Properties of Ascending Chains for Partial Difference Polynomial Systems*

Gui-Lin Zhang and Xiao-Shan Gao

Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS, Chinese Academy of Sciences
xgao@mmrc.iss.ac.cn, zhangguil@amss.ac.cn

Abstract. A characteristic set theory for partial difference polynomial systems is proposed. We introduce the concept of coherent and regular ascending chains and prove that a partial difference ascending chain is the characteristic set of its saturation ideal if and only if it is coherent and regular. This gives a method to decide whether a polynomial belongs to the saturation ideal of an ascending chain. We introduce the concept of strongly irreducible ascending chains and prove that a partial difference ascending chain is the characteristic set of a reflexive prime ideal if and only if it is strongly irreducible. This gives a simple and precise representation for reflexive prime ideals.

Keywords: Ascending chain, characteristic set, coherent chain, regular chain, irreducible chain, partial difference polynomial.

1 Introduction

The characteristic set method is a fundamental tool for studying systems of algebraic or algebraic differential equations. The method could be used to transform an equation system into so-called characteristic sets, which are systems of equations in certain triangular form also called ascending chains, or simply chains. This allows people to give the dimension, the order, and the degree of a solution set over an algebraically or differentially closed field. Also, triangular equation systems are ready for symbolic and numerical solutions.

The characteristic set method was introduced by Ritt in the 1930s as an algebraic tool to study differential equations [17, 19]. However, the algorithmic study of the characteristic set was in stagnation for quite a long time until Wu's work on zero decomposition for polynomial equations and automated geometry theorem proving appeared in the late 1970s [23,24,25]. Since then, many efficient algorithms and new properties for characteristic sets were proposed for algebraic equation systems and differential equation systems [1,2,4,5,6,7,8,9,11,12,16,22, 27]. In [13, 14, 15], a characteristic set method was also introduced for ordinary difference equation systems and ordinary differential-difference equation systems.

In this paper, we develop a characteristic set theory for partial difference polynomial systems. We obtain three main results. First, we introduce the concept

* Supported by a National Key Basic Research Project of China (2004CB318000).

D. Kapur (Ed.): ASCM 2007, LNAI 5081, pp. 307–321, 2008.

of coherent chains and this leads to a normal representation of the difference polynomials in the saturation ideal of a coherent chain. Second, we introduce the concept of regular chains and prove that a partial difference chain is the characteristic set of its saturation ideal if and only if it is coherent and regular. We also prove that the saturation ideal of a partial difference regular and coherent chain is the union of some algebraic saturation ideals. This gives a method to decide whether a polynomial belongs to the saturation ideal of a chain. Third, we introduce the concept of strongly irreducible chains and prove that a partial difference chain is the characteristic set of a reflexive prime ideal if and only if it is strongly irreducible. This gives a simple and precise representation for prime and reflexive prime ideals. These results are generalizations of similar results about algebraic polynomial systems [2], differential systems [6,16], and ordinary difference systems [13,14]. Due to the complicated structure of partial difference polynomials, our generalization is nontrivial and there still exist many problems unsolved in the partial difference case. The major open problem is to give a constructive criterion for regular and non-trivial chains. For details, please see Section 4.

In [18,20,26], the characteristic set of partial differential and difference polynomial systems was defined and used to prove the Noetherian property of the partial differential and difference polynomial ring. Dimension polynomials for differential and difference polynomial ideals were also studied in [18, 26]. But, the results presented in this paper for regular and irreducible chains were not given in these papers.

The rest of this paper is organized as follows. In Section 2, we present the notations and known results needed in this paper. In Sections 3, 4, and 5, we prove the properties of coherent, regular, and strongly irreducible chains respectively. In Section 6, we give the zero decomposition theorem and algorithm. In Section 7, we conclude the paper.

2 Preliminaries

We will introduce the notions and preliminary properties needed in this paper. For the general theory of difference algebra, please refer to [3,10,18].

2.1 Difference Polynomials and Difference Chains

Let $\mathcal{K}$ be a field of characteristic zero. We say that $\mathcal{K}$ is an inversive partial difference field with transforming operators $\{\sigma_1, \ldots, \sigma_m\}$ over $\mathcal{K}$, if $\{\sigma_1, \ldots, \sigma_m\}$ are automorphisms of $\mathcal{K}$ onto $\mathcal{K}$ which commute pairwise on the elements of $\mathcal{K}$. Let

$$T_\sigma = \{\sigma_1^{o_1} \ldots \sigma_m^{o_m} | j = 1, \ldots, m, o_j \geq 0\}.$$

We regard T_σ as a free commutative monoid. The *order* of an element $\eta = \sigma_1^{o_1} \ldots \sigma_m^{o_m}$ of T_σ is $\mathrm{ord}(\eta) = \Sigma_{j=1}^m o_j$. η is proper if $\mathrm{ord}(\eta) \neq 0$. The *vector* of an element $\eta \in T_\sigma$ is $\mathrm{vec}(\eta) = (i_1, \ldots, i_m)$ if $\eta = \sigma_1^{i_1} \ldots \sigma_m^{i_m}$. For $\eta_1, \eta_2 \in T_\sigma$, η_1 is a

(proper) multiple transform of η_2 or η_2 is a *(proper) factor transform* of η_1 if $\exists$ $\eta \in T_\sigma$ such that $\eta_1 = \eta\eta_2$ ($\mathrm{ord}(\eta) \neq 0$). It is denoted by $\eta_1 \gg \eta_2 (\eta_1 \succ \eta_2)$.

Let $\mathbb{X} = \{x_1, \ldots, x_n\}$ be a finite set of difference indeterminates over $\mathcal{K}$ and

$$T_\sigma \mathbb{X} = \{\eta x_i | \eta \in T_\sigma, i = 1, \ldots, n\}.$$

$\mathcal{R} = \mathcal{K}\{x_1, \ldots, x_n\} = \mathcal{K}[T_\sigma \mathbb{X}]$ denotes the ring of partial difference polynomials in the indeterminates $\mathbb{X}$ with coefficients in $\mathcal{K}$. For convenience, in this paper, when we say polynomials, we mean partial difference polynomials, otherwise we will point out clearly.

Let $<$ be a *total ordering* over $T_\sigma \mathbb{X}$ defined as follows: $\forall \eta, \theta \in T_\sigma, 1 \leq i, j \leq n$, $\eta x_i > \theta x_j$ if $i > j$ or $i = j$ and $\mathrm{ord}(\eta) > \mathrm{ord}(\theta)$ or else $\mathrm{ord}(\eta) = \mathrm{ord}(\theta)$ and the first nonzero element of $\mathrm{vec}(\eta) - \mathrm{vec}(\theta)$ is greater than zero. Let f be a polynomial not in $\mathcal{K}$, the *leader* of f is the highest element of $T_\sigma \mathbb{X}$ (*w.r.t.* $<$) that appears in f, and we denote it by $\mathbf{u}_f$. We write f as a univariate polynomial in $\mathbf{u}_f$:

$$f = I_d \mathbf{u}_f^d + \cdots + I_0.$$

$I_d = \mathrm{init}(f)$ is called the *initial* of f. Let $\mathbf{u}_f = \eta x_i$. Then i and x_i are called the *class* and *leading variable* of f, denoted as $\mathrm{class}(f)$ and $\mathrm{lvar}(f)$ respectively. We define $\mathrm{vec}(\eta x_i) = \mathrm{vec}(\eta)$ and $\mathrm{vec}(f, x_j) = \mathrm{vec}(\eta)$, if $\eta x_j = \max\{\tau x_j$ appears in $f\}$, $\mathrm{vec}(f) = \mathrm{vec}(f, \mathrm{lvar}(f))$.

