In: **Journal of Automated Reasoning**, 10:161–172,1993.

Automated Reasoning in Differential Geometry and Mechanics Using the Characteristic Set Method[1]

Part I. An Improved Version of Ritt–Wu's Decomposition Algorithm

Shang-Ching Chou
Department of Computer Science
The Wichita State University
Wichita, KS 67208, USA

Xiao-Shan Gao
Institute of Systems Science
Academia Sinica
Beijing 100080, P.R. China

Abstract

This is the first paper of a series of three papers under the same title. It presents an improved version of Ritt–Wu's decomposition algorithm which is the basis of our methods of mechanical theorem proving and mechanical formula derivation in differential geometry and elementary mechanics. We improve the original algorithm in two aspects. First, by using the weak ascending chain and W–prem, the sizes of the differential polynomials occurring in the decomposition can be reduced. Second, by using a special reduction procedure, the number of branches in the decomposition can be controlled effectively. The improved version enhances the efficiency of the original algorithm significantly.

Keywords Differential polynomial, weak ascending chain, W–prem, Ritt–Wu's principle, quasi zero set, Ritt–Wu's decomposition algorithm.

1. Introduction

In the past decade, highly successful algebraic methods for mechanically proving theorems in *elementary* geometries have been developed. Notably, the method introduced by Wu Wen-Tsün in [13] has been used to prove hundreds of hard theorems in Euclidean geometry and non-Euclidean geometries [2, 12]. Inspired by Wu's work, methods of mechanical theorem proving in elementary geometries using the Gröbner basis method have been also introduced [6, 7, 8].

Wu's method is based on the characteristic set (CS) method, an idea due to van der Waerden in algebraic case [11], and has been developed by J. F. Ritt to a systematical method in algebraic geometry and differential algebra [9, 10]. In [14, 15], Wu proposed a method for proving theorems in differential geometry using Ritt's CS method. The present three papers are a further development of Wu's work. The papers are a refinement of our two technical reports [3, 4]. Several new results obtained later are also included. The main contributions of the papers can be summarized as follows:

- (1) In the first paper, we present an improved version of Ritt–Wu's decomposition algorithm which enhances the efficiency of the original version significantly. The algorithm is the basis of our methods and implementation.
- (2) In the second paper, we clarify the formulation problem of mechanical theorem proving in differential geometry and mechanics and propose two formulations. The complete method of mechanical theorem proving for each formulation is introduced. We also present a method of eliminating existential quantifiers in certain cases and a language to translate geometry

[1]The work reported here was supported in part by the NSF Grant CCR-8702108.

statements into differential polynomials equations. A program based on our method has proved more than 100 nontrivial theorems in differential geometry and mechanics, including Bertrand's theorem, Mannheim's theorem, Newton's gravitational laws, etc.

- (3) In the third paper, methods for mechanical derivation of formulas from a set of differential polynomial equations and a set of differential polynomial inequations have been presented. The methods have been used successfully to solve many problems in space curve theory and mechanics. In particular, an automated derivation of Newton's gravitational law from Kepler's laws has been given without knowing Newton's laws in advance. We also give a partial method to derive polynomial relations from a set of differential polynomial equations.

1.1. Introduction to Ritt–Wu's Decomposition Algorithm

The basis of the methods of mechanical theorem proving and mechanical formula deriving in the case of differential polynomials is Ritt–Wu's zero decomposition algorithm which takes two differential polynomial sets as input and decomposes the *quasi algebraic set* defined by the two differential polynomial sets into a union of irreducible quasi algebraic sets. The algorithm was introduced by Ritt in his classic book *Differential Algebra* [10] as an effective method to construct the irreducible components of a *differential manifold*. Recently, Wu made several modifications to Ritt's algorithm such as using the quasi algebraic set instead of the algebraic set and proposed a method of mechanical theorem proving in differential geometry based on the modified algorithm [16].

In our experience, we find Wu's version of the decomposition algorithm is still time and space consuming, and in many cases makes the CS method beyond the computer time and space limits available. The main problems in the algorithm are: (1) The size growth of the differential polynomials occurring in the decomposition; (2) The large number of branches. In this paper, we present an improved version of Ritt–Wu's decomposition algorithm which can overcome the above two difficulties. A program based on this improved version of the decomposition algorithm is efficient and has mechanically proved more than 100 nontrivial theorems in differential geometry and elementary mechanics.

To overcome the size growth difficulty, we extend the concepts of weak ascending chain and W–prem for ordinary polynomials presented in [5] to the case of differential polynomials. The idea here is to reduce the number of pseudo divisions carried out in the procedure. Our branch control method is based on a special use of quasi algebraic sets and certain special reduction procedure. A new version of Ritt–Wu's decomposition algorithm with these improvements is presented in detail.

