Available online at www.sciencedirect.com
ScienceDirect
Acta Mathematica Scientia 2009,**29B**(4):1063–1080
Acta Mathematica Scientia 数学物理学报
http://actams.wipm.ac.cn

RITT-WU'S CHARACTERISTIC SET METHOD FOR ORDINARY DIFFERENCE POLYNOMIAL SYSTEMS WITH ARBITRARY ORDERING*

Dedicated to Professor Wu Wenjun on the occasion of his 90th birthday

Gao Xiaoshan (高小山)   *Yuan Chunming* (袁春明)   *Zhang Guilin* (张桂林)
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS, Chinese Academy of Sciences, Beijing 100080, China
E-mail: xgao@mmrc.iss.ac.cn; guilin80@163.com

Abstract In this paper, a Ritt-Wu's characteristic set method for ordinary difference systems is proposed, which is valid for any admissible ordering. New definition for irreducible chains and new zero decomposition algorithms are also proposed.

Key words difference polynomial; ascending chain; characteristic set; Ritt-Wu's zero decomposition theorem

2000 MR Subject Classification 12H10

1 Introduction

Ritt-Wu's characteristic set method is the cornerstone of Wu's work on mathematics mechanization [15–18]. The idea of the method is to decompose the zero set of an equation system into the union of the zero sets of equation systems in triangular forms. The characteristic set method has been developed for polynomial systems [1, 4, 6, 15, 19] and differential polynomial systems [2, 3, 10, 11, 13, 16].

Recently, a characteristic set method is also developed for ordinary difference polynomial systems [8]. The concept of characteristic set for difference polynomial systems was introduced by Ritt [14] and further studied in [12]. The theory of difference algebra was developed by Cohn [5]. But, no algorithms were given in these work. The main contribution of [8] is to introduce the concept of proper irreducible chains and to give a zero decomposition algorithm for difference polynomial systems. But the theory given in [8] has several drawbacks. First, the definition of the proper irreducible chain is not natural. Second, the variable ordering is fixed. In this paper, we propose a new characteristic set method to remedy these drawbacks.

We give a new definition for the concept of proper irreducible chain. Comparing to the old definition, the new definition is more natural. We show that if a chain is proper irreducible in the

*Received February 18, 2009

old sense, then it is also proper irreducible according to the new definition. As a consequence, results proved in the above mentioned paper are still correct. Another advantage of using the new definition is that the following result is now valid: the characteristic set of a reflexive prime ideal is coherent and strong irreducible. If using the old definition, we can only prove that: there exists a variable order such that the characteristic set of a reflexive prime ideal is coherent and strong irreducible under this variable order.

The new characteristic set method works for any admissible ordering. This extends the scope of the method significantly. As an application of this extension, we give a direct proof for an important result about difference polynomial systems, which is used in control theory in Theorem 3.15. This result cannot be proved with the theory in [8].

With the new definition of the proper irreducible chain, the zero decomposition algorithm in Section 4 is also updated. The new algorithm appears much simpler than the old one.

In [5], Cohn gave an algorithm to solve the Nullstellensatz test of perfect difference ideals. The idea is to transform the problem to a difference ideal with order less than or equal to one and then use zero decomposition algorithms in algebraic case to construct a difference kernel. This certainly simplifies the problem. On the other hand, reducing the order of difference polynomials to one by introducing new auxiliary variables destroys the structure of the ideal itself, and as consequence cannot give a zero decomposition for the equation system. In Section 5, by combining the idea of Cohn and the concept of algebraic irreducible chains, we give another algorithm of zero decomposition for difference polynomial systems.

2 Preliminaries

We will introduce the notions and preliminary properties needed in this paper. Details on these concepts can be found in [5, 12].

2.1 Difference fields, difference polynomials and difference ideals

A difference field $\mathcal{F}$ is a field with a third unitary operation σ satisfying: for any $a, b \in \mathcal{F}$, $\sigma(a+b) = \sigma a + \sigma b$, $\sigma(ab) = \sigma a \cdot \sigma b$, and $\sigma a = 0$ if and only if $a = 0$. Here, σ is called the transforming operator of $\mathcal{F}$. If $a \in \mathcal{F}$, σa is called the transform of a. If $\sigma^{-1}a$ is defined for all $a \in \mathcal{F}$, we say that $\mathcal{F}$ is inversive. Every difference field has an inversive closure [5]. In this paper, all difference fields are assumed to be inversive.