An *n-tuple* over $\mathcal{K}$ is of the form $\mathbf{a} = (a_1, \ldots, a_n)$, where the a_i are selected from some difference extension field of $\mathcal{K}$. Let $f \in \mathcal{K}\{\mathbb{X}\}$. To substitute an n-tuple $\mathbf{a}$ into f means to replace each of the ηx_i occurring in f with the corresponding ηa_i. Let $\mathbb{P}$ be a set of polynomials in $\mathcal{K}\{\mathbb{X}\}$. An n-tuple over $\mathcal{K}$ is called a *solution* of the equation set $\mathbb{P}$=0 if the result of substituting the n-tuple into each polynomial of $\mathbb{P}$ is zero. We use $\mathrm{Zero}(\mathbb{P})$ to denote the set of solutions of $\mathbb{P} = 0$. Let $f \in \mathcal{K}\{\mathbb{X}\}$. It is easy to check that $\mathrm{Zero}(f) = \mathrm{Zero}(\eta f)$ $\forall \eta \in T_\sigma$. For the sets of polynomials $\mathbb{P}$ and $\mathbb{D}$, $\mathrm{Zero}(\mathbb{P}/\mathbb{D})$ denotes the set of solutions of $\mathbb{P} = 0$ which do not annihilate any polynomial of $\mathbb{D}$.

Let g be a polynomial not in $\mathcal{K}$. A polynomial f is said to be of *less than* g, denoted as $f < g$, if $\mathbf{u}_f < \mathbf{u}_g$ or $(\mathbf{u}_f = \mathbf{u}_g) = u$ and $\deg(f, u) < \deg(g, u)$. If neither $f < g$ nor $g < f$, we say that f and g are equivalent and we write $f \equiv g$. A polynomial f is said *reduced* w.r.t. g if $\deg(f, \eta \mathbf{u}_g) < \deg(g, \mathbf{u}_g), \forall \eta \in T_\sigma$.

A subset $\mathcal{A}$ of $\mathcal{R} \backslash \mathcal{K}$, where every element is reduced w.r.t. all the others, is called an *autoreduced set*. A *chain* is an autoreduced set where the polynomials are listed in the ascending ordering: $\mathcal{A} = A_1 < A_2 < \cdots < A_p$. It is easy to show that every chain $\mathcal{A}$ in $\mathcal{R} = \mathcal{K}\{\mathbb{X}\}$ is a finite set.

If $\mathcal{A} = A_1, \ldots, A_p$ and $\mathcal{B} = B_1, \ldots, B_q$ are two chains, we say that $\mathcal{A} < \mathcal{B}$ if either there is some $j \leq \min(p, q)$ such that $A_i \equiv B_i$ for $i < j$ and $A_j < B_j$, or $q < p$ and $A_i \equiv B_i$ for $i \leq q$. If neither $\mathcal{A} < \mathcal{B}$ nor $\mathcal{B} < \mathcal{A}$, we say that $\mathcal{A}$ and $\mathcal{B}$ are of the same order and we denote $\mathcal{A} \equiv \mathcal{B}$. The following result is a basic property of chains (page 147 in [18]).

Lemma 1. *A strictly decreasing sequence of chains* $\mathcal{A}_1 > \mathcal{A}_2 > \mathcal{A}_3 > \cdots$ *is finite.*

If $\mathcal{F} \subseteq \mathcal{R}$, then the set of all the chains contained in $\mathcal{F}$ has a minimal element according to Lemma 1, which is called a *characteristic set* of $\mathcal{F}$ and it is denoted by $\mathrm{CS}(\mathcal{F})$. A polynomial f is *reduced* w.r.t. a chain if it is reduced to every polynomial in the chain. The following results are easy to prove.

Lemma 2. *If $f \neq 0$ is reduced w.r.t. $\mathrm{CS}(\mathcal{F})$, then $\mathrm{CS}(\mathcal{F} \cup \{f\}) < \mathrm{CS}(\mathcal{F})$.*

Lemma 3. *A chain $\mathcal{A} \subset \mathbb{P}$ is a characteristic set of $\mathbb{P}$ if and only if there is no nonzero polynomial in $\mathbb{P}$ which are reduced w.r.t. $\mathcal{A}$.*

A *difference ideal* is a subset $\mathcal{I}$ of $\mathcal{R} = \mathcal{K}\{x_1, \ldots, x_n\}$, which is an algebraic ideal in $\mathcal{R}$ and is closed under transforming. A difference ideal $\mathcal{I}$ is called *reflexive* if $\eta f \in \mathcal{I}$ implies $f \in \mathcal{I}$ for all $\eta \in T_\sigma$. Let S be a set of elements of $\mathcal{R}$. The difference ideal generated by S is denoted by $[S]$. Obviously, $[S]$ is the set of all linear combinations of the polynomials in S and their transforms. The ordinary or algebraic ideal generated by S is denoted as (S). A difference ideal $\mathcal{I}$ of $\mathcal{R}$ is called *perfect* if the presence in $\mathcal{I}$ of a product of transforms of an element f of $\mathcal{R}$ implies $f \in \mathcal{I}$. The perfect difference ideal generated by S is denoted as $\{S\}$. A perfect ideal is always reflexive. A difference ideal $\mathcal{I}$ is called a *prime difference ideal* if it is prime as an algebraic ideal.

Let $\mathcal{A}$ be a chain and $\mathbb{I}_\mathcal{A}$ the set of products of the initials of the polynomials in $\mathcal{A}$ and their transforms. The *saturation ideal* of $\mathcal{A}$ is defined as follows

$$\mathbf{sat}(\mathcal{A}) = \{f \in \mathcal{K}\{\mathbb{X}\} \,|\, \exists J \in \mathbb{I}_\mathcal{A}, s.t.\, Jf \in [\mathcal{A}]\}.$$

2.2 Invertibility of Algebraic Polynomials

We will introduce some notations and results about invertibility of algebraic polynomials w.r.t. an algebraic ascending chain. These results are given in [1, 2, 5, 6].

Let $\mathcal{A} = A_1, \ldots, A_m$ be a nontrivial triangular set in $\mathcal{K}[x_1, \ldots, x_n]$ over a field $\mathcal{K}$ of characteristic zero. Let y_i be the leading variable of A_i, $y = \{y_1, \ldots, y_p\}$ and $u = \{x_1, \ldots, x_n\} \setminus y$. u is called the parameter set of $\mathcal{A}$. We can denote $\mathcal{K}[x_1, \ldots, x_n]$ as $\mathcal{K}[u, y]$. I_i is the initial of A_i. For a triangular set $\mathcal{A}$, let $I_\mathcal{A}$ be the set of products of the initials of the polynomials in $\mathcal{A}$. The *algebraic saturation ideal* of a triangular set $\mathcal{A}$ is defined as follows

$$\mathbf{a\text{-}sat}(\mathcal{A}) = \{f \in \mathcal{K}[x_1, \ldots, x_n] \,|\, \exists J \in I_\mathcal{A}, s.t. Jf \in (\mathcal{A})\}.$$