The completeness of Wu's original method of mechanical theorem proving is based on the construction of some extension of the base field, which is different for different geometry statements to be proved. [2] instead uses the concept of algebraic closed field and the concept of universally true. A geometry statement is universally true iff it is true on any extension field of the base field and the decision of the universally true only depends on the existence of an algebraic closed extension of the base field. In this paper, we along the line of [2] to present the completeness of the method, since the existence of the similar concept of algebraic closed field – differential closed field – has been proved in [1].

The main contribution of the paper is the introduction of the weak asc chain in section 3 and a branch control technique in section 4. We use these new techniques to the well known Ritt-Wu's decomposition algorithm to give an improved version of the algorithm. Our implementation of the decomposition algorithm based on the improved version is the first complete implementation.

The paper is organized as follows. In section 2, we give a brief review of some known notions

and notations. In section 3, we introduce the new concept of weak ascending chains and W-prem. In section 4, we present the improved decomposition algorithm. In section 5, we discuss differential closed extensions of differential fields.

2. Preliminaries

All the concepts in this section come from [10] or [16].

A differential field is a field together with a third (unary) differential operation $'$ satisfying:

$$(a+b)' = a' + b' \qquad (ab)' = a'b + ab'.$$

Generally, we can work with a computable differential field K of characteristic zero. But for our purpose of theorem proving, in what follows, we assume that K is the rational function field $\mathbf{Q}(t)$ in the variable t and all the derivations are with respect to (ab. wrpt) t, i.e., $' = d/dt$. A differential field E is called an extension field of K if E is an extension field of K in the usual sense and the restriction of the differentiation of E on K is the same as the differentiation of K.

Let $x_1, ..., x_n$ be indeterminates. The j-th ($j \geq 0$) derivative of a variable x_i is denoted by $x_{i,j}$. Thus $x_i = x_{i,0}$, $(x_i)' = x_{i,1}$, etc. An ordinary polynomial P in variables $x_{i,j}$ and with coefficients in K is called *a differential polynomial* (ab. d-pol) in $x_1, ..., x_n$. We denote the set of all the d-pols in $x_1, ..., x_n$ by $K\{x_1, ..., x_n\} = K\{X\}$.

A non-empty subset D of $K\{X\}$ is called *an ideal* if for any $g \in D$, we have (i) $f \in D \Rightarrow f+g \in D$; (ii) $f \in K\{X\} \Rightarrow fg \in D$; and (iii) $g' \in D$. An ideal D is called *a prime ideal* if $fg \in D \Rightarrow f \in D$ or $g \in D$ for any f and g in $K\{X\}$. An ideal D is called *a radical ideal* if $f^n \in D \Rightarrow f \in D$ for any $f \in K\{X\}$ and a positive integer n. Let S be a non-empty set in $K\{X\}$, the minimal ideal D containing S is called the *ideal generated* by S and denoted by $Ideal(S)$. Obviously, $Ideal(S)$ is the set of all linear combinations of the d-pols in S and their derivatives.

Definition 2.1. Class and Order. Let P be a d-pol. The *class* of P, denoted by $class(P)$, is the least p such that $P \in K\{x_1, ..., x_p\}$. If $P \in K$, $class(P) = 0$. The *order* of P wrpt x_i, denoted by $ord(P, x_i)$, is the largest j such that $x_{i,j}$ appears in P. If P does not involve x_i, we put $ord(P, x_i) = -1$. Let a d-pol P be of class $p > 0$ and $q = ord(P, x_p)$, then x_p and $x_{p,q}$ are called the *leading variable* and the *lead* of P.

Definition 2.2. Rank. Let P_1 and P_2 be two d-pols, we say P_2 is of *higher rank* than P_1 in x_i, if either $ord(P_2, x_i) > ord(P_1, x_i)$ or $q = ord(P_2, x_i) = ord(P_1, x_i)$ and P_2 is of higher degree in $x_{i,q}$ than P_1. P_2 is said to be of *higher rank* than P_1, denote by $P_2 > P_1$, if either $class(P_2) > class(P_1)$ or $p = class(P_2) = class(P_1)$ and P_2 is of higher rank than P_1 in x_p. Two d-pols for which no difference in rank is established by the foregoing criterion are said to be of the same rank.