Let $\mathcal{K}$ be the set of rational functions in variable x defined on the complex plane. Let σ be the mapping: $\sigma f(x) = f(x+1), f \in \mathcal{K}$. Then $\mathcal{K}$ is a difference field with transforming operator σ. This is an inversive field.

Let $x_1, x_2, \cdots, x_n$ be difference indeterminants. Then $\mathcal{R} = \mathcal{K}\{x_1, \cdots, x_n\}$ is called an n-fold difference polynomial ring over $\mathcal{K}$. Any difference polynomial f (abbr. r-pol) in the ring $\mathcal{K}\{x_1, \cdots, x_n\}$ is an ordinary polynomial in variables $\sigma^k x_j$ $(k = 0, 1, 2, \cdots,\ j = 1, \cdots, n)$. For convenience, we also denote $\sigma^k x_j$ by $x_{j,k}$.

First, we need to define an ordering $\prec$ on the set of variables $\mathbb{X} = \{x_{i,j}, 1 \le i \le n, j \ge 0\}$. We call an ordering is admissible if the following conditions hold:

1) $u_1 \prec u_2 \Rightarrow \sigma u_1 \prec \sigma u_2$, for any $u_1, u_2 \in \mathbb{X}$.

2) $u \prec \sigma u$, for any $u \in \mathbb{X}$.

We always assume that $1 \prec u$, for any $u \in \mathbb{X}$. Let $f \in \mathcal{K}\{x_1, \cdots, x_n\}$ and $\prec$ is an admissible ordering on $\mathbb{X}$.

Example 2.1 Let $x_{i,j} \prec x_{l,k}$ for any $i < l$, then the ordering is called variable ordering, which is used in [8].

Let $x_{i,j} \prec x_{l,k}$ for any $j < k$, then the ordering is called total ordering.

If $x_{p,q}$ is of the highest ordering of the variables appears in f w.r.t. $\prec$, we call x_p the leading variable and $x_{p,q}$ the lead of f, denoted as $\text{lvar}(f)$ and $\text{lead}(f)$, respectively. p is called the class of f, denoted as $\text{class}(f)$. If $f \in \mathcal{K}$, we set $\text{class}(f) = 0$. The order of f w.r.t. x_i, denoted by $\text{ord}(f, x_i)$, is the largest j such that $x_{i,j}$ appears in f. When x_i does not occur in f, we set $\text{ord}(f, x_i) = 0$.

The leading coefficient of f as a univariate polynomial in $\text{lead}(f)$ is called the initial of f, and is denoted as $\text{init}(f)$.

An r-pol f_1 has higher rank than an r-pol f_2, denoted as $f_1 \succ f_2$, if

i) $\text{lead}(f_1) \succ \text{lead}(f_2)$, or

ii) $\text{lead}(f_1) = \text{lead}(f_2) = x_{c,d}$ and $\deg(f_1, x_{c,d}) > \deg(f_2, x_{c,d})$.

If no one has higher rank than the other for two r-pols, they are said to have the same rank, denoted as $f_1 \equiv f_2$. We use $f_1 \preceq f_2$ to denote the relation of either $f_1 \prec f_2$ or $f_1 \equiv f_2$. It is easy to see that $\preceq$ is a total order on the r-pol ring.

An n-tuple over $\mathcal{K}$ is of the form $\mathbf{a} = (a_1, \cdots, a_n)$, where the a_i are selected from some difference extension field of $\mathcal{K}$. Let $f \in \mathcal{K}\{x_1, \cdots, x_n\}$. To substitute an n-tuple $\mathbf{a}$ into f means to replace each of the $x_{i,j}$ occurring in f with $\sigma^j a_i$. Let $\mathbb{P}$ be a set of r-pols in $\mathcal{K}\{x_1, \cdots, x_n\}$. 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 r-pol of $\mathbb{P}$ is zero. We use $\text{Zero}(\mathbb{P})$ to denote the set of solutions of $\mathbb{P} = 0$. Let $f \in \mathcal{K}\{x_1, \cdots, x_n\}$. We use $\text{Zero}(\mathbb{P}/\mathbb{D})$ to denote the set of solutions of $\mathbb{P} = 0$ which do not annihilate any r-pol of $\mathbb{D}$.