Definition 4. *Let $\mathcal{A} = A_1, A_2, \ldots, A_m$ be a nontrivial triangular set in $\mathcal{K}[u, y]$ with u as the parameter set, and $f \in \mathcal{K}[u, y]$. f is said to be invertible w.r.t. $\mathcal{A}$ if $(f, A_1, \ldots, A_s) \cap \mathcal{K}[u] \neq \{0\}$ where $s = \mathrm{class}(f)$. $\mathcal{A}$ is called regular if the initials of A_i are invertible w.r.t. $A_1, \ldots, A_{i-1}$.*

Theorem 5. *[2, 6] Let $\mathcal{A}$ be a triangular set. Then $\mathcal{A}$ is a characteristic set of* $\mathbf{a\text{-}sat}(\mathcal{A})$ *iff $\mathcal{A}$ is regular.*

Lemma 6. *[6] A finite product of polynomials which are invertible w.r.t. $\mathcal{A}$ is also invertible w.r.t. $\mathcal{A}$.*

Lemma 7. *[6] A polynomial g is not invertible w.r.t. a regular triangular set $\mathcal{A}$ iff there is a nonzero f in $\mathcal{K}[u, y]$ such that $fg \in (\mathcal{A})$ and g is reduced w.r.t. $\mathcal{A}$.*

Lemma 8. *[25] Let $\mathcal{A}$ be an irreducible triangular set. Then a polynomial g is invertible w.r.t. $\mathcal{A}$ iff $g \notin$ **a-sat**(A).*

3 Coherent Chains

For any chain $\mathcal{A}$, after a proper renaming of variables, we could write it as the following form:

$$\mathcal{A} = \begin{cases} A_{1,1}(u, y_1), \ldots, A_{1,k_1}(u, y_1) \\ A_{2,1}(u, y_1, y_2), \ldots, A_{2,k_2}(u, y_1, y_2) \\ \ldots \\ A_{p,1}(u, y_1, \ldots, y_p), \ldots, A_{p,k_p}(u, y_1, \ldots, y_p) \end{cases} \tag{1}$$

where $\mathrm{lvar}(A_{i,j}) = y_i$, $u = \{u_1, \ldots, u_q\}$ such that $p+q = n$, $\mathbb{X} = u \bigcup \{y_1, \ldots, y_p\}$. For $c = 1, \ldots, p$, let

$$\mathcal{A}_c = A_{c,1}(u, y_1, \ldots, y_c), \ldots, A_{c,k_c}(u, y_1, \ldots, y_c) \tag{2}$$

3.1 Prolongation of Chains

We will now introduce the prolongation of a chain, which is a key concept in our theory. For instance, we will use this concept to define the pseudo-remainder of a polynomials w.r.t. a chain.

For a set of polynomials $\mathbb{P}$, we use $\mathbb{L}_{\mathbb{P}}$ to denote the set of leaders of the polynomials in $\mathbb{P}$. For $\eta x_c \in T_\sigma$, we use $\mathbb{D}_{\eta x_c}$ to denote the set of θx_c such that θ is a factor of η. More precisely, we have:

$$\begin{aligned} \mathbb{L}_{\mathbb{P}} &= \{\eta x_c \in T_\sigma \mathbb{X} \quad s.t. \quad \exists\, P \in \mathbb{P}, \mathbf{u}_P = \eta x_c\}. \\ \mathbb{D}_{\eta x_c} &= \{\theta x_c \in T_\sigma \mathbb{X} \quad s.t. \quad \eta \gg \theta\}. \end{aligned}$$

We define the *main variables* and *parameters* of a chain $\mathcal{A}$ as follows.

$$\begin{aligned} \mathbb{MV}_{\mathcal{A}} &= \{\eta x_c \in T_\sigma \mathbb{X} \quad s.t. \quad \exists\, A \in \mathcal{A}, \mathbf{u}_A = \theta x_c, \text{ and } \eta \gg \theta\}. \\ \mathbb{PA}_{\mathcal{A}} &= T_\sigma \mathbb{X} \setminus \mathbb{MV}_{\mathcal{A}}. \end{aligned}$$

For any finite set of polynomials $\mathbb{P}$ and a chain $\mathcal{A}$, we say that $\mathcal{A}_{\mathbb{P}}$ is a *prolongation of* $\mathcal{A}$ w.r.t. $\mathbb{P}$ if it satisfies the following properties:

- $\mathcal{A}_{\mathbb{P}} \supseteq \mathcal{A}$ is an algebraic triangular set under the ordering $\leq$ when all $\eta x_i \in T_\sigma \mathbb{X}$ are considered as independent variables.
- If $A \in \mathcal{A}_{\mathbb{P}}$, then there exist a $B \in \mathcal{A}$ and an $\eta \in T_\sigma$ such that $A = \eta B$ and B has the lowest degree among all elements in $\{C | \mathbf{u}_A = \mathbf{u}_{\theta C},\ C \in \mathcal{A}\}$.

– For any ηx_c occurring in $\mathbb{P} \cup \mathcal{A}_{\mathbb{P}}$, either $\eta x_c \in \mathbb{PA}_{\mathcal{A}}$ or there exists an $A \in \mathcal{A}_{\mathbb{P}}$ such that $\mathbf{u}_A = \eta x_c$.

Intuitively speaking, $\mathcal{A}_{\mathbb{P}}$ is a finite subset of $T_\sigma A$ such that each ηx_i occurring in $\mathbb{P}$ is either in $\mathbb{PA}_{\mathcal{A}}$ or a leader of a polynomial in $\mathcal{A}_{\mathbb{P}}$. It is easy to show that $\mathcal{A}_{\mathbb{P}}$ satisfies the following properties.

– The parameters of $\mathcal{A}_{\mathbb{P}}$ as an algebraic triangular set are all in $\mathbb{PA}_{\mathcal{A}}$.
– A polynomial f is reduced w.r.t. $\mathcal{A}$ if and only if f is reduced w.r.t. $\mathcal{A}_f$ in the algebraic sense, where $\mathcal{A}_f = \mathcal{A}_{\{f\}}$.

The following algorithm can be used to compute a prolongation $\mathcal{A}_{\mathbb{P}}$, for a given chain $\mathcal{A}$ and a polynomial set $\mathbb{P}$.

Algorithm 9. Prolongation$(\mathcal{A}, \mathbb{P})$

– **Input**:*A chain* $\mathcal{A}$ *of form (1) and a finite set of polynomials* $\mathbb{P}$.
– **Output**: *A prolongation* $\mathcal{A}_{\mathbb{P}}$ *of* $\mathcal{A}$ *w.r.t.* $\mathbb{P}$.

Begin
  $\mathcal{A}_{\mathbb{P}} := \mathcal{A}$
  For i=p to 1
    $\Omega_i := \{\eta \mid \eta y_i$ *appears in* $\mathcal{A}_i, \mathcal{A}_{i+1}, \ldots, \mathcal{A}_p$ *or* $\mathbb{P}\}$;
    $\tau :=$ *LCM*(Ω_i)
    For all $\eta \ll \tau$
      $\Omega_\eta := \{A \mid A \in \mathcal{A}_i, \exists\ \theta \in T_\sigma, \theta \mathbf{u}_A = \eta y_i\}$,
      choose an element A *of* Ω_η *with the least degree s.t.* $\theta \mathbf{u}_A = \eta y_i$.
      $\mathcal{A}_{\mathbb{P}} := \mathcal{A}_{\mathbb{P}} \cup \theta A$
    $\Lambda := \{\eta \mid \eta y_i$ *occurring in* $\mathcal{A}_{\mathbb{P}}, \eta y_i \notin \mathbb{PA}_{\mathcal{A}}$ *and* $\forall\ A \in \mathcal{A}_{\mathbb{P}}$, $\mathbf{u}_A \neq \eta y_i\}$
    While $(\Lambda \neq \emptyset)$
      $\theta :=$ *max* Λ
      For all $\bar{\theta} \in \Lambda$ *and* $\bar{\theta} \ll \theta$
        choose $A \in \mathcal{A}$ *with the least degree, s.t.* $\exists\ \theta' \in T_\sigma$, $\theta' \mathbf{u}_A = \bar{\theta} y_i$
        $\mathcal{A}_{\mathbb{P}} := \mathcal{A}_{\mathbb{P}} \cup \theta' A$
      $\Lambda := \{\eta \mid \eta y_i$ *occurring in* $\mathcal{A}_{\mathbb{P}}, \eta y_i \notin \mathbb{PA}_{\mathcal{A}}$ *and* $\forall\ A \in \mathcal{A}_{\mathbb{P}}$
        $\mathbf{u}_A \neq \eta y_i\}$
    End While
  $i := i - 1$
End.

