Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets [1]

Giovanni Gallo *and* **Bhubaneswar Mishra**

Courant Institute of Mathematical Sciences
New York University
New York, N.Y.10012

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 present optimal algorithms for computing a characteristic set with simple-exponential sequential and polynomial parallel time complexities. These algorithms are derived, via linear algebra, from simple-exponential degree bounds for a characteristic set. The degree bounds are obtained by using the recent effective version of Hilbert's Nullstellensatz, due to D. Brownawell and J. Kollár, and a version of Bezout's Inequality, due to J. Heintz.

1. Introduction

In the late forties, J.F. Ritt, in his now classic book *Differential Algebra* [28], introduced an effective process to construct a triangular set of equations from a set of differential equations, with various interesting properties. The techniques of Ritt, when specialized to commutative algebra, have provided various interesting tools in Symbolic Computational Algebra. Recently, such triangular sets, derived from a set of polynomial equations, were independently rediscovered by Wu Wen-Tsün [30, 29, 31] in China, and have found applications in Mechanical Theorem Provers, e.g. *China Prover*. These triangular sets have come to be known as *Wu-Ritt Characteristic Sets* of the ideal generated by the given polynomials [9, 15, 19, 28]. With its increasing popularity, characteristic sets have begun to receive closer scrutiny, especially in its power in solving algebraic problems symbolically.

The original Wu-Ritt Process, first devised by Ritt, and subsequently modified by Wu, has a non-elementary worst-case time complexity, and could be used for computing only an extended characteristic set. To the best of our knowledge, even the constructivity of the more powerful characteristic set had not been explicitly demonstrated.

[1] Supported by NSF Grant #DMS-87-03458, ONR Grant #N00014-89-J3042 and Italian Government Graduate Fellowship.

On the other hand, considerable amounts of experimental data are available, comparing the time-complexity of various implementations of Wu-Ritt Process with Gröbner Bases algorithms [7, 9, 8, 21, 24, 25]. While the worst-case complexity of Gröbner Bases algorithms are fairly well-understood at this point [2, 3, 4, 13, 14, 16, 18, 22, 23, 26, 32], the computational complexity of Wu-Ritt Characteristic Sets has remained open.

In this paper, we resolve the complexity question for Wu-Ritt characteristic sets, as follows:

- We show that the the degrees of the polynomials in a characteristic set of an ideal I in $k[x_1, \ldots, x_n]$ (where k is an arbitrary field) is bounded from both above and below, by a simple exponential function of n. More precisely, if d bounds the total degrees of the generators of a zero-dimensional ideal $I \subseteq k[x_1, \ldots, x_n]$, then we give a lower bound of $\Omega(d^n)$ and an upper bound of $O(d^{O(n)})$, for the degrees of polynomials in a characteristic set of I with respect to arbitrary ordering of the indeterminates. For non-zero-dimensional ideals, the corresponding lower and upper bounds are, respectively, $\Omega(d^{(n-\dim I)})$ and $O(sd^{O((n-\dim I)^2)})$, where s is the number of given generators of the ideal; in this case, the characteristic sets are assumed to be with respect to certain special orderings of the indeterminates.

- Using these bounds and via linear algebra, we derive several efficient parallel and sequential algorithms to compute characteristic sets. The most general classes of our algorithms have $O(s^{O(n)} d^{O(n^3)})$ sequential and $O(n^7 \log^2(s+d))$ parallel complexity. In particular, if the number of variables n is assumed to be a constant, our algorithm is in NC_2.

- Lastly, we present degree bounds and algorithms for the process of *generalized pseudo-division*, which plays a crucial role in Wu's China Prover. We give an $O(d^{O(n)})$ degree bound for g_0, the *generalized pseudo-remainder* of a polynomial g with respect to an ordered sequence of polynomials $\langle f_1, \ldots, f_r \rangle$, (the sequence of f_i's satisfy certain technical conditions), where all the polynomials have their degrees bounded by d.

- 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.

Also, these results may be of independent interest to the algebraists, as it explores the power of the techniques based on some recent results of Brownawell and Kollár on the *Effective Hilbert's Nullstellensatz* [6, 20].