A difference ideal is a subset $\mathcal{I}$ of $\mathcal{R} = \mathcal{K}\{x_1, \cdots, x_n\}$, which is an algebraic ideal in $\mathcal{R}$ and is closed under transforming. A difference ideal $\mathcal{I}$ is called reflexive if for an r-pol f, $\sigma f \in \mathcal{I}$ implies $f \in \mathcal{I}$. Let $\mathbb{P}$ be a set of elements of $\mathcal{R}$. The difference ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. The (ordinary or algebraic) ideal generated by $\mathbb{P}$ is denoted as $(\mathbb{P})$. A difference ideal $\mathcal{I}$ is called perfect if the presence in $\mathcal{I}$ of a product of powers of transforms of an r-pol f implies $f \in \mathcal{I}$. The perfect difference ideal generated by $\mathbb{P}$ is denoted as $\{\mathbb{P}\}$. A perfect ideal is always reflexive. A difference ideal $\mathcal{I}$ is called a prime ideal if for r-pols f and g, $fg \in \mathcal{I}$ implies $f \in \mathcal{I}$ or $g \in \mathcal{I}$.

2.2 Difference ascending chains

Let f_1,f_2 be two r-pols and $\text{lead}(f_1) = x_{p,q}$. f_2 is said to be reduced w.r.t. f_1 if $\deg(f_2, x_{p,q+i}) < \deg(f_1, x_{p,q)})$ for any nonnegative integer i.

A finite sequence of nonzero r-pols $\mathcal{A} = A_1, \cdots, A_p$ is called an ascending chain, or simply a chain, if one of the two following conditions holds:

i) $p = 1$ and $A_1 \neq 0$, or

ii) $0 < \text{class}(A_1)$, $A_i \prec A_j$ and A_j is reduced w.r.t. A_i for $1 \leq i < j \leq p$.

$\mathcal{A}$ is called trivial if $\text{class}(A_1) = 0$.

Example 2.2 Let us consider $f_1 = x_{1,1}^2 - x_{1,0}^2 + 1$, $f_2 = x_{1,2} + x_{1,1} \in \mathcal{K}\{x_1\}$. Since $f_1 \prec f_2$, $\deg(f_2, x_{1,1}) < \deg(f_1, x_{1,1})$ and $\deg(f_2, x_{1,2}) < \deg(f_1, x_{1,1})$, by the definition, f_2 is reduced w.r.t. f_1. Hence, f_1, f_2 is a difference chain.

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

$$\mathbf{sat}(\mathcal{A}) = \{f \in \mathcal{K}\{x_1, \cdots, x_n\} \,|\, \exists g \in \mathbb{I}_{\mathcal{A}}, fg \in [\mathcal{A}]\}.$$

Let $\mathcal{B}$ be an algebraic chain and $I_{\mathcal{B}}$ the set of products of powers of initials of the polynomials in $\mathcal{B}$. Then we define the algebraic saturation ideal of $\mathcal{B}$ to be the following

$$\mathbf{a\text{-}sat}(\mathcal{B}) = \{f \in \mathcal{K}[x_1, \cdots, x_n] \,|\, \exists g \in I_{\mathcal{B}}, fg \in (\mathcal{B})\}.$$

Note that $\mathbb{I}_{\mathcal{A}}$ is closed under transforming and multiplication. Then $[\mathcal{A}] : \mathbb{I}_{\mathcal{A}}$ is a difference ideal.

A chain $\mathcal{A} = A_1, \cdots, A_t$ is said to be of higher rank than another chain $\mathcal{B} = B_1, \cdots, B_s$, denoted as $\mathcal{A} \succ \mathcal{B}$, if one of the following conditions holds:

i) $\exists\ 0 < j \le \min\{t, s\}$, such that $\forall\ i < j,\ A_i \equiv B_i$ and $A_j \succ B_j$, or

ii) $s > t$ and $A_i \equiv B_i$ for $i \le t$.

If no one has higher rank than the other for two chains, they have the same rank, and is denoted as $\mathcal{A} \equiv \mathcal{B}$. We use $\mathcal{A}_1 \preceq \mathcal{A}_2$ to denote the relation of either $\mathcal{A}_1 \prec \mathcal{A}_2$ or $\mathcal{A}_1 \equiv \mathcal{A}_2$. It is easy to see that $\preceq$ is a total order on the difference chain set.

