Involutive Bases of Algebraic Partial Differential Equation Systems *

Yufu Chen† and Xiao-Shan Gao
Institute of Systems Science, Academia Sinica
Beijing, 100080, P.R.China
E-mail: (yfchen, xgao)@mmrc.iss.ac.cn

Abstract

In this paper, we present an algorithm to reduce a nonlinear algebraic partial differential equation system into passive involutive bases with respect to an abstract involutive division. This algorithm covers the existing algorithms based on Riquier division, Thomas division, and Pommaret division. It also provides new algorithms for computing involutive bases due to the existence of new involutive divisions found by us and other researchers. Experiments show that these new algorithms may be used to significiantly reduce the computational steps in Wu-Ritt's characteristic set method for algebraic partial differential equations.

Keywords. Involutive basis, integratebility conditions, algebraic partial differential equation system, Wu-Ritt's characteristic set method.

1 Introduction

A basic step to deal with a system of algebraic partial differential equations (abbr. PDEs) is to decompose its zero set into the union of the zero sets of PDEs in certain normal triangular form. With this kind of decomposition, we may compute the symmetric groups for PDEs [20], automatically prove theorems from differential geometries [23, 11], and solve the membership problem for radical ideals [1].

In the past ten years, extensive studies have been done for the zero decomposition algorithms of algebraic and ordinary differential equation systems[22], and most of the techniques thus developed may be extended to PDEs. The main difference between the PDE case and the algebraic (and ordinary differential) case is that integrability conditions are needed in the PDE case, which may be traced back to the classical Cauchy-Kovalevskaya theorem for the existence and uniqueness of analytic solutions to linear PDEs. There are two major approaches to deal with integrability conditions: the critical pair approach and the multiplier variable approach.

The *critical pair approach*, similar to the Gröbner basis method, was introduced by Rosenfeld [18] and improved by Kolchin [10], Boulier et al [1], Li and Wang [12], Rust et al [19], and

*This work is supported in part by a National Key Basic Research Project of China (No. G19980306), CNSF under an outstanding youth grant (NO. 69725002), and the Educational Committee of Liaoning Province
†On leave from: Department of Mathematics Jinzhou Normal College, Jinzhou 121003, China

Hubert [8]. This method is to reduce a general PDE system into *coherent forms*. The *multiplier variable approach* is to divide the variables into multipliers and non-multipliers and to do certain prolongation along non-multipliers to reduce the original equation systems into *passive triangular forms*. Riquier [16], Janet [9], Thomas [21], and Reid [15] developed integrability theories for linear PDE systems using this approach. For nonlinear algebraic PDEs, Ritt presented a zero decomposition theorem in [17]. But Ritt's theorem is not strictly constructive, because he used the implicit function theorem to express the nonlinear PDEs as linear ones in the highest derivative when computing the integrability conditions. Pommaret [14] developed new methods for non-linear PDEs. In [23], Wu gave a pure algebraic and constructive form of the zero decomposition theorem for nonlinear PDEs using Thomas' method of choosing multiplier variables.

In [5, 6], Gerdt and Blinkov extracted the common properties of the Riquier-Janet, Thomas, and Pommaret's multiplier theories for integrability to give a formal definition of the involutive division. This definition includes Riquier-Janet, Thomas, and Pommaret's multiplier theories as special cases: Riquier-Janet division, Thomas division, and Pommaret division. They also gave algorithms to construct involutive bases for polynomials and linear PDEs [7]. In [4], a vector representation for involutive division is presented and two types of new involutive divisions are found.

In this paper, we present an algorithm to reduce a nonlinear PDE system into passive forms with respect to an abstract involutive division. This algorithm covers all the existing methods using the multiplier variable approach such as Ritt's algorithm based on Riquier-Janet division and Wu's algorithm based on Thomas division. It also provides new algorithms since we know many new involutive divisions [5, 4]. Our experiments show that these new algorithms may be used to significiantly reduce the computational steps in Wu-Ritt's characteristic set method for algebraic PDEs.

The paper is organized as follows: in section 2, we will recall some basic definitions about the zero decomposition theory. In section 3, we introduce the concept of involutive directions. In section 4, we will present the zero decomposition algorithm. In section 5, we give a short conclusion.

2 Preliminaries for characteristic set method for PDEs

2.1 Basic notions and notations

Given an integral domain R with n differential operators $D_i, i = 1, 2, \cdots, n$, and m differential indeterminants $u_1, u_2, \cdots, u_m$. Let $Du = \{D_\alpha u_i | \alpha \in \mathbf{N}^n, i = 1, 2, \cdots, m\}$ and $D_\alpha = D_1^{\alpha_1} D_2^{\alpha_2} \cdots D_n^{\alpha_n}$, while $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha)$. $|\alpha| = \sum_{i=1}^n \alpha_i$ is called the order of $D_\alpha u_p$ for $p = 1, 2, \cdots, m$. We call the elements of $R[Du]$ the differential polynomials (abbr. d-pols) in $u_1, u_2, \cdots, u_m$ over R, and use the notation $R\{u_1, u_2, \cdots, u_m\}$, or simply $R\{u\}$ for them.

We say that an ordering $<$ on Du is admissible if

$$\begin{array}{ll} \text{(i)} & D_\alpha u_i < D_\sigma(D_\alpha u_i), \quad \text{for any } i,\ \alpha \text{ and } \sigma \neq 0 \\ \text{(ii)} & D_\alpha u_i < D_\beta u_j \Rightarrow D_\sigma(D_\alpha u_i) < D_\sigma(D_\beta u_j) \end{array} \tag{2.1.1}$$

In this paper, we always employ the orderly admissible orderings, i.e. the admissible orderings which satisfy

$$\text{(iii)} \quad |\alpha| < |\beta| \Rightarrow D_\alpha u_i < D_\beta u_j \tag{2.1.2}$$

and simply call them orderings.

Sometimes we use notation $u_{(j,\alpha)}$ to denote $D_\alpha u_j$. Any non-zero element of R is called a *trivial d-pol* in $R[Du]$. Given an ordering $<$ on Du, for a non-trivial d-pol f in $R[Du]$, the highest derivative with respect to (abbr. w.r.t.) the ordering $<$, effectively appearing in f, is called the leading derivative, or simply leader, of f, denoted by $ld(f)$. If $u_{(p,\alpha)}$ is the leading derivative of f, f can be rewritten as

$$f = f_d u_{(p,\alpha)}^d + f_{d-1} u_{(p,\alpha)}^{d-1} + \cdots + f_0, \quad f_d \neq 0 \tag{2.1.3}$$

where f_i's are polynomials in the derivatives lower than $u_{(p,\alpha)}$ over R. We call d the degree of f, denoted by $deg(f)$, and f_d the initial of f, denoted by $I(f)$. Furthermore, the partial derivative of f w.r.t. $u_{(p,\sigma)}$ is called the separant of f, denoted by $S(f)$.

An ordering $<$ on Du can be extended to a semi-ordering on $R[Du]$. For any two d-pols f and g in $R[Du]$, we say that f is lower than g, denoted by $f < g$, if f is trivial but g not, or f and g are both non-trivial and $ld(f) < ld(g)$, or $ld(f) = ld(g)$ and $deg(f) < deg(g)$. Otherwise, we write $f \sim g$. For a non-trivial d-pol f with leading derivative $D_\sigma u_p$ and degree d, the triple $[p, \sigma, d]$ is called the rank of f. The rank of a trivial d-pol (non-zero) is defined as $[0, 0, 0]$, where the second component is the zero vector with n dimension. It is clear that $f \sim g$ iff $rank(f) = rank(g)$. The following result is well-known any decreasing sequence of d-pols is finite under the semi-ordering $<$ [17, 23].

2.2 Pseudo-division and basic chains

Definition 2.1 *Let f and g be d-pols in $R[Du]$, and g non-trivial. We say that f is reduced w.r.t. g, if*

1. *No proper derivative of $ld(g)$ effectively appears in f; or*
2. *If $ld(g)$ effectively appears in f, the degree of f w.r.t. $ld(g)$ is less than $deg(g)$.*

If g is trivial and non-zero, then any d-pol f in $R[Du]$ is not reduced w.r.t. g.