The termination of the algorithm is apparent if we notice that the sequence of elements of $\theta := \max \Lambda$ is strictly decreasing.

Example 1. Consider the chain $\mathcal{A} = \{A_1, A_2, A_3\} \subseteq \mathcal{K}\{y\}$. The transforming operators are $\{\sigma_1, \sigma_2\}$.

$$A_1 = \sigma_2^2 \sigma_1 y^2, A_2 = \sigma_2 \sigma_1^3 y + \sigma_2 y, A_3 = \sigma_2^3 \sigma_1^2 y + \sigma_2^4 y \tag{3}$$

Let vec$(\mathcal{A})$ denotes all the vec$(\mathcal{A}_i)$ for a chain $\mathcal{A}$. Then, elements of vec$(\mathcal{A})$ are represented by circles in Figure 1. We have $\mathbb{PA}_{\mathcal{A}} = \{y, \sigma_2 \sigma_1 y, \sigma_2 \sigma_1^2 y, \sigma_1^i y, \sigma_2^j y \mid i, j \in \mathbb{N}\}$.

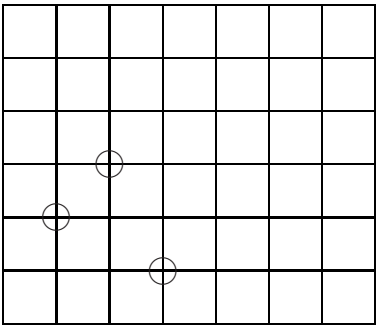

Fig. 1. The vec($\mathcal{A}$) for $\mathcal{A}$

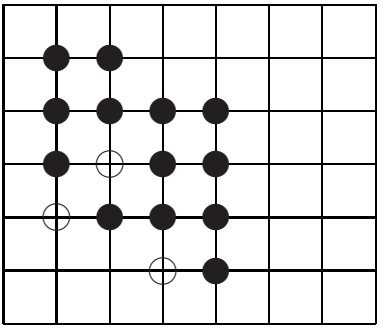

Fig. 2. The vec($\mathcal{A}_P$) for $\mathcal{A}_P$

For $P = \sigma_2^3\sigma_1^4 y + \sigma_2^4 y$, we have $\mathcal{A}_P = \{A_1, \sigma_2 A_1, \sigma_1 A_1, A_2, \sigma_2^2 A_1, A_3, \sigma_2 A_2, \sigma_1 A_2, \sigma_2^3 A_1, \sigma_2 A_3, \sigma_1 A_3, \sigma_2\sigma_1 A_2, \sigma_2^2 A_3, \sigma_2\sigma_1 A_3, \sigma_1^2 A_3, \sigma_2\sigma_1^2 A_3\}$. The elements of vec($\mathcal{A}_P$) are given in Figure 2. The new elements of vec($\mathcal{A}_P$) are represented by black dots.

We use $\mathrm{prem}(f, g, x)$ to denote the algebraic pseudo-remainder of f w.r.t. g relative to variable x, $\mathrm{prem}(f, g)$ is $\mathrm{prem}(f, g, x)$ where x is the leading variable of g.

With these notations, we define the *difference pseudo remainder* of f w.r.t. $\mathcal{A}$ to be: $\mathrm{rprem}(f, \mathcal{A}) = \mathrm{prem}(f, \mathcal{A}_f)$ where the variables and their transforms in f and $\mathcal{A}$ are treated as independent algebraic variables. The following lemma is clear.

Lemma 10. *Let $f, \mathcal{A}$ be as above and $r = \mathrm{rprem}(f, \mathcal{A})$. Then, there is a $J \in \mathbb{I}_{\mathcal{A}}$ such that $\mathbf{u}_J < \mathbf{u}_f$,*

$$Jf \equiv r \bmod [\mathcal{A}] \tag{4}$$

and r is reduced w.r.t. $\mathcal{A}$. Equation (4) is called the *remainder formula*.

3.2 Coherent Chains

It is clear that the prolongation of a chain is not unique since for some $A \in \mathcal{A}_{\mathbb{P}}$ we may choose different A_1 and A_2 in $\mathcal{A}$ to generate $A : \mathbf{u}_A = \mathbf{u}_{\theta_1 A_1} = \mathbf{u}_{\theta_2 A_2}$. The concept of coherent chain is to guarantee that all these different prolongations of a chain are equivalent in certain sense.

Definition 11. *Let $\mathcal{A} = A_1, \ldots, A_l$ be a chain in $\mathcal{K}\{\mathbb{X}\}$ and $v_i = \mathrm{vec}(\mathbf{u}_{A_i})$, $i = 1, \ldots, l$. For any $1 \le i < j \le m$, if $\mathrm{class}(A_i) = \mathrm{class}(A_j) = t$, let the least common multiple transform of $\mathbf{u}_{A_i}$ and $\mathbf{u}_{A_j}$ be $\eta_{i,j}\mathbf{u}_{A_i} = \eta_{j,i}\mathbf{u}_{A_j}$. We define the Δ-*polynomials *of A_i and A_j as $\Delta_{j,i} = \eta_{j,i}A_j$ and $\Delta_{i,j} = \eta_{i,j}A_i$. If $\mathrm{rprem}(\Delta_{i,j}, \mathcal{A}) = 0$ and $\mathrm{rprem}(\Delta_{j,i}, \mathcal{A}) = 0$, we call $\mathcal{A}$ a* coherent chain. *Let $\Delta(\mathcal{A})$ be the set of all the Δ-polynomials of $\mathcal{A}$.*

Let $\mathcal{A} = A_1, \ldots, A_l$ be a chain. A representation $g = \sum_{i,j} g_{i,j}\eta_{i,j}A_i$ is called *canonical representation* if $\eta_{i,j}A_i$ in the expression are distinct elements in $\mathcal{A}_f$ for some polynomial f. In other words, $g \in (\mathcal{A}_f)$.

Let $\mathcal{A}^* = \mathcal{A}_{\mathcal{A}}$.

Lemma 12. *With the notation of Definition 11. Then the initials appeared in* $\mathrm{rprem}(\Delta_{j,i}, \mathcal{A})$ *are all in* $I_{\mathcal{A}^*}$.