Lemma 2.3 [14] Any descending chain $\mathcal{A}_1 \succ \mathcal{A}_2 \succ \mathcal{A}_3 \succ \ldots$ is finite.

Let $\mathbb{P}$ be a set of r-pols. It is possible to form chains with r-pols in $\mathbb{P}$. Among all those chains, by the above lemma, there are some which have a lowest rank. Any of those chains contained in $\mathbb{P}$ with the lowest rank is called a characteristic set of $\mathbb{P}$, and denoted by $\mathcal{B} = C.S(\mathbb{P})$.

An r-pol is said to be reduced w.r.t. a chain if it is reduced to every r-pol in the chain.

Lemma 2.4 [14] If $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ and $\mathcal{A}^{'}$ a characteristic set of $\mathbb{P} \cup \{f\}$ for an r-pol f, then we have $\mathcal{A} \succeq \mathcal{A}^{'}$. Moreover, if f is reduced with respect to $\mathcal{A}$, we have $\mathcal{A} \succ \mathcal{A}^{'}$.

As a consequence, we have

Lemma 2.5 $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ if and only if there is no nonzero r-pol in P which is reduced w.r.t. $\mathcal{A}$.

Lemma 2.6 Let $\mathcal{A}$ be a characteristic set of an ideal I. If an r-pol f is invertible w.r.t. $\mathcal{A}$, then $f \notin I$.

Proof Let $\mathbb{V}$ be the algebraic parameter set of $\mathcal{A}_f$. Since f is invertible w.r.t $\mathcal{A}$, there exists an r-pol g and a nonzero $r \in \mathcal{K}[\mathbb{V}]$ 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 2.5, we have $r = 0$, a contradiction.

2.3 Difference Pseudo-remainders

For any chain $\mathcal{A}$, we could write it as the following form

$$\mathcal{A} = A_1, \cdots, A_m \tag{1}$$

with $A_i \in \mathcal{K}\{x_1, \cdots, x_n\}$.

A variable $x_{c,d}$ is called a principal variable of $\mathcal{A}$ if there exists an $A \in \mathcal{A}$ and integer $j \ge 0$ such that $x_{c,d} = \sigma^j \mathrm{lead}(A)$. Otherwise, it is called a parametric variable of $\mathcal{A}$. Denote the set of principal variables and the parametric variables of $\mathcal{A}$ by $\mathbb{M}_{\mathcal{A}}$ and $\mathbb{P}_{\mathcal{A}}$, respectively. It is clear that $\mathbb{M}_{\mathcal{A}} \cup \mathbb{P}_{\mathcal{A}} = \{x_{i,j} | 1 \leq i \leq n, j \geq 0\}$.

Example 2.7 Let $\mathcal{A} = \{A_1, \cdots, A_5\}$ be a chain as following with variable ordering:

$$\begin{aligned} A_1 &= x_{1,2}^2 + x_{1,0}^2 + 1, \\ A_2 &= x_{1,4} - x_{1,0}, \\ A_3 &= x_{3,2}^3 + x_{3,1}x_{3,0} + x_{1,0}, \\ A_4 &= x_{4,3} + x_{4,0}, \\ A_5 &= x_{5,0} + 1. \end{aligned} \tag{2}$$

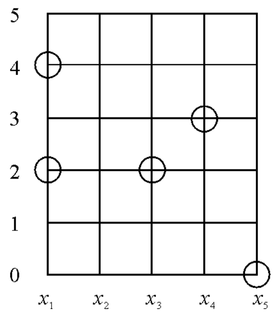

Figure 1 The leads of chain $\mathcal{A}$

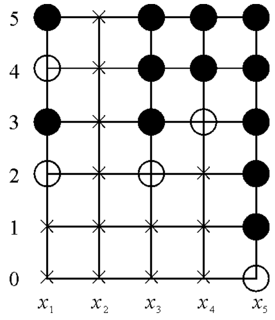

Figure 2 The principal variables of chain $\mathcal{A}$

The principal variables and the parametric variables for $\mathcal{A}$ are given in Figures 1 and 2. The horizontal axis is the variable index and the vertical axis is the number of transforms of the variables. The hollow circles are the leads of the polynomials in $\mathcal{A}$, the circles are the principal variables, and the × symbols are the parametric variables for $\mathcal{A}$.