Lemma 2.2 *Let*

$$\alpha_1, \alpha_2, \cdots, \alpha_q, \cdots \tag{2.2.1}$$

be an infinite sequence of vectors in $\mathbf{N}^n$. There is an infinite subsequence of (2.2.1)

$$\gamma_1, \gamma_2, \cdots, \gamma_p, \cdots \tag{2.2.2}$$

such that each component sequence of (2.2.2)

$$\gamma_{1i}, \gamma_{2i}, \cdots, \gamma_{pi}, \cdots \tag{2.2.3}$$

is non-decreasing, where γ_{ji} is the ith component of $\gamma_j, i = 1, 2, \cdots, n, j = 1, 2, \cdots, p, \cdots$.

Proof. Consider the first components of the vectors in sequence (2.2.1). Since $\{\alpha_{11}, \alpha_{21}, \cdots, \alpha_{q1}, \cdots\} \subseteq \mathbf{N}$, there exists a least number in $\{\alpha_{11}, \alpha_{21}, \cdots, \alpha_{q1}, \cdots\}$, say $\alpha_{j_1 1}$. Then consider the first components of the vectors in the following sequence

$$\alpha_{j_1+1}, \alpha_{j_1+2}, \cdots$$

Similarly there exits a least number in $\{\alpha_{j_1+1,1}, \alpha_{j_1+2,1}, \cdots\}$, say $\alpha_{j_2 1}$. Clearly $\alpha_{j_2 1} \geq \alpha_{j_1 1}$. To continue, we finally derive an infinite subsequence of (2.2.1)

$$\alpha_{j_1}, \alpha_{j_2}, \cdots \tag{2.2.4}$$

whose first component sequence is non-decreasing. For the sequence (2.2.4), the similar argument can be done on its second components, and we obtain an infinite subsequence of (2.2.4)

$$\beta_{k_1}, \beta_{k_2}, \cdots \tag{2.2.5}$$

whose first component sequence and second component sequence are both non-decreasing. By induction, we will derive an infinite subsequence of (2.2.1), whose component sequences are all non-decreasing. ∎

An increasing sequence of d-pols in $R[Du]$ is said to be reduced if the sequence consists of a single non-zero d-pol, or each d-pol in the sequence is non-trivial and reduced w.r.t. other d-pols in the sequence. A reduced increasing sequence is called a *chain.* A chain composed of a single trivial d-pol in $R[Du]$ is said to be *trivial.*

Lemma 2.3 *Any chain has only a finite number of terms.*

Proof. Suppose that G is a chain with infinite terms. There exists an infinite subsequence $G^{(1)}$ of G such that all the d-pols in $G^{(1)}$ have the same class, say p. It is easy to verify that $G^{(1)}$ is also a chain. Consider the sequence composed of the leaders of d-pols in $G^{(1)}$:

$$D_\alpha u_p, \cdots, D_\beta u_p, \cdots, D_\gamma u_p, \cdots \tag{2.2.6}$$

By Lemma 2.2, there are terms $D_\beta u_p, D_\gamma u_p$ in (2.2.6), such that $\gamma = \beta + \theta$, for some non-negative integer vector θ. This implies that there exists a d-pols in $G^{(1)}$ which is not reduced w.r.t. some d-pol coming before it, this is in contradiction with the definition of chains. ∎

Given two chains G and H

$$G: \quad g_1 < g_2 < \cdots, g_l; \qquad H: \quad h_1 < h_2 < \cdots < h_k \tag{2.2.7}$$

We say that G is lower than H, denoted by $G < H$, if one of the following conditions is satisfied

1. there is a subscript i, such that $g_i < h_i$, and $g_j \sim h_j$ for $j < i$;
2. $l > k$ and $g_j \sim h_j, \quad j = 1, 2, \cdots, k$.

If neither $G < H$, nor $H < G$ is the case, then G and H are said to have the same rank, denoted by $G \sim H$. In the latter case, we have $k = l$, and $g_i \sim h_i, \quad i = 1, 2, \cdots, l$. The following result is well-known [23, 17].

Lemma 2.4 *Any decreasing sequence of chains is finite.*

Based on Lemma 2.4, any nonempty set of chains has a minimal chain. For a set S of d-pols in $R[Du]$, we denote by $\mathcal{C}(S)$ the set of all chains composed of d-pols in S, and call any minimal chain in $\mathcal{C}(S)$ the *basic chain* of S. An algorithm to determine a basic chain of a finite set of d-pols can be found in [23]. Here we use the algorithm stated in Ritt's well known book [17]. Let $Red(f/G)$ denote the pseudo remainder of f w.r.t. G by the pseudo-division [17]. $Red(f/G)$, if it is not zero, is reduced w.r.t. G. For $R[Du]$, there is an analogous theorem on the pseudo-division.

Theorem 2.5 *For any non-trivial chain* $G: \quad g_1 < g_2 < \cdots < g_l$, *and any d-pol* f, *there are non-negative integers* ω_i, ε_i, *such that*

$$S_1^{\omega_1} \cdots S_l^{\omega_l} I_1^{\varepsilon_1} \cdots I_l^{\varepsilon_l} f = \sum_{p,\sigma} h_{p,\sigma} D_\sigma g_p + Red(f/G) \tag{2.2.8}$$

where $S_i = S(g_i), I_i = I(g_i), h_{p,\sigma} \in R[Du]$.

Remark 2.6 *If* R *is a unique factorization domain, the algorithm mentioned above can be refined. Hubert discussed this for the case that* R *is a field [8]. In section 4.2, we will give an analogous algorithm for* δ*-division, which is a generalization of the pseudo-division.*

A set S of d-pols in $R[Du]$ may have more than one basic chains, but any two such chains have the same rank. So the semi-ordering on chains induces a semi-ordering on the d-pol sets. We have

Lemma 2.7 *If a non-zero d-pol* f *is reduced w.r.t. a basic chain of a set* S, *then* $S \cup \{f\} < S$. *Then any decreasing sequence of sets of d-pols is finite.*

A product of the form $S_1^{\omega_1} \cdots S_l^{\omega_l} I_1^{\varepsilon_1} \cdots I_l^{\varepsilon_l}$ is called *an SI-product* of G. The set of all SI-products of a chain G is denoted by H_G^∞.

2.3 Differential ideals and pseudo-bases

An ideal I of $R[Du]$ is called a differential ideal of $R\{u\}$ if $D_i f \in I, i = 1, 2, \cdots, m$ for every $f \in I$. We denote by pi and dpi the ideal and differential ideals of $R\{u\}$ respectively. The dpi generated by d-pols $f_1, f_2, \cdots, f_t$ is denoted by $[f_1, \cdots, f_t]$.

Definition 2.8 *A non-trivial chain* G *is said to be a pseudo-basis of a system of d-pols* $f_1, \cdots, f_t$ *if the following conditions are satisfied*

1. $[f_1, \cdots, f_t] \supseteq [G]$; *and*
2. $Red(f_i/G) = 0, \; i = 1, \cdots, t$.

The following algorithm to find a pseudo basis is from [17].

Algorithm 2.9 *Determine a Pseudo-Basis for a d-pol set*

Input: *PS, a finite set of d-pols;*

Output: *G, a pseudo-basis of PS.*

begin $S := PS$

while $S \neq \phi$ *do*

determine a basic chain G of S

$T := \phi$

if G trivial, then **RETURN***(G)*

else *for every $f \in S \backslash G$* *do*

$r := Red(f/G)$

if $r \neq 0$ *then* $T := T \cup \{r\}$

if $T = \phi$ *then* **RETURN***(G)*

else $S := S \cup T$

end

end

By Lemma 2.7, Algorithm 2.9 would terminate in a finite number of steps. It is easy to prove that $[f_1, \cdots, f_t] \subseteq [G] : H_G^{\infty}$.

3 Prolongaton directions

It is clear that D_α are differential operators and

$$D_\alpha \cdot D_\beta = D_{\alpha+\beta} \tag{3.1}$$

So the monoid $(\mathbf{D}, \cdot)$ is isomorphic to the monoid $(\mathbf{N}^n, +)$, where $\mathbf{D} = \{D_\alpha | \alpha \in \mathbf{N}^n\}$. From this viewpoint, we prefer to discuss in $(\mathbf{N}^n, +)$, rather than in $\mathbf{D}$ (contrast with $Du_p = \{D_\alpha u_p | \alpha \in \mathbf{N}^n\})$ for a fixed p.