Definition 2.3. Initial and Separant. If the lead of P is $x_{p,m}$ with $p > 0$, P can be written as

$$P = a_d x_{p,m}^d + a_{d-1} x_{p,m}^{d-1} + \cdots + a_0$$

where the a_i are d-pols of lower rank than $x_{p,m}$. Then $a_d \neq 0$ is called the *initial* of P and denoted by $int(P)$. The derivation of P is

$$P' = S x_{p,m+1} + a_d' x_{p,m}^d + a_{d-1}' x_{p,m}^{d-1} + \cdots + a_0'$$

where $S = \frac{\partial P}{\partial x_{p,m}} = d a_d x_{p,m}^{d-1} + ... + a_1$ is called the *separant* of P and denoted by $sep(P)$. Note that P' is linear in $x_{p,m+1}$ with S as initial.

Definition 2.4. Pseudo remainder. Let $x_{p,m}$ ($p > 0$), I, and S be the lead, initial, and separant of a d-pol P respectively. For any d-pol G, we shall define the *pseudo remainder* of G wrpt P:

prem(G, P) as below. Let $h = ord(G, x_p)$ and $k_1 = h - m$. If $k_1 > 0$ then $P^{(k_1)}$, the k_1-th derivative of P, will be linear in $x_{p,h}$ with S as initial. Treating G and $P^{(k_1)}$ as ordinary polynomials of $x_{p,h}$ and using the algorithm of pseudo division for ordinary polynomials (see, [10]) for G and $P^{(k_1)}$, we can find the smallest nonnegative integer v_1 and d-pols C_1 and D_1 such that:

$$S^{v_1}G = C_1P^{(k_1)} + D_1$$

where $ord(D_1, x_p) < h$ as $P^{(k_1)}$ is linear in $x_{p,h}$. If $ord(D_1, x_p) > m$, we repeat the above process for D_1 and P, and so on. Finally we can find a nonnegative integer v and d-pols Q_i such that:

$$S^vG = Q_1P^{(k_1)} + \cdots + Q_sP^{(k_s)} + D$$

where $ord(D, x_p) \leq m$. If $ord(D, x_p) < m$, we define prem$(G, P) = D$. Otherwise, both D and P can be viewed as ordinary polynomials of $x_{p,m}$. Using the algorithm of pseudo division of ordinary polynomials (see [10]) for D and P, we have

$$S^vI^uG = Q'_1P^{(k_1)} + \cdots + Q'_sP^{(k_s)} + QP + R \tag{2.4.1}$$

where R is a d-pol with lower rank than P in x_p. We define $R =$ prem(G, P).

As an example, let us show how to calculate prem(q_2, q_1) for $q_2 = x'_3 + x_3$ and $q_1 = x_3^2 + x_2^2 - x_1^2$.

$q'_1 = 2x_3x'_3 + 2x_2x'_2 - 2x_1x'_1$	The differentiation of q_1.
$q_3 = 2x_3q_2 - q'_1 = 2x_3^2 - 2x_2x'_2 + 2x_1x'_1$	Pseudo division of q_2 by q'_1.
$q_4 = q_3 - 2q_1 = 2x_1x'_1 - 2x_2x'_2 + 2x_1^2 - 2x_2^2$	Pseudo division of q_3 by q_1.

Then $q_4 =$ prem(q_2, q_1). We have $Sq_2 = q'_1 + 2q_1 + q_4$, where $S = 2x_3$ is the separant of q_1.

Definition 2.5. Quasi ascending chain. A sequence of d-pols $ASC = A_1, ..., A_p$ is said to be a *quasi ascending (*ab. *asc) chain*, if either $p = 1$ and $A_1 \neq 0$ or $0 < class(A_i) < class(A_j)$ for $1 \leq i < j$. ASC is called *nontrivial* if $class(A_1) > 0$.

A quasi asc chain $ASC = A_1, ..., A_p$ is said to be of *higher rank* than another quasi asc chain $ASC' = B_1, ..., B_s$, denoted by $ASC > ASC'$, if either (i) there is a j, exceeding neither p nor s, such that A_i and B_i are of the same rank for $i < j$ and that A_j is of higher rank than B_j; or (ii) $s > p$ and A_i and B_i are of the same rank for $i \leq p$. Two quasi asc chains for which no difference in rank is established by the foregoing criterion are said to be of the same rank.

Lemma 2.6. (P. 4 [10]) Let

$$ASC_1, ASC_2, ..., ASC_i, ...$$

be an infinite sequence of quasi asc chains the ranks of which do not increase. Then there is an index i_0 such that for any $i > i_0$, ASC_i and ASC_{i_0} have the same rank.