If we use the total ordering and $x_1 \prec \cdots \prec x_5$, then $\mathcal{A} = A_5, A_1, A_3, A_4, A_2$ is also an ascending chain.

Let $h_1, \cdots, h_n$ be nonnegative integers. In order to compute the pseudo-remainder of an r-pol w.r.t. $\mathcal{A}$, we need to determine the extension of $\mathcal{A}$. First, we collect $A_i, i = 1, \cdots, m$ by the class of A_i.

Let $\mathcal{A}$ be a chain. We rewrite $\mathcal{A}$ as the following form:

$$\mathcal{A} = \begin{cases} A_{1,1}(x_1, \cdots, x_n), \cdots, A_{1,k_1}(x_1, \cdots, x_n) \\ \cdots \\ A_{p,1}(x_1, \cdots, x_n), \cdots, A_{p,k_p}(x_1, \cdots, x_n) \end{cases} \tag{3}$$

where $\text{class}(A_{i,j}) = c_i$ for $j = 1, \cdots, k_i$, and $\text{ord}(A_{i,j}, x_{c_i}) < \text{ord}(A_{i,l}, x_{c_i})$ for $j < l$.

We use algorithm Extension to define the extension of $\mathcal{A}$ w.r.t. some nonnegative integers $h_1, \cdots, h_n$. Note that the definition for $\bar{h}_i$ is used in the proof of Theorem 3.8.

We use $\mathcal{A}_{(h_1,\cdots,h_n)}$ to denote the polynomial sequence obtained by rearranging the polynomials of $\mathcal{A}'_{(h_1,\cdots,h_n)}$ according to the admissible ordering $\prec$. We have

Lemma 2.8 Use the notations above. Let $s_j = \min\limits_{A \in \mathcal{A}_{(h_1,\cdots,h_n)}} \{\text{ord}(A, x_j) | j = \text{class}(A)\}$, $e_j = \max\limits_{A \in \mathcal{A}_{(h_1,\cdots,h_n)}} \{\text{ord}(A, x_j) | j = \text{class}(A)\}$. For a $j, 1 \leq j \leq n$, if there exists no $A \in \mathcal{A}$ such that $j = \text{class}(A)$, then we denote by $V_j = \{\sigma^i x_j \,|\, 0 \leq i \leq e_j\}$ and $Y_j = \emptyset$; if there exists an $A \in \mathcal{A}$ such that $j = \text{class}(A)$, then we denote by $V_j = \{\sigma^i x_j \,|\, 0 \le i \le s_j - 1\}$ and $Y_j = \{\sigma^i x_j \,|\, s_j \le i \le e_j\}$. $V = \bigcup\limits_{j=1}^{n} V_j$, $Y = \bigcup\limits_{j=1}^{n} Y_j$. Then $\mathcal{A}_{(h_1,\cdots,h_n)}$ is an algebraic triangular set in $\mathcal{K}[V,Y]$ when the elements in V and Y are treated as independent variables. Furthermore, the parameters of $\mathcal{A}_{(h_1,\cdots,h_n)}$ as a triangular set are V.

```
Algorithm 1 — Extension $\mathcal{A}'_{(h_1,\cdots,h_n)}$
Input   A chain $\mathcal{A}$ of form (3) and a set of integers $(h_1,\cdots,h_n)$.
Output  The extension $\mathcal{A}'_{(h_1,\cdots,h_n)}$ of $\mathcal{A}$ w.r.t. $h_1,\cdots,h_n$.
S0  Let $S = \{1,\cdots,p\}$, $\mathcal{A}' = \emptyset$, $c_i = \text{class}(A_{i,j})$, $t_{i,j} = \text{ord}(A_{i,j}, x_{c_i})$.
S1  For any $i \in S$, let $o_i = \max\{\text{order of } x_i \text{ appears in } \mathcal{A} \cup \mathcal{A}'\}$, $\bar{h}_i = \max(h_i, o_i + 1)$.
S2  For all $i \in S$, let $\sigma^{\bar{h}_m} x_{c_m}$ be the largest among $\{\sigma^{\bar{h}_i} x_{c_i}\}$ w.r.t. the ordering $\prec$.
S3  Let $\mathcal{B} = \{A_{m,1}, \sigma(A_{m,1}), \cdots, \sigma^{t_{m,2}-t_{m,1}-1}(A_{m,1}), A_{m,2}, \sigma(A_{m,2}), \cdots,$
    $\sigma^{t_{m,3}-t_{m,2}-1}(A_{m,2}), \cdots, A_{m,k_m}, \cdots, \sigma^{\bar{h}_m - t_{m,k_m}}(A_{m,k_m})\}$.
    $\mathcal{A}' = \mathcal{A}' \cup \mathcal{B}, S = S \setminus \{m\}$.
S4  If $S = \emptyset$, return($\mathcal{A}'$), else goto S1. Since $S$ is a finite set, this process will terminate.
```

