended ideal I'.

By construction, $\text{class}(g_j) = j + l$. The rest involves some simple calculations. ■

5.3 Algorithms

Now, we can describe how to compute a characteristic set of an ideal, by using the degree bounds of the *General Upper Bound Theorem* 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 $O(N^{2.376})$ [11, 1] and that the parallel algorithms have time complexity $O(\log^2 N)$, (and polynomial size) [12, 5, 33]. 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, $\deg(f_i) \leq d$. 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*. The ordering on the indeterminates are so chosen that

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

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. [14].

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^{th} element g_j of $\mathcal{G}$. By the theorem 5.13, we know that $\text{class}(g_1) = (l+1), \ldots, \text{class}(g_{j-1}) = (l+j-1)$ and $\text{class}(g_j) = (l+j)$. Let

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

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, from the *General Upper Bound Theorem*, that

$$\Bigl(\exists\ a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n]\Bigr)\ \left[g_j = \sum_{i=1}^{s} a_{j,i} f_i,\right], \tag{6}$$

and $\deg(g_j), \deg(a_{j,i} f_i) \le 11(s+1)(9r)^{2r} d(d+1)^{4r^2}, \quad 1 \le i \le s$.
Thus g_j satisfying all the properties can be determined by solving an appropriate system of linear equations, involving the power products of degree less than $11(s+1)(9r)^{2r}d(d+1)^{4r^2}$, i.e., $O\Bigl(s^{O(n)}(d+1)^{O(n^3)}\Bigr)$-many linear equations.

In particular, the sequential and parallel complexity of the algorithm to compute the j^{th} element of a characteristic set are given, respectively, by $O(s^{O(n)}(d+1)^{O(n^3)})$ and $O(n^6 \log^2(s+d+1))$. 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.

Theorem 5.14 Complexity of Characteristic Sets.
Let $I = (f_1, \ldots, f_s)$ be an ideal in $k[x_1, \ldots, x_n]$, where k is an arbitrary field, and $\deg(f_i) \le d$, $1 \le i \le s$. Then with respect to any ordering on the indeterminates:

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

where the first $\dim(I)$-many variables are independent, one can compute a characteristic set of I, in $O(s^{O(n)}(d+1)^{O(n^3)})$ sequential time or $O(n^7 \log^2(s+d+1))$ parallel time. The polynomials in the computed characteristic set are of degree $O(s(d+1)^{O(n^2)})$. ■

If the ideal is zero-dimensional, then the arguments in this section can be specialized to yield better bounds (see [18]).

6. Applications: Mechanical Geometric Theorem Proving

Let us consider how the concepts of characteristic sets (or extended characteristic sets) can be used in a simple geometric theorem prover. The first such mechanical theorem prover, devised by Wu Wen-Tsün [36, 35, 37] in China, has come to be known as the *China Prover* and has been successfully used to prove many classical and some new theorems in plane analytic geometry. Some further improvements in this direction has been achieved by Shang-Ching Chou [10].

Other approaches, based on different constructive methods in computer algebra, have also been proposed for this problem: For instance, B. Kutzler and S. Stifter [27] and D. Kapur [24] have proposed methods based on Gröbner bases; G. Carrá and G. Gallo [8] have devised a method using the dimension of the underlying algebraic variety; Jia-Wei Hong [22] has introduced a seminumerical algorithm using an interesting gap theorem and 'proof-by-example' techniques. However, none of these other methods have yet achieved the kind of wide-spread acceptance that Wu's method has had.

The method based on the Wu-Ritt characteristic sets is not, however, a real theorem prover, in the sense that it does not follow any logical proof theoretic techniques; it simply takes an algebraic translation of a set of geometric statements and tries to verify its validity in the manner to be made more precise. For most of the geometric statements, however, the translation from geometry to algebra is far from being completely automated. The fundamental principle that the translation method relies on is fairly simple, i.e., the classical coordinate method of Descartes introduced in the 17th century.

Definition 6.9 By an *elementary geometry statement*, we mean a formula of the following kind:

$$\Big(f_1 = 0 \ \wedge \ f_2 = 0 \ \wedge \ \cdots \ \wedge \ f_s = 0 \Big) \quad \Rightarrow \quad \Big(g = 0 \Big), \tag{7}$$

where the f_i's and g are polynomials in $k[x_1, \ldots, x_n]$, the variables x_i's are assumed to be bound by universal quantification and their ranges are assumed to be the field k, the base field of the underlying geometry. We further assume that the base field is algebraically closed. □

The conjunct $\bigwedge_i (f_i = 0)$ is called the *premise* of the geometry statement, and will be assumed to be nontrivial, i.e., the set of points in k^n satisfying the premise is nonempty. The statement $g = 0$ is its *conclusion*.