3.1 Basic definitions and notations

For convenience, we denote by α_i the ith component of a vector α, and $\alpha \circ \beta$ the Hadamard's product of α and β, i.e.

$$\alpha \circ \beta = (\alpha_1\beta_1, \cdots, \alpha_n\beta_n) \tag{3.1.1}$$

Set $\Delta_n = \{\alpha \in \mathbf{N}^n | \alpha_i = 0 \text{ or } 1, i = 1, 2, \cdots, n\}$.

Definition 3.1 *δ is said to be a prolongation direction, or simply a direction, on $\mathbf{N}^n$, if for each finite non-empty subset Γ of $\mathbf{N}^n$, a map $\delta^\Gamma \ : \ \Gamma \to \Delta_n$ is given uniquely.*

There are two special prolongation directions, one is called full direction, defined as

$$\delta^\Gamma(\alpha) = (1, 1, \cdots, 1) \quad \forall \alpha \in \mathbf{N}^n$$

and the other is called null direction, defined as

$$\delta^\Gamma(\alpha) = (0, 0, \cdots, 0) \quad \forall \alpha \in \mathbf{N}^n$$

Definition 3.2 *A prolongation direction δ on $\mathbf{N}^n$ is said to be involutive, if the following conditions are satisfied*

1. *$\forall\ \alpha, \beta \in \Gamma$, if $\alpha + \mu \circ \delta^\Gamma(\alpha) = \beta + \nu \circ \delta^\Gamma(\beta)$, for some $\mu, \nu \in \mathbf{N}^n$, then $\beta - \alpha$ and $\delta^\Gamma(\alpha) - \delta^\Gamma(\beta)$ are both non-negative, or $\alpha - \beta$ and $\delta^\Gamma(\beta) - \delta^\Gamma(\alpha)$ are both non-negative.*
2. *If $\alpha \in \Sigma \subseteq \Gamma$, then $\delta^\Sigma(\alpha) - \delta^\Gamma(\alpha)$ is non-negative.*

We define an operator $\mathbf{b}$ on $\mathcal{F}_n$, the set of all finite nonempty subsets of $\mathbf{N}^n$, as follows

$$\mathbf{b}: \quad \Gamma \to \gamma = max(\Gamma), \quad \forall \Gamma \in \mathcal{F}_n$$

where $\gamma_i = max\{\beta_i | \beta \in \Gamma\}, \quad i = 1, 2, \cdots, n$. We call $\mathbf{b}$ the upper bound operator on $\mathcal{F}_n$. For $\Gamma \in \mathcal{F}_n$, let

$$B(\Gamma) = \{\beta \in \mathbf{N}^n | \beta_i \leq \mathbf{b}_i(\Gamma), \quad i = 1, 2, \cdots, n\}.$$

3.2 Classical and new involutive directions

Example 3.3 *Thomas direction [21] can be defined as follows*

$$\forall \alpha \in \Gamma, \delta_i^\Gamma(\alpha) = \begin{cases} 1 & \text{if } \alpha_i = \mathbf{b}_i(\Gamma) \\ 0 & \text{otherwise} \end{cases} \tag{3.2.1}$$

$i = 1, 2, \cdots, n$, where $\delta_i^\Gamma(\alpha), \mathbf{b}_i(\Gamma)$ represent the ith components of $\delta^\Gamma(\alpha)$ and $\mathbf{b}(\Gamma)$ respectively.

Example 3.4 *Janet direction [9] can be defined as follows*

$$\forall \alpha \in \Gamma, \quad \begin{array}{l} \delta_1^\Gamma(\alpha) = \begin{cases} 1 & \text{if } \alpha_1 = \mathbf{b}_1(\Gamma) \\ 0 & \text{otherwise} \end{cases} \\ \delta_i^\Gamma(\alpha) = \begin{cases} 1 & \text{if } \alpha_i = \mathbf{b}_i(\Gamma_{\alpha_1 \cdots \alpha_{i-1}}) \\ 0 & \text{otherwise} \end{cases} \end{array} \tag{3.2.2}$$

where $\Gamma_{\alpha_1 \cdots \alpha_{i-1}} = \{\beta \in \Gamma | \beta_j = \alpha_j, j = 1, \cdots, i-1\}, \quad i = 2, \cdots, n.$

Example 3.5 *Pommaret direction [14] is defined as*

$$\forall \alpha \in \Gamma, \delta_i^{\Gamma}(\alpha) = \begin{cases} 1 & \text{if } i \geq L(\alpha) \\ 0 & \text{otherwise} \end{cases} \qquad i = 1, \cdots, n \tag{3.2.3}$$

where $L(\alpha)$ is index of the last non-zero component of α if $\alpha \neq 0$. $k = 0$ if $\alpha = 0$.

We denote by $N_p(\alpha)$ the number of positive components of α. Let l be an integer not less than $[n/2]$. For any finite subset Γ of $\mathbf{N}^n$, set

$$B_l^{\Gamma}(\alpha) = \{\beta \in \Gamma | 1 \leq N_p(\beta - \alpha) \leq l\} \tag{3.2.4}$$

Example 3.6 *A direction δ on $\mathbf{N}^n$ is defined as*

$$\delta_i^{\Gamma}(\alpha) = 1 \text{ iff } \beta_i \leq \alpha_i, \text{ for all } \beta \in B_l^{\Gamma}(\alpha) \tag{3.2.5}$$

In other words, $\delta_i^{\Gamma}(\alpha) = 0$ iff there is a $\beta \in B_l^{\Gamma}(\alpha)$, s.t. $\beta_i > \alpha_i$.

A direction defined in Example 3.6 is called *Thomas type direction*, denoted by T_l. Clearly, T_n is just Thomas direction and $T_{[n/2]}$ corresponds to the involutive division I introduced by Gerdt [5].

An ordered partition with length l of a positive integer n is a vector $(n_1, n_2, \cdots, n_l)$, where the n_i are positive integers, such that

$$n = n_1 + n_2 + \cdots + n_l.$$

Set $s_0 = 0, s_k = n_1 + \cdots + n_k, \ k = 1, \cdots, l$.

Example 3.7 *For any ordered partition $(n_1, n_2, \cdots, n_l)$ of n, we define a direction δ on $\mathbf{N}^n$: for every finite subset Γ of $\mathbf{N}^n, \forall \beta \in \Gamma$,*

$$\begin{array}{l} \delta_i^{\Gamma}(\beta) = 1 \text{ iff } \beta_i = \mathbf{b}_i(\Gamma), \text{ if } i \leq s_1; \\ \delta_i^{\Gamma}(\beta) = 1 \text{ iff } \beta_i = \mathbf{b}_i(\Gamma_{\beta_1 \cdots \beta_{s_k}}), \text{ if } s_k < i \leq s_{k+1}, \end{array} \tag{3.2.6}$$

$k = 1, \cdots, l-1$, where $\Gamma_{j_1 \cdots j_m}$ is defined as in Example 3.4.

A direction such defined is called *Janet type direction*, denoted by $J_{(n_1, \cdots, n_l)}$. It is clear that $J_{(1,1,\cdots,1)}$ is just Janet dirction and $J_{(n)}$ is just Thomas direction.

Example 3.8 *Induced directions[5]. An ordering on $\mathbf{N}^n$ is said to be admissibe if*

$$\alpha < \beta \Rightarrow \alpha + \sigma < \beta + \sigma \tag{3.2, 7}$$

for all $\alpha, \beta, \sigma \in \mathbf{N}^n$. Given an admissible ordering $<$, we state the induced direction as follows

$$\begin{array}{c} \forall \alpha \in \Gamma, \quad \delta_i^{\Gamma}(\alpha) = 0 \text{ iff there exists a } \beta \in \Gamma, \text{such that} \\ \beta < \alpha \text{ and } \alpha_i < \beta_i \end{array} \tag{3.2.8}$$

$i = 1, 2, \cdots, n$.

All the directions mentioned in the above examples are involutive[4].

3.3 Some important properties

Some properties of involutive diections are needed in the latter sections. Here we give a brief summary for the purpose. For the proofs, please refer to [4]. In what below, we assume that δ is an involutive direction on $\mathbf{N}^n$ and Γ is a finite subset of $\mathbf{N}^n$.

