Characteristic Sets and Zero Structure of Polynomial Sets[†]

DONGMING WANG

Research Institute for Symbolic Computation

Johannes Kepler University, A-4040 Linz, Austria

Laboratoire d'Informatique Fondamentale et d'Intelligence Artificielle

Institut IMAG, 46, avenue Félix Viallet, 38031 Grenoble, France

This paper provides a tutorial on the theory and method of characteristic sets and some relevant topics. The basic algorithms as well as their generalization for computing the characteristic set and characteristic series of a set of multivariate polynomials are presented. The characteristic set, which is of certain triangular form, reflects in general the major part of zeros, and the characteristic series, which is a sequence of polynomial sets of triangular form, furnishes a complete zero decomposition of the given polynomial set. Using this decomposition, a complete solution to the algebraic decision problem and a method for decomposing any algebraic variety into irreducible components are described. Some applications of the method are indicated.

1. Introduction

The concept of characteristic sets was introduced by J. F. Ritt (1932, 1950) in the context of his work on differential algebra. The original goal of Ritt was to study differential equations from an algebraic standpoint. Nevertheless, the method developed in his work has very strong algorithmic features and it is efficient and applicable for many practical problems in present day research. It seems that Ritt's work received little attention until it was revitalized by Wu Wentsün in 1978 when he introduced an algebraic method for mechanical geometry theorem proving. Wu claimed in the preface of his book (Wu, 1984b) that the discovery of his theorem proving method was inspired mainly by Chinese ancient mathematics,[†] in particular, the algebraization of geometry and algorithmic operations and elimination of polynomials. However, Wu recognized that the constructive algebraic tools such as the well-ordering of polynomial sets underlying his method were developed early in Ritt's two books, and he employed these tools later on for the algorithmic design and theoretical completion of his method. Throughout his research, Wu has considerably developed Ritt's work by removing his analytic argumentation like the use of continuity and limit, which makes Ritt's theory and method more accordant with demands of the mechanization of geometry. Wu's method is now known to be efficient for proving non-trivial theorems in many kinds of geometries and its great success has stimulated researchers to pursue various algebraic approaches for geometry problem solving and the renewed interest in the characteristic set method.

There exists some literature on the general method of characteristic sets, but it is quite limited. The applications of this method in diverse problems, which have been recently exploited and reported, appear still far from its real applicability and powerfulness. The treatment of

[†] This paper is part of the lecture notes for two courses given by the author at RISC-Linz in Winter 1989, 1992 and Summer 1994, 1995. The preliminary version was prepared in November 1989 and this revised version in June 1995. Several intermediate versions also exist.

[†] As the author knows, at that time Wu was keenly interested in the history of Chinese mathematics (cf. Wu, 1987a).

characteristic sets in Ritt's books is general for differential polynomials[‡] and not algorithmized enough for the purpose of computer programming. The paper of Wu (1984a), which was organized for presenting his method of geometry theorem proving, contains a comprehensive composition of the method in considering only ordinary polynomials which is conceptually simple and sufficient for many interesting applications. A more detailed introduction of the method to geometry theorem proving is also given in Chou (1988). The purpose of this paper is to provide an easy-to-read version of the method by algorithmization and illustrative examples. We shall present the basic algorithms as well as their generalization for computing the characteristic set and characteristic series of a set of multivariate polynomials. The characteristic set, which is of certain triangular form, reflects in general the major part of zeros, and the characteristic series, which is a sequence of polynomial sets of triangular form, furnishes a complete zero decomposition of the given polynomial set. Using these two concepts, we can completely solve the algebraic decision problem and decompose any algebraic variety into irreducible components.

In detail the remaining part of this paper is structured as follows. In the next section we give a few comments on elimination methods and consider first the simple case of triangulating a set of liner equations. It is noted that the well known Gauss elimination method appeared also in Chinese literature in the first century which is much earlier than that proposed by Gauss in 1826. Section 3 deals essentially with the notations and definitions which will be used throughout the paper. The rank of polynomials and ascending sets as well as the basic reduction — successive pseudo-division — of polynomials with respect to an ascending set are all introduced in this section. In Section 4 we shall present the main algorithm (well-ordering principle) which demonstrates how to triangulate a finite set of polynomials, i.e., how to compute the characteristic set of such a polynomial set. The algorithms for computing the (irreducible) characteristic series of any polynomial set are described in Section 5, from which the complete zero decomposition (namely, the explicit formulae of zero structure of polynomial sets) is then established. A generalization of the characteristic set algorithm is proposed in Section 6 by introducing the notion of medial sets, which leads to several variants of the standard algorithm. The extended characteristic series algorithms are also described in this section. Section 7 devotes to a complete solution to the algebraic decision problem, i.e., the radical ideal membership problem, by computing characteristic sets. Two algorithms are given, of which one is based on the division principle and has proved very efficient in practice. Using the complete zero decomposition and a method for computing the finite basis of an ideal from its characteristic set, the irreducible decomposition of an algebraic variety can be achieved immediately, which is presented in Section 8. In Section 9 we briefly indicate various applications of the method which have been reported. Some information about implementations of the method and complexity results are finally given.

The author must say that the writing of this paper depends heavily upon the work of Ritt and, particularly, that of Wu. The author not only frequently uses the materials available in Wu's publications but also borrows many ideas and viewpoints from his lectures and conversations.

2. Comments on Elimination Methods

In the West elimination theory has been developed since the 18th century. It appears that the earliest elimination methods are due to Euler and Bézout while the best known ones are the elimination method of Gauss for systems of linear equations and the dialytic method of Sylvester for general systems of polynomial equations (see Gauss, 1873 and Sylvester, 1904). The former has been widely used in many different areas, and the latter started at studying algebraic invariants and was further developed as resultant theory through the British school of mathematicians: Cayley, Macaulay, Hodge, Pedoe and others. It is of interest in noting that the method of triangulating a system of linear equations, associated with the name of Gauss, was also described in the ancient Chinese book *Jiu Zhang Suan Shu* (Nine Chapters on Mathematical Art, abbreviated as *Jiu Zhang* hereafter) which appeared early in the first century and was

‡ The reader may also refer to Wu (1989d), in particular, for the case of partial differential polynomials.

commentated by *Liu Hui* in 260 AD. The following example, extracted from the eighth chapter (*Fang Cheng Shu*, the way of calculating by tabulation), is one of the 246 problems included in the book,† see Needham (1959) and Boyer (1968).

Example 2.1
Solve the following system of simultaneous linear equations

$$\begin{aligned}3x + 2y + z &= 39,\\ 2x + 3y + z &= 34,\\ x + 2y + 3z &= 26.\end{aligned}$$

The method given in *Jiu Zhang* proceeds by first placing the quantities, i.e., the coefficients and constant terms, in a matrix form as follows

$$A: \qquad \begin{array}{ccc} 1 & 2 & 3\\ 2 & 3 & 2\\ 3 & 1 & 1\\ 26 & 34 & 39\end{array}$$

and then reducing the matrix A with column operations to another matrix

$$B: \qquad \begin{array}{ccc} 0 & 0 & 3\\ 0 & 5 & 2\\ 36 & 1 & 1\\ 99 & 24 & 39\end{array}.$$

The form B represents the equations $36z = 99,\ 5y + z = 24$, and $3x + 2y + z = 39$, from which the values of $z,\ y$, and x are successively found with ease. ■

Of course, in the original Chinese book there were no symbols like $x,\ y$ and z, but with the corresponding Chinese ones. *Fang Cheng Shu* demonstrated by 18 problems deals with simultaneous linear equations, using both positive and negative numbers. The last problem, involving four equations and five unknowns, foreshadows indeterminate equations. From the illustration we may see that the method described in *Jiu Zhang* has the same algorithmic procedure as that proposed by Gauss in 1826. In view of this fact and that the authors of *Jiu Zhang* are unknown, we shall call this method *China-Gauss elimination*. In fact, the method has already been called *Chinese matrix method* by historians (see Boyer, 1968).

Leaving aside the above historical arguments, let us consider a general system of linear equations in n indeterminates $x_1, \ldots, x_n$ as follows

$$\begin{aligned}&a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = a_{10},\\ &a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = a_{20},\\ &\quad\cdots\cdots\\ &a_{s1}x_1 + a_{s2}x_2 + \cdots + a_{sn}x_n = a_{s0},\end{aligned} \tag{2.1}$$

where a_{ij} are all elements in a fixed basic field (e.g., the rational number field $\boldsymbol{Q}$). An equation is said to be *contradictory* if it is not an identity and contains none of the variables $x_1, \ldots, x_n$. The China-Gauss elimination permits to get from (2.1) either a contradictory equation or a system of linear equations of triangular form, proceeding as follows.

Let p_r be the biggest integer such that not all $a_{ip_r}, i = 1, \ldots, s$, are 0, and suppose, without loss of generality, $a_{sp_r} \not\equiv 0$. For each i, let us multiply the ith equation by a_{sp_r}, the sth equation by a_{ip_r} and take their difference. We then obtain either a contradictory equation, a non-contradictory equation or an identity. If the first case happens for some i, the procedure terminates with some

† The book *Jiu Zhang* was designed by first asking a daily life question and then giving an answer and a method (called *Shu* in Chinese) for deriving the answer.

information. Otherwise, we get, by removing the identities and keeping the last equation of (2.1), a new system of linear equations of the form

$$(2.2)\qquad \begin{aligned} &b_{11}x_1 + b_{12}x_2 + \cdots + b_{1\ p_r-1}x_{p_r-1} = b_{10},\\ &b_{21}x_1 + b_{22}x_2 + \cdots + b_{2\ p_r-1}x_{p_r-1} = b_{20},\\ &\ \cdots\cdots\\ &b_{t1}x_1 + b_{t2}x_2 + \cdots + b_{t\ p_r-1}x_{p_r-1} = b_{t0},\\ &a_{s1}x_1 + a_{s2}x_2 + \cdots + a_{s\ p_r-1}x_{p_r-1} + a_{sp_r}x_{p_r} = a_{s0}, \end{aligned}$$

where b_{ij} are still in the basic field and p_{r-1} is an integer such that not all $b_{ip_{r-1}}, i = 1, \ldots, t$, are 0. Again, suppose $b_{tp_{r-1}} \neq 0$. Then we can form new equations by taking the difference of the ith equation multiplied with $b_{tp_{r-1}}$ and the tth equation multiplied with $b_{ip_{r-1}}$ in (2.2) for $i = 1, \ldots, t-1$. Continuing in this way, the procedure must terminate after a finite number of steps and finally, we obtain either a contradictory equation, or a triangularized set of linear equations of the form

$$(2.3)\qquad \begin{aligned} &c_{11}x_1 + \cdots + c_{1p_1}x_{p_1} = c_{10},\\ &c_{21}x_1 + \cdots + c_{2p_1}x_{p_1} + \cdots + c_{2p_2}x_{p_2} = c_{20},\\ &\ \cdots\cdots\\ &c_{r1}x_1 + \cdots + c_{rp_1}x_{p_1} + \cdots + c_{rp_2}x_{p_2} + \cdots + c_{rp_r}x_{p_r} = c_{r0}, \end{aligned}$$

where all c_{ij} are in the basic field as well and $0 < p_1 < p_2 < \cdots < p_r$.

As a convention, let us denote the coefficient of x_j in a linear equation A_i by the corresponding indexed lowercase letter a_{ij} for each j $(1 \leq j \leq n)$ and the constant term of A_i by a_{i0}. Then the triangulating procedure described above may be written in the following algorithmic form.

ChinaGaussElimination(Input: $(A_1, \ldots, A_s)$; Output: $(C_1, \ldots, C_r)$)

 $t := s$; $r := 1$; $(B_1, \ldots, B_t) := (A_1, \ldots, A_t)$

 while $t > 0$ do

  if $\exists j_0$ such that B_{j_0} is contradictory then stop [*information*]

  choose p, q such that $b_{pq} \neq 0$ and $b_{ij} = 0$ for $1 \leq i \leq t, j > q$

  $C_r := B_p$; $k := 0$

  for j from 1 to t while $j \neq p$ do

   $k := k + 1$

   $B_k := c_{rq}B_j - b_{jq}C_r$

   if B_k is an identity then $k := k - 1$

  $t := k$; $r := r + 1$

 $(C_1, \ldots, C_r) := (C_r, \ldots, C_1)$

If the procedure terminates due to a contradictory equation, then the set of simultaneous linear equations (2.1) has no solution in the basic field. Otherwise, the systems (2.1) and (2.3) have the same set of solutions. The number of solutions is finite if and only if $r = n$. In the case $r < n$, the number of solutions is infinite and the dimension of solution space is $n - r$. Evidently, the above algorithmic procedure works also for the coefficients and constant terms a_{ij} in certain domain. But if, in particular, the coefficients and constant terms a_{ij} are polynomials or other functions, any solution of (2.3) is longer a solution of (2.2) only under the conditions $c_{ip_i} \neq 0$.

The elimination method described above is rather elementary in the sense that it is known even in high school algebra. However, an algorithmic presentation in the general form cannot be easily found in popular books and is provided here as background and motivation for the characteristic set method considered as a generalization.

For the sake of simplicity, we assume from now on that all terms on the right-hand side of the equations are moved to the left-hand side and consider only polynomials instead of equations.

The above China-Gauss method reduces, by successively eliminating the variables, the given set of linear polynomials into a triangular form. We shall call such an elimination *well-ordering*, which has numerous applications in many fields, in particular for solving systems of simultaneous linear equations. However, the method can only deal with linear polynomials. If systems involve polynomials of high degree, it is then inapplicable. As we know, general polynomials occur frequently in various mechanization and algorithmic problems, and algorithms which can triangulate polynomial sets would be useful.

Well-Ordering Problem
Given a finite non-empty set PS of polynomials in n variables $x_1, \ldots, x_n$ with coefficients in some fixed field $\boldsymbol{K}$, find an efficient algorithm which computes, from the given set PS, a set CS of "well-ordered" polynomials and establish the relationships between the set of common zeros of the polynomials in CS and that of the polynomials in PS.

Clearly, any method which provides a solution to this problem is a generalization of the China-Gauss elimination and can be used to solve systems of simultaneous algebraic equations of high degree and problems about the solvability of such systems. The best known such elimination method is the method of resultants as already mentioned. It is worth noting that the exploration of general elimination methods in China is also of long standing. Early in the 13th century, Chinese mathematicians could already solve systems of algebraic equations of high degree in four variables by developing a method called *Si Yuan Shu.* Polynomial manipulation including algorithmic operations and elimination is one of the most important achievements of Chinese ancient mathematics. The methods developed were used not only for the efficient solutions of algebraic equations but also as algebraic tools for systematically solving geometric problems.

To mention other notable elimination methods, we should refer to the characteristic set method introduced by J. F. Ritt (1932, 1950) which has been considerably developed by Wu Wen-tsün (1984a, 1984b) and the Gröbner basis method introduced by B. Buchberger (1965). In this paper we mainly deal with the former and some relevant topics. For the latter, the reader may consult the widely known survey article by Buchberger (1985).

After solving the well-ordering problem, it is of reason to study the relationships of zeros between polynomials and sets of polynomials, namely, to determine whether all zeros of a set of polynomials are those of the other, or simply, whether a given non-zero polynomial vanishes over all zeros of a set of polynomials. This can also be regarded as the membership problem of radical ideals and has a number of applications. Let us formulate the problem as follows.

Algebraic Decision Problem
Given a finite set of polynomials $F_1, \ldots, F_s$ and any other non-zero polynomial G with coefficients in some fixed field $\boldsymbol{K}$, decide whether $G = 0$ is a formal consequence of $F_1 = 0, \ldots, F_s = 0$, i.e., whether any common zero of $F_1, \ldots, F_s$ is a zero of G (over some extension field of $\boldsymbol{K}$).

3. Ascending Sets and Successive Pseudo-Division

From now on we are concerned with notions related to characteristic sets and the general method for triangulating sets of polynomials. Most materials and results presented below originate directly from Ritt (1932, 1950) and Wu (1984a, 1984b).

In what follows, we fix a basic field $\boldsymbol{K}$ of characteristic 0 and a set of n variables

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

with the given order. By a *polynomial* we mean one in the variables $x_1, \ldots, x_n$ with coefficients in $\boldsymbol{K}$, i.e, an element in the ring $\boldsymbol{K}[x_1, \ldots, x_n]$. Any element of $\boldsymbol{K}$ as a polynomial is called a *constant.*

Definition 3.1
For any non-zero polynomial $F(x_1, \ldots, x_n)$, the class of F, denoted by $\mathrm{cls}(F)$, *is defined to be the greatest subscript p such that x_p actually occurs in F if F is not a constant, 0 otherwise. If* $\mathrm{cls}(F) = p > 0$, *then x_p is defined to be the* leading variable *of F, denoted by* $\mathrm{lvar}(F)$, *and the degree of F in x_p is simply called the* degree of F.

Let F be any polynomial and x_i a variable. We denote the degree of F in x_i by $\deg_{x_i}(F)$, and write $\deg(F)$ for $\deg_{x_p}(F)$ when $\mathrm{cls}(F) = p > 0$. The phrase "with respect to" will be abbreviated to "wrt" in the description of algorithms.

Example 3.1
Consider the polynomial

$$F_1 = x_4^2 + x_1 x_4^2 - x_2 x_4 - x_1 x_2 x_4 + x_1 x_2 + 3x_2.$$

Then

$$\mathrm{cls}(F_1) = 4, \quad \deg_{x_2}(F_1) = 1, \quad \deg(F_1) = 2, \quad \mathrm{lvar}(F_1) = x_4. \qquad \blacksquare$$

Definition 3.2
For two non-zero polynomials F and G, we say that F has a lower rank than G or G has a higher rank than F, which is denoted as

$$F \prec G \quad \text{or} \quad G \succ F,$$

if either

(*a*) $\mathrm{cls}(F) < \mathrm{cls}(G)$; *or*
(*b*) $\mathrm{cls}(F) = \mathrm{cls}(G) > 0$, *while* $\deg(F) < \deg(G)$.