For a nontrivial quasi asc chain $ASC = A_1, ..., A_p$, we define the pseudo remainder of G wrpt ASC inductively as prem$(G, ASC) =$ prem$($prem$(G, A_p), A_1, ..., A_{p-1})$. Let $R =$ prem(G, ASC), then by (2.4.1) there is a product J of powers of the initials and separants of d-pols in ASC such that

$$JG - R \in Ideal(A_1, ..., A_p). \tag{2.7}$$

(2.7) is called the *remainder formula* of prem(G, ASC). For a quasi asc chain ASC, we introduce the following important notation

$$PD(ASC) = \{G \mid G \in K\{X\} \text{ and } \text{prem}(G, ASC) = 0\}.$$

Definition 2.8. Quasi zero set. For a set of d-pols HS and an extension field E of K, we define

$$\text{E-Zero}(HS) = \{z \in E^n : \forall P \in HS, P(z) = 0, \}$$

Let DS be another set of d-pols, the *quasi zero set* defined by HS and DS is

$$\text{E-Zero}(HS/DS) = \text{E-Zero}(HS) - \cup_{r \in DS}\text{E-Zero}(r).$$

Definition 2.9. Asc chain and irreducible asc chain. Let $ASC = A_1, ..., A_p$ be a quasi asc chain. ASC is called an *asc chain* if for each $1 < i \leq p$, A_i is of lower rank than A_j in the leading variable of A_j $(j = 1, ..., i-1)$. An asc chain ASC is said to be *irreducible* if ASC is irreducible as a polynomial asc chain (p107 [10]).

Theorem 2.10. (p.107 [10]) If ASC is an irreducible asc chain then $PD(ASC)$ is a prime ideal.

Theorem 2.11. (p.97 and p.107, [10]) If the asc chain $ASC' = A_1, ..., A_{p-1}$ is irreducible and the asc chain $ASC = A_1$, ..., A_{p-1}, A_p is reducible, then we can find nonzero d-pols G and F with the same lead as A_p but with lower rank than A_i in the leading variable of A_i, $i = 1, ..., p$, such that $GF \in Ideal(A_1, ..., A_p)$.

Definition 2.12. Dimension and order of an asc chain. For a quasi asc chain $ASC = A_1, ..., A_p$, we always make a renaming of the variables. If A_i is of class m_i, we rename x_{m_i} as y_i, other variables among x_i are renamed as $u_1, ..., u_q$, where $q = n - p$. The variables $u_1, ..., u_q$ are called *the parameter set* of ASC. If ASC is irreducible, $DIM(ASC) = q = n - p$ is defined to be the *dimension* of ASC and $ORD(ASC) = \sum_{i=1}^{p} ord(A_i, y_i)$ is defined to be the *order of ASC wrpt to the given parameter set*. $DIM(ASC)$ and $ORD(ASC)$ are actually the dimension and order of the prime ideal $PD(ASC)$ respectively [10].

3. The Weak Ascending Chains and W–prem

In this section, we introduce the notions of weak ascending chain and W–prem which are the key concepts in our improved algorithm.

Definition 3.1. Weak asc chain. Let $ASC = A_1, ..., A_p$ be a quasi asc chain. It is called a *weak asc chain*, if for each i $(1 < i \leq p)$ the pseudo remainders of the initial and separant of A_i wrpt $A_1, ..., A_{i-1}$ are not zero.

Definition 3.2. W–prem. For a d-pol P and a nontrivial quasi ascending chain $ASC = A_1, ..., A_p$, W-prem(P, ASC) can be defined inductively as follows. We assume W-prem$(P, \emptyset) = P$.

- Case a. We put W–prem(P, ASC) = W–prem(prem$(P, A_p), A_1, ..., A_{p-1}$) if $class(P) = class(A_p)$. Otherwise do Case b.
- Case b. W–prem(P, ASC) = W–prem$(P, A_1, ..., A_{p-1})$ if $class(P) < class(A_p)$. Otherwise do Case c.
- Case c. W–prem(P, ASC) = prem(P, ASC), if the pseudo remainder of the separant or the initial of P wrpt ASC is zero. Otherwise do Case d.
- Case d. W–prem$(P, ASC) = P$.

If W–prem$(P, ASC) = P$, we say P is *W–reduced* wrpt ASC. It is easy to see that W–prem(P, ASC) is always W–reduced wrpt ASC and a quasi asc chain $ASC = A_1, ..., A_p$ is a weak asc chain if each A_i is W–reduced wrpt $A_1, ..., A_{i-1}$.

Lemma 3.3. For a differential polynomial P and a weak ascending chain $ASC = A_1, ..., A_p$, if W–prem$(P, ASC) = 0$ then prem$(P, ASC) = 0$.