For $\alpha \in \Gamma$, we call $\alpha + \mu \circ \delta^\Gamma(\alpha)$ a prolongation of α w.r.t. Γ. The set of all prolongations of α w.r.t.Γ is denoted by $P_\delta^\Gamma(\alpha)$. Set $P_\delta(\Gamma) = \bigcup_{\alpha\in\Gamma} P_\delta^\Gamma(\alpha),\ P(\Gamma) = \{\alpha + \mu | \alpha \in \Gamma,\ \mu \in \mathbf{N}^n\}$.

Definition 3.9 *Given a direction δ on $\mathbf{N}^n$.*

1. *If $P_\delta(\Gamma) = P(\Gamma)$, then Γ is said to be complete w.r.t. δ;*
2. *Assume that Γ' is complete w.r.t. δ. If $\Gamma' \supseteq \Gamma$ and $P(\Gamma) = P(\Gamma')$, then Γ' is called a completion of Γ;*
3. *If each finite subset of $\mathbf{N}^n$ has a finite completion w.r.t. δ, then δ is said to be Noetherian.*

Thomas type, Janet type and induced directions are Noetherian, but Pommaret direction is not [4].

Definition 3.10 *A set Γ is said to be separable w.r.t. δ if*

$$\alpha + \mu \circ \delta^\Gamma(\alpha) = \beta + \nu \circ \delta^\Gamma(\beta) \Rightarrow \alpha = \beta \tag{3.3.1}$$

$\forall \alpha, \beta \in \Gamma$. If each finite subset of $\mathbf{N}^n$ is separable w.r.t. δ, then δ is said to be separable.

Janet type directions, Thomas type directions are separable, but Pommaret direction is not [4]. It is clear that Γ is separable w.r.t. δ iff $P_\delta^\Gamma(\alpha) \cap P_\delta^\Gamma(\beta) = \phi$ for $\alpha \neq \beta$.

For convenience, we use $\delta^{(i)}$ to represent the vector whose ith component is 1 and the other components are all zeros. For $\alpha \in \Gamma$, if $\delta_i^\Gamma(\alpha) = 0$, then we call $\alpha + \delta^{(i)}$ a non-multiplicative prolongation of α w.r.t. Γ.

Definition 3.11 *Given an involutive direction δ,*

1. *$\alpha, \beta \in \Gamma, \beta$ is said to be a pseudo-divisor of α w.r.t. Γ if there exists an index i and a vector $\mu \in \mathbf{N}^n$, s.t.*
$$\delta_i^\Gamma(\alpha) = 0 \quad \text{and} \quad \alpha + \delta^{(i)} = \beta + \mu \circ \delta^\Gamma(\beta) \tag{3.3.2}$$
2. *If for each finite set Γ, each pseudo-divisor sequence composed of elements in Γ is finite, then δ is said to be Artinian.*

All the directions mentioned above are Artinian [4]. We have [4].

Theorem 3.12 *Let δ be an Artinian direction. A finite set Γ is complete w.r.t. δ iff*

$$\delta_i^\Gamma(\alpha) = 0 \Rightarrow \alpha + \delta^{(i)} \in P_\delta(\Gamma) \tag{3.3.3}$$

for all $\alpha \in \Gamma$.

Definition 3.13 *Given an involutive direction δ. A non-multiplicative prolongation $\alpha + \delta^{(i)}$ of $\Gamma \in \mathcal{F}_n$ is said to be critical if the following conditions are satisfied:*

1. $\alpha + \delta^{(i)} \notin P_\delta(\Gamma)$;
2. *If $\alpha + \delta^{(i)} = \beta + \delta^{(j)} + \gamma$, where $\beta + \delta^{(j)}$ is also a non-multiplicative prolongation of Γ and $\gamma \neq 0$, then $\beta + \delta^{(j)} \in P_\delta(\Gamma)$.*

A direction δ is said to be *constructive* if, for every finite set Γ, no critical prolongation $\alpha+\delta^{(i)}$ of Γ can be expressed as

$$\alpha + \delta^{(i)} = \beta + \mu \circ \delta^{\Gamma}(\beta) + \nu \circ \delta^{\Gamma'}(\beta') \tag{3.3.4}$$

where $\beta \in \Gamma, \beta' = \beta + \mu \circ \delta^{\Gamma}(\beta), \Gamma' = \Gamma \cup \{\beta'\}$. All the directions mentioned in the examples are constructive [4]. We have [4].

Theorem 3.14 *Let δ be Artinian and constructive. Any completion Γ' of a finite set Γ contains all critical prolongations of Γ.*

Based on Theorem 3.14, we can give an algorithm to determine a minimal completion of a given finite set if its finite completion exists. We define a special partial ordering $<_+$ on $\mathbf{N}^n$ as

$$\alpha <_+ \beta \quad \text{iff} \quad \beta = \alpha + \sigma, \quad \text{for some } \sigma \neq 0$$

where $\alpha, \beta, \sigma \in \mathbf{N}^n$.

Algorithm 3.15 *Let δ be a direction of Noetherity, Artinity, and constuctivity. The algorithm will determine a minimal completion of a given vector set.*

Input Γ, *a finite subset of $\mathbf{N}^n$;*

output Γ', *a minimal completion of Γ.*

begin $\Gamma' := \Gamma, \quad \Phi := \{-1\}$;

  while $\Phi \neq \phi$ **do** $\Sigma := \phi;\ \Gamma_0 := \Gamma'$;

    while $\Gamma_0 \neq \phi$ **do**

      for $\gamma \in \Gamma_0, \quad \Gamma_0 := \Gamma_0 \backslash \{\gamma\}$;

        if there exists an index i, s.t.

          $\delta_i^{\Gamma'}(\gamma) = 0$ and $\gamma + \delta^{(i)} \notin P_\delta(\Gamma')$

        then $\Sigma := \Sigma \cup \{\gamma + \delta^{(i)}\}$;

    end

    while *exist* $\beta, \alpha \in \Sigma$, *s.t.* $\alpha <_+ \beta$ **do**

      $\Sigma := \Sigma \backslash \{\beta\}$

end

$\Gamma' := \Gamma' \cup \Sigma$; $\Phi := \Sigma$;

end

end

If δ is a Janet type direction, then $P(\Gamma) \cap B(\Gamma)$ is a completion of Γ. For Thomas direction, $P(\Gamma) \cap B(\Gamma)$ is a minimal completion of Γ, but it is not true for Janet direction.

4 δ-reduced, δ-division and involutive bases

4.1 $\delta-$chain and $\delta-$reduced

In this section, we work on a differential polynomial (abbr. d-pol) ring $\mathbf{F}\{u_1, u_2, \cdots, u_m\}$ over a differential field $\mathbf{F}$ with rational field as a subfield. We assume that an orderly admissible ordering $<$ on Du mentioned in section 2 and a prolongation direction δ on $\mathbf{N}^n$ mentioned in section 3 have been given. If $D_\sigma u_p$ is the leading derivative (or simply, leader) of a d-pol f, then p is called the *class* of f. Let S be a finite set of non-trivial d-pols. Denote by $E_p(S)$ the set of d-pols in S with class p and by $L_p(S)$ the leaders of the d-pols in $E_p(S)$. We will use the following notations

$$\Gamma_p(S) = \{\alpha \in \mathbf{N}^n | D_\alpha u_p \in L_p(S)\};\ PL_p(S) = \{D_\alpha u_p | \alpha \in P(\Gamma_p(S))\}.$$

$$L(S) = \bigcup_{p=1}^m L_p(S);\ PL(S) = \bigcup_{p=1}^m PL_p(S);\ NL(S) = Du \backslash PL(S).$$

For convenience, we often omit S in the above notations if no confusions occur. The derivatives in $PL(S)$ (resp. $NL(S)$) are called the *principal (resp. parametric) derivatives* of S. A derivative $D_\alpha u_p$ is called a multiplicative derivative of S, if $\alpha \in P_\delta(\Gamma_p) \backslash \Gamma_p$. An index i is called a *multiplier (resp. non-multiplier)* of a d-pols g in S if $\delta_i^{\Gamma_p}(\alpha) = 1$ (resp. $\delta_i^{\Gamma_p}(\alpha) = 0$), where $ld(g) = D_\alpha u_p$.