Proof: It is apparent due to the definition of the coherent chain. ∎

Lemma 13. *Let* $\mathcal{A}$ *be a coherent chain of form (1),* $A \in \mathcal{A}$, *and* $\eta \in T_\sigma$. *Then there is a* $J \in \mathbb{I}_{\mathcal{A}}$ *such that* $\mathbf{u}_J < \mathbf{u}_{\eta A}$ *and* $J\eta A$ *has a canonical representation.*

Proof: Let $c = \mathrm{class}(A)$. The polynomials in $\mathcal{A}$ with class c are $A_{c,1}, \ldots, A_{c,i-1}$, $A_{c,i} = A, \ldots, A_{c,k_c}$.

First, if $\mathbf{u}_{\eta A}$ is not the multiple transform of any one of $\mathbf{u}_{A_1}, \ldots, \mathbf{u}_{A_{i-1}}$, $\mathbf{u}_{A_{i+1}} \ldots, \mathbf{u}_{A_{c,k_c}}$, then $\eta A \in \mathcal{A}_{\eta A}$. Second, suppose that $\mathbf{u}_{\eta A}$ is the multiple transform of $\mathbf{u}_{A_{c,k}}$, but $\eta A \in \mathcal{A}_{\eta A}$.

Otherwise, we will prove this by induction on the ordering of $\mathbf{u}_{\eta A}$. Let the least common transform of $\mathbf{u}_A$ and $\mathbf{u}_{A_{c,k}}$ be $\mathbf{u}_{\eta_i A} = \mathbf{u}_{\eta_k A_{c,k}}$, $\Delta_{i,k} = \eta_i A$, $\bar{\eta}\eta_i = \eta$, so $\eta A = \bar{\eta}\Delta_{i,k}$. Since $\mathcal{A}$ is a coherent chain, $\mathrm{rprem}(\Delta_{i,k}, \mathcal{A}) = 0$. We have

$$\bar{J}\Delta_{i,k} = g_1\tau_1 B_1 + g_2\tau_2 B_2 + \cdots$$

where $B_j \in \mathcal{A}$, $\tau_j B_j \in \mathcal{A}_{\Delta_{i,j}}$, and $\mathbf{u}_{\bar{J}} < \mathbf{u}_{\Delta_{i,k}}$, $\mathrm{degree}(\Delta_{i,k}, \mathbf{u}_{\Delta_{i,k}}) \geq \mathrm{degree}(\tau_1 B_1, \mathbf{u}_{\tau_1 B_1})$, $\mathbf{u}_{\Delta_{i,k}} = \mathbf{u}_{\tau_1 B_1} > \mathbf{u}_{\tau_2 B_2} > \cdots$. Let $\bar{\eta}$ act on the two sides of the above equation and we get

$$\bar{\eta}\bar{J} \cdot \bar{\eta}\Delta_{i,j} = \bar{\eta}g_1 \cdot \bar{\eta}\tau_1 B_1 + \bar{\eta}g_2 \cdot \bar{\eta}\tau_2 B_2 + \cdots$$

We denote it by

$$J_1\eta A = \bar{g}_1 \cdot \rho_1 B_1 + \bar{g}_2 \cdot \rho_2 B_2 + \cdots$$

where $J_1 = \bar{\eta}\bar{J}$, $\mathbf{u}_{J_1} < \eta A$, $\rho_j = \bar{\eta}_j\tau_j$. If $\rho_1 B_1$ is not of the first two cases, we continue the above process on $\rho_1 B_1$ until we get (after rearrange the symbols properly)

$$J_2\eta A = f_1 \cdot \theta_1 C_1 + f_2 \cdot \theta_2 C_2 + \cdots$$

where $C_j \in \mathcal{A}$ $\theta_j \in T_\sigma$ $\mathbf{u}_{\eta A} = \mathbf{u}_{\theta_1 C_1} > \mathbf{u}_{\theta_2 C_2} > \cdots$ and $\theta_1 C_1$ is of the first two cases, any $\theta_2 C_2, \theta_3 C_3, \ldots$ satisfy the induction hypothesis. Then there is a $J \in \mathbb{I}_{\mathcal{A}}$ such that $J\eta A$ has a canonical representation.

The following is the main property of the coherent chain.

Theorem 14. *If* $\mathcal{A} = A_1, \ldots, A_l$ *is a coherent chain, then for any* $f = \sum g_{i,j}\eta_j A_i$, *there is a* $J \in \mathbb{I}_{\mathcal{A}}$ *such that* $J \cdot f$ *has a canonical representation and* $\mathbf{u}_J < \max\{\mathbf{u}_{\eta_j A_i}\}$.

Proof: This is a direct consequence of Lemma 13.

Canonical representations are useful because in a canonical representation $\sum g_{i,j}\eta_j A_i$ the polynomial $\eta_i A_i$ with the largest leader is unique and can be eliminated under certain conditions.

4 Regular Chains

Let $\mathcal{A}$ be a chain of form (1), f a polynomial. f is said to be *partial difference invertible, (or invertible)* w.r.t. $\mathcal{A}$ if it is invertible w.r.t. $\mathcal{A}_f$ when f and $\mathcal{A}_f$ are treated as algebraic polynomials.

Definition 15. *Let $\mathcal{A} = A_1, \ldots, A_m$ be a chain and $I_i = \mathrm{init}(A_i)$. $\mathcal{A}$ is said to be (difference) regular if ηI_j is invertible w.r.t. $\mathcal{A}$ for any $\eta \in T_\sigma$ and $1 \leq j \leq m$.*

Lemma 16. *Let $\mathcal{A}$ be a characteristic set of an ideal I. If a polynomial f is invertible w.r.t. $\mathcal{A}$, then $f \notin I$.*

Proof: Let $\mathbb{U}$ be the algebraic parameter set of $\mathcal{A}$. Since f is invertible w.r.t. $\mathcal{A}$, there exists a polynomial g and a nonzero $r \in \mathcal{K}[\mathbb{U}]$ such that $gf = r \mod [\mathcal{A}]$. If $f \in I$, we have $r \in I$. Since r is reduced w.r.t. $\mathcal{A}$, by Lemma 3, we have $r = 0$, a contradiction. ∎

Lemma 17. *If $\mathcal{A}$ is a regular chain of form (1), then $\mathcal{A}_f$ is a regular algebraic triangular set for any polynomial f.*

Proof: If $\mathcal{A}$ is difference regular, then by Definition 15, all ηI_j are invertible w.r.t. $\mathcal{A}$. The initials of the polynomials in $\mathcal{A}_f$ are all of the form ηI_j and they are of ordering lower than the highest ordering of the polynomials in $\mathcal{A}_f$. Then, by Definition 4, $\mathcal{A}_f$ is a regular algebraic triangular set. ∎

Lemma 18. *If a chain $\mathcal{A}$ of form (1) is the characteristic set of $\mathbf{sat}(\mathcal{A})$, then for any polynomial f, $\mathcal{A}_f$ is a regular algebraic triangular set.*

Proof. By Lemma 5, we need only to prove that $\mathcal{B} = \mathcal{A}_f$ is the characteristic set of $\mathbf{a\text{-}sat}(\mathcal{B})$. Let W be the set of all the ηy_j such that ηy_j is of lower or equal ordering than an $\bar{\eta} y_j$ occurring in $\mathcal{B}$. Then $\mathcal{B} \subset \mathcal{K}[W]$. If $\mathcal{B}$ is not the characteristic set of $\mathbf{a\text{-}sat}(\mathcal{B})$, then there is a $g \in \mathbf{a\text{-}sat}(\mathcal{B}) \cap \mathcal{K}[W]$ which is reduced w.r.t. $\mathcal{B}$ and is not zero. g does not contain ηy_i which is of higher ordering than those in W. As a consequence, g is also reduced w.r.t. $\mathcal{A}$. Since $g \in \mathbf{a\text{-}sat}(\mathcal{B}) \subset \mathbf{sat}(\mathcal{A})$ and $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$, g must be zero, a contradiction. ∎