Proof. Use induction on p. It is obvious when $p = 1$. Suppose $p > 1$. There are four cases a–d. For case a, if prem$(P, A_p) = 0$ then the lemma is true; otherwise the lemma comes from the induction hypothesis. Case b is trivial. For case c, the lemma is also true because W–prem(P, ASC) = prem(P, ASC). In case d, W–prem$(P, ASC) \neq 0$. Then the lemma is obviously true in this case. ∎

Lemma 3.4. Let ASC_1 be a quasi asc set and ASC_2 be an irreducible asc chain. If the pseudo remainders of the d-pols in ASC_1 wrpt ASC_2 are zero and the pseudo remainders of the initials and separants of the d-pols in ASC_1 wrpt ASC_2 are not zero, then $PD(ASC_1) \subset PD(ASC_2)$.

Proof. By Theorem 2.10, $PD(ASC_2)$ is a prime ideal. We have $ASC_1 \subset PD(ASC_2)$ and $J \notin PD(ASC_2)$ where J is any product of the separants and initials of the d-pols in ASC_1. Let $P \in PD(ASC_1)$, then there exists a product J_1 of the separants and initials of the d-pols in ASC_1 such that $J_1 P \in Ideal(ASC_1)$. Therefore, we have $J_1 P \in PD(ASC_2)$. Then $P \in PD(ASC_2)$ as J_1 is not in $PD(ASC_2)$. ∎

Theorem 3.5. For a nontrivial weak asc chain $ASC = A_1, ..., A_p$, let $ASC' = A'_1, ..., A'_p$ where $A'_1 = A_1$ and $A'_i = \text{prem}(A_i, A_1, ..., A_{i-1})$ $(i = 2, ..., p)$. Then either (a) we can find two nonzero d-pols G and H which are W–reduced wrpt ASC such that $HG \in Ideal(ASC)$, or (b) ASC' is an irreducible asc chain and $PD(ASC) = PD(ASC')$.

Proof. Induction on p. If $p = 1$, the result is obviously true. Assuming the result is true for $p = k - 1$, we want to prove the result is true for $p = k$. By the induction hypothesis, either (a) or (b) is true for $ASC_{k-1} = \{A_1, ..., A_{k-1}\}$. If (a) is true for ASC_{k-1}, then (a) is also true for ASC_k. Now we suppose (b) is true for ASC_{k-1}, i.e., $ASC'_{k-1} = \{A'_1, ..., A'_{k-1}\}$ is irreducible and $PD(ASC_{k-1}) = PD(ASC'_{k-1})$ is a prime ideal. Note that $A'_k = \text{prem}(A_k, A_1, ..., A_{k-1})$, then by (2.7), we have

$$A'_k - JA_k \in Ideal(ASC_{k-1}) \subset PD(ASC_{k-1}) \tag{3.6}$$

where J is a product of the initials and separants of $A_1, ..., A_{k-1}$. Since ASC is a weak asc chain, A'_k and A_k have the same lead and the same degree wrpt the lead. Thus ASC' is an asc chain. If ASC' is reducible, then by theorem 2.11, we can find non-zero d-pols H and G which are W–reduced wrpt ASC' (hence also to ASC) such that $HG \in Ideal(ASC')$. By (3.6), we have $HG \in Ideal(ASC)$. In this case, (a) is true. Now we assume ASC' is irreducible. As ASC is a weak asc chain, the pseudo remainders of the initial and separant of A_k wrpt ASC_{k-1}, hence wrpt ASC'_{k-1}, are not zero. By (3.6), the pseudo remainder of A_k wrpt ASC' is zero. Thus $PD(ASC) \subset PD(ASC')$ follows from Lemma 3.4 and the induction hypothesis. The reverse direction also comes from Lemma 3.4 since $A'_i \in PD(ASC)$ and the initials and separants of A'_i are W-reduced wrpt ASC_i. ∎

In case (b) of Theorem 3.5, we say that the *weak asc chain ASC is irreducible*. Notice that it is incorrect to say that a weak asc chain is irreducible if it is irreducible as a polynomial asc chain.

4. An Improved Ritt–Wu's Zero Decomposition Algorithm

In what follows, whenever we talk about a finite set of d-pols, we always assume it is non-empty and does not contain 0.

Lemma 4.1. For a finite d-pol set HS, we can find a weak asc chain ASC in HS which is not higher than other weak asc chains in HS. Such a weak asc chain is called a *weak basic set* of HS.

Proof. Let B_1 be a d-pol which has the lowest rank in $P_0 = HS$. If B_1 is in K then the asc chain B_1 satisfies the condition of the lemma. Otherwise, the class of B_1 is positive. Let P_1 be the set of

the d-pols in P_0 which are W–reduced wrpt B_1. If P_1 is empty, then B_1 satisfies the condition of the lemma. Otherwise, let B_2 be a d-pol of the lowest rank in P_1. Then B_2 must be of higher class than B_1. Repeat the above process, at last we get a weak asc chain $B_1, B_2, ..., B_k$ with the desired property. ∎

Lemma 4.2. If a nonzero d-pol P is W–reduced wrpt a weak basic set of HS, then a weak basic set of $HS \cup \{P\}$ is of lower rank than a weak basic set of HS.