We first give the δ-completion algorithm of a chain, which is a generalization of Wu's completion algorithm for the case that δ is the Thomas direction[23]. We assume that δ is of Noetherity, Artinity, and constructivity.

Algorithm 4.1 *δ-Completion of a Chain*

Input G, *a non-trivial chain*

Output G^+, *the completion of* G

begin $H := \phi$;

for $p = 1, 2, \cdots, m$ **do**

$\Gamma_p := \Gamma_p(G)$,

determine a minimal completion of Γ_p *using Algorithm 3.15 w.r.t.* δ*, say* Γ'_p

for every $\alpha \in \Gamma'_p \backslash \Gamma_p$ **do**

$r := Red(D_\alpha u_p/G)$*, say* $JD_\alpha u_p = \sum_{i,\sigma} h_{i,\alpha} D_\sigma g_i + r$

$H := H \cup \{JD_\alpha u_p - r\}$

end

end $G^+ := G \cup H$

end

Definition 4.2 *An increasing sequence* G *of non-trivial d-pols* $g_1 < g_2 < \cdots < g_l$*, is said to be a* δ*-chain, if the following conditions are satisfied*

1. *No two d-pols in* G *have the same leader;*
2. *No multiplicative derivative of* G *appears in any* $g_i, i = 1, \cdots, l$*;*
3. *If some* $ld(g_i)$ *appears in* $g_j, j \neq i$*, then the degree of* g_j *w.r.t.* $ld(g_i)$ *is lower than* $deg(g_i)$*.*

We call any non-zero element of $\mathbf{F}$ *a trivial* δ*-chain.*

A chain is surely a δ-chain. If G is a non-trivial chain, then its δ-completion G^+ is a δ-chain. A δ-chain G is said to be *δ-separable (resp. δ-complete)* if each $\Gamma_p(G)$ is δ-separable (resp. δ-complete) w.r.t. δ, $p = 1, 2, \cdots, m$.

Definition 4.3 *Let* G *be a* δ*-chain, and* f *a d-pol. We say that* f *is* δ*-reduced w.r.t.* G*, if the following conditions are satisfied*

1. *No multiplicative derivatives of* G *appear in* f*;*
2. *If the leader* $D_\sigma u_p$ *of a d-pol* g *in* G *appears in* f*, then the degree of* f *w.r.t.* $D_\sigma u_p$ *is lower than* $deg(g)$*.*

The separants and initials of a δ-chain G are all δ-reduced w.r.t. G. If G is a chain, then a d-pol f is reduced w.r.t. G implies that f is δ-reduced w.r.t. G. But the converse is not true.

Lemma 4.4 *If* G *is a complete* δ*-chain, then a d-pol* f *is* δ*-reduced w.r.t.* G *iff* f *is reduced w.r.t.* G*.*

Proof. If f is not reduced w.r.t. G, then either there exists a proper principal derivative $D_\alpha u_p$ of G which appears in f, or there exists the leader $D_\alpha u_p$ of some element g in G such that the degree of f w.r.t. $D_\alpha u_p$ is not lower than $deg(g)$. In the latter case, f is not δ-reduced w.r.t. G by Definition 2.1. In the first case, $D_\alpha u_p$ must be a multiplicative derivative of G since $\Gamma_p(G)$ is complete, this means that f is not δ-reduced w.r.t. G. ∎

4.2 Fine combination and δ-division

For any d-pol $f, D_\sigma f$ is called the *prolongation* of f. For a d-pol g in a δ-chain G, with leader $D_\alpha u_p$, if $\sigma + \alpha \in P_\delta^{\Gamma_p}(\alpha)$, then $D_\sigma g$ is called a *multiplicative prolongation* of G. If i is a non-multiplier of g, then $D_i g$ is called a *non-multiplicative prolongation* of G.

Definition 4.5 *Let $G: \; g_1 < g_2 < \cdots < g_l$ be a δ-chain. A combination of elements in $G: \sum_{\alpha,i} h_{\alpha.i} D_\alpha g_i$ is said to be fine, if*

1. *the $D_\alpha g_i$'s appear in the sum satisfy that $ld(D_\alpha g_i) = ld(D_\beta g_j)$ iff $\alpha = \beta$ and $i = j$; and*
2. *either $\alpha \neq 0, D_\alpha g_i$ is a multiplicative prolongation of G and $h_{\alpha,i}$ is a polynomial in $ld(D_\alpha g_i)$ with coefficients of d-pols the multiplicative derivatives appear in which are lower than $ld(D_\alpha g_i)$; or*
3. *$\alpha = 0$, $h_{\alpha,i}$ is a polynomial in $ld(g_i)$ involving no multiplicative derivatives, and $h_{\alpha,i}$ is δ-reduced w.r.t. g_j for $j > i$.*

It is clear that a fine combination of G can be separated into two parts:

$$\sum_{\alpha,i} h_{\alpha,i} D_\alpha g_i = \sum_{i,\alpha\neq 0} h_{\alpha,i} D_\alpha g_i + \sum_i h_i g_{j_i} \tag{4.2.1}$$

Following Wu [23], the first part is called the *M-part* and the second part is called the *N-part*.

For a δ-chain G, any finite product of the factors of the separants or initials of G is called an *si-product* of G. K_G^∞ denotes the set of all si-products of G, which is a monoid containing H_G^∞. We have $[G] : K_G^\infty = [G] : H_G^\infty$.

Theorem 4.6 *Let $G: \; g_1 < g_2 < \cdots < g_l$ be a δ-chain, f a d-pol. Then there is an si-product J of G, such that*

$$Jf = \sum_{\alpha,i} h_{\alpha,i} D_\alpha g_i + r \tag{4.2.2}$$

where the right side sum is a fine combination of G, r is zero or a d-pol which is δ-reduced w.r.t. G.

We give the following algorithm to prove Theorem 4.6.

Algorithm 4.7 *δ-Division*

Input f, *a d-pol; G, a δ-chain.*

Output r, *a δ-remainder of f modulo G.*

begin $r := f$;

while *some multiplicative derivatives of G appear in r,* **do**

choose the highest of them, say $D_\beta u_p$;

pick out the highest $g_i \in G$, s.t.

$ld(g_i) = D_\alpha u_p$ *and* $\beta \in P_\delta^{\Gamma_p}(\alpha)\backslash\Gamma_p$, *say,* $\beta = \alpha + \sigma$;

$$r := \frac{[S(g_i), I'(r)]}{I'(r)} \cdot r - \frac{[S(g_i), I'(r)]}{S(g_i)} \cdot (D_\beta u_p)^{k-1} \cdot D_\sigma g_i \tag{4.2.3}$$

where $[P, Q]$ *stands for the least common multiple of* P *and* Q

end

while *some leaders of* G *appear in* r *with degree not lower than*

the degree of the d-pol in G *with the same leader,* **do**

choose the highest one of them, say, $D_\beta u_p = ld(g_i)$;

pick out $g_i \in G$ *with the leader* $D_\beta u_p$;

$$r := \frac{[I(g_i), I'(r)]}{I'(r)} \cdot r - \frac{[I(g_i), I'(r)]}{I(g_i)} \cdot (D_\beta u_p)^{k-deg(g_i)} \cdot g_i \tag{4.2.4}$$

end

end

where $I'(r)$ *and* k *are the leading coeffecient and degree of* r *w.r.t.* $D_\beta u_p$ *respectively. The output* r *is denoted by* $Re\delta(f/G)$, *and is called the* δ*-remainder of* f *modulo* G.

Note that a δ-division is just the pseudo-division on ordinary polynomials when δ is null direction, and is just the pseudo-division on d-pols with refinement metioned in the Remark 2.6 when δ is full direction[17]. So δ-division is the generalization of pseudo-division.

From now on we assume that δ is an involutive direction. A d-pol f is said to be *fine w.r.t. a* δ*-chain* G if there exists an si-product J of G such that Jf can be expressed as a fine combination of G.

Lemma 4.8 *Let* G *be a non-trivial* δ*-chain. If two d-pols* f_1, f_2 *are both fine w.r.t.* G*, then* $f_1 + f_2$ *is also fine w.r.t* G.