As pointed out in [13], the Rosenfeld Lemma [21] for differential equations can not be extended to difference case. Correspondingly, we have:

Lemma 19. *Let $\mathcal{A}$ be a coherent and regular chain, and r a polynomial reduced w.r.t. $\mathcal{A}$. If $r \in \mathbf{sat}(\mathcal{A})$, then $r = 0$.*

Proof. Let $\mathcal{A} = A_1, A_2, \ldots, A_l$. Since $r \in \mathbf{sat}(\mathcal{A})$, there is a $J_1 \in \mathbb{I}_\mathcal{A}$ such that $J_1 \cdot r \equiv 0 \bmod [\mathcal{A}]$. By Lemma 6, J_1 is difference invertible w.r.t. $\mathcal{A}$, i.e. there is a polynomial $\bar{J}_1$ and a nonzero $N \in \mathcal{K}[V]$ such that

$$\bar{J}_1 \cdot J_1 \equiv N \bmod [\mathcal{A}]$$

where V is the set of parameters of A_{J_1} as an algebraic triangular set. Hence,

$$Nr \equiv \bar{J}_1 \cdot J_1 \cdot r \equiv 0 \bmod [\mathcal{A}].$$

Or equivalently,

$$N \cdot r = \sum g_{i,j}\eta_{i,j}A_j. \tag{5}$$

Since $\mathcal{A}$ is a coherent chain, by Theorem 14, there is a $J_2 \in \mathbb{I}_{\mathcal{A}}$ such that $J_2 \cdot N \cdot r$ has a canonical representation in $[\mathcal{A}]$, where $\mathbf{u}_{J_2} < \max\{\mathbf{u}_{\eta_{i,j}A_j}\}$ in (5). That is

$$J_2 \cdot N \cdot r = \sum_{ij} \bar{g}_{i,j}\rho_{i,j}A_j, \tag{6}$$

where, $\mathbf{u}\rho_{i,j}A_j$ are pairwise different. If $\max\{\mathbf{u}_{\rho_{i,j}A_j}\}$ in (6) is lower in ordering than $\max\{\mathbf{u}_{\eta_{i,j}A_j}\}$ in (5), we have already reduced the highest ordering of $\mathbf{u}_{\eta_{i,j}A_j}$ in (5). Otherwise, assume $\mathbf{u}_{\rho_a A_b} = \max\{\mathbf{u}_{\rho_{i,j}A_j}\}$ and $A_b = I_b \cdot \mathbf{u}_{A_b}^{d_b} + R_b$. Substituting $\mathbf{u}_{\rho_a A_b}^{d_b}$ by $-\frac{\rho_a R_b}{\rho_a I_b}$ in (6), the left side keeps unchanged since $\mathbf{u}_{J_2} < \mathbf{u}_{\rho_a A_b}$, N is free of $\mathbf{u}_{\rho_a A_b}$ and $\deg(r, \mathbf{u}_{\rho_a A_b}) < \deg(\rho_a A_b, \mathbf{u}_{\rho_a A_b})$. In the right side, the $\rho_a A_b$ becomes zero, i.e. $\max\{\mathbf{u}_{\rho_{i,j}A_j}\}$ decreases. Clearing denominators of the substituted formula of (6), we obtain a new equation:

$$(\rho_a I_b)^t \cdot J_2 \cdot N \cdot r = \sum f_{ij}\tau_{i,j}A_j. \tag{7}$$

Note that in the right side of (7), the highest ordering of $\tau_{i,j}A_j$ is less than $\mathbf{u}_{\rho_a A_b}$ and $(\rho_a I_b)^t \cdot J_2$ is invertible w.r.t. $\mathcal{A}$. Then after multiplying a polynomial which is invertible w.r.t. $\mathcal{A}$ and can be represented as a linear combination of $\tau_{i,j}A_j$ all of which is strictly lower than $\mathbf{u}_{\rho_a A_b}$. Repeating the above process, we can obtain a nonzero $\bar{N}$, such that $\bar{N} \cdot r = 0$. Then $r = 0$. By Lemma 3, $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$. ∎

The following is one of the main results in this paper.

Theorem 20. *A chain $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$ iff $\mathcal{A}$ is coherent and difference regular.*

Proof: If $\mathcal{A}$ is coherent and difference regular, then by Lemma 19, any polynomial in $\mathbf{sat}(\mathcal{A})$ which is difference reduced w.r.t. $\mathcal{A}$ is zero. So $\mathcal{A}$ is a characteristic set of $\mathbf{sat}(\mathcal{A})$. Conversely, let $\mathcal{A} = A_1, A_2, \ldots, A_l$ be a characteristic set of the saturation ideal $\mathbf{sat}(\mathcal{A})$ and $I_i = \mathrm{init}(A_i)$. For any $1 \leq i < j \leq l$, let $r = \mathrm{rprem}(\Delta_{i,j}, \mathcal{A})$ as in Definition 11. Then r is in $\mathbf{sat}(\mathcal{A})$ and is difference reduced w.r.t. $\mathcal{A}$. Since $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$, $r = 0$. Then $\mathcal{A}$ is coherent. To prove that $\mathcal{A}$ is regular, for any $0 \leq i \leq l$, $\eta \in T_\sigma$ we need to prove that $f = \eta I_i$ is invertible w.r.t. $\mathcal{A}$. Assume this is not true. By definition, f is not invertible w.r.t. $\mathcal{A}_f$ when they are treated as algebraic equations. By Lemma 18, $\mathcal{A}_f$ is a regular algebraic triangular set. By Lemma 7, there is a $g \neq 0$ which is reduced w.r.t. $\mathcal{A}_g$ (and hence $\mathcal{A}$) such that $f \cdot g \in (A_f) \subset [A]$. Since $f = \eta I_i \in \mathbb{I}_{\mathcal{A}}$, $g \in \mathbf{sat}(\mathcal{A})$ and g is reduced w.r.t. $\mathcal{A}$. Since $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$, we have $g = 0$, a contradiction. Hence, $f = \eta I_i$ is invertible w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is difference regular. ∎

Theorem 21. *If $\mathcal{A}$ is a coherent and difference regular chain of form (1),then*

$$\mathbf{sat}(\mathcal{A}) = \cup_{f \in \mathcal{K}\{\mathbb{X}\}} \mathbf{a\text{-}sat}(\mathcal{A}_f).$$

Proof: It is easy to see that $\mathbf{sat}(\mathcal{A}) \supset \bigcup_{f \in \mathcal{K}\{\mathbb{X}\}} \mathbf{a\text{-}sat}(\mathcal{A}_f)$. If $f \in \mathbf{sat}(\mathcal{A})$, since $\mathcal{A}$ is coherent and difference regular chain, and $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$, we have $\mathrm{rprem}(f, \mathcal{A}) = 0$, or $\mathrm{prem}(f, \mathcal{A}_f) = 0$, that is $f \in \mathbf{a\text{-}sat}(\mathcal{A}_f)$. Hence $\mathbf{sat}(\mathcal{A}) \subset \bigcup_{f \in \mathcal{K}\{\mathbb{X}\}} \mathbf{a\text{-}sat}(\mathcal{A}_f)$. ∎

Note that we cannot check whether a chain is regular directly due to the reason that T_σ contains an infinite number of elements. To give a complete zero decomposition algorithm like the one in [13,15], we need to define a type of chains such that we have a constructive criterion to check whether it is regular and the chain $\mathcal{A}$ is non-trivial in the sense that $\mathrm{Zero}(\mathbf{a\text{-}sat}(\mathcal{A})) \neq \emptyset$. These problems are the major open ones for the characteristic set method of partial difference polynomial systems.