The paper is organized as follows: In section 2, we provide a quick introduction to the concepts, relevant to characteristic sets, extended characteristic sets and Wu-Ritt Process. In section 3, we derive the degree bounds for characteristic sets. In this section, we also prove a single-exponential lower bound for the degree of an extended characteristic set. In section 4, we present efficient sequential and parallel algorithms for computing a characteristic set of an ideal. In section 5, we present quantitative versions of pseudo-division lemmas, with algorithms for computing the pseudo-remainders. We conclude the paper, with some discussion of the open problems.

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; 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 $1 \le j \le n$, *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* [2] *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*:

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

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*, $f_1 \sim f_2$. $\Box$

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

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

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). $\Box$

[2] Our definition of *degree* is somewhat nonstandard; however, it makes the subsequent discussion considerably simpler.

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 $g = \mathrm{prem}(g, f)$.* $\square$

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 $(n - r)$. $\square$

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

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

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*, $\mathcal{F} \sim \mathcal{G}$. $\square$

Hence,

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

Thus the map, *type*, is a partially ordered homomorphism from the family of ascending sets to $(\mathbf{N} \cup \{\infty\})^{n+1}$, where $(\mathbf{N} \cup \{\infty\})^{n+1}$ 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 component is in I,

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

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. □

It can be easily shown that if $\mathcal{G}$ is a characteristic set of I then

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

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.

Lemma 2.2 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,*

$$(\exists!\ q_i')\ (\exists!\ \alpha_i)\ \Big[\operatorname{in}(f_i)^{\alpha_i} g_i = q_i' f_i + g_{i-1}\Big]$$

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

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

*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 $\mathcal{F}$, $g_0 = \operatorname{prem}(g, \mathcal{F})$. *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 $g = \operatorname{prem}(g, \mathcal{F})$.* □

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

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

Proposition 2.3 *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*

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

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

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

Proposition 2.4 *Let I be an ideal in $k[x_1, \ldots, x_n]$ with a characteristic set $\mathcal{G} = \langle g_1, \ldots, g_r \rangle$. Then*

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

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

Lemma 2.5 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*

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

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

```
Wu-Ritt Process:
Input:     F = {f1, ..., fs} ⊆ k[x1, ..., xn].
Output:    G, an extended characteristic set of F.

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};
        end{loop };
        for all f ∈ F \ G loop
                if r := prem(f, G) ≠ 0 then
                        R := R ∪ {r};
                end{if };
        end{loop };
until R = ∅;
return G;
end{Wu-Ritt Process}.  □
```

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.

Proposition 2.6 *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*

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

We conclude this section, with the following technical lemma:

Lemma 2.7 *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:*

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

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:

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

PROOF.[3]

First, note that $\mathcal{H}$ is an extended characteristic set of H (with respect to the ordering $x_1 \prec x_2 \prec \cdots \prec x_n$); this is easily seen by an application of the WU-RITT PROCESS to the set H. Thus

$$H \subseteq \mathcal{M}(\mathcal{H}).$$

We claim that the set $\mathcal{M}(\mathcal{H})$ is an ideal. Thus

$$(H) \subseteq \Big(\mathcal{M}(\mathcal{H})\Big) = \mathcal{M}(\mathcal{H}),$$

and $\mathcal{H}$ is a characteristic set of (H), since $\Big(\forall\, f \in (H)\Big)$ $\mathrm{prem}(f, \mathcal{H}) = 0$.

In order to prove the claim, we make the following simple observations:

1. Since $\mathrm{in}(h_j) = 1$, for all $1 \le j \le n$,

$$\Big[\mathrm{prem}(g', \mathcal{H}) = g_0' \;\wedge\; \mathrm{prem}(g'', \mathcal{H}) = g_0''\Big] \;\Rightarrow\; \begin{array}{l} (A)\ \mathrm{prem}(g' + g'', \mathcal{H}) = g_0' + g_0'' \\ (B)\ \mathrm{prem}(cg', \mathcal{H}) = cg_0', \quad \Big(\forall\, c \in k\Big). \end{array}$$