In the case neither of F and G is of higher or lower rank than the other, F and G will be said to be of the same rank, *denoted as*

$$F \sim G.$$

Let F be any non-zero polynomial with $\mathrm{cls}(F) = p > 0$ and $\deg(F) = m$. Then F can be written in the form

$$F = f_0 x_p^m + f_1 x_p^{m-1} + \cdots + f_m,$$

in which all $f_i \in \boldsymbol{K}[x_1, \ldots, x_{p-1}]$, containing none of $x_p, x_{p+1}, \ldots, x_n$, for $i = 0, \ldots, m$, with $f_0 \neq 0$ in particular. The leading coefficient f_0 of F as polynomial in x_p will be called the *initial of* F and denoted by $\mathrm{ini}(F)$, which plays a special role in the whole theory. Any other polynomial G with $\deg_{x_p}(G) < \deg(F)$ is said to be *reduced* with respect to F. Obviously the initial of F is of class $< p$ and is already reduced with respect to F. If G is not reduced with respect to F, then G can always be put in the form

$$G = g_0 x_p^M + g_1 x_p^{M-1} + \cdots + g_M,$$

in which

$$g_i \in \boldsymbol{K}[x_1, \ldots, x_{p-1}, x_{p+1}, \ldots, x_n], \quad i = 0, \ldots, M,$$

and

$$g_0 \neq 0, \quad M \geq m.$$

Pseudo-dividing G by F — considered as polynomials in x_p, we have the following division algorithm.

prem(Input: G, F; Output: R)

$R := G$

while $\deg_{x_p}(R) \geq m$ do

$r_0 :=$ the leading coefficient of R wrt x_p

$R := f_0 R - r_0 x_p^{\deg_{x_p}(R)-m} F$

As $\deg_{x_p}(R)$ is strictly decreasing for each iteration, the algorithm terminates clearly. With the output R, one gets an expression of the form

$$f_0^s G = QF + R,$$

where $s \leq M - m$, Q and R are both polynomials with, in the case $R \neq 0$, $\deg_{x_p}(R) < m$ so that R is already reduced with respect to F. Modifying the division algorithm by allowing removal of f_0 as a factor, the integer s may be determined as the smallest to make the above expression possible. Such an s is unique. If G is already reduced with respect to F, we can simply take $s = 0, Q = 0, R = G$ so that the above expression holds true still. In any way, the polynomial R will be called the *pseudo-remainder* (or *remainder* for short) of F with respect to G, denoted by $\mathrm{prem}(F, G)$. The procedure to get the remainder R from G will be called the *reduction* of G with respect to F.

Example 3.2
In addition to F_1 in Example 3.1, we consider the following two polynomials

$$F_2 = x_1 x_4 + x_3 - x_1 x_2,$$
$$F_3 = x_3 x_4 - 2x_2^2 - x_1 x_2 - 1.$$

Then,

$$\mathrm{cls}(F_1) = \mathrm{cls}(F_2) = \mathrm{cls}(F_3) = 4,$$
$$\mathrm{lvar}(F_1) = \mathrm{lvar}(F_2) = \mathrm{lvar}(F_3) = x_4,$$

and

$$\mathrm{ini}(F_1) = x_1 + 1, \quad \mathrm{ini}(F_2) = x_1, \quad \mathrm{ini}(F_3) = x_3.$$

From the definition, we have

$$F_3 \sim F_2, \quad F_2 \prec F_1.$$

Hence, F_2 and F_3 are both reduced with respect to F_1, but F_1 is not reduced with respect to F_2, nor reduced with respect to F_3. Also, none of F_2 and F_3 is reduced with respect to the other. Pseudo-dividing, for instance, F_1 and F_3 by F_2 as polynomials in x_4, we get the following remainder formulae

$$x_1^2 \cdot F_1 = Q_1 F_2 + F_4,$$
$$x_1 \cdot F_3 = Q_2 F_2 + F_5,$$

where

$$Q_1 = x_1^2 x_4 + x_1 x_4 - x_1 x_3 - x_3,$$
$$Q_2 = x_3,$$
$$F_4 = \mathrm{prem}(F_1, F_2) = x_1 x_3^2 + x_3^2 - x_1^2 x_2 x_3 - x_1 x_2 x_3 + x_1^3 x_2 + 3x_1^2 x_2,$$
$$F_5 = \mathrm{prem}(F_3, F_2) = -x_3^2 + x_1 x_2 x_3 - 2x_1 x_2^2 - x_1^2 x_2 - x_1. \quad \blacksquare$$

It should be clear from the preceding section what we mean by a *triangular form*. The following is a precise definition. For the development of theory we have to impose further restrictions in order to define what we call *ascending set*.

Definition 3.3
A finite sequence of polynomials

$$AS \qquad A_1, A_2, \ldots, A_r,$$

is called a quasi-ascending set[†] *or a* triangular form *if either*

(*a*) $r = 1$ *and* $A_1 \neq 0$*; or*

(*b*) $r > 1$ *and* $0 < \mathrm{cls}(A_1) < \mathrm{cls}(A_2) < \cdots < \mathrm{cls}(A_r)$.

A quasi-ascending set AS is called an ascending set *if in the case* $r > 1$*,* A_j *is, moreover, reduced with respect to* A_i *for each pair* $j > i$.

A quasi-ascending set AS is called a weak-ascending set *if in the case* $r > 1$*, the initial of* A_j *is, moreover, reduced with respect to* A_i *for each pair* $j > i$.

A quasi-ascending set, a weak-ascending set or an ascending set, will be said to be contradictory *if* $r = 1$*, and* $A_1 \neq 0$ *with* $\mathrm{cls}(A_1) = 0$*, i.e.,* A_1 *is a non-zero constant.*

Clearly, a non-contradictory quasi-ascending set, and thus weak-ascending set or ascending set, can be written in the form

$$AS \qquad \begin{array}{l} A_1(x_1, \ldots, x_{p_1}), \\ A_2(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}), \\ \quad \cdots\cdots \\ A_r(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}, \ldots, x_{p_r}), \end{array}$$

where $p_i = \mathrm{cls}(A_i)$ and $0 < p_1 < p_2 < \cdots < p_r$.

In the following sections we shall consider merely ascending sets. Most of the notions, definitions and results are also valid for weak-ascending sets and quasi-ascending sets. To make it clear, some remarks will be given at the end of each section.

Consider a second ascending set

$$AS' \qquad A'_1, A'_2, \ldots, A'_{r'}.$$

Definition 3.4
We say that the ascending set AS has a higher rank *than AS′ or AS′ has a* lower rank *than AS, which is denoted as*

$$AS \succ AS' \quad \text{or} \quad AS' \prec AS,$$

if either (*a*) *or* (*b*) *below holds:*

(*a*) *There exists a* $j \leq \min(r, r')$ *such that*

$$A_1 \sim A'_1, \ldots, A_{j-1} \sim A'_{j-1}, \quad \textit{while} \quad A_j \succ A'_j;$$

(*b*) $r' > r$ *and*

$$A_1 \sim A'_1, \ldots, A_r \sim A'_r.$$

† *AS* is also considered as an ordered set $\{A_1, \ldots, A_r\}$.

If neither of the ascending sets AS and AS' is of higher rank than the other, then we say that AS and AS' are of the same rank, denoted as $AS \sim AS'$. In that case we have

$$r = r', \quad \textit{and} \quad A_1 \sim A'_1, \ldots, A_r \sim A'_r.$$

Example 3.3
Polynomials are the same as those in the previous examples. Let $AS_1 = \{F_4, F_2\}$, $AS_2 = \{F_5, F_2\}$ and $AS_3 = \{F_4, F_1\}$. By definition, AS_1, AS_2 and AS_3 are all ascending sets and, AS_1 and AS_2 have the same rank but a lower rank than AS_3, i.e., $AS_1 \sim AS_2 \prec AS_3$. ■

Note that the above $\prec$ is a partial order, i.e., the collection of all ascending sets is partially ordered by the rank. Hence for any set of ascending sets we are free to speak of the notion of *minimal ascending set* if it exists. The following basic lemma is important for the termination of our main algorithm as will be seen later.

Lemma 3.1 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
Let

$$AS_1, AS_2, \ldots, AS_q, \ldots$$

be a sequence of ascending sets AS_q for which the rank never increases, or for any q we have either $AS_{q+1} \prec AS_q$ or $AS_{q+1} \sim AS_q$. Then there is an index q' such that for any $q > q'$ we have

$$AS_q \sim AS_{q'}.$$

In other words, there is a q' such that any AS_q for $q > q'$ is a minimal ascending set of the above sequence.

Proof. For each ascending set AS_q let us denote the first polynomial and the number of polynomials in AS_q by A_q and r_q respectively. Then

$$A_1, A_2, \ldots, A_q, \ldots$$

is a sequence of polynomials for which the rank never increases, or for any q we have either $A_{q+1} \prec A_q$ or $A_{q+1} \sim A_q$. Consequently, for any q we have $\mathrm{cls}(A_{q+1}) \leq \mathrm{cls}(A_q)$ and in the case $\mathrm{cls}(A_{q+1}) = \mathrm{cls}(A_q) > 0$, $\deg(A_{q+1}) \leq \deg(A_q)$. As both class and degree are non-negative integers, there should be an index q_1 such that all A_q are of same rank for $q \geq q_1$.

If there is some $q'_1 \geq q_1$ such that all $r_q = 1$ for any $q \geq q'_1$, then the lemma is clearly true. Otherwise, there should be a $q'_1 \geq q_1$ such that all $r_q \geq 2$ for any $q \geq q'_1$. Denote the second polynomial in such AS_q by $A_q^{(1)}$. Then

$$A_{q'_1}^{(1)}, A_{q'_1+1}^{(1)}, \ldots, A_q^{(1)}, \ldots$$

will be a sequence of polynomials with non-increasing ranks. As before there will be a $q_2 \geq q'_1$ such that all $A_q^{(1)}$ are of the same rank for any $q \geq q_2 \geq q'_1 \geq q_1$.

If all $r_q \leq 2$, then the lemma is proved already. Suppose the contrary. Then there will be a $q'_2 \geq q_2$ such that all $r_q \geq 3$ for any $q \geq q'_2$ and we may take the third polynomials in $A_q^{(2)}$ in such AS_q's to form a sequence of polynomials with non-increasing ranks. As for all q we have $r_q \leq n$, so proceeding in this way we should stop at some r and some q' such that for all $q \geq q'$ we have $r_q = r$ and the r-th polynomials taken from such AS_q will all have the same rank. It follows that all such AS_q's will have the same rank and the lemma is proved. ■

From this lemma we immediately have the following

Corollary 3.1
If in a sequence of ascending sets the ranks are steadily decreasing, then such a sequence can only be composed of a finite number of ascending sets.

Let AS be an ascending set as before and I_i the initial of A_i. Consider an arbitrary polynomial B and set $B = R_r$. With respect to the polynomials in AS starting from A_r to A_1, we can form successively by pseudo-division the remainders $R_{r-1}, \ldots, R_0$ of R_r so that we get ($s_i \geq 0$):

$$\begin{aligned} I_r^{s_r} R_r &= Q_r A_r + R_{r-1}, \\ I_{r-1}^{s_{r-1}} R_{r-1} &= Q_{r-1} A_{r-1} + R_{r-2}, \\ &\cdots\cdots \\ I_1^{s_1} R_1 &= Q_1 A_1 + R_0. \end{aligned}$$

Set $R_0 = R$. Then we obtain an expression of the form

$$I_1^{s_1} \cdots I_r^{s_r} B = Q_1' A_1 + \cdots + Q_r' A_r + R,$$

in which Q_i' are all polynomials. The polynomial R determined from B and the ascending set AS by successive pseudo-division is called the *pseudo-remainder* (or *remainder* for short) of B with respect to AS. The above expression will also be called the *remainder formula*.

From the formation one knows that R is reduced with respect to all polynomials in AS, i.e., $\deg_{x_{p_i}}(R) < \deg(A_i)$ for all i. We call the above procedure of getting R from B and AS the *reduction* of B with respect to AS. Any polynomial which is reduced with respect to all polynomials in an ascending set AS will be briefly said to be *reduced* with respect to AS. Let us state the determination of such a remainder in the form of the following

Lemma 3.2
Given any non-zero polynomial B and a non-contradictory ascending set AS as above, one can get the pseudo-remainder of B with respect to AS by the following algorithm:

```
PseudoRemainder(Input: B, AS; Output: R)
    R := B
    r := the number of polynomials in AS
    for i from r step −1 to 1 do
        A := the ith polynomial in AS
        R := prem(R, A)
```

Example 3.4
Polynomials and the ascending set AS_1 are the same as in Examples 3.2-3.3. One can verify that

$$\begin{aligned} \mathsf{PseudoRemainder}(F_3, \mathit{AS}_1) &= \mathsf{PseudoRemainder}(F_3, \mathit{AS}_1) = 0, \\ F_6 = \mathsf{PseudoRemainder}(F_1, \mathit{AS}_1) &= 2x_1x_2^2 + 2x_1^2x_2^2 - 2x_1^2x_2 + x_1^2 + x_1. \end{aligned}$$ ■

Remark 3.1
The rank between two weak-ascending sets and between two quasi-ascending sets can be similarly defined. Lemmas 3.1, 3.2 and Corollary 3.1 still hold when the corresponding ascending set is replaced by weak-ascending set or quasi-ascending set.

4. Characteristic Sets: Well-Ordering Principle

Consider any finite non-empty set PS of non-zero polynomials. Let Φ be the set of all ascending sets contained in PS. Naturally, Φ is non-empty since each single polynomial forms by itself an ascending set. Any minimal ascending set of Φ is called a *basic set* of PS. Such a basic set evidently exists and can be determined in an algorithmic manner.

Lemma 4.1 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
Let PS be a finite non-empty set of non-zero polynomials. The following algorithm computes a basic set BS of PS.

BasicSet(Input: PS; Output: BS)

$QS := PS$
$BS := \emptyset$
while $QS \neq \emptyset$ do
  $B :=$ an element of QS with lowest rank
  $BS := BS \cup \{B\}$
  if $\mathrm{cls}(B) = 0$ then $QS := \emptyset$ else
    $QS := \{Q \in QS \setminus \{B\} \mid Q$ is reduced wrt $B\}$

Proof. Let B_i be the polynomial adjoined to BS at the ith iteration of the while-loop. Since the classes of the polynomials $B_1, B_2, B_3, \ldots$ are steadily increasing and unlikely to become greater than n, the algorithm must terminate in a finite number of steps. By definition the output polynomial set BS is a basic set of PS. ■

One can see that the basic set of PS is contradictory if and only if PS contains a constant. In that case the algorithm terminates at the first iteration of the while-loop.

Lemma 4.2 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
Let PS be a finite non-empty set of non-zero polynomials with a basic set

$$BS \qquad B_1, B_2, \ldots, B_r,$$

of which $\mathrm{cls}(B_1) > 0$*. If B is a non-zero polynomial reduced with respect to BS, then the set PS' obtained from PS by adjunction of B will have a basic set of rank lower than that of BS.*

Proof. If $\mathrm{cls}(B) = 0$, then B alone forms a basic set of PS' of lower rank than that of BS. Suppose therefore $\mathrm{cls}(B) = p > 0$. As B is already reduced with respect to BS, there should be some $i \geq 1$ and $\leq r$ such that $p \leq \mathrm{cls}(B_i)$, and $p > \mathrm{cls}(B_{i-1})$ when $i > 1$. Moreover, in the case $p = \mathrm{cls}(B_i)$, $\deg_{x_p}(B) < \deg(B_i)$. Hence

$$B_1, B_2, \ldots, B_{i-1}, B$$

will be an ascending set contained in PS' with a rank lower than that of BS. The basic set of PS' has therefore a rank lower than that of BS. ■

Come now to the well-ordering problem of a polynomial set. Let us first review the notion of *zero* of such a set.

Let $\tilde{\boldsymbol{K}}$ be some extension of the basic field $\boldsymbol{K}$. Consider the linear space $\tilde{\boldsymbol{K}}^n$ of dimension n over the field $\tilde{\boldsymbol{K}}$, with a basis corresponding to $x_1, \ldots, x_n$. Let $F = F(x_1, \ldots, x_n)$ be any polynomial and

$$\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n$$

a set of numbers in $\tilde{\boldsymbol{K}}$ which may be considered as the coordinates of a point in the linear space $\tilde{\boldsymbol{K}}^n$.

Definition 4.1
$\bar{x} = (\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ is called a zero of the polynomial F *or alternatively* a solution of the equation $F = 0$ *if $F(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n) = 0$. If the various $\bar{x}_i$ are not numbers of $\boldsymbol{K}$, $\bar{x}$ is called an* extended zero of F *or an* extended solution of $F = 0$. *In order to make the involved field $\tilde{\boldsymbol{K}}$ explicit, it is also called a* $\tilde{\boldsymbol{K}}$-zero of F *or a* $\tilde{\boldsymbol{K}}$-solution of $F = 0$.

Let PS be a finite non-empty set of polynomials and G any other non-zero polynomial. Any common zero of all the polynomials in PS is simply called a *zero of PS*. We use the following notations:

$\mathrm{Zero}(PS) = \{x \mid P(x) = 0, P \in PS\}$ — the totality of zeros of PS,
$\mathrm{Zero}(PS/G) = \{x \mid P(x) = 0, G(x) \neq 0, P \in PS\}$ — the difference set of zeros of PS and G.

If the zeros are specified in a certain field, for instance, $\boldsymbol{K}$ or $\tilde{\boldsymbol{K}}$, the corresponding zero sets are denoted by $\boldsymbol{K}$-Zero(PS), $\boldsymbol{K}$-Zero(PS/G) or $\tilde{\boldsymbol{K}}$-Zero(PS), $\tilde{\boldsymbol{K}}$-Zero(PS/G), respectively. Apparently, $\mathrm{Zero}(PS/G) = \mathrm{Zero}(PS)$ when G is a non-zero constant.

Theorem 4.1 (*Well-Ordering Principle*, Ritt, 1932, 1950, Wu, 1984a, 1984b)
Given a finite non-empty set PS of non-zero polynomials, the algorithm below computes an ascending set, called a characteristic set *of PS, which, when non-contradictory, is of the form*

$$CS \quad \begin{array}{l} C_1(x_1, \ldots, x_{p_1}), \\ C_2(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}), \\ \quad \cdots\cdots \\ C_r(x_1, \ldots, x_{p_1}, \ldots, x_{p_2}, \ldots, x_{p_r}), \end{array}$$

with $I_i = \mathrm{ini}(C_i)$ such that

$$\mathrm{Zero}(CS/J) \subset \mathrm{Zero}(PS) \subset \mathrm{Zero}(CS), \tag{4.1}$$

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/J) \cup \bigcup_{i=1}^{r} \mathrm{Zero}(PS_i), \tag{4.2}$$

where $J = I_1 \cdots I_r$ and $PS_i = PS \cup \{I_i\}$.

```
CharacteristicSet(Input: PS; Output: CS)
    QS := PS
    RS := PS
    while RS ≠ ∅ do
        CS :=BasicSet(QS)
        if CS is contradictory then RS := ∅ else
            RS := {R| R =PseudoRemainder(Q, CS), R ≠ 0, Q ∈ QS \ CS}
            QS := QS ∪ RS
```

Proof. The above algorithm may be sketched as follows

$$\begin{array}{ccccccccccc} PS & = & QS_1 & \subset & QS_2 & \subset & \cdots & \subset & QS_m & & \\ & & \cup & & \cup & & & & \cup & & \\ & & BS_1 & & BS_2 & & \cdots & & BS_m & = & CS \\ & & RS_1 & & RS_2 & & & & RS_m & = & \emptyset \end{array}$$

where

$$RS_i = \{R|\ R = \mathsf{PseudoRemainder}(Q, BS_i), R \neq 0, Q \in QS_i \setminus BS_i\}$$
$$QS_{i+1} = QS_i \cup RS_i$$

for each i.