Proof By the procedure of Extension, we can assume that $S = \{m_1, m_2, \cdots, m_p\}$ and m_i is chosen before m_{i+1} for $1 \le i \le p-1$.

For the first time, we select $\sigma^{\bar{h}_{m_1}} x_{c_{m_1}}$ as the largest one among $\{\sigma^{\bar{h}_i} x_{c_i}\}$ w.r.t. the ordering $\prec$. Since the ordering is admissible, all the variables presented in $\mathcal{B}$ and $\mathcal{A}$ is of lower ordering than $\sigma^{\bar{h}_{m_1}} x_{c_{m_1}}$. Similarly, when we select m_2 from S, all the variables presented in $\mathcal{B}$ is of lower ordering than $\sigma^{\bar{h}_{m_2}} x_{c_{m_2}}$, where $\mathcal{B}$ and $\bar{h}_{m_2}$ is redefined and $\sigma^{\bar{h}_{m_2}} x_{c_{m_2}} \prec \sigma^{\bar{h}_{m_1}} x_{c_{m_1}}$.

As a consequence, when the procedure is terminated, $\mathcal{A}'_{(h_1,\cdots,h_n)}$ must have the following form:

$$\mathcal{A}'_{(h_1,\cdots,h_n)} = \begin{cases} B_{1,1}(x_1,\cdots,x_n), \cdots, B_{1,s_1}(x_1,\cdots,x_n) \\ \cdots \\ B_{p,1}(x_1,\cdots,x_n), \cdots, B_{p,s_p}(x_1,\cdots,x_n). \end{cases} \tag{4}$$

Where $\mathcal{B}_i = \{B_{i,1}(x_1,\cdots,x_n), \cdots, B_{i,s_i}(x_1,\cdots,x_n)\}, 1 \le i \le p$ and $\mathcal{B}_i$ is obtained in the procedure after $\mathcal{B}_{i+1}$ for $1 \le i \le p-1$.

Then, $B_{1,s_1} \prec B_{2,s_2} \prec \cdots \prec B_{p,s_p}$ and all the $B_{i,j}$ have different leads. So, after rearrange the polynomials in $\mathcal{A}'_{(h_1,\cdots,h_n)}$ w.r.t. the ordering $\prec$, the polynomials in $\mathcal{A}_{(h_1,\cdots,h_n)}$ have different leads and it forms an algebraic triangular set for the ordering induced by $\prec$. The conclusion follows by the definition of triangular set.

Example 2.9 Let $\mathcal{A} = \{A_1,\cdots,A_5\}$ be a chain as following with total ordering and $x_1 \prec x_2 \prec x_3 \prec x_4 \prec x_5$:

$$\begin{aligned} A_1 &= x_{1,3}^2 + x_{2,2}^2 + x_{1,0}, \\ A_2 &= x_{1,1} - x_{3,0}, \\ A_3 &= x_{3,5}^3 + x_{3,1}x_{1,4} + x_{1,0}, \\ A_4 &= x_{4,3} + x_{4,0} + x_{1,3}, \\ A_5 &= x_{5,2} + x_{4,1} + x_{3,0} + 1. \end{aligned} \tag{5}$$