2. Since $h_j \in k[x_j] \setminus k$, for all $1 \le j \le n$,

$$\Big[\mathrm{prem}(g', \mathcal{H}) = 0\Big] \;\Rightarrow\; \mathrm{prem}(x_i g', \mathcal{H}) = 0, \quad \Big(\forall\, x_i\Big).$$

[3] 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

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

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

Assume that $h_i = x_i^d + c_{d-1}x_i^{d-1} + \cdots + c_0$, and let the following sequence

$$g'_0(=0), g'_1, \ldots, g'_{i-1}, \ldots, g'_n(=g')$$

denote the sequence of pseudo-remainders, obtained by dividing g' by $\mathcal{H}$. If $\deg_{x_i} g'_{i-1} < (d-1)$ then, clearly

$$\mathrm{prem}(x_i g', \mathcal{H}) = \mathrm{prem}\Big(x_i g', \langle h_{i-1}, \ldots, h_1\rangle\Big) = 0.$$

Otherwise, $\deg_{x_i} g'_{i-1} = (d-1)$, and

$$\begin{aligned} x_i g'_{i-1} &= \alpha_d(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)x_i^d \\ &\quad + \alpha_{d-1}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)x_i^{d-1} + \cdots \\ &\quad + \alpha_1(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)x_i, \end{aligned}$$

where $\mathrm{prem}(\alpha_k, \langle h_{i-1}, \ldots, h_1\rangle) = 0$. But

$$\mathrm{prem}(x_i g'_{i-1}, h_i) = (\alpha_{d-1} - c_{d-1}\alpha_d)x_i^{d-1} + \cdots + (\alpha_1 - c_1\alpha_d)x_i - c_0\alpha_d,$$

and, by (1), $\mathrm{prem}((\alpha_k - c_k\alpha_d), \langle h_{i-1}, \ldots, h_1\rangle) = 0$.
Hence

$$\mathrm{prem}(x_i g', \mathcal{H}) = \mathrm{prem}\Big(\mathrm{prem}(x_i g'_{i-1}, h_i), \langle h_{i-1}, \ldots, h_1\rangle\Big) = 0.$$

Thus if g', $g'' \in \mathcal{M}(\mathcal{H})$ and $f \in k[x_1, \ldots, x_n]$ then, by observation (1A), $g' + g'' \in \mathcal{M}(\mathcal{H})$ and, by observations (1) and (2), $fg' \in \mathcal{M}(\mathcal{H})$. $\square$

3. Degree Bounds

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:

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

Let $\mathcal{G} = \langle g_1, \ldots, g_r\rangle$ be a characteristic set of the ideal, and let $D = \max\{\deg(g_i) : 1 \le i \le r\}$ 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.

3.1 Lower Bounds

Theorem 3.8 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, $\quad D \geq \operatorname{cdeg}(g_1) = \min\Big\{\deg(f) : f \in I \cap (k[x_i] \setminus k)\Big\} = d^n.$

(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 2.6,

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

Hence

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

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

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 3.8 is given by,

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

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 3.8.

We note that the ideal I of theorem 3.8 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.

3.2 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 [20].

Theorem 3.9 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 $\deg(b_i f_i) \leq 2(\delta+1)(d+1)^n, 1 \leq i \leq s$. $\square$

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.

3.2.1 Zero-Dimensional Case

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 3.10 *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 [17], 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 $j^{\rm th}$ coordinate of the $i^{\rm th}$ 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 3.9, 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 3.9,

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

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, $h_j \in k[x_j]$. $\square$

Corollary 3.11 *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 3.10) as rewriting rules modulo $J = (h_1, \ldots, h_n) \subseteq I$, g may be expressed as follows:

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

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

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

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

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 $\deg(a_i f_i) \leq \max_{1 \leq i \leq s} \left\{ \deg(a_i'' f_i), \deg(a_i' f_i) \right\} \leq \max\{d, \Delta\} + 6n(d+1)^{2n}$. $\square$

Theorem 3.12 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. $\mathrm{class}(g_j) = j$.
2. $\deg(g_j) \leq 2n(d+1)^{2n}$.
3. $$\left(\exists\, a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n]\right) \left[g_j = \sum_{i=1}^{s} a_{j,i} f_i, \right],$$

   and $\deg(a_{j,i} f_i) \leq 8n(d+1)^{2n}, 1 \leq i \leq s$.