Termination. To prove the termination, i.e., the while-loop has only a finite number of iterations, we need just to prove the finiteness of m in the sketch. If a certain BS_i is contradictory, then the algorithm terminates obviously. Otherwise, by Lemma 4.2 every BS_{i+1} has a rank lower than that of BS_i. Hence, the basic sets $BS_1, BS_2, \ldots$ have steadily decreasing ranks. Now by Corollary 3.1, such a sequence can have only a finite number of, say m, terms. In other words, let QS_m be the corresponding enlarged polynomial set with BS_m as its basic set in the sketch. Then the remainder of any polynomial in QS_m (but not in BS_m) with respect to BS_m is 0, i.e., $RS_m = \emptyset$ and the algorithm terminates.

Correctness. From the remainder formula we know that the remainder of each polynomial Q in QS_i with respect BS_i, when non-zero, is a linear sum of polynomials in BS_i as well as the polynomial Q itself, with polynomial coefficients. It follows that the set QS_{i+1} has the same set of zeros (extended zeros, or $\tilde{\boldsymbol{K}}$-zeros for any extended field $\tilde{\boldsymbol{K}}$) as the original set QS_i, and thus as PS does for each i.

Let the last basic set BS_m be

$$CS \qquad C_1, C_2, \ldots, C_r,$$

with $I_i = \mathrm{ini}(C_i)$. Since CS is a subset of QS_m, any zero of QS_m and thus any zero of PS is also a zero of CS.

On the other hand, from $RS_m = \emptyset$ we know that for any polynomial G in QS_m, there are non-negative integers $s_i \geq 0$ such that

$$I_1^{s_1} \cdots I_r^{s_r} G = Q_1 C_1 + \cdots + Q_r C_r.$$

It follows that any zero of CS, if not a zero of any of the initials $I_1, \ldots, I_r$, is necessarily also a zero of QS_m and thus a zero of $QS_1 = PS$. The same is clearly true for extended zeros or $\tilde{\boldsymbol{K}}$-zeros for any extension field $\tilde{\boldsymbol{K}}$. Finally, one can see that the zeros of PS which make some I_i vanish are considered additionally as those of PS_i. Hence the last basic set BS_m, namely CS, satisfies the zero relations (4.1) and (4.2) and is a characteristic set as required. This completes the proof of the well-ordering principle. ■

The above procedure for getting the characteristic set CS from PS is called the *well-ordering* of PS. A *characteristic set* above is introduced as an output of the algorithm. One can also give a definition of a characteristic set of PS by requiring it to satisfying certain properties such as the zero relation (4.1) (cf. Definition 6.1). However, such an attempt does not enrich the contents, because characteristic sets so defined are usually not unique unless many conditions are imposed.

Example 4.1
Let all polynomials considered be the same as those given in Examples 3.1-3.4 with $PS = \{F_1, F_2, F_3\}$. Then the sequence of polynomial sets and their basic sets corresponding to those in the proof of Theorem 4.1 are as follows

$$\begin{array}{llllll}
PS = & QS_1 = \{F_1, F_2, F_3\} & \subset & QS_2 = \{F_1, \ldots, F_5\} & \subset & QS_3 = \{F_1, \ldots, F_6\} \\
& \cup & & \cup & & \cup \\
& BS_1 = \{F_2\} & & BS_2 = \{F_4, F_2\} & & BS_3 = \{F_6, F_4, F_2\} = CS \\
& RS_1 = \{F_4, F_5\} & & RS_2 = \{F_6\} & & RS_3 = \emptyset.
\end{array}$$

Hence, the last basic set BS_3 is the characteristic set CS of PS. The three initials of the polynomials in CS are $I_1 = x_1^2 + x_1, I_2 = x_1 + 1, I_3 = x_1$. Clearly, $I_1 \neq 0$ implies that $I_1 \cdot I_2 \cdot I_3 \neq 0$, since I_2 and I_3 are factors of I_1. So only the initial I_1 has to be further considered. Let PS_1 and PS_2 be the enlarged polynomial sets obtained from PS by adjoining x_1+1 and x_1 respectively, i.e., $PS_1 = PS \cup \{x_1+1\}$ and $PS_2 = PS \cup \{x_1\}$. Then we have the following zero relation

$$\text{(4.3)} \qquad \mathrm{Zero}(PS) = \mathrm{Zero}(CS/I_1) \cup \mathrm{Zero}(PS_1) \cup \mathrm{Zero}(PS_2). \qquad \blacksquare$$

Remark 4.1
It is important to remark that, during the computation of characteristic sets, there appear inevitably some superfluous factors of the initials. These factors should be removed in order to control the growth of polynomial size. The appearance of superfluous factors during the computation of polynomial remainder sequence was discovered by G. E. Collins (1967). Such factors appearing in the computation of characteristic sets was studied in Li (1987, 1988). If we denote the removed factors by $F_1, \ldots, F_t$, then the zero relation (4.2) can be modified as

$$\text{(4.4)} \qquad \mathrm{Zero}(PS) = \mathrm{Zero}(CS/J) \cup \bigcup_{i=1}^{r} \mathrm{Zero}(PS_i) \cup \bigcup_{j=1}^{t} \mathrm{Zero}(QS_j),$$

where $J = I_1 \cdots I_r \cdot F_1 \cdots F_t$ and $PS_i = PS \cup \{I_i\}, QS_j = PS \cup \{F_j\}$. The zero relation (4.1) remains true when the corresponding J is modified. Moreover, let $H_1, \ldots, H_q$ be any choice of polynomials such that $H_1 \cdots H_q = 0$ if and only if $J = 0$. Then (4.4) can be replaced by

$$\text{(4.5)} \qquad \mathrm{Zero}(PS) = \mathrm{Zero}(CS/J) \cup \bigcup_{k=1}^{q} \mathrm{Zero}(PS \cup \{H_k\}).$$

Remark 4.2
The inevitable occurrence of initial factors often renders the appearing polynomials too large to be manageable. The incessant trial for removing such factors costs much computing time. It can be observed that in the computation of characteristic sets one expensive process is the formation of pseudo-remainder sequences, for which there are more efficient methods based on subresultant theory. Wu (1991) has incorporated this theory in developing advanced algorithms via the resolution of linear equations.

Remark 4.3
Weak-basic sets and quasi-basic sets can also be defined. The algorithms for computing the weak-basic set and quasi-basic set BS of a polynomial set PS can be obtained from the basic set algorithm in Lemma 4.1 by replacing the last line with $QS := \{Q \in QS \setminus \{B\} | \ \mathrm{cls}(Q) > \mathrm{cls}(B), \mathrm{ini}(Q) \text{ is reduced wrt } B\}$ and $QS := \{Q \in QS \setminus \{B\} | \ \mathrm{cls}(Q) > \mathrm{cls}(B)\}$ respectively. Lemma 4.2 and Theorem 4.1 are still true when basic set is replaced by weak-basic set or quasi-basic set, and the corresponding weak-ascending set or quasi-ascending set CS computed as in Theorem 4.1 is called a *weak-characteristic set* or *quasi-characteristic set* of PS respectively. Let a quasi-ascending set AS be as in Definition 3.3. If in the case $r > 1$, the remainder of the initial of A_j with respect to the quasi-ascending set $\{A_1, \ldots, A_{j-1}\}$ is not equal 0 for each i, then AS is called a *loose ascending set*. It is easy to see that the well-ordering principle is also applicable when ascending set and basic set are replaced by the corresponding loose ascending set and loose basic set (cf. Chou, 1988). We will see that the method in the standard sense is theoretically more complete than that in the other senses.

5. Characteristic Series: Complete Zero Decomposition

Let us take a look at the zero relation (4.2). As the initial of each polynomial in an ascending set is reduced with respect to the ascending set itself, by Lemma 4.2 the basic set of any polynomial set $PS_i \cup CS$ should have its rank lower† than that of CS. Therefore, in proceeding further with each $PS_i \cup CS$ as PS by means of the well-ordering principle (note that $\mathrm{Zero}(PS_i \cup CS) = \mathrm{Zero}(PS_i)$), we may arrive after a finite number of steps at a zero decomposition of the form

$$\mathrm{Zero}(PS) = \bigcup_{i=1}^{e} \mathrm{Zero}(CS_i/J_i), \tag{5.1}$$

in which each CS_i is an ascending set and J_i the product of initials of the polynomials in CS_i. The sequence of ascending sets $CS_1, \ldots, CS_e$ is called a *characteristic series* of PS.

Theorem 5.1 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
The following algorithm computes a characteristic series Ψ of any given polynomial set† PS.

CharacteristicSeries(Input: PS; Output: Ψ)
- $\Phi := \{PS\}$
- $\Psi := \emptyset$
- while $\Phi \neq \emptyset$ do
  - $QS :=$ an element of Φ
  - $\Phi := \Phi \setminus \{QS\}$
  - $CS :=$ CharacteristicSet(QS)
  - if CS is non-contradictory then
    - $\Psi := \Psi \cup \{CS\}$
    - $\Phi := \Phi \cup \{QS \cup CS \cup \{I\} \mid I = \mathrm{ini}(C), C \in CS, \mathrm{cls}(I) > 0\}$

If the output Ψ is empty, it is meant that $\mathrm{Zero}(PS) = \emptyset$, and the same below.

Example 5.1
Let $PS = \{F_1, F_2, F_3\}$ and CS be the characteristic set of PS as in Example 4.1. Then one can easily compute the characteristic set CS_1 of $PS_1 \cup CS$ and CS_2 of $PS_2 \cup CS$ as follows

$$\begin{aligned} CS_1 &= \{x_1 + 1, x_2, x_3^2 - 1, -x_4 + x_3\}, \\ CS_2 &= \{x_1, 2x_2^2 + 1, x_3, -x_4^2 + x_2x_4 - 3x_2\}. \end{aligned}$$

Observe that all initials of the polynomials in CS_1 and CS_2 are constant. Therefore, we obtain a characteristic series $\Psi = \{CS, CS_1, CS_2\}$ of PS which furnishes a zero decomposition of the form

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/I_1) \cup \mathrm{Zero}(CS_1) \cup \mathrm{Zero}(CS_2). \qquad \blacksquare$$

For convenience, let us change the variables as $y_1 = x_{p_1}, \ldots, y_r = x_{p_r}$ and denote all other x's by $u_1, \ldots, u_d$ $(d + r = n)$. Then an ascending set AS can be written in the form

$$\begin{array}{l} A_1(u_1, \ldots, u_d, y_1), \\ A_2(u_1, \ldots, u_d, y_1, y_2), \\ \quad \cdots\cdots \\ A_r(u_1, \ldots, u_d, y_1, y_2, \ldots, y_r). \end{array} \tag{5.2}$$

† Neither the basic set nor the characteristic set of PS_i necessarily has its rank lower than that of CS. However, under some assumption the various characteristic series algorithms described in this and the next section are still guaranteed to terminate when PS_i is used instead of $PS_i \cup CS$ (cf. Wang, 1990a).

† A polynomial set is always understood as a finite non-empty set of non-zero polynomials.

As before, we denote the initial of A_i by $I_i = I_i(u_1, \ldots, u_d, y_1, \ldots, y_{i-1})$ for each i. Let $\boldsymbol{K}_0$ be the transcendental extension field $\boldsymbol{K}(u_1, \ldots, u_d)$ of $\boldsymbol{K}$ got by adjoining $u_1, \ldots, u_d$. We define inductively the *irreducibility* and *generic points* of an ascending set as follows.

Definition 5.1
An ascending set AS as above consisting of a single polynomial (i.e., $r = 1$) is said to be irreducible if A_1 as a polynomial in $\boldsymbol{K}_0[y_1]$ is irreducible. In this case, let η_1 be any extended zero of $A_1 = 0$; then $(u_1, \ldots, u_d, \eta_1)$ is called a generic point of AS.

Suppose the irreducibility and generic points of any ascending set containing less than r polynomials has already been defined.

An ascending set AS as above consisting of r polynomials ($r > 1$) is said to be irreducible if the ascending set formed by the first $r-1$ terms $\{A_1, \ldots, A_{r-1}\}$ is irreducible with a generic point $(u_1, \ldots, u_d, \eta_1, \ldots, \eta_{r-1})$ while the polynomial $\bar{A}_r$ in $\boldsymbol{K}_{r-1}[y_r]$ obtained by substituting $\eta_1, \ldots, \eta_{r-1}$ for $y_1, \ldots, y_{r-1}$ in A_r is irreducible, where $\boldsymbol{K}_{r-1} = \boldsymbol{K}_0(\eta_1, \ldots, \eta_{r-1})$ is the algebraic extension field of $\boldsymbol{K}_0$ got by adjoining $\eta_1, \ldots, \eta_{r-1}$. In this case, let η_r be any extended zero of $\bar{A}_r = 0$; then $(u_1, \ldots, u_d, \eta_1, \ldots, \eta_r)$ is called a generic point of AS.

Evidently, a generic point $(u_1, \ldots, u_d, \eta_1, \ldots, \eta_r)$ of *AS* can be considered as a point of the linear space $\boldsymbol{K}_r^{d+r} = \tilde{\boldsymbol{K}}^n$. we shall call $\tilde{\boldsymbol{K}}$ a *generating field* of *AS*.

Lemma 5.1 (Wu, 1984a, 1984b)
If an ascending set AS is irreducible with a generic point $\bar{\eta} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_r)$, then for a polynomial $F \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ to have remainder 0 with respect to AS, it is necessary and sufficient that $\bar{\eta}$ is an extended zero of F.

Proof. Denote the ascending set formed by the first k polynomials in *AS* by

$$AS_k \qquad\qquad A_1, A_2, \ldots, A_k.$$

Let $\boldsymbol{K}_k$ be the $(d+k)$-dimensional linear space over $\boldsymbol{K}$ with basis $u_1, \ldots, u_d, y_1, \ldots, y_k$. Then AS_k is clearly irreducible, and

$$\bar{\eta}_k = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_k),$$

when considered as a point in $\boldsymbol{K}_k^{d+k}$, is a generic point of AS_k while $\boldsymbol{K}_k$ is a generating field of AS_k.

We shall prove by induction on k the following two assertions:

1_k. $\bar{\eta}_{k-1}$ is not an extended zero of I_k;

2_k. if $R_k \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ is already reduced with respect to AS_k and $\bar{\eta}_k$ is an extended zero of R_k, then R_k is identically 0.

As $I_{k+1} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ is known to be reduced with respect to AS_k and is $\neq 0$, so 1_{k+1} is a consequence of 2_k.

Suppose 2_{k-1} has already been proved. Consider any R_k satisfying the conditions in 2_k. Write R_k as a polynomial in y_k

$$R_k = S_0 y_k^s + S_1 y_k^{s-1} + \cdots + S_s,$$

in which $S_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k-1}]$ with $s < m_k = \deg(A_k)$. Substitute $y_1, \ldots, y_{k-1}$ in S_i by $\eta_1, \ldots, \eta_{k-1}$ with the resulting S_i as $\bar{S}_i \in \boldsymbol{K}_{k-1}$. Set

$$\bar{R}_k = \bar{S}_0 y_k^s + \bar{S}_1 y_k^{s-1} + \cdots + \bar{S}_s \in \boldsymbol{K}_{k-1}[y_k].$$

By hypothesis η_k is an extended zero of $\bar{R}_k$. As $s < m_k$ and η_k is an extended zero of the irreducible $\bar{A}_k$ in $\boldsymbol{K}_{k-1}$, $\bar{R}_k$ is identically 0 and so $\bar{S}_0 = 0, \ldots, \bar{S}_s = 0$. Since R_k is reduced with respect to AS_k so that each S_i is reduced with respect to AS_{k-1}, by induction hypothesis 2_{k-1} we have necessarily $S_i = 0$ so that $R_k = 0$, i.e., 2_k holds true. It follows that 1_{k+1} is also true. The above proof is clearly valid for 2_1 while 1_1 is quite evident. Consequently 1_k and 2_k are true for $k = 1, 2, \ldots, r$.

It is now easy to complete the proof of Lemma 5.1 as follows.

Let the remainder of F with respect to $AS_r = AS$ be R; then we have the following remainder formula

$$I_1^{s_1} \cdots I_r^{s_r} F = \sum_{i=1}^{r} Q_i A_i + R.$$

Suppose $R = 0$. Since $\bar{\eta}$ is an extended zero of all A_i's while by 1_k it is not an extended zero of any I_k, so by the formula above it is an extended zero of F. Conversely, if $\bar{\eta}$ is an extended zero of F, then by the same formula $\bar{\eta}$ is also an extended zero of R. By 2_r we have necessarily $R = 0$. This proves Lemma 5.1. ∎

If an ascending set AS as before is reducible, then there is a k such that

$$AS_{k-1} \qquad A_1, A_2, \ldots, A_{k-1}$$

is irreducible with

$$\bar{\eta}_{k-1} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_{k-1})$$

as a generic point, and the polynomial $\bar{A}_k$ obtained from A_k by substituting $\eta_1, \ldots, \eta_{k-1}$ for $y_1, \ldots, y_{k-1}$ is reducible in $\boldsymbol{K}_{k-1}[y_k]$, where $\boldsymbol{K}_{k-1} = \boldsymbol{K}_0(\eta_1, \ldots, \eta_{k-1})$. Let the irreducible factorization of $\bar{A}_k$ in $\boldsymbol{K}_{k-1}[y_k]$, which can be determined by some known methods, be given as

$$\bar{A}_k = H_1 \cdots H_h,$$

in which each $H_i \in \boldsymbol{K}_{k-1}[y_k]$ is irreducible, and $h \geq 2$. As the coefficients of H_i in y_k are all elements of $\boldsymbol{K}_{k-1}$ and thus can be expressed as quotients of polynomials in $u_1, \ldots, u_d, \eta_1, \ldots, \eta_{k-1}$, we would get, by multiplying a common denominator, an expression of the form

$$\bar{D}\bar{A}_k = \bar{G}_1 \cdots \bar{G}_h,$$

where $\bar{D}, \bar{G}_i$ are polynomials in $\boldsymbol{K}_{k-1}[y_k]$, got from some D, G_i by substituting $\eta_1, \ldots, \eta_{k-1}$ for $y_1, \ldots, y_{k-1}$ with $D \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k-1}], G_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$. We may consider D as already reduced with respect to AS_{k-1} and G_j as already reduced with respect to AS_k.