Proof. Assume that J_1, J_2 are the si-products of G such that $J_1 f_1, J_2 f_2$ can be expressed as fine combinations, then $J_1 J_2(f_1 + f_2)$ can be expressed as

$$\sum_{i,\alpha\neq 0} h_{\alpha,i} D_\alpha g_i + \sum_{k=1}^{l} h_k g_{i_k} \tag{4.2.5}$$

where the first sum is fine, the second sum satisfies $g_{i_1} < \cdots < g_{i_l}$ and no multiplicative dedrivatives appear in any h_k. Let g be the highest of elements in G with the property that there is an h_k which is not δ-reduced w.r.t. g and $g_{i_k} < g$. For each h_k not reduced w.r.t. g, by δ-division, there exists a product J_k of $I(g)$ such that $J_k h_k = \bar{h}_k g + \bar{r}_k$, whence $J_k h_k g_{i_k} = (\bar{h}_k g_{i_k})g + \bar{r}_k g_{i_k}$. Let J' be the product of all the J_k's, then $J_1' J_1 J_2(f_1 + f_2)$ can be expressed as

$$\sum_{i,\alpha\neq 0} h'_{\alpha,i} D_\alpha g_i + \sum_{j=1}^{l'} h'_j g_{i_j} + h'g \tag{4.2.6}$$

where $l' \leq l$ and the first sum is still a fine combination of G, the second sum satisfies the same conditions as that the second sum in (4.2.5) does. But the highest element g' in G with the property that there is an h'_j which is not δ-reduced w.r.t. g' and $g_{i_j} < g'$, is lower than g. Thus the Lemma can be proved by induction. ∎

Lemma 4.9 *If G is a separable δ-chain, $g \in G$ and $D_\sigma g$ is a multiplicative prolongation of G, then $f \cdot D_\sigma g$ is fine w.r.t. G for any d-pol f.*

Proof. We suppose first that $\sigma \neq 0$ and prove the proposition by induction on the multiplicative derivatives of G that appear in f. If no multiplicative derivative of G that is higher than $ld(D_\sigma g)$ appears in f, then $f \cdot D_\sigma g$ is itself a fine combination of G. Now suppose that $D_\alpha u_p$ is a multiplicative derivative of G which appears in f and $ld(D_\sigma g) < D_\alpha u_p$. Then, by the separability of G, there is unique $g_k \in G$, such that $D_\tau g_k$ is a multiplicative prolongation of G and $D_\alpha u_p = ld(D_\tau g_k)$. By δ-division, there is a product of some factors of $S(g_k)$, such that

$$J'f = h_{\tau,k} D_\tau g_k + r$$

where $h_{\tau,k} D_\tau g_k$ is a fine combination of G and r is a d-pol that multiplicative derivatives of G appear in which are lower than $D_\alpha u_p$. So

$$J' f D_\sigma g = (h_{\tau,k} D_\sigma g) D_\tau g_k + r D_\sigma g$$

By the inductive hypothesis, there exists an si-product J'' such that $J'' r D_\sigma g$ can be expressed as a fine combination of G.

Second, we suppose that $\sigma = 0$. By the proof for the first case, there exists an si-product J' of G such that

$$J' f g = \sum_{k,\tau\neq 0} h_{\tau,k} D_\tau g_k + rg$$

where r is a d-pol in which no multiplicative derivatives appear. If r is not δ-reduced w.r.t. some g' in G which is higher than g, we can choose the highest of such g', say g_l. By δ-division, there exists a product J_l of some factors of $I(g_l)$, such that $J_l r = h_l g_l + r_l$. Hence

$$J_l J' f g = \sum_{k,\tau\neq 0} J_l h_{\tau,k} g_k + (h_l g) g_l + r_l g$$

where the right side, except the last summand, is a fine combination of G. But the highest element in G (if there exists), which is not δ-reduced w.r.t. r_l and higher than g, is lower than g_l. The proof can be completed by induction. ∎

4.3 Involutive bases

There exists interesting work on constructing bases for d-pols, such as the differential Gröbner bases found in [3] and in [13], the involutive differential bases found in [5]. Here we adhere to the passivity used in Wu's work [23], and define the *involutive basis* for arbitrary DPEs systems.

Definition 4.10 *A δ-chain G is said to be passive if, for each $g \in G, \sigma \in \mathbf{N}^n$, the prolongation $D_\sigma g$ is fine w.r.t. G.*

Theorem 4.11 *Let δ be an Artinian direction and G a separable and complete δ-chain. G is passive if each non-multiplicative prolongation $D_i g$ of G is fine w.r.t. G.*

Proof. We will prove the theorem by induction on the leading derivatives of $D_\alpha g$'s. By the hypothesis, the prolongation $D_i g$ is fine w.r.t. G for any non-negative integer i and any $g \in G$. Now we consider the prolongation $D_\alpha g$ with $|\alpha| \geq 2$, and assume that $D_\beta g_i$ is fine w.r.t. G for every prolongation $D_\beta g_i$ satisfying $ld(D_\beta g_i) < ld(D_\alpha g), g_i \in G, \beta \in \mathbf{N}^n$.

If $D_\alpha g$ is a multiplicative prolongation of G, then it is itself a fine combination of G. Now assume that $D_i g$ is a non-multiplicative prolongation of G and $\alpha = \beta + \delta^{(i)}$. Then $D_\alpha g = D_\beta(D_i g)$ and, by the hypothesis, there exists an si-productJ_1 of G, such that $J_1 D_i g$ can be expressed as a fine combination of G:

$$J_1 D_i g = \sum_{j,\sigma} h_{j,\sigma} D_\sigma g_j \tag{4.3.1}$$

Differentiate two sides of (4.3.1) by D_β and then translate some terms from left to right:

$$\begin{aligned} J_1 D_\alpha g = & - \textstyle\sum_{\beta'+\beta''=\beta, \beta' \neq 0} (D_{\beta'} J_1) D_{\beta''} D_i g \\ & + \textstyle\sum_{j,\sigma} \sum_{\gamma'+\gamma''=\beta, \gamma' \neq 0} (D_{\gamma'} h_{j,\sigma}) D_{\gamma''} D_\sigma g_j + \sum_{j,\sigma} h_{j,\sigma} D_\beta D_\sigma g_j \end{aligned} \tag{4.3.2}$$

Let $ld(g) = D_\xi u_p$ and assume that $ld(D_{\sigma^{(1)}} g_{j_1}) = ld(D_i g) = D_i D_\xi u_p$ and $D_{\sigma^{(1)}} g_{j_1}$ is a multiplicative prolongation of G(since G is complete). By the separability of $\Gamma_p(G)$, $D_i g$ and $D_{\sigma^{(1)}} g_{j_1}$ are of degree one, whence the derivatives appear in $h_{j_1, \sigma^{(1)}}$ and $\sum_{\sigma \neq \sigma^{(1)}} h_{j,\sigma} D_\sigma g_j$ are lower than $D_i D_\xi u_p$. This implies that $ld(D_\beta D_{\sigma^{(1)}} g_{j_1}) = ld(D_\alpha g)$ is the highest principal derivative appears in the right side of (4.3.2), and it does not appear in any summand except $h_{j_1,\sigma^{(1)}} D_\beta D_{\sigma^{(1)}} g_{j_1}$. Set $\alpha^{(1)} = \beta + \sigma^{(1)}$. (4.3.2) can be rewritten as

$$J_1 D_\alpha g = h_{j_1,\sigma^{(1)}} D_{\alpha^{(1)}} g_{j_1} + \sum_{j,\sigma} h_{j,\sigma} D_\sigma g_j \tag{4.3.3}$$

where $ld(D_{\alpha^{(1)}} g_{j_1}) = ld(D_\alpha g)$, $ld(D_\sigma g_j) < ld(D_\alpha g)$, the principal deriatives of G appear in $h_{j,\sigma}$ is lower than $ld(D_\alpha g)$.