Let $(h_1,\cdots,h_5)=(0,\cdots,0)$, following the procedure of Extension. Firstly, $S=\{1,3,4,5\}$, we select $x_{3,6}$ as the largest one w.r.t.the total ordering $\prec$, $\mathcal{B}=\{A_3,\sigma A_3\}$; secondly, $S=\{1,4,5\}$, we select $x_{1,5}$ as the largest one, $\mathcal{B}=\{A_2,\sigma A_2,A_1,\sigma A_1,\sigma^2 A_1\}$; thirdly, $S=\{4,5\}$, we select $x_{4,4}$ as the largest one, $\mathcal{B}=\{A_4,\sigma A_4\}$; at last, $S=\{5\}$, we select $x_{5,3}$ as the largest one, $\mathcal{B}=\{A_5,\sigma A_5\}$. Then

$$\mathcal{A}'_{(0,\cdots,0)}=\begin{cases} A_5,\sigma A_5\\ A_4,\sigma A_4\\ A_2,\sigma A_2,A_1,\sigma A_1,\sigma^2 A_1\\ A_3,\sigma A_3.\end{cases} \tag{6}$$

And $\mathcal{A}_{(0,\cdots,0)}=\{A_2,\sigma A_2,A_5,A_1,A_4,\sigma A_5,\sigma A_1,\sigma A_4,\sigma^2 A_1,A_3,\sigma A_3\}$.

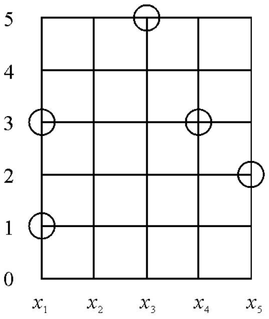

Figure 3 The leads of chain $\mathcal{A}$

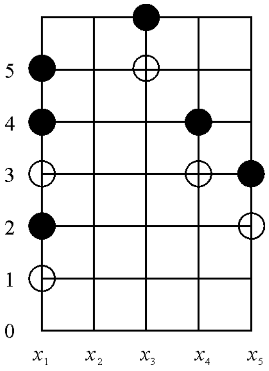

Figure 4 The leads of $\mathcal{A}_{(0,\cdots,0)}$

The leads of $\mathcal{A}$ and $\mathcal{A}_{(0,\cdots,0)}$ are given in Figures 3 and 4, respectively.

For a chain $\mathcal{A}$ and an r-pol f, let

$$\begin{aligned}\mathcal{A}^* &= \mathcal{A}_{(0,\cdots,0)},\\ \mathcal{A}_f &= \mathcal{A}_{(\mathrm{ord}(f,x_1),\cdots,\mathrm{ord}(f,x_n))}.\end{aligned} \tag{7}$$

Note that $\mathcal{A}^*=\mathcal{A}_{\sigma\mathcal{A}}$ by the definition of Extension.

We define the pseudo-remainder of an r-pol g w.r.t. a chain $\mathcal{A}=A_1,\cdots,A_m$ as

$$\mathbf{prem}(f,\mathcal{A})=\mathbf{a\text{-}prem}(f,\mathcal{A}_f), \tag{8}$$

where **a-prem** is the algebraic pseudo-remainder [17] and the variables and their transforms in $\mathbf{a\text{-}prem}(P,\mathcal{A}_f)$ are treated as independent algebraic variables, and the ordering of $\mathcal{A}_f$ is induced by $\prec$. Due to the way to compute $\mathcal{A}_f$ and the property of the algebraic pseudo-remainder, we have

Lemma 2.10 Let $g,\mathcal{A}$ be as above. Then there is a $J\in\mathbb{I}_{\mathcal{A}}$ with $\mathrm{lead}(J)\prec\mathrm{lead}(g)$ such that $Jg\equiv r \bmod [\mathcal{A}]$ and r is reduced w.r.t. $\mathcal{A}$.

2.4 Coherent and regular difference chains

In this section, properties of coherent and regular chains are introduced.

Note that in Example 2.2, we have $\sigma f_1-(x_{1,2}+x_{1,1})f_2=1$, i.e., $1\in[f_1,f_2]$. This fact leads to the following concept.