Write the polynomial $G_1 \cdots G_h - DA_k$ in a form according to powers of y_k, say

$$G_1 \cdots G_h - DA_k = \sum_j B_j y_k^j,$$

in which $B_j \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k-1}]$. Denote by b_j the element in $\boldsymbol{K}_{k-1}$ got from B_j by substituting $\eta_1, \ldots, \eta_{k-1}$ for $y_1, \ldots, y_{k-1}$. Then we have $b_j = 0$, since $\bar{D}\bar{A}_k = \bar{G}_1 \cdots \bar{G}_h$. In other words, all B_j have $\bar{\eta}_k$ as an extended zero. It follows from Lemma 5.1 that all B_j have remainders 0 with respect to the irreducible ascending set AS_{k-1}, so that there are non-negative integers $s_{j1}, \ldots, s_{j\ k-1}$ and polynomials $Q_{ji} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ satisfying the relation

$$I_1^{s_{j1}} \cdots I_{k-1}^{s_{j\ k-1}} B_j = \sum_{i=1}^{k-1} Q_{ji} A_i.$$

Let $s_i = \max_j s_{ji}$; then we get

$$I_1^{s_1} \cdots I_{k-1}^{s_{k-1}}(G_1 \cdots G_h - DA_k) = \sum_{i=1}^{k-1} Q_i A_i, \tag{5.3}$$

in which Q_i are polynomials in $u_1, \ldots, u_d, y_1, \ldots, y_k$.

As noted already, there are methods, for example, those described in Hu & Wang (1986) and Wang (1992a), for factorizing polynomials over any algebraic extension field of $\boldsymbol{K}$. Polynomial factorization is a full research subject and is much beyond the scope of this paper, so we assume that one knows how to factorize polynomials over algebraic extension fields. Thus, from the above discussions, we may state the following

Lemma 5.2
There is an algorithmic method which determines whether an ascending set is irreducible, and if not, determines a certain k such that the ascending set AS_{k-1} formed by the first $k-1$ terms of AS is irreducible with $\bar{\eta}_{k-1} \in \boldsymbol{K}_{k-1}$ as a generic point, while the polynomial got from A_k by substituting $\bar{\eta}_{k-1}$ for the corresponding variables is reducible with an irreducible factorization of the form

$$DA_k = G_1 \cdots G_h, \tag{5.4}$$

where the polynomials $D \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k-1}]$, $G_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ are all reduced and $DA_k - G_1 \cdots G_h$ has remainder 0 with respect to AS_{k-1}.

Equivalently, the formula (5.3) can be written in the form

$$I_1^{s_1} \cdots I_{k-1}^{s_{k-1}} G_1 \cdots G_h = \sum_{i=1}^{k} Q_i A_i, \tag{5.5}$$

in which Q_i are still polynomials in $u_1, \ldots, u_d, y_1, \ldots, y_i$. Therefore, one can easily get the following decomposition lemma.

Lemma 5.3 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
Let a polynomial set PS have AS as a basic set with $\mathrm{cls}(A_i) > 0$, *$I_i = \mathrm{ini}(A_i)$ for $i = 1, \ldots, r$. Suppose that AS is reducible, so that there is a k for which the kth term A_k of AS has an irreducible factorization into polynomials $G_1, \ldots, G_h$ as of the form* (5.4). *Then there is a zero decomposition of the form*

$$\mathrm{Zero}(PS) = \bigcup_{i=1}^{k-1} \mathrm{Zero}(PS_i) \cup \bigcup_{j=1}^{h} \mathrm{Zero}(QS_j), \tag{5.6}$$

where $PS_i = PS \cup \{I_i\}$ and $QS_j = PS \cup \{G_j\}$.

Proof. Any zero of either PS_i or QS_j on right-hand side of (5.6) is clearly also a zero of PS. Conversely, any zero of PS is a zero of the A_i's. From the expression (5.5) it is also a zero of some I_i or some G_j, and thus a zero of some PS_i or QS_j. ■

As in Lemma 5.3 each I_i is already reduced with respect to AS and each G_j is also assumed to be reduced with respect to AS_k and hence also reduced with respect to AS, the basic set of any polynomial set $PS_i \cup CS$ or $QS_j \cup CS$ has rank lower than that of AS by Lemma 4.2. Therefore, in proceeding with each $PS_i \cup CS$ or $QS_j \cup CS$ as PS to get further zero decomposition of the form (5.6), we will arrive at a decomposition of the same form (5.1) with all CS_i irreducible. In this case, the sequence of ascending sets $CS_1, \ldots, CS_e$ is called an *irreducible characteristic series* of PS.

Theorem 5.2 (Ritt, 1932, 1950, Wu, 1984a, 1984b)
The following algorithm computes an irreducible characteristic series Ψ of any given polynomial set PS.

IrreducibleCharacteristicSeries(Input: PS; Output: Ψ)

$\Phi := \{PS\}$
$\Psi := \emptyset$
while $\Phi \neq \emptyset$ do
 $QS :=$ an element of Φ
 $\Phi := \Phi \setminus \{QS\}$
 $CS :=$ CharacteristicSet(QS)
 if CS is non-contradictory then
  if CS is irreducible then
   $\Psi := \Psi \cup \{CS\}$
   $\Phi := \Phi \cup \{QS \cup CS \cup \{I\} | \; I = \mathrm{ini}(C), C \in CS, \mathrm{cls}(I) > 0\}$
  else
   factorize certain C_k in CS into $G_1, \ldots, G_h$
   $\Phi := \Phi \cup \{QS \cup CS \cup \{I\} | \; I = \mathrm{ini}(C), C \in CS, \mathrm{cls}(C) <$
    $\mathrm{cls}(C_k), \mathrm{cls}(I) > 0\} \cup \{QS \cup CS \cup \{G_j\} | \; 1 \leq j \leq h\}$

Example 5.2
In Example 4.1 the first polynomial, say C_1, in the characteristic set CS, as a multivariate polynomial, is reducible (it has a factor x_1). But C_1 is irreducible over the transcendental extension field $\boldsymbol{Q}(x_1)$ since, in $\boldsymbol{Q}(x_1)$, x_1 is a non-zero element. Moreover, we can remove x_1 from C_1 because it is a factor of the initial of C_1 which has been additionally considered. On the other hand, x_1 is also the initial of the third polynomial C_3 in CS, we can even simply remove this factor from C_1 without additional consideration. The obtained ascending set may still be regarded as a characteristic set of PS. One can check by known methods of polynomial factorization that the polynomial obtained from C_1 by removing x_1, denoted by C_1 still, is irreducible. To decide whether the ascending set is irreducible, one needs to verify whether the second polynomial C_2 in CS is irreducible over $\boldsymbol{Q}(x_1, \eta)$ with η an extended zero of C_1. It is thus necessary to consider polynomial factorization over the algebraic extension field $\boldsymbol{Q}(x_1, \eta)$. We may find, by using either of the two methods described in Hu & Wang (1986) and Wang (1992a), that C_2 can be factorized as

$$C_2 = (x_1 + 1)(x_3 - 2x_1x_2 + x_1)(x_3 + x_1x_2 - x_1).$$

Let

$$\begin{aligned} PS_1 &= \{x_1, F_1, F_2, F_3\}, & PS_3 &= \{F_1, F_2, F_3, x_3 - 2x_1x_2 + x_1\}, \\ PS_2 &= \{x_1 + 1, F_1, F_2, F_3\}, & PS_4 &= \{F_1, F_2, F_3, x_3 + x_1x_2 - x_1\}. \end{aligned}$$

Then by Lemma 5.3, we have a decomposition

$$\mathrm{Zero}(PS) = \bigcup_{i=1}^{4} \mathrm{Zero}(PS_i).$$

As given already in Example 5.1, $PS_1 \cup CS$ and $PS_2 \cup CS$ have their characteristic sets CS_1 and CS_2 respectively. The characteristic sets of $PS_3 \cup CS$ and $PS_4 \cup CS$ are

$$\begin{aligned} CS_3 &= \{C_1, x_3 - 2x_1x_2 + x_1, x_1(x_4 + x_2 - 1)\}, \\ CS_4 &= \{C_1, x_3 + x_1x_2 - x_1, -x_1(x_4 - 2x_2 + 1)\}. \end{aligned}$$

By the same reason, the factor x_1 of the third polynomials in CS_3 and CS_4 can be simply removed too, and the obtained ascending sets are denoted still by CS_3 and CS_4.

Let us check whether the four ascending sets $CS_1, \ldots, CS_4$ are irreducible. First, one can easily see that both CS_3 and CS_4 are irreducible because all of their polynomials are linear in their leading variables. Secondly, one can find that the second polynomial in CS_1 can be factorized as

$$x_3^2 - 1 = (x_3 - 1)(x_3 + 1)$$

and the third polynomial in CS_2 can be factorized as

$$x_4^2 - x_2x_4 + 4x_2 = (x_4 + x_2 - 1)(x_4 - 2x_2 + 1).$$

By using Lemma 5.3 again, we have further decompositions with the corresponding irreducible ascending sets as follows

$$\begin{aligned} CS_1' &= \{x_1 + 1, x_2, x_3 + 1, x_4 + 1\}, \\ CS_1'' &= \{x_1 + 1, x_2, x_3 - 1, x_4 - 1\}, \\ CS_2' &= \{x_1, 2x_2^2 + 1, x_3, x_4 + x_2 - 1\}, \\ CS_2'' &= \{x_1, 2x_2^2 + 1, x_3, x_4 - 2x_2 + 1\}. \end{aligned}$$

Now, $CS_1', CS_1'', CS_2', CS_2'', CS_3$ and CS_4 constitute an irreducible characteristic series of PS, and we finally obtain the following irreducible decomposition

$$\begin{aligned} \mathrm{Zero}(PS) = {} & \mathrm{Zero}(CS_1') \cup \mathrm{Zero}(CS_1'') \cup \mathrm{Zero}(CS_2') \\ & \cup \mathrm{Zero}(CS_2'') \cup \mathrm{Zero}(CS_3/x_1 + 1) \cup \mathrm{Zero}(CS_4/x_1 + 1). \end{aligned}$$

■

Remark 5.1

To reduce the expenses for computing characteristic series, we may heuristically factorize some intermediate polynomials at an appropriate stage of the computation. Let us illustrate this by looking at the proof of Theorem 4.1. If some polynomial in QS_i can be factorized, for instance, into two polynomials and thus QS_i can be decomposed into two polynomial sets, say QS_i' and QS_i'', such that $\mathrm{Zero}(PS) = \mathrm{Zero}(QS_i) = \mathrm{Zero}(QS_i') \cup \mathrm{Zero}(QS_i'')$, then we may compute the irreducible characteristic series of QS_i' and QS_i'', respectively, instead of computing that of PS. Polynomial factorization is expensive in general, but making proper use of it may improve the efficiency of the characteristic series algorithms.

Remark 5.2

Even though the previous example is not due to this case, it happens quite often that all polynomials other than the first in the characteristic set of a polynomial set are linear in their leading variables. The reason comes from the feature of the characteristic set algorithm. The major operation involved in this algorithm is the pseudo-division which, in the normal case, reduces the divided polynomial to a polynomial of degree one less than that of the dividing polynomial. Making an observation on this matter of fact, we may see that, for computing irreducible characteristic series, polynomial factorization over algebraic extension fields (or algebraic factorization for short) is not necessary for the first characteristic set in the normal case, which makes the irreducible decomposition practically feasible because in general the first characteristic set is the most complex one with respect to the size. An ascending set in which all polynomials other than the first are linear in their leading variables is said to be *quasilinear.* During the computation of characteristic series the adjunction of initials often destroys the quasilinearity of characteristic sets of the enlarged polynomial sets, however. Therefore, algebraic factorization is often required for verifying the irreducibility of these characteristic sets.

Remark 5.3
Without irreducibility test, there is no guarantee for each $\mathrm{Zero}(CS_i/J_i)$ in the decomposition (5.1) to be non-empty. That is, a redundant branch with empty set of zeros in the characteristic series is not necessarily detected without performing the irreducible decomposition. Instead of using algebraic factorization, the empty branches can also be detected by using a projection theorem of Wu (1990a).

Remark 5.4
During the computation of characteristic series, many branches of the decomposition tree are produced due to the recursive generation of enlarged polynomial sets. Some of these branches are completely redundant and should be removed. Various techniques have been developed for controlling the expansion of branches (see Chou & Gao, 1990b). For example, if the complete decomposition of some PS_i is already obtained, then any branch PS_j which contains PS_i as a subset need not be further considered.

On the other hand, we have observed that the characteristic series as well as the irreducible decomposition of algebraic varieties to be presented in Section 8 are well suited for parallel computation as different branches can be treated individually by parallel processors. Some preliminary experiments on the parallelization of several characteristic-set-based algorithms utilizing workstation networks have been reported in Wang (1991b).

Remark 5.5
The algorithm given in Theorem 5.1 works in the weak-sense and quasi-sense as well. That is, the weak- and quasi-characteristic series of a polynomial set can be computed by the same algorithm in altering respectively characteristic sets to weak- and quasi-characteristic sets. However, in the quasi-sense the algorithm can no longer be guaranteed to terminate. Irreducible weak-ascending sets can be defined too, but neither can irreducible quasi-ascending sets. The algorithm given in Theorem 5.2 can also be used to compute the irreducible weak-characteristic series of a polynomial set by modifying the corresponding notions.

6. Generalization, Modifications and Extensions

In the characteristic set algorithm, each enlarged polynomial set QS_{i+1}, as shown in the proof of Theorem 4.1, is the union of QS_i and RS_i. This results in rapid expansion of the number of polynomials in QS_{i+1} as i increases. To reduce computational expenses, one strategy is to let QS_{i+1} just be the union of BS_i and RS_i and check finally whether all polynomials in PS have remainders 0 with respect to the last basic set. This strategy has been used by Wu (1987b, 1989a) and his followers. To extend this idea, we give, in the first half of this section, a generalized characteristic set algorithm which may lead to several variants of the standard one. For this purpose, let us introduce a couple of new notions. Given a polynomial set, say $PS = \{F_1(x_1, \ldots, x_n), \ldots, F_s(x_1, \ldots, x_n)\}$, let

$$\Psi = \{\sum_{i=1}^{s} Q_i F_i |\ Q_i \in \boldsymbol{K}[x_1, \ldots, x_n]\}.$$

Then the infinite set Ψ of polynomials forms a polynomial ideal, denoted by $\mathrm{Ideal}(PS)$ as usual, and the polynomials $F_1, \ldots, F_s$ are called the generators of Ψ.

Definition 6.1
Any ascending set which is contained in Ψ and has rank not higher than that of the basic set of PS is called a medial set of PS.

A medial set MS is called a characteristic set if all polynomials in PS have remainders 0 with respect to MS.

Apparently, any basic set itself is a medial set of PS, and the characteristic set defined here satisfies the zero relations (4.1) and (4.2).

Lemma 6.1 (Wang, 1989e)
Let PS be a finite non-empty set of non-zero polynomials with a medial set

$$MS \qquad M_1, M_2, \ldots, M_r,$$

of which $\mathrm{cls}(M_1) > 0$. *If M is a non-zero polynomial reduced with respect to MS, then any medial set MS' of the polynomial set $PS' = PS \cup MS \cup \{M\}$ has rank lower than that of MS.*

Proof. Let BS' and BS^* be the basic sets of PS' and $PS \cup MS$ respectively. Then BS^* has rank not higher than that of MS. If BS^* has the same rank as that of MS, then M is reduced with respect to BS^*. Hence, by Definition 6.1 and Lemma 4.2 we have

$$MS' \preceq BS' \prec BS^* \sim MS,$$

where $\preceq$ stands for *lower than or the same as*. If BS^* has rank lower than that of MS, then

$$MS' \preceq BS' \preceq BS^* \prec MS$$

holds. Therefore, in either case MS' has rank lower than that of MS. ■

Now we are ready to describe a generalized characteristic set algorithm.

Theorem 6.1 (Wang, 1989e)
The following algorithm computes a characteristic set CS of any polynomial set PS.

GeneralizedCharacteristicSet(Input: PS; Output: CS)
    $QS := PS$
    $RS := PS$
    while $RS \neq \emptyset$ do
        $CS :=$ a medial set of QS
        if CS is contradictory then $RS := \emptyset$ else
            $RS := \{R \mid R =$PseudoRemainder$(Q, CS), R \neq 0, Q \in QS \setminus CS\}$
            $QS := QS \cup CS \cup RS$

By taking different medial sets, we may get different variants of the characteristic set algorithm. In particular, if we take basic set as medial set, then the generalized characteristic set algorithm is identical to the previous characteristic set algorithm. Now let CharacteristicSetN be the algorithm obtained from CharacteristicSet by replacing the last line with $QS := CS \cup RS$. Then this algorithm computes clearly a medial set of the input polynomial set. While replacing the fourth line of the generalized characteristic set algorithm by

$$CS := \mathsf{CharacteristicSetN}(QS)$$

one obtains immediately a modification of the characteristic set algorithm as mentioned at the beginning of this section.

Proof of Theorem 6.1. This algorithm has the same structure as that of the characteristic set algorithm. While replacing each BS_i by an arbitrary medial set MS_i of QS_i, and letting each enlarged polynomial set QS_{i+1} be $QS_i \cup RS_i \cup MS_i$, we should get a sketch similar to that given in the proof of Theorem 4.1, but each MS_i is no longer a subset of QS_i. Then, the termination of the above algorithm is guaranteed by Corollary 3.1 and Lemma 6.1. From the formation of each QS_i and the remainder formula, the correctness can be easily proved by an argument similar to the correctness proof of Theorem 4.1. ■

If one intends only to compute quasi-characteristic sets (triangular forms), then the algorithm may have plenty of scope for variation. We provide a variant analogous to the China-Gauss elimination, by taking quasi-medial sets computed with the following algorithm.

```
TriangularForm(Input: PS; Output: MS)
    n := the number of variables
    MS := ∅
    QS_i := {P ∈ PS | cls(P) = i}
    for i from n step −1 to 1 do
        if QS_0 = ∅ then TriangularFormSub(QS_0, ..., QS_i, i)
    if QS_0 ≠ ∅ then MS := an element of QS_0 else
        MS := QS_1 ∪ ··· ∪ QS_n

TriangularFormSub(Transient: QS_0, ..., QS_i, i)
    while QS_i contains more than one element do
        Q := an element of QS_i with lowest rank
        TS := QS_i \ {Q}
        QS_i := {Q}
        for all P in TS do
            R := prem(P, Q)
            if R ≠ 0 then QS_cls(R) := QS_cls(R) ∪ {R}
```

Proof. The termination of TriangularForm is evident if the termination of TriangularFormSub is proved. To prove that the algorithm TriangularFormSub terminates, i.e., the while-loop has only a finite number of iterations, we suppose, at the outset, the number of polynomials in QS_i is r. If $r \leq 1$, then the algorithm terminates trivially. Otherwise, let Q be an element of QS_i with lowest rank. Then in each iteration QS_i is reset to be the set of all non-zero remainders of class i of polynomials in $QS_i \setminus \{Q\}$ with respect to Q, together with Q itself; therefore either the number of polynomials in the newly formed QS_i is less than r or the lowest rank of polynomials in QS_i is lower than the rank of Q. Proceeding recursively with the new QS_i as the original QS_i in the while-loop, the number of polynomials in QS_i must come to 1 after a finite number of steps and the algorithm terminates finally.