If $D_{\alpha^{(1)}} g_{j_1}$ is not a multiplicative prolongation of G, we assume that $\alpha^{(1)} = \beta' + \delta^{(i')}$ and $D_{i'} g_{j_1}$ is a non-multiplicative prolongation of G. By the hypothesis, there exists an si-product J_1' of G such that $J_1' D_{i'} g_{j_1} = h'_{j_2,\sigma^{(2)}} D_{\sigma^{(2)}} g_{j_2} + \sum_{j',\sigma'} h_{j',\sigma'} D_{\sigma'} g_{j'}$, where $ld(D_{i'} g_{j_1}) = ld(D_{\sigma^{(2)}} g_{j_2}), D_{\sigma^{(2)}} g_{j_2}$ is a multiplicative prolongation of G. We can derive as above that

$$J_1' D_{\alpha^{(1)}} g_{j_1} = h'_{j_2,\sigma^{(2)}} D_{\alpha^{(2)}} g_{j_2} + \sum_{j',\sigma'} \bar{h}_{j',\sigma'} D_{\sigma'} g_{j'} \tag{4.3.4}$$

where $\alpha^{(2)} = \sigma^{(2)} + \beta'$. Substituting (4.3.4) into (4.3.3) we have

$$J_2 D_\alpha g = h_{j_2,\sigma^{(2)}} D_{\alpha^{(2)}} g_{j_2} + \sum_{j,\sigma} h_{j,\sigma} D_\sigma g_j \tag{4.3.5}$$

where $J_2 = J_1 J_1'$, $ld(D_{\alpha^{(2)}} g_{j_2}) = ld(D_\alpha g), ld(D_\sigma g_j) < ld(D_\alpha g)$, the principal derivatives appear in $h_{j,\sigma}$ are lower than $ld(D_\alpha g)$, and $D_{\sigma^{(2)}} g_{j_2}$ is an multiplicative prolongation of G.

If $D_{\alpha^{(2)}} g_{j_2}$ is not yet a multiplicative prolongation of G, we can discuss about it as about $D_{\alpha^{(1)}} g_{j_1}$ and so on. We claim that such process must stop in a finite number of steps, and arrive finally that

$$J_k D_\alpha g = h_{j_k,\sigma^{(k)}} D_{\alpha^{(k)}} g_{j_k} + \sum_{j,\sigma} h_{j,\sigma} D_\sigma g_j \tag{4.3.6}$$

where J_k is an si-product of G, $ld(D_{\alpha^{(k)}} g_{j_k}) = ld(D_\alpha g), ld(D_\sigma g_j) < ld(D_\alpha g)$, the principal derivatives of G appear in $h_{j,\sigma}$ is lower than $ld(D_\alpha g)$, and $D_{\alpha^{(k)}} g_{j_k}$ is a multiplicative prolongation of G.

In fact, let $ld(g_{j_1}) = D_\eta u_p$, then $ld(D_{\sigma^{(1)}} g_{j_1}) = ld(D_i g)$ implies that

$$\xi + \delta^{(i)} = \eta + \sigma^{(1)} \circ \delta^{\Gamma_p}(\eta) \tag{4.3.7}$$

since $D_{\sigma^{(1)}} g_{j_1}$ is a multiplicative prolongation of G. But $D_i g$ is a non-multiplicative prolongation of G, i.e. i is a non-multiplier of ξ in $\Gamma_p = \Gamma_p(G)$. So η is a pseudo-divisor of ξ in Γ_p. Similarly, let $ld(g_{j_2}) = D_\zeta u_p$, then $ld(D_{\sigma^{(2)}} g_{j_2}) = ld(D_{i'} g_{j_1})$, and the facts that $D_{\sigma^{(2)}} g_{j_2}$ is a multiplicative prologation of G and $D_{i'} g_{j_1}$ is a non-multiplicative prolongation of G implies that ζ is a pseudo-divisor of η. And likewise for each $D_{\sigma^{(k)}} g_{j_k}$, there would be a infinite pseudo-divisor sequence

$$\xi,\ \eta,\ \zeta,\ \cdots$$

in Γ_p if the process could not stop in a finite number of steps. This is a contradiction with the Artinity of δ.

We note that the sum $\sum_{j,\sigma} h_{j,\sigma} D_\sigma g_j$ in (4.3.6) need not to be a fine combination of G, since any $D_\sigma g_j$ need not to be a multiplicative prolongation of G. But each $ld(D_\sigma g_j)$ is lower than $ld(D_\alpha g)$, each $D_\sigma g_j$ in the sum is fine w.r.t. G by the inductive hypothesis. Hence $J_k D_\alpha g$ is fine w.r.t. G by Lemma 4.8 and Lemma 4.9, whence $D_\alpha g$ is fine w.r.t. G. ∎

Corollary 4.12 *Let G be a δ-chain. If the δ-remainder of each non-multiplicative prolongation of G modulo G is zero, then G is δ-passive.*

Definition 4.13 *A non-trivial chain G is said to be an involutive basis for a system S of d-pols if G is a pseudo-basis of S and G^+ is δ-passive.*

In the following algorithm, we assume that the involutive direction δ is of separabiliy, Noetherity, Artinity and constructivity.

Algorithm 4.14 *Determine an Involutive Basis*

Input *S, a finite set of d-pols;*

Output *G, an involutive basis of S.*

begin $T := S$; $S_0 := \phi$;

while $T \neq \phi$ **do**

$S_0 := S_0 \cup T$; $T := \phi$;

determine a pseudo-basis of S_0, say G, with Algorithm 2.9;

if G is trivial, then **RETURN***(G);*

else

determine G^+ with Algorith 4.1; $S_0 := S_0 \cup G^+$;

for each $g \in G^+$, and every non-multiplicative prolongation $D_i g$ of G^+ **do**

$r := Re\delta(D_i g/G^+)$;

if $r \neq 0$, then $T := T \cup \{r\}$;

end

end **RETURN***(G);*

end

Remark 4.15 *Since G^+ is complete w.r.t. δ, any δ-remainder r of a d-pol f modulo G^+, if not zero, must be reduced w.r.t.G^+ by Lemma 4.4. Particularly, r is reduced w.r.t. G. So, in Algorithm 4.14, $S_0 \cup T$ has a lower basic chain, as well as a lower pseudo-basis than G if $T \neq \phi$. Algorithm 4.14 would terminate in a finite number of steps since δ is Noetherian. Furthermore, the output G is an involutive basis of S by Corollary 4.12.*

Let G be a non-trivial chain: $g_1 < g_2 < \cdots < g_l$. We call $G_k: \ g_1 < \cdots < g_k$ the truncation of G at k, and $\tilde{G}_k: \ g_k < \cdots < g_l$ the co-truncation of G at $k, 1 \leq k \leq l$. A d-pol h is said to be *G-trivial* if h is either trivial or a d-pol with leader lower than $ld(g_l)$ and is reduced w.r.t. G. Set $G_0 = 0$. A chain G is said to be differential(resp. algebraic) irreducible if, for each $g_k(1 \leq k \leq l)$, there is no G_k-trivial d-pol h_k such that

$$h_k g_k \equiv g_{k1} g_{k2} \ (mod[G_{k-1}])(\text{resp. } mod(G_{k-1})) \tag{4.3.8}$$

where g_{k1}, g_{k2} are d-pols with the same leader as that of g_k.

It is clear that G is irreducible implies that G_k is irreducible for any truncation of G at k. In addition, that G is differential irreducible implies that G is algebraic irreducible since $(G_{k-1}) \subseteq [G_{k-1}]$ for all $k = 1, 2, \cdots, l$. In [23], Wu proved that the converse is also true and described the process to decompose a non-trivial chain into irreducible chains. For a irreducible and passive chain, Wu proposed an algorithm to construct the formal power series solution, which is a generic solution, of the chain. Based on this, Wu derived the *zero decomposition theorem* for partial diiferential equation systems. All these results can be extended to the following form without difficulty.

Theorem 4.16 *Let δ be an involutive direction, which is of separability, Artinity, Noetherity and constructivity, and G an irreducible δ-passive chain. Then*

$$\mathrm{sat}(G) = \{P \in R\{u\} \mid Re\delta(P, G) = 0\}$$

is a primde ideal.