5 Characteristic Set of Reflexive Prime Difference Ideals

In the algebraic and differential cases, prime ideals can be described by irreducible chains. In this section, we will extend this result to the partial difference case. In order to do that, we need to introduce the concept of strongly irreducible chains.

A chain $\mathcal{A}$ is called *strongly irreducible* if

- $\mathcal{A}_f$ is an irreducible algebraic triangular set for any $f \in \mathcal{K}\{\mathbb{X}\}$, and
- For $\eta \in T_\sigma$ and $h \in \mathcal{K}\{\mathbb{X}\}$, if $\eta h \in \mathbf{a\text{-}sat}(\mathcal{A}_f)$ then $h \in \mathbf{a\text{-}sat}(\mathcal{A}_f)$.

Theorem 22. *Let $\mathcal{A}$ be a coherent and strongly irreducible difference chain. Then $\mathbf{sat}(\mathcal{A})$ is a reflexive prime difference ideal.*

Proof: Let f, g be two r-pols such that $fg \in \mathbf{sat}(\mathcal{A})$. By Lemma 21, there exists a polynomial h such that $fg \in D = \mathbf{a\text{-}sat}(\mathcal{A}_h)$. Since $\mathcal{A}$ is strongly irreducible, $\mathcal{A}_h$ is an irreducible algebraic triangular set and hence D is a prime ideal. We thus have $f \in D$ or $g \in D$. In other words, $f \in \mathbf{sat}(\mathcal{A})$ or $g \in \mathbf{sat}(\mathcal{A})$. Hence, $\mathbf{sat}(\mathcal{A})$ is a prime ideal. We still need to show that $\mathbf{sat}(\mathcal{A})$ is reflexive. If $\sigma_i f \in \mathbf{sat}(\mathcal{A})$ then $\exists\ h \in \mathcal{K}\{\mathbb{X}\}$, $\sigma_i f \in \mathbf{a\text{-}sat}(\mathcal{A}_h)$. $f \in \mathbf{a\text{-}sat}(\mathcal{A}_h)$ according to the definition of strongly irreducible chain. Then $f \in \mathbf{sat}(\mathcal{A})$. ∎

To prove that the characteristic set of any prime ideal is strongly irreducible, we need the following lemmas.

Lemma 23. *Let $\mathcal{I}$ be a prime difference ideal, $\mathcal{A}$ its characteristic set. Then $\mathcal{I} = \mathbf{sat}(\mathcal{A})$.*

Proof: It is clear that $\mathcal{I} \subset \mathbf{sat}(\mathcal{A})$. Let $f \in \mathbf{sat}(\mathcal{A})$. Then there is a $J \in \mathbb{I}_\mathcal{A}$ such that $Jf \in [A] \subset \mathcal{I}$. By Theorem 20, J is invertible w.r.t. $\mathcal{A}$. Hence J is not in $\mathcal{I}$ by Lemma 16. Since $\mathcal{I}$ is a prime ideal, $f \in \mathcal{I}$. ∎

Lemma 24. *Let $\mathcal{I}$ be a reflexive prime difference ideal, $\mathcal{A}$ its characteristic set. Then $\forall\ h \in f \in \mathcal{K}\{\mathbb{X}\}$, $\mathcal{A}_h$ is algebraic irreducible.*

Proof: Otherwise, there exists an $h \in f \in \mathcal{K}\{\mathbb{X}\}$, such that $\mathcal{A}_h$ is a reducible algebraic triangular set. By definition, there exist polynomials f and g which are reduced w.r.t. $\mathcal{A}_h$ such that $fg \in \mathcal{A}_h \subset \mathbf{sat}(\mathcal{A}) = \mathcal{I}$. From this, we have $f \in \mathcal{I}$ or $g \in \mathcal{I}$, which is impossible since f and g are reduced w.r.t. $\mathcal{A}$. ∎

Theorem 25. *Let $\mathcal{I}$ be a reflexive prime difference ideal, $\mathcal{A}$ a characteristic set of $\mathcal{I}$. Then $\mathcal{A}$ is coherent, strongly irreducible, and $\mathcal{I} = \mathbf{sat}(\mathcal{A})$.*

Proof: By Lemma 23, for any characteristic set $\mathcal{A}$ of $\mathcal{I}$, we have $\mathcal{I} = \mathbf{sat}(\mathcal{A})$. By Theorem 20, $\mathcal{A}$ is coherent. By Lemma 24, we have for any $h \in \mathcal{K}\{\mathbb{X}\}$, $\mathcal{A}_h$ is algebraic irreducible. Also, if $\sigma_i g \in \mathbf{a\text{-}sat}(\mathcal{A}_h)$, then $\sigma_i g \in \mathcal{I}$. Since $\mathcal{I}$ is reflexive, $g \in \mathcal{I}$. Then $g \in \mathbf{a\text{-}sat}(\mathcal{A}_h)$. ∎

The following example shows that it is difficult to decide whether a chain is strongly irreducible. Even in the the ordinary case, deciding whether a chain is strongly irreducible is a major difficult problem in difference algebra.

Example 2. [10] Let $\mathcal{K} = Q(t)$. The transforming operators over $\mathcal{K}$ is σ such that $\sigma t = (t+1)$. $\mathcal{A} \subseteq \mathcal{K}\{x_1, x_2\}$ and $\mathcal{A} = \{\mathcal{A}_1, \mathcal{A}_2\}$ where $A_1 = x_1^2 + t, A_2 = x_2^2 + t + k$. If $k > 1$, $A_2 - \sigma^k A_1 = (x_2 - \sigma^k x_1)(x_2 + \sigma^k x_1)$, $x_2 - \sigma^k x_1 \notin \mathbf{sat}(\mathcal{A})$, $x_2 + \sigma^k x_1 \notin \mathbf{sat}(\mathcal{A})$. $\mathbf{sat}(\mathcal{A})$ is not a prime difference ideal, and $\mathcal{A}$ is not strongly irreducible.

6 Algorithms of Zero Decomposition

In this section, we will present an algorithm which can be used to decompose the zero set of a general polynomial set into the zero sets of coherent chains.

Lemma 26. *Let $\mathbb{P}$ be a finite set of polynomials, $\mathcal{A} = A_1, \ldots, A_m$ a characteristic set of $\mathbb{P}$, $I_i = \mathrm{init}(A_i)$, and $J = \prod_{i=1}^m I_i$. If $\mathrm{prem}(P, \mathcal{A}) = 0$ for all $P \in \mathbb{P}$, then*

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathcal{A}/J) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \{I_i\})$$
$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbf{sat}(\mathcal{A})) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \{I_i\})$$

Proof: This is direct consequence of the remainder formula (4). ∎

Now, we can give the *zero decomposition theorem.*

Theorem 27. *Let $\mathbb{P}$ be a finite set of polynomials in $\mathcal{K}\{y_1, \ldots, y_n\}$, then we can obtain a sequence of coherent chains $\mathcal{A}_i$, $i = 1, \ldots, k$ such that*

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathcal{A}_i / I_{\mathcal{A}_i}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i)) \tag{8}$$

We first give the following algorithm to find the decomposition.