To prove the correctness, we need only to prove that the output set MS is a quasi-ascending set and has rank not higher than that of the quasi-basic set BS of the input polynomial set PS. The former is obvious. To prove the latter, i.e., $MS \prec BS$ or $MS \sim BS$ which is simply denoted as $MS \preceq BS$, let $BS = \{B_1, \ldots, B_s\}, MS = \{M_1, \ldots, M_r\}$ and $p_i = \mathrm{cls}(B_i)$. Since $B_1 \in PS$ and $\mathrm{cls}(B_1) = p_1$, QS_{p_1} is always non-empty and MS contains thus an element of class p_1. This implies that $\mathrm{cls}(M_1) \leq \mathrm{cls}(B_1)$. If $\mathrm{cls}(M_1) < \mathrm{cls}(B_1)$, then $MS \prec BS$ and the correctness is already proved. Otherwise, $\mathrm{cls}(M_1) = \mathrm{cls}(B_1)$. From the formation of each QS_i, one knows clearly that $\deg(M_1) \leq \deg(B_1)$. Hence $M_1 \prec B_1$ or $M_1 \sim B_1$. In the former case, the correctness is proved. Suppose otherwise the latter happens. Similarly, MS should contain a polynomial of class p_2 and we have thus $\operatorname{cls}(M_2) \leq \operatorname{cls}(B_2)$ etc. By the same argumentation, we know that either there is a $j \leq \min(r, s)$ such that $M_1 \sim B_1, \ldots, M_{j-1} \sim B_{j-1}$ while $M_j \prec B_j$, or $s = r$ and $M_1 \sim B_1, \ldots, M_r \sim B_r$. In any case MS has rank not higher than that of BS and the correctness of the algorithm is proved. ■

To get a characteristic set of PS, we may also first compute a triangular form and then make the jth polynomial be reduced with respect to the ith polynomial in the triangular form for each pair $j > i$. This can be done by taking medial sets computed with the following algorithm:

```
TriangularFormC(Input: PS; Output: MS)
    MS := TriangularForm(PS)
L   r := number of polynomials in MS
    if r > 1 then
        M_i := the ith polynomial in MS
        for i form 2 to r do
            R := PseudoRemainder(M_i, {M_1, ..., M_{i-1}})
            if R = 0 then MS := a medial set of PS; return MS
            else
                if cls(R) = cls(M_i) then M_i := R else
                    MS := TriangularForm({M_1, ..., M_{i-1}, R})
                          ∪{M_{i+1}, ..., M_r}
                    go to L
            MS := {M_i| 1 ≤ i ≤ r}
```

One can benefit from this algorithm only if the remainders of the polynomials M_i in the triangular form of PS with respect to the triangular form $\{M_1, \ldots, M_{i-1}\}$ are not 0. The termination and correctness of the algorithm can be easily proved by noting that the quasi-basic set has rank lower than that of the basic set for any polynomial set and by using the following

Lemma 6.2 (Wang, 1989e)
Let $MS = \{M_1, \ldots, M_{i-1}\}$ be an ascending set, $MS^+ = \{M_1, \ldots, M_{i-1}, M_i\}$ a quasi-ascending set and R the remainder of M_i with respect to MS. Suppose $R \neq 0$ and $\operatorname{cls}(R) \neq \operatorname{cls}(M_i)$. If MS^* is a medial set of $MS \cup \{R\}$ computed by the algorithm TriangularForm*, then $MS^* \prec MS^+$.*

Proof. Let BS^*, BS' and BS^+ be the quasi-basic sets of $MS \cup \{R\}, MS^+ \cup \{R\}$ and MS^+, respectively. Then

$$MS^* \preceq BS^* \preceq BS' \prec BS^+ = MS^+.$$ ■

Various modifications of the characteristic set algorithm naturally lead to modifications of the characteristic series algorithms, for which we omit the details. The reader may also refer to Chou (1988), Ko (1988), Chou & Gao (1990a), Kalkbrener (1991) and other relevant work for variants, modifications and extensions.

In what follows we discuss some extensions of the characteristic series algorithms. Let PS be a polynomial set and G any other non-zero polynomial. Our goal is to give algorithms for decomposing a more general set $\operatorname{Zero}(PS/G)$ of zeros. For simplicity of notations, we denote the pair of a polynomial set PS and a non-zero polynomial G by PS/G. In case G is a constant, PS/G is replaced by PS. Then the decomposition (5.1) can be extended to the form

$$\operatorname{Zero}(PS/G) = \bigcup_{i=1}^{e} \operatorname{Zero}(CS_i/R_i), \tag{6.1}$$

in which CS_i is an ascending set, R_i the non-zero remainder of J_iG_i with respect to CS_i, J_i the product of initials of the polynomials in CS_i and G_i some non-zero polynomial for each i.

The sequence of pairs $CS_1/R_1, \ldots, CS_e/R_e$ is called again a *characteristic series* (and accordingly, *irreducible characteristic series* when all CS_i are irreducible) of PS/G.

Theorem 6.2 (Wu, 1986a)
The following algorithms compute a characteristic series and an irreducible characteristic series Ψ of PS/G, respectively.

```
ExtendedCharacteristicSeries(Input: PS/G; Output: Ψ)
   Φ := {PS/G}
   Ψ := ∅
   while Φ ≠ ∅ do
      QS/H := an element of Φ
      Φ := Φ \ {QS/H}
      CS := CharacteristicSet(QS)
      if CS is non-contradictory then
         J := ∏_{C∈CS} ini(C)
         R := PseudoRemainder(JH, CS)
         if R ≠ 0 then Ψ := Ψ ∪ {CS/R}
         Φ := Φ ∪ {QS ∪ CS ∪ {I}/H| I = ini(C), C ∈ CS, cls(I) > 0}

ExtendedIrreducibleCharacteristicSeries(Input: PS/G; Output: Ψ)
   Φ := {PS/G}
   Ψ := ∅
   while Φ ≠ ∅ do
      QS/H := an element of Φ
      Φ := Φ \ {QS/H}
      CS := CharacteristicSet(QS)
      if CS is non-contradictory then
         Φ := Φ ∪ {QS ∪ CS ∪ {I}/H| I = ini(C), C ∈ CS, cls(I) > 0}
         J := ∏_{C∈CS} ini(C)
         if CS is irreducible then
            R := PseudoRemainder(JH, CS)
            if R ≠ 0 then Ψ := Ψ ∪ {CS/R}
         else
            factorize certain C_k in CS such that DC_k = H_1 ··· H_h
            for i from 1 to h do
               DS := CS ∪ {H_i} \ {C_k}
               Φ := Φ ∪ {DS/DJH}
            Φ := Φ ∪ {QS ∪ {D}/JH}
```

Since the basic sets of the successively adjoined polynomial sets are of steadily decreasing ranks, the above algorithms terminate obviously. Their correctness can be easily seen from the previous discussions.

Remark 6.1
Weak-medial sets and *quasi-medial sets* can be similarly defined. The corresponding weak-characteristic sets or quasi-characteristic sets can be computed by the same generalized characteristic set algorithm described in Theorem 6.1 in replacing medial set by weak-medial set or quasi-medial set. Theorem 6.2 is still true in the weak sense.

Remark 6.2
Actually, a medial set or quasi-medial set computed by the algorithm CharacteristicSetN, TriangularFormC or TriangularForm from PS is "nearly" a characteristic set or quasi-characteristic set. For a nearly (weak-, quasi-) characteristic set CS, the zero relations (4.1) and (4.2) no more hold; we only have

$$\mathrm{Zero}(PS) \subset \mathrm{Zero}(CS).$$

It is worth noting that the nearly (weak-, quasi-) characteristic sets are sometimes sufficient for applications such as solving systems of algebraic equations. If, in particular, CS has only a finite number of zeros, whether every zero of CS is also a zero of PS can be verified by simple substitutions.

Remark 6.3
To determine whether a nearly (weak-, quasi-) characteristic set CS is indeed a (weak-, quasi-) characteristic set, we have to follow the generalized characteristic set algorithm by verifying whether all polynomials in the input set have remainders 0 with respect to CS. Experiments show that in most cases the remainders are 0 (i.e., the generalized characteristic set algorithm terminates after the first iteration of the while-loop) and the verification of 0 remainders takes a great amount of computing time. There are some strategies which can be used to partially avoid the verification of 0 remainders. This is done by examining the factor-relations of some initials and removed factors (see Wang, 1992b, 1992c).

Remark 6.4
For a non-contradictory (week) ascending set $AS = \{A_1(u_1, \ldots, u_d, y_1), \ldots, A_r(u_1, \ldots, u_d, y_1, \ldots, y_r)\}$, the initial I_i of A_i usually involves the variables $u_1, \ldots, u_d$ and $y_1, \ldots, y_{i-1}$. If, in particular, I_i involves only the variables $u_1, \ldots, u_d$ for all i, we call AS a *normal (weak-) ascending set*. In most cases (when AS is "well-behaved"), we can compute a normal weak-ascending set AS^* and a polynomial F from AS such that

$$\mathrm{Zero}(AS/F) \subset \mathrm{Zero}(AS^*), \quad \mathrm{Zero}(AS^*/J^*) \subset \mathrm{Zero}(AS/J), \tag{6.2}$$

in which J and J^* are respectively the product of initials of the polynomials in AS and in AS^* (cf. Wang, 1990b). Moreover, one can compute a characteristic series Ψ of PS with all ascending set in Ψ normal.

7. Algebraic Decision Problem: Division Principle

We consider a polynomial set $PS = \{F_1, \ldots, F_s\}$ and any other polynomial G. As before, all polynomials are assumed to be non-zero and in $\boldsymbol{K}[x_1, \ldots, x_n]$. While speaking that a polynomial G vanishes on a set V $(\subset \tilde{\boldsymbol{K}}^n)$, we mean that any point of V is a zero of G, which is denoted as

$$G|_V \equiv 0. \tag{7.1}$$

The algebraic decision problem proposed in Section 2 may be recalled as follows.

Algebraic Decision Problem
Determine whether $G = 0$ is a formal consequence of $PS = 0$, i.e., whether or not the polynomial G vanishes on Zero(PS)*, where the zeros considered may be in $\boldsymbol{K}$ or some extension field $\tilde{\boldsymbol{K}}$ of $\boldsymbol{K}$.*

Any effective method which provides a solution to this problem will lead to a number of important applications, for instance, to geometry theorem proving and problems about relationships between algebraic varieties. In what follows, we consider the problem only for the case that zeros may be in some extension of $\boldsymbol{K}$. In other words, we shall solve the problem completely only over algebraically closed fields. Hilbert's Nullstellensatz says that, if the solution to this problem is positive, then there exists an integer q such that

$$(7.2) \qquad G^q = \sum_{i=1}^{s} A_i F_i.$$

Hence this problem is equivalent to deciding whether G belongs to the radical ideal generated by *PS* and thus can be regarded as the membership problem of radical ideals. The existential and constructive proofs of Hilbert's Nullstellensatz may be found in many textbooks of algebraic geometry. However, there is no easy way to find an exact representation as of the form (7.2) for given polynomials.

In this section we demonstrate how characteristic sets can be applied to the algebraic decision problem. Before illustrating the method, let us prove some lemmas which not only are needed for the proof of our main principle in this section but also have several other applications. The ascending sets considered below are assumed to have the form (5.2).

Lemma 7.1 (Wu, 1984a, 1984b)
Let an ascending set AS be irreducible with a generic point $\bar{\eta} = (u_1, \ldots, u_d, \eta_1, \ldots, \eta_r)$. *If a polynomial* $F \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ *has remainder* $\neq 0$ *with respect to AS, then there is an algorithm by which one can find polynomials D and* $Q_i, i = 1, \ldots, r$ *in* $\boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ *such that*

$$G \cdot F - \sum_{i=1}^{r} Q_i C_i = D \in \boldsymbol{K}[u_1, \ldots, u_d]$$

and

$$G(\bar{\eta}) \neq 0.$$

Proof. By induction on r, the case $r = 0$ is trivial. Suppose the lemma has been proved already for $k < r$. Let us prove it for $k + 1$.

Since the initial I_{k+1} of A_{k+1} has remainder $\neq 0$ with respect to the irreducible ascending set

$$AS_k \qquad A_1, \ldots, A_k,$$

by induction hypothesis there are polynomials $H_k, R_{k1}, \ldots, R_{kk} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ such that

$$H_k I_{k+1} - \sum_{i=1}^{k} R_{ki} A_i \in \boldsymbol{K}[u_1, \ldots, u_d]$$

and

$$H_k(\bar{\eta}_k) = H_k(\bar{\eta}_{k+1}) \neq 0,$$

where $\bar{\eta}_k$ is the corresponding generic point of AS_k.

Suppose $F_{k+1} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k+1}]$ has remainder $\neq 0$ with respect to AS_{k+1}. By Lemma 6.1 we have $F_{k+1}(\bar{\eta}_{k+1}) \neq 0$. Now let us form the resultant of F_{k+1} and A_{k+1} as polynomials in y_{k+1}. Then there are polynomials $U_{k+1}, V_{k+1} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k+1}]$ and $F_k \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ such that

$$U_{k+1}F_{k+1} + V_{k+1}A_{k+1} = F_k \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k],$$

in which $\deg_{y_{k+1}}(U_{k+1}) < \deg(A_{k+1}) = m_{k+1}, \deg_{y_{k+1}}(V_{k+1}) < \deg_{y_{k+1}}(F_{k+1})$. Let $\bar{U}_{k+1}, \bar{V}_{k+1}$ etc. be polynomials obtained from U_{k+1}, V_{k+1} by substituting $\eta_1, \ldots, \eta_k$ for $y_1, \ldots, y_k$, respectively. Then the above expression leads to

$$\bar{U}_{k+1}\bar{F}_{k+1} + \bar{V}_{k+1}\bar{A}_{k+1} = \bar{F}_k.$$

As $\bar{A}_{k+1}$ is an irreducible polynomial in $\boldsymbol{K}[y_{k+1}]$ and $\bar{A}_{k+1}(\eta_{k+1}) = 0$, $\bar{F}_{k+1}(\eta_{k+1}) = F_{k+1}(\bar{\eta}_{k+1}) \neq 0$, $\bar{F}_{k+1}$ and $\bar{A}_{k+1}$ cannot have common divisors of y_{k+1}; thereby we have $\bar{F}_k \neq 0$ or $F_k(\bar{\eta}_k) = F_k(\bar{\eta}_{k+1}) \neq 0$. Since $A_{k+1}(\bar{\eta}_{k+1}) = 0, U_{k+1}(\bar{\eta}_{k+1}) \neq 0$.

From $F_k(\bar{\eta}_k) \neq 0$, by Lemma 5.1 we know that the remainder of F_k with respect to AS_k is not equal to 0. Thus, by induction hypothesis there are polynomials $G_k, Q_{k1}, \ldots, Q_{kk} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_k]$ such that

$$G_kF_k - \sum_{i=1}^{k} Q_{ki}A_i \in \boldsymbol{K}[u_1, \ldots, u_d]$$

and

$$G_k(\bar{\eta}_k) = G_k(\bar{\eta}_{k+1}) \neq 0.$$

Now set

$$\begin{aligned} G_{k+1} &= G_kU_{k+1}, \\ Q_{k+1\ i} &= Q_{ki}, \ i = 1, \ldots, k, \\ Q_{k+1\ k+1} &= -G_kV_{k+1}. \end{aligned}$$

Then we have

$$\begin{aligned} &G_{k+1}, Q_{k+1\ 1}, \ldots, Q_{k+1\ k+1} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_{k+1}], \\ &G_{k+1}F_{k+1} - \sum_{i=1}^{k+1} Q_{k+1\ i}A_i \in \boldsymbol{K}[u_1, \ldots, u_d], \end{aligned}$$

and

$$G_{k+1}(\bar{\eta}_{k+1}) = G_k(\bar{\eta}_k)U_{k+1}(\bar{\eta}_{k+1}) \neq 0.$$

This proves the lemma. ∎

The following lemma is extracted from the proof of a theorem in Wu (1984b).

Lemma 7.2
Let AS be an irreducible ascending set as before and I_i the initial of the ith polynomial in AS. Then there is a point $(\bar{u}, \bar{y}) = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_r) \in \tilde{\boldsymbol{K}}^{d+r}$ such that $A_i(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) = 0$ while $I_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) \neq 0$ for all i.

Proof. Since each I_i itself is reduced with respect to $\mathcal{AS}$, by Lemma 7.1 there are polynomials $J_i, Q_{ij} \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ such that

$$H_i = J_i I_i - \sum_{j=1}^{i-1} Q_{ij} A_j \in \boldsymbol{K}[u_1, \ldots, u_d],$$

and $H_i \neq 0$. Hence, there is a point $\bar{u} = (\bar{u}_1, \ldots, \bar{u}_d) \in \boldsymbol{K}^d$ such that

$$H_1 \cdots H_r \neq 0$$

at $\bar{u}$. Such $\bar{u}$ may be chosen as a rational point.

We shall prove by induction on i that there are numbers $\bar{y}_i$ in a certain extension field $\tilde{\boldsymbol{K}}$ of $\boldsymbol{K}$ such that the point $(\bar{u}, \bar{y}) = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_r) \in \tilde{\boldsymbol{K}}^{d+r}$ satisfies the relations

$$A_i(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) = 0, \quad I_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) \neq 0.$$

First, let the polynomials obtained from A_1 and I_1 by substituting $\bar{u}_1, \ldots, \bar{u}_d$ for $u_1, \ldots, u_d$ be $\bar{A}_1 \in \boldsymbol{K}[y_1]$ and $\bar{I}_1 \in \boldsymbol{K}$. Since

$$H_1 = J_1 I_1$$

is not equal to 0 at $\bar{u}$, $\bar{I}_1 \neq 0$ and $\bar{A}_1$ is a polynomial in y_1 with $\deg_{y_1}(\bar{A}_1) = m_1 \geq 1$. Thus, one can choose a number $\bar{y}_1$ in a certain extension field of $\boldsymbol{K}$ such that $\bar{A}_1(\bar{y}_1) = 0$ or $A_1(\bar{u}, \bar{y}_1) = 0$. Again,

$$H_2 = J_2 I_2 - Q_{21} A_1,$$
$$H_2(\bar{u}, \bar{y}_1) = H_2(\bar{u}) \neq 0.$$

Hence

$$I_2(\bar{u}, \bar{y}_1) \neq 0,$$

i.e., the induction hypothesis is true for $i = 1$.

Suppose we have already found $\bar{y}_1, \ldots, \bar{y}_i$ satisfying the induction hypothesis and want to find further $\bar{y}_{i+1}$.