PROOF.
Note that $\mathcal{H} = \langle h_1, \ldots, h_n \rangle$ of lemma 3.10, is an ascending set in $\mathbf{S}_I$. The conditions (1) and (2) follows from the facts that, for all $1 \leq j \leq n$,
1. $\mathrm{class}(g_j) = \mathrm{class}(h_j) = j$, and $\mathrm{cdeg}(g_j) \leq \mathrm{cdeg}(h_j) \leq \deg(h_j) \leq 2(d+1)^{2n}$.
2. For all $1 \leq i < j$, $\deg_{x_i}(g_j) < \deg_{x_i}(g_i)$, as g_j is reduced with respect to the preceding g_i's. Thus

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

Since each g_j is in I, the condition (3) is an immediate consequence of the corollary 3.11. $\square$

3.2.2 General Cases

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, $\deg(f_i) \leq d$. Assume that the indeterminates, $x_{\pi(1)} = u_1, \ldots, x_{\pi(l)} = u_l$, are the *independent* variables with respect to I. 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

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

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

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

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 $\le 8r(d+1)^{2r}$, 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 $\le \Gamma$ and with entries of degree $\le d$ 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 3.13 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. $\mathrm{class}(g_j) = j + l$.
2. $\deg(g_j) \leq 4(s+1)(9r)^{2r} d(d+1)^{4r^2}$.
3. $$\left(\exists\, a_{j,1}, \ldots, a_{j,s} \in k[x_1, \ldots, x_n]\right) \left[g_j = \sum_{i=1}^{s} a_{j,i} f_i,\right],$$

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

PROOF.
As before, let us assume that the independent variables with respect to I are $u_1 = x_1, \ldots,$ 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, $\mathrm{class}(g_j) = j + l$. The rest involves some simple calculations. $\square$

4. Algorithms

In this section, we show how one can 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 shall use, 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 $O(N^{2.376})$ [10, 1] and that the parallel algorithms have time complexity $O(\log^2 N)$, (and polynomial size) [11, 5, 27]. Our complexity model assumes a $O(1)$-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 $(n-l)$ 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. [12].

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 3.13, 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

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

and $\deg(g_j), \deg(a_{j,i} f_i) \leq 11(s+1)(9r)^{2r} d(d+1)^{4r^2}, \quad 1 \leq i \leq s.$
Thus g_j satisfying all the properties can be determined by solving an appropriate system of linear equations.

Let $M_1, M_2, \ldots, M_\rho$ be an enumeration of all the power products in $x_1, \ldots, x_n$ (called, $\text{PP}(x_1, \ldots, x_n)$) of degree less than $11(s+1)(9r)^{2r} d(d+1)^{4r^2}$; thus ρ satisfies the following bound,

$$\rho = \binom{11(s+1)(9r)^{2r} d(d+1)^{4r^2} + n}{n} = O\left(s^{O(n)} (d+1)^{O(n^3)}\right).$$

The enumeration on the power products is assumed to be so chosen that the indices $\lambda < \mu$, *only if* one of the following three conditions is satisfied:

1. $M_\lambda \in \text{PP}(x_1, \ldots, x_{l+j})$ and $M_\mu \in \text{PP}(x_1, \ldots, x_n) \setminus \text{PP}(x_1, \ldots, x_{l+j})$.
2. $M_\lambda, M_\mu \in \text{PP}(x_1, \ldots, x_{l+j})$ and

$$(\forall\, l < i < l+j) \left[\deg_{x_i}(M_\lambda) < d_i\right] \quad \text{and} \quad (\exists\, l < i < l+j) \left[\deg_{x_i}(M_\mu) \geq d_i\right].$$

3. $M_\lambda, M_\mu \in \text{PP}(x_1, \ldots, x_{l+j})$,

$$(\forall\, l < i < l+j) \left[\deg_{x_i}(M_\lambda), \deg_{x_i}(M_\mu) < d_i\right],$$

and $\deg_{x_{l+j}}(M_\lambda) < \deg_{x_{l+j}}(M_\mu)$.