Theorem 4.17 *For any set S of d-pols, there is an algorithmic procedure to determine finite number of irreducible δ-passive chains $G_1, \cdots, G_c$, such that*

$$d\text{-}zero(S) = \cup_{k=1}^{c} d\text{-}zero(\mathrm{sat} G_k).$$

In Wu-Ritt characteristic method, the notion 'passive chain' is the special case of our terminology 'δ-passive chain' that δ is Thomas direction. For a non-trivial chain G, the passivity guarantees that each prolongation of G^+ can be expressed as the M-polynomials, which is needed in constructing the formal series solution for the irreducible and passive chain. But the latter requirement would be satisfied as long as G^+ is δ-passive for any involutive direction δ which is of separability, Artinity, Noetherity and constructivity. So we can take any such prolongation direction to replace Thomas direction in Wu-Ritt characteristic method, and we would get analogous results by the analogous discussion. Here we omit it.

Example[2] This example shows that there may be a great difference in computing the involutive bases by choosing different prolongation directions and orderings. **Exd4**

$$\begin{array}{l}
2\,\frac{\partial^3}{\partial x^3}v(x,y) + y\,\frac{\partial^2}{\partial x^2}v(x,y),\\
\frac{\partial}{\partial y}u(x,y),\\
\frac{\partial^2}{\partial y^2}v(x,y),\\
2\,\frac{\partial^3}{\partial x^3}u(x,y) - 6\,\frac{\partial^3}{\partial x^2\partial y}v(x,y) + y\,\frac{\partial^2}{\partial x^2}u(x,y) - 2\,y\,\frac{\partial^2}{\partial x\partial y}v(x,y),\\
6\,\frac{\partial^3}{\partial x^3}u(x,y) - 6\,\frac{\partial^2}{\partial x\partial y}v(x,y) - y\,\frac{\partial}{\partial x}u(x,y) - v(x,y)
\end{array}$$

Set $idp = [x, y],\ dep = [u, v]$.

tho2i2: 6's; jan11i2: 5's'; rom2i2: 5's

$$\begin{array}{l}
-3\,y\,\frac{\partial}{\partial x}u - 3\,v,\\
\frac{\partial}{\partial y}u,\\
-9\,\frac{\partial}{\partial x}v,\\
3\,y\,\frac{\partial}{\partial y}v - 3\,v
\end{array}$$

iduclli2: 1's;

$$\begin{array}{l}
\frac{\partial}{\partial y}u,\\
\frac{\partial^2}{\partial y^2}v,\\
6\,\frac{\partial^3}{\partial x^3}u - 6\,\frac{\partial^2}{\partial x\partial y}v - y\,\frac{\partial}{\partial x}u - v,\\
2\,\frac{\partial^3}{\partial x^3}v + y\,\frac{\partial^2}{\partial x^2}v,\\
-18\,\frac{\partial^3}{\partial x^2\partial y}v + 3\,y\,\frac{\partial^2}{\partial x^2}u - 6\,y\,\frac{\partial^2}{\partial x\partial y}v + 6\,\frac{\partial^2}{\partial x\partial y}v + y\,\frac{\partial}{\partial x}u + v
\end{array}$$

tho2i1: 8's;

$$
\begin{aligned}
&54\, y \frac{\partial^2}{\partial x^2} u, \\
&\frac{\partial}{\partial y} u, \\
&90\, y^4 \frac{\partial}{\partial x} u + 90\, y^3 v
\end{aligned}
$$

jan11i1: 7's;

$$
\begin{aligned}
&180\, y^2 \frac{\partial^2}{\partial x^2} u(x, y), \\
&\frac{\partial}{\partial y} u(x, y), \\
&-120\, y^3 \frac{\partial}{\partial x} u(x, y) - 120\, y^2 v(x, y)
\end{aligned}
$$

rom2i1: 21's;

$$
\begin{aligned}
&-139590\, y^3 \frac{\partial^2}{\partial x^2} u(x, y) + 177147\, y^4 \frac{\partial^2}{\partial x^2} u(x, y), \\
&\frac{\partial}{\partial y} u(x, y), \\
&-46530\, y^7 \frac{\partial}{\partial x} u(x, y) - 46530\, y^6 v(x, y) + 59049\, y^8 \frac{\partial}{\partial x} u(x, y) + 59049\, y^7 v(x, y)
\end{aligned}
$$

This example is some surprising to us. Involutive bases may be of various numbers of elements for the various orderings and prolongation directions.

5 Conclusion

We start with a prolongation direction δ on $\mathbf{N}^n$ defined by an axiom system and determine an involutive base for a given set of algebraic PDEs. Since we have known many directions satisfying the axiom system, the algorithm provides more space to choose suitable schemes to deal with concrete problems.

It is shown that a passive chain is coherent [12]. An interesting problem is to investigate the relation and compare the effectiveness among various δ-passive chains and coherent chains.

References

[1] Boulier, F., Lazard, D., Ollivier, F., Petitot, M., Representation for the radical of a finitely generated differential ideal. In: Levelt, A.H.M. (ed.): *Proc. Int. Symp. on Symbolic and Algebraic Computation*, Montreal, Canada, ACM Press, pp.158–166, 1999.

[2] Chao, L. T.and Gao, X.-S., Nearly Differential Characteristic Set for Differential Polynomial System. Research Report AMSS-V-2000-042.

[3] Carr'Ferro, G., Differential Gröbner bases in one variable and in the partial case, *Math. Comput. Modeling*, **25**, No.8/9 pp.1-10, 1997.

[4] Chen, Y. F. and Gao, X.-S., Involutive directions and new involutive divisions, preprint, 1999, accepted by Comp. and Math. with Appl.

[5] Gerdt, V.P., Gröbner bases and involutive methods of algebraic and differential equations. *Math. Comput. Modeling*, **25**(8/9), 75-90, 1997.

[6] Gerdt, V.P., Completion of linear differential systems to involution. In: *Computer Algebra in Scientific Computing/CASC'99*, pp.115-137. Springer-Verlag, Berlin, 1999.

[7] Gerdt, V.P. and Blinkov, Yu. A., Involutive bases of polynomials, *Math. Comp. in Simulation*, **45**, 519-541, 1998.

[8] Hubert, E., Factorization-free decomposition algorithms in differential algebra. *J. Symbolic Computation*, **29**, 641-662, 2000.

[9] Janet, M., Sur les systémes d'équations aux partielles, *J. de Math.*, **3**, 65-151, 1920.

[10] Kolchin, E., *Differential algebra and algebraic groups.* New York: Academic Press, 1973.

[11] Li, Z., Mechanical theorem proving of the local theory of surfaces. *Ann. Math. Artif. Intell.*, **13**, 25–46, 1995.

[12] Li, Z.M. and Wang, D.M., Coherent, regular and simple system in zero decompositions of partial differential system. *J. Sys. & Math. Sci.*, **12**(5), 43-60, 1999.

[13] Mansfield, E. *Differential Gröbner bases*, Ph.D. Thesis, University of Sydney, 1993.

[14] Pommaret, J. F., Systems of partial differential equations and Lie pseudo-groups. Gordon and Breach, 1978, Now York.

[15] Reid, G., Algorithms for reducing a system of PDEs to standard form, determining the dimension of its solution space and calculating its Taylor series solution, *European J. of Appl. Math.*, **2**, 293-318, 1991.

[16] Riquier, C., *Les systemes d'équations aux dérivées partielles*, Gauthies-Villars, Paris, 1910.

[17] Ritt, J. F., *Differential algebra*, Amer. Math. Soc., 1950.

[18] Rosenfeld, A., Specializations in differential algebra. *Trans. Amer. Math. Soc.* **90**, 394–407, 1959.

[19] Rust, C. J., Reid, G. J., and Wittkopf, A. D., Existence and uniqueness theorems for formal power series solutions of analytic differential systems, *Proc. of ISSAC'99*, pp.105-112, ACM Press, 1999.

[20] Schwarz, F., The Riquier-Janet theory and its application to nonlinear evolution equations. *Physica*, 11**D**, 243-251, 1984.

[21] Thomas, J., *Differential systems.* AMS. Colloquium Publication, vol.21, N.Y., 1937.

[22] Wang, D., *Elimination Methpds,*, Springer-Verlag, Berlin, 2001.

[23] Wu, W.-T., On the foundation of algebraic differential geometry, Mathematics-Mechanization Research Preprint, No.3, pp.1-26, 1989.

[24] Wu W.-T., On the construction of Gröbner basis of a polynomial ideal on Riquier-Janet theory, *Systems Science and Mathematical Science*, **4**(3), 193-207, 1991.