To prove a statement, then, is to show that a geometric formula is valid. For a complete analysis of the classes of geometric propositions included in definition 6.9, refer to [10].

However, one problem with the above algebraic statement is that it does not mention certain *geometric degeneracies* that are implicitly excluded: For instance, when a geometric statement mentions a *triangle*, it is conventionally assumed to mean those non-degenerate triangles whose vertices are non-collinear. But, on the other hand, spelling out all the conceivable geometric degeneracies makes the process unappealingly cumbersome. Wu's approach permits one to circumvent this problem as it produces these nondegeneracy conditions as a natural by-product. In fact, Wu's approach proves an elementary geometry statement, in the sense that it shows that the *conclusion is true whenever the premises are generically true*. In geometric terms, it shows that the conclusion polynomial vanishes on *some open subset* (under the Zariski topology) of the zero set of the system of polynomials, f_1, f_2, …, f_s. Following Wu, in this case, we will say that the corresponding geometric statement is *generically true*.

The Wu's algorithm is as follows: Assume that the input to the algorithm is an elementary geometry formula which is obtained after the theorem has been translated algebraically.

```
Wu's Algorithm:
Input:    Premises = F = {f_1, ..., f_s} ⊆ k[x_1, ..., x_n],
          Conclusion = g ∈ k[x_1, ..., x_n].
Output:   Trivial, if the premises are contradictory;
          True, if the geometry statement is generically true.

1. Compute 𝒢, a characteristic set of I;
2. if 𝒢 = ⟨1⟩ then
3.    return Trivial;
2. elsif prem(g, 𝒢) = 0 then
3.    return True;
4. else
5.    return Unknown;
end{Wu's Algorithm}. ■
```

In order to understand Wu's algorithm we need to make the following observations:

- If $\mathcal{G} = \langle 1 \rangle$ then, since every $g_i \in \mathcal{G}$ also belongs to the ideal (F), we see that $(F) = (1)$ and that $\mathcal{Z}(F) = \emptyset$. In this case, the system of premises are inconsistent and the geometry statement is trivially true.

  Also observe that if the ideal $(F) = (1)$ then, by definition, its characteristic set must be $\langle 1 \rangle$. Thus, the algorithm always correctly detects a trivial geometry statement.

- Suppose $\mathcal{G} = \langle g_1, \ldots, g_r \rangle \neq \langle 1 \rangle$. If $r = \mathrm{prem}(g, \mathcal{G}) = 0$ then

$$\mathrm{in}(g_r)^{\alpha_r}\mathrm{in}(g_{r-1})^{\alpha_{r-1}} \cdots \mathrm{in}(g_1)^{\alpha_1} g = \sum_{i=1}^{r} q_i g_i \in (f_1, \ldots, f_s). \tag{8}$$

  Thus at every point $p \in k^n$, at which f_i's (hence, g_i's) vanish, but not $\mathrm{in}(g_i)$'s, we note that the conclusion polynomial g must also vanish. The clause

$$\mathrm{in}(g_1) = 0 \vee \cdots \vee \mathrm{in}(g_r) = 0$$

  has been interpreted by Wu as the associated degeneracy condition for the original geometry statement. Thus, when **Wu's Algorithm** returns the value "True," the following holds:

$$\begin{aligned} \Big(\forall\, p \in k^n\Big) \Bigg[& \Big(f_1(p) = 0 \wedge \cdots \wedge f_s(p) = 0\Big) \wedge \\ & \neg\Big(\mathrm{in}(g_1)(p) = 0 \vee \cdots \vee \mathrm{in}(g_r)(p) = 0\Big) \\ \Rightarrow \quad & g(p) = 0 \Bigg] \end{aligned}$$

Geometrically, we have

$$\mathcal{Z}(g) \supseteq \mathcal{Z}(f_1, \ldots, f_s) \setminus \bigcup_{i=1}^{r} \mathcal{Z}(\mathrm{in}(g_i)),$$

that is, g vanishes on *some open set* (in the sense of Zariski topology) of $\mathcal{Z}(f_1, \ldots, f_s)$.

We also note that, in line 1 of Wu's Algorithm, one could have used an extended characteristic set instead of characteristic set and the argument would still hold with appropriate changes.