Let us express $a_{i,j}$ and g_j symbolically as follows:

$$\begin{aligned} a_{i,j} &= \sum_{\lambda=1}^{\rho} \alpha_{(i-1)+\lambda} M_\lambda, \quad 1 \le i \le s, \\ g_j &= \sum_{\mu=1}^{\rho} \beta_\mu M_\mu. \end{aligned}$$

By equating the the terms of the same monomials on both sides of the equation 6, we get at most

$$\binom{d+l+j}{l+j} \cdot \rho \le (d+1)^n \rho$$

equations, in $(s+1)\rho$ unknowns, α's and β's. We represent the homogeneous system as follows:

$$\left[A_1 \cdots A_{s\rho} \vdots B_1 \cdots B_\rho \right] \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_{s\rho} \\ \cdots \\ \beta_1 \\ \vdots \\ \beta_\rho \end{bmatrix} = \mathbf{0}.$$

Any solution of this system that minimizes the index of the last nonzero entry of the β's will correspond to the desired g_j. The existence of a solution of the desired nature follows from the theorem 3.13, and the rest follows simply from the choice of the ordering on the power products.

Let $\lambda_1 (= 1)$, λ_2, …, λ_l and m, be a sequence of indices such that, for $1 \le i < l$,

$$\begin{aligned} 0 &< \operatorname{rank}\left[A_1 \cdots A_{\lambda_i} \right] = \operatorname{rank}\left[A_1 \cdots A_{\lambda_i + 1} \right] = \cdots = \operatorname{rank}\left[A_1 \cdots A_{\lambda_{i+1} - 1} \right] \\ &< \operatorname{rank}\left[A_1 \cdots A_{\lambda_{i+1}} \right], \end{aligned}$$

and

$$\begin{aligned} \operatorname{rank}\left[A_1 \cdots A_{s\rho} \right] &< \operatorname{rank}\left[A_1 \cdots A_{s\rho} \vdots B_1 \right] < \cdots < \operatorname{rank}\left[A_1 \cdots A_{s\rho} \vdots B_1 \cdots B_{m-1} \right] \\ &= \operatorname{rank}\left[A_1 \cdots A_{s\rho} B_1 \cdots B_m \right]. \end{aligned}$$

Then, we know that in the desired solution all the α's and β's, not including α_{λ_1}, …, α_{λ_l} and β_1, …, β_m, must be zero. Thus, we need to solve the following system of linear equations

$$\left[A_{\lambda_1} \cdots A_{\lambda_l} \vdots B_1 \cdots B_{m-1} \right] \begin{bmatrix} \alpha_{\lambda_1} \\ \vdots \\ \alpha_{\lambda_l} \\ \cdots \\ \beta_1 \\ \vdots \\ \beta_{m-1} \end{bmatrix} = B_m.$$

Again by a sequence of rank computations (while adding one row at a time), all but $(l+m-1)$ rows can be eliminated, to yield a square matrix in the left. This system can be solved by Cramer's rule, which only requires computations of the appropriate set of determinants. Then g_j is a monic polynomial given by:

$$g_j = M_m - \beta_{m-1} M_{m-1} - \cdots - \beta_1 M_1.$$

If $\Sigma = ((d+1)^n + s + 1)\rho$, then in the computation, we require, $O(\Sigma)$-many rank and determinant computations, each requiring $O(\Sigma^{2.376})$ sequential time and $O(\log^2 \Sigma)$ parallel time. Since Σ is $O(s^{O(n)}(d+1)^{O(n^3)})$, we see that 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 4.14 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 $O(s(d+1)^{O(n^2)})$. $\square$

If the ideal is zero-dimensional, then the arguments in this section can be specialized to yield better bounds.