Proof. Let $BS = B_1, ..., B_p$ be a weak basic set of HS and k be the largest index such that $class(B_k) < class(P)$. If $class(B_{k+1}) > class(P)$ then $B_1, ..., B_k, P$ will be a weak asc chain contained in $HS \cup \{P\}$ which has lower rank than BS. Otherwise, $class(B_{k+1}) = class(P)$. As P is W–reduced to BS then P must be of lower rank than B_{k+1} by (a) of Definition 3.2. Then $B_1, ..., B_k, P$ is a weak asc chain contained in $HS \cup \{P\}$ which is of lower rank than BS. ∎

Lemma 4.3. (A modified Ritt–Wu's Principle) For a finite set HS of d-pols, we can find either a nonzero d-pol $P \in K \cap Ideal(\text{HS})$ or a nontrivial weak asc chain ASC and an enlarged d-pol set HS' of HS such that:

(a) ASC is a weak basic set of HS'.
(b) E-Zero(HS) = E-Zero(HS').
(c) E-Zero(HS) = E-Zero$(ASC/J) \bigcup \cup_{1 \le i \le t}$E-Zero$(HS' \cup \{h_i\}/\{h_1, ..., h_{i-1}\})$.
(d) E-Zero(HS) = E-Zero$(PD(ASC)) \bigcup \cup_{1 \le i \le t}$E-Zero$(HS' \cup \{h_i\}/\{h_1, ..., h_{i-1}\})$.

where $J = \{h_1, ..., h_t\}$ is the set of the initials and separants of the d-pols in ASC.

Proof. Let BS_0 be a weak basic set of HS. If $BS_0 = \{B_1\}$ and $B_1 \in K$ then $B_1 \in K \cap Ideal(HS)$. We have proved the lemma. Otherwise, let RS be the nonzero W–prem(g, BS_0) for all $g \in HS - BS_0$. If RS is empty, let $ASC = BS_0$ and $HS' = HS$. (a) and (b) are obviously true. (c) comes from the remainder formula (2.7) (for details see [3]). (d) comes from (c) and (2.7). If RS is not empty, we set $HS_1 = HS \cup RS$. Since $RS \subset Ideal(HS)$, HS and HS_1 have the same zeros. By Lemma 4.2, HS_1 has a weak basic set BS_1 with lower rank than BS_0. Repeating the above process for HS_1 and so on, we either get a d-pol $P \in K \cap Ideal(HS)$ or get a sequence of d-pol sets which have the same zeros

$$HS \subset HS_1 \subset \cdots$$

and a sequence of nontrivial, strictly decreasing weak asc chains:

$$BS_0 > BS_1 > \cdots$$

By Lemma 2.6, the above iteration must terminate in finite steps, i.e., there is an i_0 such that W–prem$(G, BS_{i_0}) = 0$ for all $G \in HS_{i_0}$. Then Let $ASC = BS_{i_0}$ and $HS' = HS_{i_0}$. (a) and (b) are obviously true. (c) and (d) come from the remainder formula (2.7). ∎

Remark. Note that by changing the original version of Ritt–Wu's principle to the above form, each two of the zero sets in the right side of (c) have no common zeros. This is our *major technique in branch control*.

Theorem 4.4. (Ritt–Wu's Zero Decomposition Algorithm: the Coarse Form) Let HS and DS be two finite sets of d-pols, then in a finite number of steps, we can either detect the emptiness of E-Zero(HS/DS) or furnish a decomposition of the following forms:

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{l} \text{E-Zero}(ASC_i/DS \cup J_i) * \quad (4.4.1)$$
$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{l} \text{E-Zero}(PD(ASC_i)/DS) \quad (4.4.2)$$

where for each $i \le l$, ASC_i is a weak asc chain such that prem$(P, ASC_i) \neq 0$ for $\forall P \in DS$ and J_i is the set of initials and separants of the d-pols in ASC_i.