- One problem with Wu's Algorithm, as presented here, is that it is not complete, and in fact, it is only the first half of the algorithm developed by Wu. Nevertheless, just this portion of the algorithm has found many applications, as one can argue heuristically that the algorithm succeeds in vast majority of the cases [10].

  Wu's Algorithm, as presented here, guarantees that whenever the algorithm claims that a statement is generically true, it is indeed so; however, the converse does not hold. In fact, we may have a conclusion g that vanishes on some open set of the zero set of the premises, but Wu's Algorithm may fail to detect this without further *decomposition* of the characteristic set. We will say more about this in section 7.

- Even the complete Wu's Algorithm has several hard-to-eliminate drawbacks. First it is unable to work with arbitrary fields (not algebraically closed, e.g., $\mathbb{R}$). If propositions about real geometry are investigated in this way, a false proposition will be rejected (because it is false also in the complex field), but sometimes a true theorem (over real closed field) may unfortunately be rejected. For example, consider the hypothesis $x^2 + y^2 = 0$ and the conclusion $y = 0$. This is of course true on $\mathbb{R}^{\not\models}$ but false on $\mathbb{C}^{\not\models}$.

- Lastly, the method is unable to handle inequalities. So geometric propositions involving "*internal*," "*external*," or "*between*" are not in the range of such a prover. In this sense, the so called "Wu geometry" is smaller in scope than the more general "Tarski geometry" which includes all the propositions that can be proved by real quantifier elimination algorithms [21].

However, in spite of many obvious shortcomings, Wu's Algorithm remains a powerful and efficient tool for a large class of geometry statements.

6.1 Complexity of Wu's Algorithm

The techniques of the previous section can be adapted to develop good sequential and parallel procedures for computing the pseudo-remainder of a given polynomial f and hence, efficient implementation of Wu's Algorithm. We state the relevant lemmas and omit their proofs; the easy proofs can be found in [18].

Lemma 6.15 Quantitative Pseudo-Division Lemma.
Consider two polynomials f and $g \in k[x_1, \ldots x_n]$, where k is an arbitrary field, $\deg(f) \leq d$ and $\deg(g) \leq \delta$. If $r = \mathrm{prem}(g, f)$ is the pseudo-remainder of g with respect to f then

$$\deg(r) \leq (d+1)(\delta+1) - 1.$$

Also, the pseudo-remainder r can be computed in sequential time $O((d\delta+1)^{O(n)})$ and parallel time $O(n^2\log^2(d\delta+1))$. ■

Lemma 6.16 Quantitative Generalized Pseudo-Division Lemma.
Consider an ascending set $\mathcal{F} = \langle f_1, \ldots, f_r\rangle \subseteq k[x_1, \ldots, x_n]$ and a polynomial $g \in k[x_1, \ldots x_n]$, where k is an arbitrary field, $\deg(f_i) \le d$, for all $1 \le i \le s$, and $\deg(g) \le \delta$. If $g_0 = \mathrm{prem}(g, \mathcal{F})$ is the generalized pseudo-remainder of g with respect to $\mathcal{F}$ then

$$\deg(g_0) \le (d+1)^r(\delta+1).$$

Also, the generalized pseudo-remainder g_0 can be computed in sequential time $O(\delta^{O(n)}(d+1)^{O(nr)})$ and parallel time $O(n^2r^3\log^2(d\delta+1))$. ■

Combining all of the above results, we have

Theorem 6.17 Complexity of Wu's Algorithm.
Consider a set of premises $F = \{f_1, \ldots, f_s\} \subseteq k[x_1, \ldots, x_n]$ and a conclusion $g \in k[x_1, \ldots x_n]$, where k is an arbitrary field, $\deg(f_i) \le d$, for all $1 \le i \le s$, and $\deg(g) \le d$.

Then the Wu's Algorithm *for geometric theorem proving takes $O(s^{O(n^2)}(d+1)^{O(n^4)})$ sequential time and $O(n^7\log^2(s+d+1))$ parallel time.* ■

As an immediate corollary of the above results, we see that a geometric theorem (involving no inequalities) can be verified in $O(2^{O(C(P+C)^3)})$ sequential time and $O(C^2(P+C)^7)$ parallel time, where it is assumed that the geometric theorem is presented by P points in the plane, and C constructions involving straight lines and circles.