Theorem 4.15 Complexity of Characteristic Sets of a Zero-Dimensional Ideal.
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 $\deg(f_i) \le d$, $1 \le i \le s$. Then with respect to any ordering on the indeterminates:

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

one can compute a characteristic set of I, in $O(s^{3.376}(d+1)^{O(n^2)})$ sequential time or $O(n^5 \log^2(s+d+1))$ parallel time. The polynomials in the computed characteristic set are of degree $O((d+1)^{O(n)})$. $\square$

5. Generalized Pseudo-Division

The techniques used above can be adapted to develop a parallelizable procedure for computing the pseudo-remainder of a given polynomial f.

Lemma 5.16 Quantitative Pseudo-Division Lemma.
Consider two polynomials f and $g \in k[x_1, \ldots x_n]$, where k is an arbitrary field, $\deg(f) \le d$ and $\deg(g) \le \delta$. If $r = \mathrm{prem}(g, f)$ is the pseudo-remainder of g with respect to f then

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

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

PROOF.

Since r is a pseudo-remainder of g with respect to f then there is a quotient q and a minimal possible integer $\alpha \leq \delta+1$ such that

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

Thus $\deg(\mathrm{in}(f)^\alpha g) \leq (d+1)(\delta+1)-1$, which implies that

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

Now, it is easily seen that r can be determined by solving at most $(\delta+1)$ linear systems, each consisting of at most $(d+1)^n\rho$ equations in 2ρ unknowns, where

$$\rho = \binom{(d+1)(\delta+1)+n}{n} = O\left((d\delta+1)^{O(n)}\right).$$

Thus as before, if $\Sigma = ((d+1)^n+2)\rho$, then this involves at most $O(\Sigma)$-many rank and determinant computations, each requiring $O(\Sigma^{2.376})$ sequential time and $O(\log^2 \Sigma)$ parallel time. Since Σ is $O((d\delta+1)^{O(n)})$, the complexity given in the statement of the lemma is immediate. □

Lemma 5.17 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, $\deg(f_i) \leq d$, for all $1 \leq i \leq s$, and $\deg(g) \leq \delta$. If $g_0 = \mathrm{prem}(g, \mathcal{F})$ is the generalized pseudo-remainder of g with respect to $\mathcal{F}$ then

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

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

PROOF.

Let $g_0, g_1, \ldots, g_r = g$ be the pseudo-remainder sequence of g with respect to $\mathcal{F}$, satisfying the following equation

$$\mathrm{in}(f)^{\alpha_i} g_i = q_i' f_i + g_{i-1},$$

where

$$\begin{aligned} \alpha_i &\leq \deg(g_i)+1 \\ \deg(q_i' f_i), \deg(g_{i-1}) &\leq d\alpha_i + \deg(g_i) \leq (\deg(g_i)+1)(d+1)-1. \end{aligned}$$

Thus, we see that $\deg(g_i)$ satisfies the following recurrence equation

$$\begin{aligned} \deg(g_r)+1 &= \delta+1 \\ \deg(g_{i-1})+1 &\leq (d+1)(\deg(g_i)+1). \end{aligned}$$

Thus, for all $1 \leq i \leq r$, $\deg(g_i) \leq (d+1)^{r-i}(\delta+1)$.

Hence, if we assume that g_{i+1} is available then g_i can be computed in $O(\delta^{O(n)}(d+1)^{O(n(r-i))})$ sequential time, and in $O(n^2(r-i)^2\log^2(d\delta+1))$ parallel time. Thus g_0 can be computed in sequential time $O(\delta^{O(n)}(d+1)^{O(nr)})$ and parallel time $O(n^2 r^3 \log^2(d\delta+1))$. Since $r \leq n$, r may be eliminated in the above bounds to yield a simpler formula. □

6. Conclusion

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.

Acknowledgement

We are grateful to Joos Heintz for introducing us to the results of Dickenstein et. al.[12] and to Pina Carrá, Teo Mora and an anonymous referee for many useful discussions and comments on an earlier draft.

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] 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.

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

[10] 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.

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

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

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

[14] 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.

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

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

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

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

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

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

[21] 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.

[22] 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.

[23] 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.

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

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

[26] 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.

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

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

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

[30] 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.

[31] 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.

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