Let the polynomial obtained from A_{i+1} by substituting $\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_i$ for $u_1, \ldots, u_d$, $y_1, \ldots, y_i$ be $\bar{A}_{i+1} \in \boldsymbol{K}'[y_{i+1}]$, where $\boldsymbol{K}'$ is some extension of $\boldsymbol{K}$ involving $\bar{y}_1, \ldots, \bar{y}_i$. Now the leading coefficient of $\bar{A}_{i+1}$ as a polynomial in y_{i+1} is $I_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) \neq 0$. Therefore, one can choose a number $\bar{y}_{i+1}$ in a certain extension of $\boldsymbol{K}'$ and then of $\boldsymbol{K}$ such that $\bar{A}_{i+1}(\bar{y}_{i+1}) = 0$ or $A_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_{i+1}) = 0$. Thus

$$H_{i+2} = J_{i+2} I_{i+2} - \sum_{j=1}^{i+1} Q_{i+2\ j} A_j,$$

$$H_{i+2}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_{i+1}) = H_{i+2}(\bar{u}) \neq 0,$$

and

$$A_1(\bar{u}, \bar{y}_1, \ldots, \bar{y}_{i+1}) = A_1(\bar{u}, \bar{y}_1) = 0, \ldots, A_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_{i+1}) = 0$$

imply immediately that

$$I_{i+2}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_{i+1}) \neq 0.$$

This completes the proof of Lemma 7.2. ∎

Using an alternative description of Hilbert's Nullstellensatz, to determine whether G belongs to the radical ideal generated by PS, we need only to check whether the polynomial set $PS \cup \{z \cdot G - 1\}$ (where z is a new indeterminate) has no zero or $\mathrm{Ideal}(PS \cup \{z \cdot G - 1\})$ is a unity. Thus we may state the following

Theorem 7.1
For a polynomial set PS and a non-zero polynomial G, $G = 0$ is a formal consequence of $PS = 0$ if and only if

$$\mathrm{Zero}(PS \cup \{z \cdot G - 1\}) = \emptyset$$

over some extension field of $\boldsymbol{K}$, where z is a new indeterminate.

From this theorem the algebraic decision problem is reduced to determining the existence of zeros of a polynomial set over some extension field of $\boldsymbol{K}$, and thus can be solved by computing the irreducible characteristic series of $PS \cup \{z \cdot G - 1\}$. To economize somewhat the computational expenses, we propose to use the following algorithm:

AlgebraicDecisionA(Input: PS, G; Output: Yes or No)
  $\Psi := \{PS \cup \{z \cdot G - 1\}\}$
  while $\Psi \neq \emptyset$ do
    $QS :=$ an element of Ψ
    $\Psi := \Psi \setminus \{QS\}$
    $CS :=$ CharacteristicSet(QS)
    if CS is non-contradictory then
      if CS is irreducible then stop $[No]$
      else
        factorize certain C_k in CS into $G_1, \ldots, G_h$
        $\Psi := \Psi \cup \{QS \cup CS \cup \{I\} \mid I = \mathrm{ini}(C), C \in CS, \mathrm{cls}(C) <$
          $\mathrm{cls}(C_k), \mathrm{cls}(I) > 0\} \cup \{QS \cup CS \cup \{G_j\} \mid 1 \leq j \leq h\}$
  $[Yes]$

This algorithm has a structure close to that of the irreducible characteristic series algorithm and its termination is guaranteed evidently. The correctness of this algorithm follows from that of the irreducible characteristic series algorithm and Lemma 7.2.

Example 7.1
Consider the following two polynomials

$$G_1 = x_1 x_4^2 + x_2 x_3 - 3x_1 x_2^2 + 3x_1 x_2 - x_1,$$
$$G_2 = -2x_2 x_4 - x_3 + 2x_1 x_2^2 + 2x_2 + 1,$$

and let PS be the same polynomial set as in Examples 4.1-5.2. Then, one can verify by the above algorithm that G_1 is a formal consequence of $PS = 0$, but neither is G_2. As the characteristic set of $PS \cup \{z \cdot G_1 - 1\}$ with respect to the ordering $x_1 \prec x_2 \prec x_3 \prec x_4 \prec z$ is contradictory, further decomposition is not required in this case. For determining that $G_2 = 0$ is not a consequence of $PS = 0$, the irreducible decomposition is however needed. ∎

For detecting the emptiness of $\mathrm{Zero}(PS \cup \{z \cdot G - 1\})$, another method is based on a direct use of the pseudo-reduction, which has proved very efficient in the case of geometry theorem proving. For this method, the following principle is crucial.

Theorem 7.2 (*Division Principle*, Wu, 1984a, 1984b)
For an ascending set AS and a non-zero polynomial G, let $I_1, \ldots, I_r$ be all initials of the polynomials in AS and R the remainder of G with respect to AS. If $R \equiv 0$, then under the subsidiary conditions

$$DS \qquad I_i \neq 0, \quad i = 1, \ldots, r,$$

$G = 0$ is a formal consequence of $AS = 0$. Conversely, if AS is irreducible and under the subsidiary conditions DS, $G = 0$ is a formal consequence of $AS = 0$ (over some extension field of K), then $R \equiv 0$.

Proof. Since R is the remainder of G with respect to AS, there are integers $s_i \geq 0$ and polynomials $B_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ such that

$$I_1^{s_1} \cdots I_r^{s_r} G = \sum_{i=1}^{r} B_i A_i + R. \tag{7.3}$$

By this formula, no matter whether or not the ascending set AS is irreducible, the sufficiency of the condition is evident.

Let us prove the necessary condition when AS is irreducible. Otherwise, we suppose $R \neq 0$ and try to derive a contradiction. By Lemma 7.1, there are polynomials $S, Q_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ such that

$$T = S \cdot R - \sum_{i=1}^{r} Q_i A_i \in \boldsymbol{K}[u_1, \ldots, u_d], \tag{7.4}$$

and $T \neq 0$. By Lemma 7.2, there is a point $(\bar{u}, \bar{y}) = (\bar{u}_1, \ldots, \bar{u}_d, \bar{y}_1, \ldots, \bar{y}_r) \in \tilde{\boldsymbol{K}}^{d+r}$ such that

$$A_i(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) = 0, \quad I_{i+1}(\bar{u}, \bar{y}_1, \ldots, \bar{y}_i) \neq 0.$$

From the proof of Lemma 7.2, such $\bar{u}$ can be moreover chosen so that $T(\bar{u}) \neq 0$ in the meantime. According to the hypothesis that $G = 0$ is a formal consequence of $AS = 0$ under the subsidiary conditions $I_i \neq 0$ and the choice of $(\bar{u}, \bar{y})$, we should have

$$G(\bar{u}, \bar{y}) = 0.$$

Substituting $(\bar{u}, \bar{y})$ for (u, y) in the remainder formula (7.3), we have

$$R(\bar{u}, \bar{y}) = 0.$$

Finally, we substitute $(\bar{u}, \bar{y})$ for (u, y) in the formula (7.4) and thus get a contradiction. Hence the remainder R must be 0 and the theorem is proved. ■

Now we are ready to give the second algorithm for solving the algebraic decision problem.

AlgebraicDecisionB(Input: PS, G; Output: *Yes* or *No*)
  $\Psi := \{PS\}$
  while $\Psi \neq \emptyset$ do
    $QS :=$ an element of Ψ
    $\Psi := \Psi \setminus \{QS\}$
    $CS :=$ CharacteristicSet(QS)

if CS is non-contradictory then
    if PseudoRemainder(G, CS)$= 0$ then
        $\Psi := \Psi \cup \{QS \cup CS \cup \{I\} |\ I = \text{ini}(C), C \in CS, \text{cls}(I) > 0\}$
    else
        if CS is irreducible then stop $[No]$
        else
            factorize certain C_k in CS into $G_1, \ldots, G_h$
            $\Psi := \Psi \cup \{QS \cup CS \cup \{I\} |\ I = \text{ini}(C), C \in CS, \text{cls}(C) <$
                $\text{cls}(C_k), \text{cls}(I) > 0\} \cup \{QS \cup CS \cup \{G_j\} |\ 1 \leq j \leq h\}$
$[Yes]$

This algorithm also has a structure close to that of the irreducible characteristic set algorithm, and is thus guaranteed to terminate. Its correctness is based on the division principle. Obviously, in the case the answer is negative, the algorithm not only gives a solution but also indicates in which component the polynomial G does not vanish, which is important for some applications.

Note that, in the case of geometry theorem proving (by using the division principle), the subsidiary conditions DS, in general, reflect the non-degenerate cases of the theorem. Thus the cases $I_i = 0$ usually do not need to be further considered, which makes the involved computation much simpler.

Example 7.2
Let the polynomials and polynomial set be those in Example 7.1. The same conclusion can be reached by applying the algorithm AlgebraicDecisionB. Also, the irreducible decomposition is not needed for determining the inference relation for polynomial G_1. For polynomial G_2, while the answer *No* is given, one can also know that the inference relation does not hold on the components CS_1', CS_2'' and CS_4 (which are given in Example 5.2). ■

Remark 7.1
Various modifications and extensions of the irreducible characteristic series algorithm lead naturally to corresponding modifications and extensions of the algebraic decision algorithms. One may note that it is not an economic way to first compute an irreducible characteristic series of PS and then check whether the remainder of G with respect to each ascending set in the series is 0 because for computing irreducible characteristic series one has to perform algebraic factorization. Applying the algebraic decision algorithms posed above, algebraic factorization can often, particularly in the positive case as for G_1 in Example 7.1, be avoided.

Remark 7.2
The problem of deciding whether $G = 0$ is a formal consequence of $PS = 0$ under the condition $H \neq 0$, i.e., whether G vanishes on $\text{Zero}(PS/H)$, can be solved by using the algorithm AlgebraicDecisionA with a slight modification: letting the input be $PS/H, G$ and using $PS \cup \{z_1 \cdot G - 1, z_2 \cdot H - 1\}$ (where z_1 and z_2 are two newly introduced indeterminates) instead of $PS \cup \{z \cdot G - 1\}$ in the second line of the algorithm. For solving this problem, one can also design, by noticing the extended irreducible characteristic series algorithm presented in Section 6, an algorithm similar to AlgebraicDecisionB.

8. Irreducible Decomposition of Algebraic Varieties

As before, let $\boldsymbol{K}$ be a basic field and $\tilde{\boldsymbol{K}}$ some extension of $\boldsymbol{K}$. A polynomial is always understood as one in $\boldsymbol{K}[x_1, \ldots, x_n]$ and a point as one in the n-dimensional linear space $\tilde{\boldsymbol{K}}^n$.

Definition 8.1
A collection V of points is called an algebraic variety, *or simply a* variety, *if there is a polynomial set PS such that $V = \text{Zero}(PS)$. In that case, we call PS the* defining set *and, alternatively, $PS = 0$ the* defining equations *of V.*

A variety V_1 is said to be a subvariety *of the other V_2 if any point of V_1 is also a point of V_2.*

A variety V_1 is said to be a true subvariety *of V_2 if V_1 is a subvariety of V_2 while $V_1 \neq V_2$.*

A variety V is said to be irreducible *if it cannot be expressed as the union of two true subvarieties V_1 and V_2 of V. In that case, its defining set is also said to be* irreducible.

Algebraic varieties are the main objects studied in algebraic geometry. From constructive aspects, decomposing a given variety V into irreducible components, namely, expressing V as the union of a family of irreducible subvarieties, is a fundamental task. In this section we are dealing with this task by using the method developed in the previous sections. First of all, let us define the important notion of *generic points* of a variety as follows.

Definition 8.2
Any point η of an algebraic variety V, naturally over some extension field of $\boldsymbol{K}$, which is such that every polynomial annulled by η vanishes on V, will be called a generic point *of V.*

Consider now the problem of deciding the *irreducibility* of an algebraic variety or its defining polynomial set. Below are two well-known criteria.

Lemma 8.1
An algebraic variety V is irreducible if and only if one of the following holds:

(i) There cannot exist two non-zero polynomials G and H such that the polynomial $G \cdot H$ vanishes on V while both the polynomials G and H do not vanish on V;

(ii) V has generic points.

This lemma gives the necessary and sufficient conditions for the irreducibility of an algebraic variety, which are however merely existential (non-constructive) in character. Given the defining set of a variety, there is no means to determine in an algorithmic manner whether or not the conditions in Lemma 8.1 can be satisfied. Our purpose is mainly lying in determining algorithmically whether a variety given by its defining set is irreducible, and if not, completing an irreducible decomposition.

Let AS be an ascending set and J the product of initials I_i of the polynomials in AS. In general, the difference set $\text{Zero}(AS/J)$ is not a variety. Now suppose AS is irreducible with a generic point $\bar{\eta}$. Let

$$\Psi = \{F \mid \mathsf{PseudoRemainder}(F, AS) = 0, F \in \boldsymbol{K}[x_1, \ldots, x_n]\}.$$

By Lemma 5.1, Ψ forms an ideal and by Hilbert's basis theorem it has a finite basis, called the *prime basis* of AS and denoted by Ψ_{AS}, with $\bar{\eta}$ as an extended zero.

Let G be any polynomial with $\bar{\eta}$ as an extended zero. By Lemma 5.1 G has remainder 0 with respect to AS and thus is contained in Ψ. As Ψ_{AS} is a finite basis of Ψ, G is a linear combination of polynomials is Ψ_{AS} with polynomial coefficients. It follows that any extended zero of Ψ_{AS} is also an extended zero of G or that Ψ_{AS} is an irreducible polynomial set with $\bar{\eta}$ as a generic point.

Although Hilbert's basis theorem is existential, there are methods such as those described in Ritt (1932, 1950), van der Waerden (1945) and Wu (1986b, 1989b) for determining prime bases from irreducible ascending sets. However, these methods are all somewhat complicated. Below we present a method, which is based on the computation of Gröbner bases and appears to be rather simple as it is, for the exact determination of such prime bases. The method was discovered independently by the author (Wang, 1989c) and Chou, Schelter & Yang (1990) and it can also be considered as an application of Gröbner's Primbasissatz (Gröbner, 1949) and the trick of Gianni, Trager and Zacharias (1988).

Let *AS* be an ascending set and suppose the variables $x_1, \ldots, x_n$ have been changed to $u_1, \ldots, u_d, y_1, \ldots, y_r$ so that *AS* is of the form (5.2). Denote as usual the initial of each A_i by $I_i = I_i(u_1, \ldots, u_d, y_1, \ldots, y_{i-1})$. We want to determine a finite set Ψ_{AS} of polynomials that forms an irreducible algebraic variety with any generic point of *AS* as its generic point. For this purpose, we form a new set of polynomials

$$BS \quad \begin{array}{l} B_1 = z_1 \cdot I_1(u_1, \ldots, u_d) - 1, \\ B_2 = z_2 \cdot I_2(u_1, \ldots, u_d, y_1) - 1, \\ \quad \cdots\cdots \\ B_r = z_r \cdot I_r(u_1, \ldots, d_d, y_1, \ldots, y_{r-1}) - 1, \end{array}$$

where $z_1, \ldots, z_r$ are r newly introduced variables. Fix the ordering of all the variables as

$$u_1 \prec \cdots \prec u_d \prec y_1 \prec \cdots \prec y_r \prec z_1 \prec \cdots \prec z_r$$

and denote the union of *AS* and *BS* by *US*, i.e., $US = \{A_1, \ldots, A_r, B_1, \ldots, B_r\}$. Clearly, *US* is still an irreducible ascending set in $\boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r, z_1, \ldots, z_r]$. Again, let $\bar{\Psi}$ be the ideal generated by all polynomials of *US* in $\boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r, z_1, \ldots, z_r]$, i.e., $\bar{\Psi} = \mathrm{Ideal}(US)$. Our method is based on the following quite simple theorem.

Theorem 8.1 (Wang, 1989c)
Let Ψ and $\bar{\Psi}$ be as above. If AS is irreducible, then

$$\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r] = \Psi.$$

Proof. Let F be any polynomial in $\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$. On the one hand, F may be expressed as a linear combination of polynomials of *US*, so $F = 0$ is a formal consequence of $US = 0$. Since *US* is irreducible, F has remainder 0 with respect to *US*. On the other hand, as $F \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ and thus contains none of $z_1, \ldots, z_r$, the remainder of F with respect to *BS* is itself. Hence F has remainder 0 with respect to *AS* and thus belongs to Ψ.

Conversely, if F is any polynomial in Ψ, then we have the following remainder formula

$$I_1^{s_1} \cdots I_r^{s_r} \cdot F = \sum_{i=1}^{r} Q_i A_i,$$

in which the integers $s_i \geq 0$ and $Q_i \in \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$. Multiplying the above formula by $J = z_1^{s_1} \cdots z_r^{s_r}$ and using the equalities in *BS*, we obtain immediately the following representation

$$(8.1) \qquad (B_1 + 1)^{s_1} \cdots (B_r + 1)^{s_r} \cdot F = \sum_{i=1}^{r} R_i A_i,$$

where $R_i = Q_i J$. Expanding the powers $(B_i + 1)^{s_i}$ and products on the left-hand side and moving all terms except F to the right-hand side, we would have an expression of the form

$$(8.2) \qquad F = \sum_{i=1}^{r} R_i A_i + \sum_{i=1}^{r} T_i B_i,$$

where all T_i are polynomials in $\boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r, z_1, \ldots, z_r]$. Therefore, F is contained in $\bar{\Psi}$.

Clearly, F involves the variables $u_1, \ldots, u_d, y_1, \ldots, y_r$ only. Hence, F belongs to $\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$. This completes the proof of Theorem 8.1. ■

From this theorem, to determine the prime basis of AS we need only to find those generators of $\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$. This can be done by computing the Gröbner basis of US.

Lemma 8.2 (Buchberger, 1985)
Let GB be a Gröbner basis of US with respect to the purely lexicographical ordering of power products determined by $u_1 \prec \cdots \prec u_d \prec y_1 \prec \cdots \prec y_r \prec z_1 \prec \cdots \prec z_r$. *Then*

$$\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r] = \mathrm{Ideal}(GB \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]),$$

where the ideal on the right-hand side is formed in $\boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$.

Therefore, those elements in the Gröbner basis GB of US which involve the variables $u_1, \ldots, u_d, y_1, \ldots, y_r$ only form the prime basis Ψ_{AS} of AS, i.e., $\Psi_{AS} = GB \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$. If we add all polynomials of AS to Ψ_{AS} and denote the enlarged polynomial set by Ψ_{AS}^{+}, then Ψ_{AS}^{+} will define the same variety as that defined by Ψ_{AS} with AS as its characteristic set.

Based on the previous discussions the irreducible decomposition of an algebraic variety can now be achieved with ease. Let V be any variety with defining set PS. By computing the irreducible characteristic series, we may decompose PS into a sequence of ascending sets CS_i so that PS has an irreducible decomposition of the form (5.1). For each CS_i, by the method introduced above we can determine a finite set Ψ_{CS_i} of polynomials which form an irreducible variety with any generic point of the ascending set as its generic point. Clearly, any zero of such a finite set of polynomials is also a zero of the polynomial set PS, so we obtain a decomposition of the form

$$\text{(8.3)} \qquad \mathrm{Zero}(PS) = \bigcup_{i=1}^{e} \mathrm{Zero}(\Psi_{CS_i}).$$

Letting the irreducible variety defined by Ψ_{CS_i} be V_i, we have accomplished an equivalent decomposition of the algebraic variety V as follows

$$\text{(8.4)} \qquad V = V_1 \cup \cdots \cup V_e.$$

Note that this decomposition may be contractible, that is, some variety may be a subvariety of the other (and thus can be simply removed). As noted in Remark 5.4, we may first remove some redundant branches during the computation of irreducible characteristic series as long as possible. According to the affine dimension theorem in algebraic geometry (Hartshorne, 1978), the dimension of an irredundant component of V should not be less than $n - s$, where n is the number of variables and s the number of polynomials in PS. Therefore, if the numbers of polynomials in CS_i is greater than s, then Ψ_{CS_i} must define a true subvariety of V and need not be computed at all. This fact can thus be used to remove some redundant varieties in the decomposition (cf. Chou & Gao, 1990b). The following lemma gives a criterion for canceling all redundant varieties in order to get a non-contractible irreducible decomposition.