Proof. Let ASC_1 and HS_1 be the weak asc chain and the enlarged d-pol set obtained from HS as in Lemma 4.3. If ASC_1 is trivial, E-Zero(HS/DS) is empty. Otherwise, compute the pseudo remainders of the d-pols in DS wrpt to ASC_1. If one of them is zero, E-Zero$(ASC_1/DS \cup J_1)$ is empty, where $J_1 = \{h_1, ..., h_t\}$ is the initial and separant set of ASC_1. Thus, by (c) of Lemma 4.3, we have

$$\text{E-Zero}(HS/DS) = \cup_{1 \le i \le t} \text{E-Zero}(HS' \cup \{h_i\}/DS \cup \{h_1, ..., h_{i-1}\}).$$

Otherwise, we have

$$\begin{aligned} &\text{E-Zero}(HS/DS) = \text{E-Zero}(ASC_1/DS \cup J_1) \\ &\bigcup \cup_{1 \le i \le t} \text{E-Zero}(HS' \cup \{h_i\}/DS \cup \{h_1, ..., h_{i-1}\}) \end{aligned}$$

For each $h_i \in J_1$, let $h_i' = \text{W–prem}(h_i, ASC_1)$. We have

$$\text{E-Zero}(HS_1 \cup \{h_i, h_i'\}) = \text{E-Zero}(HS_1 \cup \{h_i\}).$$

Repeating the above process for $HS_1 \cup \{h_i, h_i'\}$, we get another weak asc chain ASC_2. Since $\text{prem}(h_i, ASC_1) \neq 0$, h_i' is not zero by lemma 3.3. Hence ASC_2 must be of lower rank than ASC_1 by lemma 4.2. By Lemma 2.6, the above process must terminate within a finite number of steps and we will get a decomposition like

$$\text{E-Zero}(HS/DS) = \cup_{i=1}^{l} \text{E-Zero}(ASC_i/DS \cup J_i \cup DS_i)$$

Since W–prem$(g, ASC_i) = 0$ for all $g \in HS$, DS_i can be dropped and we get a decomposition as (4.4.1). (4.4.2) can be obtained similarly. ∎

Theorem 4.5. (Ritt–Wu's Zero Decomposition Algorithm: the Refined Form) The same as Theorem 4.4, except the ASC_i in (4.4.1) and (4.4.2) are irreducible.

Proof. Similar to the proof of Theorem 4.4, let ASC_1 and HS_1 be the weak asc chain and the enlarged d-pol set obtained from HS as in Lemma 4.3. If ASC_1 is irreducible or trivial, then do the same decomposition as Theorem 4.4. Otherwise, by Theorem 3.5, we can find two non-zero d-pols G and F which are W–reduced wrpt ASC_1 such that $GF \in Ideal(ASC_1)$. We have:

$$\text{E-Zero}(HS/DS) = \text{E-Zero}(HS_1 \cup \{F\}/DS) \cup \text{E-Zero}(HS_1 \cup \{G\}/DS)$$

We can repeat the above process for $HS_1 \cup \{F\}$ and $HS_1 \cup \{G\}$. As F and G are W–reduced wrpt ASC_1, each weak basic set of $HS_1 \cup \{F\}$ or $HS_1 \cup \{G\}$ must be of lower rank than ASC_1. Thus the process will terminate at a finite number of steps. ∎

In our implementation, the following facts are used to enhance the efficiency of the program.

(i). For a d-pol set HS and d-pols f and g, it is obvious that

$$\text{E-Zero}(HS \cup \{fg\}) = \text{E-Zero}(HS \cup \{f\}) \cup \text{E-Zero}(HS \cup \{g\}).$$

Since f and g have less degree and generally less size than fg, the decomposition of $HS \cup \{f\}$ and $HS \cup \{g\}$ is generally easier to carry out than $HS \cup \{fg\}$.

(ii). In Theorem 4.4, when each new weak asc chain ASC and an enlarged set HS' of HS are produced, we check whether there are some d-pols in DS which can be reduced to zero by $HS_1 = \{f, f' : f \in HS'\}$ using the reduction procedure used in Gröbner bases method when all the d-pols in DS and HS_1 are treated as ordinary polynomials of $x_{i,j}$. If such a d-pol exists then E-Zero(HS/DS) is empty.

5. Some Properties of Differential Closed Field

A differential field E is called *differential closed* if each nonunit ideal in $E\{x_1, \cdots, x_n\}$ has zeros in E^n.

Lemma 5.1. For an extension field E of K, the following statements are equivalent:

(a) E is a differential closed extension of K.

(b) Let $G, F_1, ..., F_s$ be d-pols in $K\{X\}$. If G vanishes on the E-zeros of $F_1, ..., F_s$, then a power of G is in $Ideal(F_1, \cdots, F_s)$.

(c) For a radical ideal D in $K\{X\}$, D equals the set of the d-pols vanishing on E-Zero(D).