7. Concluding Remarks

Although the concept characteristic set has proven to be quite useful in the realm of geometry, several extensions are necessary to improve its power: one such idea is that of an irreducible characteristic set.

Definition 7.10 Irreducible Characteristic Set. Let $I = (f_1, \ldots, f_s)$ be an l-dimensional ideal in $k[x_1, \ldots, x_n]$. Further assume that the first l variables, $x_1, \ldots, x_l$, are the independent variables, the last $r = (n-l)$ variables, $x_{l+1}, \ldots, x_n$, the dependent variables and the ordering on the variables is the following:

$$x_1 \prec \cdots \prec x_l \prec x_{l+1} \prec \cdots \prec x_n.$$

A characteristic set of I, $\mathcal{G} = \langle g_1, \ldots, g_r\rangle$, is said to be an *irreducible characteristic set* of I, if

$$\begin{aligned}
g_1 &= \text{irreducible over } k_1 = k(x_1, \ldots, x_l)\\
g_2 &= \text{irreducible over } k_2 = QF\Big(k_1[x_{l+1}]/(g_1)\Big)\\
&\vdots\\
g_j &= \text{irreducible over } k_j = QF\Big(k_{j-1}[x_{l+j-1}]/(g_{j-1})\Big)\\
&\vdots\\
g_r &= \text{irreducible over } k_r = QF\Big(k_{r-1}[x_{r-1}]/(g_{r-1})\Big)
\end{aligned}$$

where QF denotes the quotient field of fractions over a domain.

The definition above is constructive, in the sense that the irreducibility of an ascending set can be tested algorithmically, since there are factorization algorithms over a field, and over the successive algebraic extensions of a given field. However, these algorithms have a very high intrinsic time complexity [13].

The significance of the notion of an irreducible characteristic set becomes clear from the following proposition whose proof, using the concept of a *generic point* of an irreducible variety, can be found in [34] or [36].

Proposition 7.18 *Let I be an ideal, and $\mathcal{G}$, a characteristic set of I. Then*

$$\mathcal{G} \text{ is irreducible} \quad \Leftrightarrow \quad I \text{ is prime.}$$

■

The idea of irreducible characteristic set extends the domain of applicability to a larger class of algebraic problems.

1. **Test for Deciding Primality of an Ideal:** This can be achieved by using the characteristic set algorithm together with the test for irreducibility of a univariate polynomial over an arbitrary field. The validity of the algorithm is a simple consequence of the preceding proposition.

2. **Test for Deciding Membership in a Prime Ideal:** Recall that if I = prime and its characteristic set is $\mathcal{G}$, then

   $$g \in I \quad \Leftrightarrow \quad \mathrm{prem}(g, \mathcal{G}) = 0.$$

   Thus membership problem for a prime ideal can be solved by simply computing a characteristic set and then using the pseudo-division algorithm.

3. For a given ideal I, by using the factorization algorithm, one can construct a sequence of *irreducible characteristic sets* $\mathcal{G}_1$, ..., $\mathcal{G}_k$ such that

   $$\mathcal{Z}(I) = \mathcal{Z}(\mathcal{G}_1) \cup \cdots \cup \mathcal{Z}(\mathcal{G}_k).$$

   Thus,

   $$g \in \sqrt{I} \quad \Leftrightarrow \quad (\forall\ i)\ [\mathrm{prem}(g, \mathcal{G}_i) = 0].$$

   This provides a test for checking the membership in the radical of an ideal.

4. Lastly, using above *geometric decomposition*, one can construct a *complete scheme* for geometric theorem proving, where one decides if a formula of the kind

   $$\begin{aligned} \Big(\forall\ p \in k^n\Big) \Bigg[& \Big(f_1(p) = 0 \wedge \cdots \wedge f_s(p) = 0\Big) \wedge \\ & \neg\Big(\mathrm{in}(g_1)(p) = 0 \vee \cdots \vee \mathrm{in}(g_r)(p) = 0\Big) \\ \Rightarrow \qquad & g(p) = 0 \Bigg], \end{aligned}$$

is “generically true.”

References

[1] Alfred V. Aho, John E. Hopcroft, and Jeffery D. Ullman. *The Design and Analysis of Computer Algorithms*. Addison-Wesley Publishing Company, Reading, Massachusetts, 1974.

[2] D. Bayer and M. Stillman. A Criterion for Detecting m-Regularity. *Inventiones Mathematicae*, 87:1–11, 1987.