Lemma 8.3 (Wu, 1984a, 1984b)
Let a variety V with its defining set PS be irreducible and PS have its irreducible characteristic set CS. If PS' is an arbitrary polynomial set and any polynomial in PS' has remainder 0 with respect to CS, then the variety V is a subvariety of V' defined by PS'.

Proof. Since any polynomial G' in PS' has remainder 0 with respect to CS, the generic point of CS or the generic point of V is an extended zero of PS'. Therefore G' vanishes on $\mathrm{Zero}(PS)$. It follows that $\mathrm{Zero}(PS) \subset \mathrm{Zero}(PS')$, i.e., V is a subvariety of V'. ■

Then, the method for decomposing a variety into irreducible components described above can be stated in the form of the following

Theorem 8.2 (Wang, 1989c)
The algorithm below decomposes any algebraic variety V into irreducible components $V_1, \ldots, V_e$, where the input PS is the defining set of V and the output Ψ is the set of defining sets of the irreducible varieties $V_1, \ldots, V_e$.

IrreducibleVarietyDecomposition(Input: PS; Output: Ψ)

  $\Phi :=$ IrreducibleCharacteristicSeries(PS)
  $\Psi := \emptyset$
  for all $CS \in \Phi$ do
    $r :=$ the number of polynomials in CS
    $I_i =$ the initial of the ith polynomial in CS
    $QS := CS \cup \{z_i I_i - 1 | \; 1 \leq i \leq r\}$
    $GB :=$ the Gröbner basis of QS wrt the lexical ordering determined by
      $x_1 \prec \cdots \prec x_n \prec z_1 \prec \cdots \prec z_r$
    $GS := \{G | \; G \in GB, G \in \boldsymbol{K}[x_1, \ldots, x_n]\}$
    $\Psi := \Psi \cup \{GS\}$
  while $\exists GS, GS' \in \Psi$ such that $\{R | \; R =$ PseudoRemainder(G',
      CharacteristicSet(GS)), $G' \in GS', R \neq 0\} = \emptyset$ do
    $\Psi := \Psi \setminus \{GS\}$

Note that the characteristic set of GS in the second line from the bottom, which is already contained in Ψ, should not be recomputed.

Remark 8.1
From the proof of Theorem 8.1, it is easy to see that, in the case AS is reducible, the inclusion relation

$$\Psi \subset \bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$$

still holds. Let us denote the finite basis of $\bar{\Psi} \cap \boldsymbol{K}[u_1, \ldots, u_d, y_1, \ldots, y_r]$ by Ψ_{AS}. Then

$$\mathrm{Zero}(\Psi_{AS}) \subset \mathrm{Zero}(\Psi) \subset \mathrm{Zero}(PS).$$

Hence, for a certain ascending set CS_i in decomposition (5.1), no matter whether it is irreducible or not, we can always determine a finite basis Ψ_{CS_i} using the same method, but there is no guarantee for $\mathrm{Zero}(\Psi_{CS_i}) = \mathrm{Zero}(\Psi)$. However, if $\mathrm{Zero}(\Psi_{CS_i})$ is simply equal to $\mathrm{Zero}(CS_i)$, then any zero of CS_i which even makes some initials vanish is still a zero of PS. Therefore, the corresponding polynomial set enlarged from PS by adjoining J_i to it is then unnecessary to be further considered and $\mathrm{Zero}(CS_i/J_i)$ in the decomposition can be simply replaced by $\mathrm{Zero}(CS_i)$.

Remark 8.2
As the computational expenses for both characteristic sets and Gröbner bases depend strongly upon the ordering of variables. Some optimal ordering should be considered. First, one could choose an appropriate order for x's so as to get an irreducible decomposition of the polynomial set into ascending sets. Secondly, to use Lemma 8.2 we need only to arrange the variables such that the x's are lower than the z's, no matter how the order of x's and the order of z's are.

In forming the polynomial set BS, $I_1, \ldots, I_r$ may of course be replaced by any choice of polynomials $H_1, \ldots, H_t$ which are such that $H_1 \cdots H_t = 0$ if and only if $I_1 \cdots I_r = 0$.

Example 8.1
The algebraic variety V is defined by the following set of three polynomials

$$PS \quad \begin{array}{l} F_1 = -3x_3x_4 + x_2^2 - 2x_1 + 2, \\ F_2 = -3x_1^2x_4 - 4x_2x_3 - 6x_1x_3 + 2x_2^2 + 3x_1x_2, \\ F_3 = -3x_3^2x_4 - x_1x_4 + x_2^2x_3 + x_2. \end{array}$$

Then PS may be decomposed into 2 irreducible ascending sets CS_1 and CS_2 such that

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS_1/2x_2 + 3x_1^2) \cup \mathrm{Zero}(CS_2/x_2),$$

where

$$\begin{aligned} CS_1 = \{&2x_2^4 + 8x_2^2x_1 - 8x_2^2 - 12x_1^2x_2^3 + 24x_1^3x_2 - 24x_1^2x_2 - 9x_1^4x_2^2 + 18x_1^5 \\ &- 18x_1^4 + 9x_2^3x_1, -x_2^2 + 2x_3x_2 + 3x_3x_1^2, 2x_2x_4 - 2x_2^2 - 3x_1x_2 + 3x_4x_1^2\}, \\ CS_2 = \{&x_1, -x_2 + 2x_3, -4 + 3x_2x_4 - 2x_2^2\}. \end{aligned}$$

To obtain an irreducible decomposition of V, we determine the prime bases of CS_1 and CS_2 using the method described above. By computing the Gröbner basis GB_1 of $CS_1 \cup \{z_1(2x_2+3x_1^2)-1\}$ and GB_2 of $CS_2 \cup \{x_2z_1 - 1\}$, we find that they consist of 8 and 4 polynomials, respectively. The three polynomials involving only the variable $x_1, \ldots, x_4$ in GB_2 are the same as those in CS_2. Let us denote the polynomial set consisting of all polynomials, 7 in number, involving $x_1, \ldots, x_4$ only in GB_1 by VS_1, viz,

$$\begin{aligned} VS_1 = \{&2x_2^4 + 8x_2^2x_1 - 8x_2^2 - 12x_1^2x_2^3 + 24x_1^3x_2 - 24x_2x_1^2 - 9x_1^4x_2^2 + 18x_1^5 \\ &- 18x_1^4 + 9x_2^3x_1, \\ &- 12x_1^2 + 9x_2^2x_1 - 8x_2 - 15x_1^2x_2^2 - 27x_3x_1^3 + 2x_2^3 + 12x_1^3 + 8x_1x_2 + 27x_1^4x_3, \\ &- x_2^2 + 2x_3x_2 + 3x_3x_1^2, 12x_3^2x_1 - 12x_3^2 - 9x_3x_1^2 - 2x_2^2x_1 + 3x_2^2 - 4x_1 + 4x_1^2, \\ &- x_4x_1 + 2x_1x_3 - 2x_3 + x_2, -x_2x_4 - 3x_3x_1^2 + 3x_1x_3 + x_2^2, \\ &x_2^2 - 2x_1 - 3x_3x_4 + 2\}. \end{aligned}$$

Then VS_1 defines an irreducible variety with any generic point of CS_1 as its generic point. If we add the last polynomial of CS_1 to VS_1 and denote the enlarged polynomial set by VS_1^+, then VS_1^+ clearly has CS_1 as its characteristic set. Let the algebraic varieties defined by VS_1 and CS_2 be V_1 and V_2 respectively. V is then decomposed into two irreducible components V_1 and V_2. One can check with ease that this decomposition is non-contractible. ■

For this example, to decompose PS into irreducible ascending sets we need to factorize polynomials only over the rational number field rather than over its algebraic extension fields, since the second and third polynomials in the characteristic set of PS are linear in x_3 and x_4, respectively. This phenomenon, i.e., all polynomials other than the first in the characteristic set are linear in their leading variables, happens often as mentioned in Remark 5.2. Nevertheless, the example discussed throughout the paper is not due to this case. Let us consider it again.

Example 8.2
The algebraic variety V is defined by a set of three polynomials F_1, F_2, F_3 shown in Examples 3.1-5.2.

As the ascending sets CS_1', CS_1'', CS_2' and CS_2'' all have constant initials, they constitute by themselves irreducible algebraic varieties. To determine finite bases for CS_3 and CS_4, we compute the Gröbner bases of $CS_3 \cup \{z \cdot x_1 - 1\}$ and $CS_4 \cup \{z \cdot x_1 - 1\}$ respectively, and find easily that in both cases the polynomials involving the variables $x_1, \ldots, x_4$ only in the corresponding bases are themselves. Therefore, the irreducible decomposition of V is obtained immediately, in which four true subvarieties CS_1', CS_1'', CS_2' and CS_2'' can be removed. ■

9. Applications

The author is going to write a survey on the applications of the characteristic set method as a sequel of this paper. In this section only some of the applications are briefly indicated. For more details the reader may consult the forthcoming paper and the original publications and preprints.

Mechanical Geometry Theorem Proving

Research in this area has been initiated by Wu since 1978 when he discovered his algebraic method (Wu, 1984a, 1984b). An important observation made by Wu is that, in various (elementary) geometries, most of the theorems involve only axioms of incidence, parallelism and congruence but no axioms of order and continuity in Hilbert's axiomatic system. The standard geometric relations such as *collinearity, perpendicularity* and *equidistance* can all be algebraized, by introducing number systems and coordinate systems, so that both the hypothesis and the conclusion of a theorem may be given by systems of polynomial equations in certain geometric entities as variables. To prove a theorem, it suffices to decide whether the conclusion of the theorem is a formal consequence of the hypothesis, i.e., whether all zeros of the algebraic equations corresponding to the hypothesis are zeros of the algebraic equations corresponding to the conclusion. Usually this is not the case because most geometric theorems are true only generically. Thus, in the case of geometry, one needs first to find some non-degenerate conditions† and decide under these conditions whether the inference relations hold. This is a geometric version of the algebraic decision problem. For solving this problem Wu employed the characteristic set method described in the previous sections with a particular emphasis on determining non-degenerate conditions and proving non-trivial theorems. Wu's method is very efficient in practice and has been used for proving a large number of theorems in elementary geometries (see Wu, 1984a, 1984b, Chou, 1988, Kutzler, 1989, Wang & Gao, 1987 and references therein). Some new theorems have also been discovered (Chou, 1988, Wang, 1989a).

Mechanical Derivation of Unknown Relations and Locus Equations

The method of characteristic sets together with Wu's general theory of mechanical theorem proving can be applied to derive and discover unknown geometric relations and locus equations (Wu, 1986c, Chou, 1987, Chou & Gao, 1989, Wang, 1991d). A simple yet typical example is the mechanical derivation of Heron's formula‡ (the algebraic representation of the area of a triangle in terms of its three sides). The basic idea of deriving such unknown relations and locus equations is to first arrange carefully the variables among which the relations should exist with a lower order, then formulate the geometry hypotheses into algebraic expressions in order to obtain a set of polynomial equations. By well-ordering the corresponding polynomial set, one would get certain polynomials in the characteristic set involving only those variables among which the relations are intended to be found. Thus, the vanishing of these polynomials constitutes the relations that one wants to derive.

Solving Systems of Algebraic Equations

As ascending sets are of special form, a direct yet very important application of the characteristic set method is solving systems of algebraic equations. From the zero decompositions, we see that, for any given set of algebraic equations one can decide whether or not it has only a finite number of solutions. If so, one can compute successively all those rational solutions accurately by using Gauss' lemma and simple substitutions and all those real and complex solutions approximately by methods of numerical iteration from the triangular forms. If the given system has infinitely

† Pointing out precisely the non-degenerate conditions and the difference between geometric statements and algebraic formulation is an important contribution of Wu to the completeness and rigor of theorem proving in geometry.

‡ A similar formula appeared also in the Chinese classical book *Shu Shu Jiu Zhang* (Mathematical Treatise in Nine Sections) by Qin Jiu-Shao in 1247. As a consequence, this formula was named as *Qin-Heron formula* by Wu (1986c).

many solutions (i.e., it is of positive dimension), one can decompose the algebraic variety given by its zero set into irreducible components and determine the dimension of each component. The illustrative examples given in Wu (1986a, 1986e, 1987b, 1988, 1990b) have shown the efficiency of the characteristic set method for solving algebraic equations. Some systematic experiments on the performance of this method have been reported in Wang (1991c, 1992c). Other work on this subject include Liu (1989, 1990a, 1990b), Gao & Chou (1992), Wu (1989c, 1989e) and Wu (1991).

Polynomial Factorization and Decomposition

On the one hand, the theoretical development of the characteristic set method requires polynomial factorization, in particular, over algebraic extension fields which is thought difficult in general. On the other hand, the characteristic set method can also be applied to polynomial factorization over any extension field. This, however, does not cause recursive use of the method, for the latter has no requirement on the irreducibility of characteristic sets. There are two methods, based on the computation of characteristic sets, for polynomial factorization over algebraic extension fields proposed in Hu & Wang (1986) and Wang (1992a) respectively. The idea of the first method is to form a system of algebraic equations by using the "undetermined coefficient" technique and then find a set of rational function solutions to the system by computing characteristic series and using Gauss' lemma. This idea can also be generalized to compute the decomposition of unary polynomials (Wang, 1987a). Experiments show that this method is feasible only for polynomials of small degree, however. The second method, which is more efficient than the first one, proceeds by reducing polynomial factorization over an algebraic extension field to factorization over the rational number field via linear transformation and the computation of characteristic sets with respect to a proper variable ordering. The factors over the algebraic extension field are finally determined via GCD (greatest common divisor) computation.

Constructive Algebraic Geometry

Modern algebraic geometry is mainly of existential feature and pays no attention to the exact construction of geometric objects. Nonetheless, for practical applications the constructive aspects which were the major theme of classical algebraic geometry should be of first importance. Even Ritt's work aims basically at investigating algebraic differential equations, his theory and method provide an effective tool for the study of constructive algebraic geometry. This tool has been recognized and greatly developed by Wu since 1978. Current research in this field includes dimension theory of algebraic varieties (Wu, 1984a, 1984b), singularities of algebraic hypersurfaces (Wang, 1989d) and irreducible decomposition of algebraic varieties as presented in Section 8.

Discriminant Systems and Singularities of Algebraic Hypersurfaces

Discriminants have been widely used for determining the existence of multiple roots of unary polynomials. The notion of discriminants was extended to discriminant systems in Gao (1987) for studying the multiplicity of roots, and the characteristic set method was employed for the exact computation of such systems. In Wang (1989d) discriminants as well as discriminant systems of multivariate polynomials are introduced to determine the necessary and sufficient conditions for the existence of singularities of any multiplicity of algebraic hypersurfaces (in particular, algebraic curves and algebraic surfaces), where the characteristic set method is again employed for carrying out the exact computation. Furthermore, if an algebraic hypersurface has singular points, then the method can be used to find all such points when they are finite, and to compute an irreducible decomposition of the singular variety otherwise (cf. Wang 1989d, 1991d).

Implicitization of Parametric Objects

Some geometric objects like curves and surfaces can be algebraically represented either by implicit equations or by parametric equations. The advantage of each representation depends upon the type of problems to be treated. In geometric modeling, one often needs to convert one representation into the other. The method of characteristic sets together with a projection theorem of quasi-varieties can be applied to the determination of implicit equations from the parametric equations (see Wu, 1990a, Li, 1989, Chou, Gao & Li, 1991, Wang, 1991d).

Definiteness of Polynomials and Proving Inequalities

Although Wu's general method cannot deal with theorems whose algebraic expressions involve inequalities, some additional effort has made the method applicable for determining definiteness of multivariate polynomials and proving certain inequalities. Such applications are reported in Wu (1984b, 1988), Wang (1987b) and Chou, Gao & Arnon (1990). These approaches are based on some modification of and combination with the decision procedures for real closed fields, the use of Lagrangian multiplier technique and the resolution of polynomial equations.

Complex Root Isolation

A method for isolating complex roots of a unary polynomial has been proposed in Liu (1987) on the basis of the characteristic set method. The first step of this method is to substitute the real representation of a complex variable into the unary complex polynomial, then equate the real part and imaginary part to 0 so as to get a set of two polynomials in two real variables. The second step is to triangulate such a polynomial set twice with different order of variables by the well-ordering principle and get two unary real polynomials. The isolation of complex roots is finally achieved by isolating the real roots of these two polynomials, respectively.

Qualitative Problems of Differential Equations

One important tool for studying qualitative problems of differential equations is Liapunov's second method (i.e., studying the behavior of trajectories of differential equations by determining the Liapunov functions and LaSalle's invariant sets). Many problems in this area can be reduced to problems about the zero structure of polynomial sets, algebraic decision and algebraic simplification. The applications of the characteristic set method to deal with two classes of such problems have been reported (Wang, 1987a, 1989b, 1991a, Liu, Lu & Wang, 1989, 1991). For one class, the method is applied to simplify the Liapunov constants, which can be computed by an algorithm procedure, and to establish the algebraic relations among the Liapunov constants and relations between them and other given conditions, where a family of existing results have been checked to be incomplete. For the other class, the method is applied to derive the necessary conditions for LaSalle's invariant sets to contain non-constant periodic solutions for Lotka-Volterra prey-predator chain systems.

Proving by Examples

The method of proving-by-examples was introduced by J. W. Hong (1986a, 1986b) and extended later by this author (Wang, 1988) based on the method of characteristic sets and Wu's theory of geometry theorem proving. The extension of this method in another direction was made by J. Z. Zhang and L. Yang (see Yang, 1988). Using this method, to prove a geometric theorem one needs only to prove it to be true for some concrete examples by numerical computation. The method appears quite graceful in theory but it does not seem to be efficient enough for proving non-trivial theorems. Further exploration of the method from practical aspects still remains for research.