Proof. (a) $\Rightarrow$ (b). Let z be a new variable. As G vanishes on all E-zeros of $F_1, ..., F_s$, the ideal $D = Ideal(F_1, ..., F_s, zG - 1)$ has no E-zero. By (a), 1 is in D, i.e., 1 is a linear combination of the F, $zG - 1$ and their derivatives, with d-pols in $K\{x_1, ..., x_n, z\}$ as coefficients. Set $z = 1/G$ in this expression and clear the denominators. Note that $z' = -G'/G^2, z'' = (2G'^2 - G''G)/G^3, ...$ Therefore, some power of G can be expressed as linear combination of the F and their derivatives. This proves (b). The proof of (b) $\Rightarrow$ (c) and (c) $\Rightarrow$ (a) is trivial. ∎

From [1], we know that for a differential field K of characteristic zero, there always exists a differential closed extension of K. The completeness of our methods of mechanical theorem proving in the differential polynomial case is based on the following theorem.

Theorem 5.2. Let ASC be an irreducible weak asc chain and R be a d-pol with nonzero pseudo remainder wrpt ASC. Then for a differential closed extension E of K, a nonzero d-pol G vanishes on E-Zero($PD(ASC)/R$) iff $\text{prem}(G, ASC) = 0$.

Proof. The if part is obvious. As ASC is irreducible, $PD(ASC)$ is a prime ideal. Since G vanishes on E-Zero($PD(ASC)/R$), GR vanishes on E-Zero($PD(ASC)$). Then $GR \in PD(ASC)$ by lemma 5.1 (c), because a prime ideal is a radical ideal. Since R is not in $PD(ASC)$, we have $G \in PD(ASC)$, i.e., $\text{prem}(G, ASC) = 0$. ∎

Acknowledgement. We thank one of the refrees for informing us a better way of doing pseudo divisions.

References

[1] L. Blum, Differentially Closed Fields: a Model-Theoretic Tour, pp 37–62, *Contributions to Algebra*, (H.Bass et al ed.), Academic Press, New York, 1977.

[2] S.C. Chou, *Mechanical Geometry Theorem Proving,* D.Reidel Publishing Company, 1988.

[3] S.C. Chou and X.S. Gao, Mechanical Theorem Proving in Differential Geometry, I. Space Curves, TR-89-08, Computer Sciences Department, The University of Texas at Austin, March 1989.

[4] S.C. Chou and X.S. Gao, Automated Reasoning In Mechanics Using Ritt-Wu's Method, TR-89-11, Computer Sciences Department, The University of Texas at Austin, April, 1989.

[5] S.C. Chou and X.C. Gao, Ritt–Wu's Decomposition Algorithm and Geometry Theorem Proving, *CADE'10*, M.E. Stickel (Ed.) pp 207–220, Lect. Notes in Comp. Sci., No. 449, Springer-Verlag, 1990.

[6] S.C. Chou and W.F. Schelter, Proving Geometry Theorem with Rewrite Rules, *J. of Automated Reasoning* 2(4), 253-273.

[7] D. Kapur, Geometry Theorem Proving Using Hilbert's Nullstellensatz, *Proc. of SYMSAC'86*, Waterloo, 1986, 202–208.

[8] B. Kutzler and S. Stifter, Automated Geometry Theorem Proving Using Buchberger's Algorithm, Proc. of SYMSAC'86, Waterloo, 1986, 209–214.

[9] Ritt, J.F., *Differential Equations From the Algebraic Standpoint*, Amer. Math. Soc. Colloquium, vol 14, New York, 1932.

[10] Ritt, J.F., *Differential algebra*, Amer. Math. Sco. Colloquium, (1950).

[11] van der Waerden, Mathematische Annalen, vol. 96(1927), p.189.

[12] D.M. Wang and X.S. Gao, Geometry Theorems Proved Mechanically Using Wu's Method, Part on Elementary Geometries, MM preprint No. 2, 1987.

[13] Wu Wen-tsün, On the Decision Problem and the Mechanization of Theorem in Elementary Geometry, Scientia Sinica 21(1978), 159 –172; Re-published in Automated Theorem Proving: After 25 years, American Mathematics Society, Contemporary Mathematics, 29(1984), 213–234.

[14] Wu Wen-tsün, Mechanical Theorem Proving In Elementary Differential Geometry, Scientia Sinica, Mathematics Supplement (I), 1979, 94–102. (in Chinese)

[15] Wu Wen-tsün, Mechanical Theorem Proving in Elementary Geometry and Differential Geometry, Proc. 1980 Beijing, DD1 Symp. Vol. 2, Science Press, 1982, 1073–1092.

[16] Wu Wen-tsün, A constructive theory of differential algebraic geometry, Lect. Notes in Math., No. 1255, pp 173–189, Springer-verlag, 1987.