Algorithm 28. ZDT($\mathbb{P}$)

- **Input:** *a finite set* $\mathbb{P}$ *of polynomials.*
- **Output:** $W = \{\mathcal{A}_1, \ldots, \mathcal{A}_k\}$ *s.t.* $\mathcal{A}_i$ *is coherent and* $\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i))$.

Begin
  $\mathcal{B} = CS(\mathbb{P})$ *//This gives the characteristic set of* $\mathbb{P}$.
  If $\mathcal{B} = 1$ *then* $W = \{\}$
  Else
    $\mathbb{R} = \{\mathrm{prem}(f, \mathcal{B}) \neq 0 \mid f \in (\mathbb{P} \setminus \mathcal{B}) \cup \triangle(\mathcal{B})\}$
    If $\mathbb{R} = \emptyset$ *then* $W = \{\mathcal{B}\} \cup \cup_i \mathbf{ZDT}(\mathbb{P} \cup \{I_i\})$
    Else $W = \mathbf{ZDT}(\mathbb{P} \cup \mathbb{R})$
      where I_j *are the initials of the polynomials in* $\mathcal{B}$.
End.

Proof of Correctness of Algorithm 28. If $\mathbb{R} = \emptyset$, by Lemma 26, we obtain a chain. Since I_j is reduced w.r.t. $\mathcal{B}$, by Lemma 2, the characteristic set of $\mathbb{P} \cup \{I_i\}$ is of lower ordering than that of $\mathcal{B}$. Similarly, the characteristic set of $\mathbb{P} \cup \mathbb{R}$ is of lower ordering than that of $\mathcal{B}$. By Lemma 1, the algorithm will end and give the decomposition. ∎

Example 3. Let $\mathcal{A} = \{A_1, A_2\}$ where $A_1 = \sigma_1^2 y_3^2 + \sigma_2 y_2$, $A_2 = \sigma_2 y_3 + \sigma_1^2 y_1$. $\mathcal{A}$ is not coherent, since the remainder $A_3 = \mathrm{rprem}(\sigma_2 A_1, \mathcal{A}) = \sigma_2^2 y_2 + \sigma_1^4 y_1^2$ is reduced w.r.t. $\mathcal{A}$. If we do the zero decomposition for $\mathcal{A}$ we obtain $\{A_3, A_1, A_2\}$ which is a coherent chain.

7 Conclusion

In this paper, we extend some of the main properties of chains to the partial difference polynomial systems. We prove that a partial difference chain is the characteristic set of its saturation ideal if and only if it is coherent and regular. We also prove that a partial difference ascending chain is the characteristic set of a reflexive prime ideal if and only if it is strongly irreducible. Finally, we give the zero decomposition algorithm.

Comparing to the algebraic, differential, and ordinary difference cases, there still exist major problems unsolved in the partial difference case. These include to give a constructive criterion for a chain to be regular and non-trivial and to solve the perfect ideal membership problem.

References

1. Aubry, P.: Ensembles Triangulaires de polynômes et Résolution de Systèmes Algébriques, Implantation en Axiom. Thèse de l'université Pierre et Marie Curie (1999)
2. Aubry, P., Lazard, D., Moreno Maza, M.: On the Theory of Triangular Sets. Journal of Symbolic Computation 28, 105–124 (1999)

3. Bentsen, I.: The Existence of Solutions of Abstract Partial Difference Polynomial. Trans. of AMS 158, 373–397 (1971)
4. Boulier, F., Lazard, D., Ollivier, F., Petitot, M.: Representation for the Radical of a Finitely Generated Differential Ideal. In: Proc. of ISSAC 1995, pp. 158–166. ACM Press, New York (1995)
5. Boulier, F., Lemaire, F., Moreno Maza, M.: Well Known Theorems on Triangular Systems and the D5 Principle. In: Proc. of Transgressive Computing 2006, pp. 79–91 (2006)
6. Bouziane, D., Kandri Rody, A., Mârouf, H.: Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. Journal of Symbolic Computation 31, 631–649 (2001)
7. Cheng, J.S., Gao, X.S., Yap, C.K.: Complete Numerical Isolation of Real Zeros in Zero-dimensional Triangular Systems. In: Prof. ISSAC 2007, pp. 92–99. ACM Press, New York (2007)
8. Chou, S.C.: Mechanical Geometry Theorem Proving. Kluwer Academic Publishers, Norwell (1987)
9. Chou, S.C., Gao, X.S.: Ritt-Wu's Decomposition Algorithm and Geometry Theorem Proving. In: Stickel, M.E. (ed.) CADE 1990. LNCS, vol. 449, pp. 207–220. Springer, Heidelberg (1990)
10. Cohn, R.M.: Difference Algebra. Interscience Publishers (1965)
11. Dahan, X., Moreno Maza, M., Schost, E., Wu, W., Xie, Y.: Lifting Techniques for Triangular Decompositions. In: Proc. ISSAC 2005, pp. 108–115. ACM Press, New York (2005)
12. Gao, X.S., Chou, S.C.: A Zero Structure Theorem for Differential Parametric Systems. Journal of Symbolic Computation 16, 585–595 (1994)
13. Gao, X.S., Luo, Y.: A Characteristic Set Method for Difference Polynomial Systems. In: International Conference on Polynomial System Solving, November 24-26 (2004); Submitted to JSC
14. Gao, X.S., Luo, Y., Zhang, G.: A Characteristic Set Method For Ordinary Difference Polynomial Systems. MM-Preprints 25, 84–102 (2006)
15. Gao, X.S., van der Hoeven, J., Yuan, C., Zhang, G.: A Characteristic Set Method for Differential-Difference Polynomial Systems. In: MEGA 2007, Strobl, Austria (July 2007)
16. Hubert, E.: Factorization-free Decomposition Algorithms in Differential Algebra. Journal Symbolic Computation 29, 641–662 (2000)
17. Kolchin, E.: Differential Algebra and Algebraic Groups. Academic Press, New York (1973)
18. Kondratieva, M.V., Levin, A.B., Mikhalev, A.V., Pankratiev, E.V.: Differential and Difference Dimension Polynomials. Kluwer Academic Publishers, Dordrecht (1999)
19. Ritt, J.F.: Differential Algebra, Amer. Math. Soc. Colloquium (1950)
20. Ritt, J.F., Raudenbush Jr., H.W.: Ideal Theory and Algebraic Difference Equations. Trans. of AMS 46, 445–452 (1939)
21. Rosenfeld, A.: Specialization in Differential Algebra. Trans. Am. Math. Soc 90, 394–407 (1959)
22. Wang, D.: Elimination Methods. Springer, Berlin (2000)
23. Wu, W.T.: On the Decision Problem and the Mechanization of Theorem in Elementary Geometry. Scientia Sinica 21, 159–172 (1978)
24. Wu, W.T.: A Constructive Theorey of Differential Algebraic Geometry. Lect. Notes in Math, vol. 1255, pp. 173–189. Springer, Heidelberg (1987)

25. Wu, W.T.: Basic Principle of Mechanical Theorem Proving in Geometries (in Chinese). Science Press, Beijing (1984); English Edition. Springer, Wien (1994)
26. van der Hoeven, J.: Differential and Mixed Differential-Difference Equations from the Effective Viewpoint (preprints, 1996)
27. Yang, L., Zhang, J.Z., Hou, X.R.: Non-linear Algebraic Equations and Automated Theorem Proving (in Chinese). ShangHai Science and Education Pub., ShangHai (1996)