Others

There are several other applications of the characteristic set method, for example, to solving transcendental equations (Wu & Wu, 1989), proving Khovanskii's finiteness theorem (Richardson, 1991) and the pole assignment of linear control systems (Shi, 1989, 1990). It appears that the method of characteristic sets has its superiority for attacking various geometry-related problems. Since geometry is so fundamental in such active areas as computer vision, robotics, computer aided design and geometric modeling, the power of the characteristic set method in geometry problem solving should lead to a number of significant applications in geometry engineering. Some of these applications have been reported (Mundy, 1986, Swain & Mundy, 1986, Kapur, 1988, Wang, 1991d). For areas in which the characteristic set method might find potential applications, we want to mention, in addition to those we have mentioned, the theory of algebraic invariants, synthetic geometry, computational geometry, polynomial ideal theory, the theory of transcendental functions and constraint logic programming.

10. Implementations and Complexity

Most of the existing implementations of the characteristic set method are made for the special purpose of mechanical theorem proving in geometries and do not have wide availability. Such implementations include the China-Prover by Wu (1984a, 1984c) and the systems CPS, PS and DPMS by Wang & Gao (1987) in Fortran, the GEO-prover by Chou (1988) and the ALGE-prover by Ko & Hussain (1985) in Macsyma, the prover GPP by Kusche, Kutzler & Stifter (1989) in SAC-2 and Scratchpad II, the GEO-prover by Alberti et al. and the GEOPROVER by Kanchanasut & Nam in Mathematica and the G-prover by Gao et al. in C on an IBM PC/386. Wu (1986d) also implemented a SOLVER based on his method for solving systems of algebraic equations. Different pieces of code have been written by individuals for various applications of the method, mainly in geometries. A few polynomial equations solvers based on characteristic sets have also been developed recently. All the above mentioned implementations are incomplete due to the lack of complete routines for polynomial factorization over successive algebraic extension fields.

A complete, general-purpose package for the characteristic set method, called CharSets,† has been implemented in Maple by this author (Wang, 1995). It contains functions with possible variants (an implementation of most of the algorithms described in the previous sections by taking many of the remarks into account) for computing characteristic sets, characteristic series and irreducible characteristic series of polynomial sets, decomposing algebraic varieties into irreducible components, factorizing polynomials over algebraic extension fields and solving systems of polynomial equations. Based on this package, a complete geometry theorem prover GEOTHER (Wang, 1990b) and several application routines have also been implemented. The author has recently learned that an implementation of the method in Reduce is ongoing at the University of Bath and the others in Scratchpad II by M. C. Gontard and in Lisp by S. C. Chou and X. S. Gao.

The practical complexity of the characteristic set method has been analyzed through a large number of experimental examples, in particular, for geometry theorem proving (Wang & Gao, 1987, Chou, 1988, Kutzler, 1989) and for polynomial equations solving (Wang, 1991c, 1992c). There are rather few results on the theoretical complexity of this method. It has been proved in Gallo & Mishra (1991) that the degrees of polynomials in a characteristic set are bounded by a simple exponential function of n, and a characteristic set may be computed in $O(s^{O(n)}d^{O(n^3)})$ sequential and $O(n^7 \log^2(s+d))$ parallel time complexity by using effective Nullstellensatz, where n, s and d are the number of variables, the number and the degree bound of input polynomials, respectively. Gallo and Mishra also derived some degree bounds and time complexities for the computation of pseudo-remainders and the verification of geometric theorems.

References

It is not our intention to give an exhaustive bibliography on the method of characteristic sets and its applications. In particular, we have omitted a number of relevant papers whose scope is much on the subject of mechanical geometry theorem proving. The references listed below were chosen mainly for our presentation of the materials and the author apologizes for being unable to mention all significant papers.

† This package has been available in the Maple share library since January 1991. The Maple code for its first version can be obtained via anonymous FTP at two sites: 129.132.101.33 (neptune) ETH Zurich, Switzerland and 129.97.128.58 (daisy) University of Waterloo, Canada. The interested reader may also contact the author for an up-to-date version of the package.

Boyer, C. B. (1968). *A History of Mathematics.* New York: John Wiley & Sons.

Buchberger, B. (1965). *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Ph.D thesis, Universität Innsbruck, Austria.

Buchberger, B. (1985). Gröbner bases: an algorithmic method in polynomial ideal theory. In: (N. K. Bose, ed.) *Multidimensional Systems Theory*, pp. 184–232. Dordrecht-Boston-Lancaster: D. Reidel Publishing Company.

Chou, S. C. (1987). A method for the mechanical derivation of formulas in elementary geometry. *J. Automated Reasoning* **3**, 291–299.

Chou, S. C. (1988). *Mechanical Geometry Theorem Proving.* Dordrecht-Boston-Lancaster: D. Reidel Publishing Company.

Chou, S. C. and Gao, X. S. (1989). Mechanical formula derivation in elementary geometries. *Technical Report* TR-89-21, Dept. Comput. Sci., University of Texas at Austin, USA.

Chou, S. C. and Gao, X. S. (1990a). Ritt-Wu's decomposition algorithm and geometry theorem proving. *Proc. 10th Int. Conf. Automated Deduction* (Kaiserslautern, 1990), *Lecture Notes Comput. Sci.* **449**, pp. 207–220. Berlin-New York: Springer-Verlag.

Chou, S. C. and Gao, X. S. (1990b). Techniques for Ritt-Wu's decomposition algorithm. *MM Research Preprints No.* 5, 88–111. Academia Sinica, China.

Chou, S. C., Gao, X. S. and Arnon, D. S. (1990). On the mechanical proof of geometry theorems involving inequalities. In: (Ch. Hoffmann et al. eds.) *Issues in Robotics and Non-linear Geometry.* JAI Press, to appear.

Chou, S. C., Gao, X. S. and Li, Z. M. (1991). Computations with rational parametric equations. *MM Research Preprints No.* 6, 56–78. Academia Sinica, China.

Chou, S. C., Schelter, W. F. and Yang, J. G. (1990). An algorithm for constructing Gröbner bases from characteristic sets and its application to geometry. *Algorithmica* **5**/2, 147–154.

Collins, G. E. (1967). Subresultants and reduced polynomial remainder sequences. *J. ACM* **14**, 128–142.

Gallo, G. and Mishra, B. (1991). Efficient algorithms and bounds for Wu-Ritt characteristic sets. *Proc. MEGA'90, Progress in Math.* **94**, pp. 119–142. Boston: Birkhäuser.

Gao, X. S. (1987). The discriminant systems of unary equations and their computation. *MM Research Preprints No.* 1, 13–32. Academia Sinica, China.

Gao, X. S. and Chou, S. C. (1992). Solving parametric algebraic systems. *Proc. ISSAC '92* (Berkeley, July 27–29, 1992), pp. 335–341.

Gauss, C. F. (1873). *Werke.* Band IV, Herausgegeben von der Königlichen Gesellschaft der Wissenshaft zu Göttingen.

Gianni, P., Trager, B. and Zacharias, G. (1988). Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Computation* **6**, 149–167.

Gröbner, W. (1949). *Moderne Algebraische Geometrie.* Wien-Innsbruck: Springer-Verlag.

Hartshorne, R. (1978). *Algebraic Geometry.* Berlin-New York: Springer-Verlag.

Hilbert, D. (1956). *Grundlagen der Geometrie*, Achte Auflage. Stuttgart: B. G. Teubner Verlagsgesellschaft.

Hodge W. V. D. and Pedoe, D. (1947/1952). *Methods of Algebraic Geometry*, Vol. I, II. Cambridge: Cambridge University Press.

Hong, J. W. (1986a). Can we prove geometry theorems by computing an example? *Sci. Sinica* **29**, 824–834.

Hong, J. W. (1986b). Proving by example and gap theorems. *Proc. 27th Ann. Symp. Foundations of Computer Science* (FOCS), pp. 107–116. Washington: IEEE Comput. Soc. Press.

Hu, S. and Wang, D. M. (1986). Fast factorization of polynomials over rational number field or its extension fields. *Kexue Tongbao* **31**, 150–156.

Kalkbrener, M. (1991). *Three Contributions to Elimination Theory.* Ph.D thesis, RISC-LINZ, Johannes Kepler University, Austria.

Kapur, D. and Mundy, J. L. (1988). Wu's method and its application to perspective viewing. *Artificial Intelligence* **37**, 15–26.

Ko, H. P. (1988). Geometry theorem proving by decomposition of quasi-algebraic sets: An application of the Ritt-Wu principle. *Artificial Intelligence* **37**, 95–122.

Ko, H. P. and Hussain, M. A. (1985). ALGE-prover: An algebraic geometry theorem proving software. *Technical Report* 85CRD139, General Electric Company, Schenectady, USA.

Kusche, K., Kutzler, B. and Stifter, S. (1989). Implementation of a geometry theorem proving package in Scratchpad II. *Proc. EUROCAL'87* (J. Davenport, ed.), pp. 246–257. Heidelberg: Springer-Verlag.

Kutzler, B. (1988). *Algebraic Approaches to Automated Geometry Theorem Proving.* Ph.D thesis, RISC-LINZ, Johannes Kepler University, Austria.

Li, Z. M. (1987). On the triangulation for any finite polynomial set (I). *MM Research Preprints No.* 2, 48–54. Academia Sinica, China.

Li, Z. M. (1988). Determinant polynomial sequence. *Kexue Tongbao* **38**/18, 1369–1372 (in Chinese).

Li, Z. M. (1989). Automatic implicitization of parametric objects. *MM Research Preprints No.* 4, 54–62. Academia Sinica, China.

Liu, L., Lu, Z. Y. and Wang, D. M. (1989). Mechanical manipulation for LaSalle's invariant sets of Lotka-Volterra systems. *RISC-LINZ Series no.* 89-52.0. Johannes Kepler University, Austria.

Liu, L., Lu, Z. Y. and Wang, D. M. (1991). The structure of LaSalle's invariant set of Lotka-Volterra systems. *Sci. China Ser. A* **34**, 783–790.

Liu, Z. J. (1987). A method of isolating complex roots of polynomials — An application of Wu-Ritt principle. *Chinese Quart. J. Math.* **3**/4, 101–108.

Liu, Z. J. (1989). An algorithm on finding all isolated zeros of polynomial equations. *MM Research Preprints No.* 4, 63–76. Academia Sinica, China.

Liu, Z. J. (1990a). On the characteristic set of elementary symmetric polynomial systems. *MM Research Preprints No.* 5, 30–38. Academia Sinica, China.

Liu, Z. J. (1990b). On one Ulam's fixed point problem. *MM Research Preprints No.* 5, 39–46. Academia Sinica, China.

Mundy, J. (1986). Reasoning about 3-D space with algebraic deduction. *Robotics Research: The third international symposium*, pp. 117–124. Cambridge-London: The MIT Press.

Needham, J. (1959). *Science and Civilisation in China*, Vol. 3. Cambridge: Cambridge University Press.

Richardson, D. (1991). Wu's method and the Khovanskii finiteness theorem. *J. Symbolic Computation* **12**/2, 127–141.

Ritt, J. F. (1932). *Differential Equations from the Algebraic Standpoint.* New York: Amer. Math. Soc.

Ritt, J. F. (1950). *Differential Algebra.* New York: Amer. Math. Soc.

Shi, H. (1989). The pole assignment of linear systems. *MM Research Preprints No.* 4, 87–103. Academia Sinica, China.

Shi, H. (1990). The robustness of pole assignment. *MM Research Preprints No.* 5, 56–65. Academia Sinica, China.

Swain, M. J., Mundy, J. L. (1986). Experiments in using a theorem prover to prove and develop geometrical theorems in computer vision. *Proc. 1986 IEEE Int. Conf. Robotics and Automation*, pp. 280–285. Washington: IEEE Comput. Soc. Press.

Sylvester, J. J. (1904). *The Collected Mathematical Papers*, Vol. I. Cambridge: Cambridge University Press.

van der Waerden, B. L. (1945). *Einführung über Algebraische Geometrie.* New York: Dover Publications.

Wang, D. M. (1987a). *Mechanical Approach for Polynomial Set and its Related Fields.* Ph.D thesis, Academia Sinica, China (in Chinese).

Wang, D. M. (1987b). A decision method for definite polynomials. *MM Research Preprints No.* 2, 68–74. Academia Sinica, China.

Wang, D. M. (1988). Proving-by-examples method and inclusion of varieties. *Kexue Tongbao* **33**, 1121–1123.

Wang, D. M. (1989a). A new theorem discovered by computer prover. *J. Geometry* **36**, 173–182.

Wang, D. M. (1989b). Computer algebraic methods for investigating plane differential systems of center and focus type. In: (E. Kaltofen and S. M. Watt, eds.) *Computers & Mathematics*, pp. 91–99. New York-Berlin: Springer-Verlag.
419–424.

Wang, D. M. (1989c). A method for determining the finite basis of an ideal from its characteristic set with application to irreducible decomposition of algebraic varieties. *MM Research Preprints No.* 4, 124–140. Academia Sinica, China.

Wang, D. M. (1989d). On the singularities of algebraic hypersurfaces — The discriminant systems. *Preprint.* School of Math. Scis., Queen Mary College, University of London, England.

Wang, D. M. (1989e). A generalization of characteristic sets algorithm. *RISC-LINZ Series no.* 89-51.0. Johannes Kepler University, Austria.

Wang, D. M. (1990a). A note on the termination of zero decomposition algorithms. *MM Research Preprints No.* 5, 112–115. Academia Sinica, China.

Wang, D. M. (1990b). Some notes on algebraic methods for geometry theorem proving. *Preprint.* RISC-

LINZ, Johannes Kepler University, Austria. Presented at Medlar 12-Month Workshop (Weinberg Castle, Austria, November 4–7, 1990).

Wang, D. M. (1991a). Mechanical manipulation for a class of differential systems. *J. Symbolic Computation* **12**/2, 233–254.

Wang, D. M. (1991b). On the parallelization of characteristic-set-based algorithms. *Proc. 1st Int. Conf. ACPC* (Salzburg, September 30 – October 2, 1991), LNCS **591**, 338–349.

Wang, D. M. (1991c). On Wu's method for solving systems of algebraic equations. *RISC-Linz Series no.* 91-52.0. Johannes Kepler University, Austria.

Wang, D. M. (1991d). Reasoning about geometric problems using algebraic methods. *Proc. MEDLAR 24-Month Workshop* (Grenoble, December 8–11, 1991), Department of Computing, Imperial College, University of London, UK.

Wang, D. M. (1992a). A method for factorizing multivariate polynomials over successive algebraic extension fields. *Preprint.* RISC-LINZ, Johannes Kepler University, Austria.

Wang, D. M. (1992b). A strategy for speeding-up the computation of characteristic sets. *Proc. 17th Int. Symp. Math. Foundations of Comput. Sci.* (Prague, August 24–28, 1992), LNCS **629**, 504–510.

Wang, D. M. (1992c). Some improvements on Wu's method for solving systems of algebraic equations. *Proc. Int. Workshop on Math. Mechanization* (Beijing, July 16–18, 1992), 89–100.

Wang, D. M. (1995). An implementation of the characteristic set method in Maple. *Automated Practical Reasoning: Algebraic Approaches* (J. Pfalzgraf and D. Wang, eds.), pp. 187–201. Wien-New York: Springer-Verlag.

Wang, D. M. and Gao, X. S. (1987). Geometry theorems proved mechanically using Wu's method — Part on Euclidean geometry. *MM Research Preprints No.* 2, 75–106. Academia Sinica, China.

Wu, T. J. (1991). Some test problems on applications of Wu's method in nonlinear programming problems. *MM Research Preprints No.* 6, 144–155. Academia Sinica, China.

Wu, W. T. (1978). On the decision problem and the mechanization of theorem-proving in elementary geometry. *Sci. Sinica* **21**, 159–172. Also in: Automated Theorem Proving: after 25 years. *Contemp. Math.* **29**(1984), 213–234.

Wu, W. T. (1984a). Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. & Math. Scis.* **4**, 207–235. Also: *J. Automated Reasoning* **2**(1986), 221–252.

Wu, W. T. (1984b). *Basic Principles of Mechanical Theorem Proving in Geometries (Part on elementary geometries).* Beijing: Science Press (in Chinese). English translation by X. F. Jin and D. M. Wang. Wien-New York: Springer-Verlag (1994).

Wu, W. T. (1984c). Some recent advances in mechanical theorem-proving of geometries. *Contemp. Math.* **29**, 235–241.

Wu, W. T. (1986a). On zeros of algebraic equations — An application of Ritt principle. *Kexue Tongbao* **31**, 1–5.

Wu, W. T. (1986b). A mechanization method of geometry I. Elementary geometry. *Chinese Quart. J. Math.* **1**, 1–14.

Wu, W. T. (1986c. A mechanization method of geometry and its applications I. Distances, areas and volumes. *J. Sys. Sci. & Math. Scis.* **6**, 204–216.

Wu, W. T. (1986d). A general description of the SOLVER software system. *Math. Practice & Theory No.* 2, 32–39 (in Chinese).

Wu, W. T. (1986e). Examples of the application of the SOLVER software system. *Math. Practice & Theory No.* 3, 1–11 (in Chinese).

Wu, W. T. (1987a). Recent studies of the history of Chinese mathematics. *Proc. Int. Congress Math.* (Berkeley, 1986), pp. 1657–1667. New York: Amer. Math. Soc.

Wu, W. T. (1987b). A zero structure theorem for polynomial equations-solving. *MM Research Preprints No.* 1, 2–12. Academia Sinica, China.

Wu, W. T. (1988). A mechanization method of geometry and its applications III. Mechanical proving of polynomial inequalities and equations-solving. *Systems Sci. Math. Sci.* **1**/1, 1–17.

Wu, W. T. (1989a). Some remarks on characteristic-set formation. *MM Research Preprints No.* 3, 27–29. Academia Sinica, China.

Wu, W. T. (1989b). On the generic zero and Chow basis of an irreducible ascending set. *MM Research Preprints No.* 4, 1–21. Academia Sinica, China.

Wu, W. T. (1989c). A mechanization method of geometry and its applications IV. Some theorems in planar kinematics. *Systems Sci. Math. Sci.* **2**/2, 97–109.

Wu, W. T. (1989d). On the foundation of algebraic differential geometry. *Systems Sci. Math. Sci.* **2**/4, 289–312.

Wu, W. T. (1989e). A mechanization method of geometry and its applications VI. Solving inverse kinematic equations of PUMA-type robots (a sketch). *MM Research Preprints No.* 4, 49–53. Academia Sinica, China.

Wu, W. T. (1990a). On a projection theorem of quasi-varieties in elimination theory. *Chinese Ann. Math. Ser. B* **11**/2, 220–226.

Wu, W. T. (1990b). On the chemical equilibrium problem and equations-solving. *Acta Math. Sci.* **10**/4, 361–374.

Wu, W. T. (1991). On a linear equations method of non-linear polynomial equations-solving. *MM Research Preprints No.* 6, 23–36. Academia Sinica, China.

Wu, W. T. and Wu, T. J. (1989). A mechanization method of geometry and its applications V. Solving transcendental equations by algebraic methods. *MM Research Preprints No.* 3, 30–32. Academia Sinica, China.

Yang, L. (1988). A new method of automated theorem proving. *Research Report* CMA-R45-88. Centre for Math. Analysis, The Australian National University, Australia.