[3] D. Bayer and M. Stillman. On the Complexity of Computing Syzygies. *Journal of Symbolic Computation*, 6:135–147, 1988.

[4] David Bayer. *The Division Algorithm and the Hilbert Scheme*. PhD thesis, Harvard University, 1982.

[5] Stuart J. Berkowitz. On Computing the Determinant in Small Parallel Time using a Small Number of Processors. *Information Processing Letters*, 18:147–150, 1984.

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

[7] B. Buchberger. *Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory*. Recent Trends in Multidimensional System Theory. Reidel, 1985. (Ed. Bose).

[8] G. Carrá and G. Gallo. A Procedure to Prove Geometrical Statements. In *Lecture Notes in Computer Science*, volume 365, pages 141–150, 1986.

[9] S.C. Chou. *Proving and Discovering Theorems in Elementary Geometries Using Wu's Method*. PhD thesis, Department of Mathematics, University of Texas at Austin, 1985.

[10] Shang-Ching Chou. *Mechanical Geometry Theorem Proving*. D. Reidel Publishing Company, Kluwer Academic Publishers Group, Dordrecht, Boston, 1988.

[11] 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.

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

[13] J.H. Davenport, Y. Siret, and E. Tournier. *Computer Algebra*. Academic Press, 1988.

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

[15] T. Dubé, B. Mishra, and C. K. Yap. Complexity of Buchberger's algorithm for Gröbner bases. Extended Abstract, 1986.

[16] Thomas William Dubé. *Quantitative Analysis Problems in Computer Algebra: Gröbner Bases and the Nullstellensatz*. PhD thesis, Courant Institute of Mathematical Sciences, New York University, January 1989.

[17] G. Gallo. La Dimostrazione Automatica in Geometria e Questioni di Complessita' Correlate. Tesi di Dottorato. Catania, 1989.

[18] G. Gallo and B. Mishra. Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets. In *Proceedings of MEGA 90: Meeting on Effective Methods in Algebraic Geometry*, Castiglioncello, Livorno, Italy, April 1990.

[19] M. Giusti. *Some Effectivity Problems in Polynomial Ideal Theory*, pages 159–171. Lecture Notes in Computer Science, 174. Springer-Verlag, 1984.

[20] J. Heintz. Definability and Fast Quantifier Elimination over Algebraically Closed Fields. *Theoretical Computer Science*, 24:239–277, 1983.

[21] J. Heintz, T. Recio, and M.-F. Roy. *Algorithms in Real Algebraic Geometry and Applications to Computational Geometry*. 1991. *in the same volume*.

[22] Jiawei Hong. Proving by Example and Gap Theorem. In *27th Annual Symposium on Foundations of Computer Science*, pages 107–116. IEEE Computer Society Press, 1986.

[23] D.T. Huynh. A Superexponential Lower Bound for Gröbner Bases and Church-Rosser Commutative Thue Systems. *Information and Control*, 86:196–206, 1986.

[24] D. Kapur. Geometry Theorem Proving using Gröbner Bases. *Journal of Symbolic Computation*, 2:399–412, 1986.

[25] E.R. Kolchin. *Differential Algebra and Algebraic Groups*. Academic Press, New York, 1973.

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

[27] B. Kutzler and S. Stifter. Automated Geometry Theorem Proving Using Buchberger's Algorithm. In *Proceedings of the 1986 Symposium on Symbolic and Algebraic Computation*, pages 209–214, 1986.

[28] D. Lazard. *Gröbner Bases, Gaussian Elimination and Resolution of Systems of Algebraic Equations*, pages 146–157. Lecture Notes in Computer Science, 162. Springer-Verlag, 1983.

[29] E.W. Mayr and A.R. Meyer. The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals. *Advances in Mathematics*, 46:305–329, 1982.

[30] Bhubaneswar Mishra. Algorithmic algebra. (Accepted for publication by Springer-Verlag in the Texts and Monographs in Computer Science Series.), 1989.

[31] Bud Mishra and Chee Yap. Notes on Gröbner Bases. *Information Sciences*, 48:219–252, 1989.

[32] H.M. Möller and F. Mora. *Upper and Lower Bounds for the Degree of Gröbner Bases*, pages 172–183. Lecture Notes in Computer Science, 174. Springer-Verlag, 1984.

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

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

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

[36] 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.

[37] 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.

[38] Chee-keng Yap. A Double-Exponential Lower Bound for Degree-Compatible Gröbner Bases. Report 181, NYU-Courant Robotics Laboratory, 1988.