Let $\mathcal{A} = A_1, \cdots, A_m$ be a difference chain in $\mathcal{K}\{x_1, \cdots, x_n\}$ and $k_i = \mathrm{ord}(A_i, \mathrm{lvar}(A_i)),\ i = 1, \cdots, m$. For any $1 \le i < j \le m$, if $\mathrm{class}(A_i) = \mathrm{class}(A_j) = t$, then $k_i < k_j$, let $\Delta_{ij} = \textbf{a-prem}(\sigma^{k_j - k_i} A_i, A_j, x_{t,k_j})$ be the algebraic pseudo-remainder of $\sigma^{k_j-k_i}A_i$ w.r.t. A_j about variable x_{t,k_j}; otherwise, let $\Delta_{ij} = 0$. If $\textbf{prem}(\Delta_{ij}, \mathcal{A}) = \textbf{a-prem}(\Delta_{ij}, \mathcal{A}_{\Delta_{ij}}) = 0$, we call $\mathcal{A}$ a coherent difference chain.

Let $\mathcal{A}$ be a difference chain of form (1), f an r-pol. f is said to be 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 polynomial and triangular set.

Let $\mathcal{A} = A_1, \cdots, A_m$ be a difference chain and $I_i = \mathrm{init}(A_i)$. $\mathcal{A}$ is said to be (difference) regular if $\sigma^i I_j$ is invertible w.r.t. $\mathcal{A}$ for any non-negative integer i and $1 \le j \le m$.

The following results show that it is easy to solve the ideal membership problem of $\textbf{sat}(\mathcal{A})$ for a coherent and regular chain $\mathcal{A}$. The proof of these results under a general admissible ordering is similar to those for the variable ordering given in [8]. Their proofs are omitted.

Theorem 2.11 A difference chain $\mathcal{A}$ is the characteristic set of $\textbf{sat}(\mathcal{A})$ iff $\mathcal{A}$ is coherent and difference regular.

Theorem 2.12 If $\mathcal{A}$ is a coherent and regular chain of form (1), then

$$\textbf{sat}(\mathcal{A}) = \bigcup_{h_1 \ge 0, \cdots, h_n \ge 0} (\textbf{a-sat}(\mathcal{A}_{(h_1, \cdots, h_n)})).$$

The following lemma will be used later in this paper. Its proof is also similar to the proof of Lemma 3.5 in [8].

Lemma 2.13 Let $\mathcal{A}$ be a coherent chain of form(1), $f \in (\mathcal{A}_{(l_1, \cdots, l_n)})$ for $l_i \ge \max_{A \in \mathcal{A}^*} \mathrm{ord}(A, y_i)$. Then $\exists J \in I_{\mathcal{A}^*}$ s.t. $\mathrm{lead}(J) \prec \mathrm{lead}(\sigma f)$ and $J\sigma f \in (\mathcal{A}_{(l_1+1, \cdots, l_n+1)})$.

3 Proper and Strong Irreducible Chains

Note that there is no direct methods to check if a given chain is difference regular since we need to check that all possible transforms of the initials are invertible. In this section, we will give a constructive criterion for a chain to be difference regular.

3.1 Invertibility of algebraic polynomials

We will first introduce some notations and known results about invertibility of algebraic polynomials w.r.t. a chain. In this section, all notions mean to be algebraic case.

Let $\mathcal{A} = A_1, \cdots, A_m$ be a nontrivial triangular set in $K[x_1, \cdots, x_n]$ over a field K of characteristic zero. Let y_i be the leading variable of A_i, $y = \{y_1, \cdots, y_p\}$ and $u = \{x_1, \cdots, x_n\} \setminus y$. u is called the parameter set of $\mathcal{A}$. We can denote $K[x_1, \cdots, x_n]$ as $K[u, y]$. A polynomial f is said to be invertible w.r.t. $\mathcal{A}$ if $(f, A_1, \cdots, A_s) \cap \mathcal{K}[u] \ne \{0\}$ where $\mathrm{lvar}(f) = \mathrm{lvar}(A_s)$. $\mathcal{A}$ is called regular if the initials of A_i are invertible w.r.t. $\mathcal{A}$.

Theorem 3.1 [1, 3] Let $\mathcal{A}$ be a triangular set. Then $\mathcal{A}$ is a characteristic set of $(\mathcal{A}) : I_{\mathcal{A}}$ iff $\mathcal{A}$ is regular.

Lemma 3.2 [3] A finite product of polynomials which are invertible w.r.t. $\mathcal{A}$ is also invertible w.r.t. $\mathcal{A}$.

Lemma 3.3 [3] A polynomial f is not invertible w.r.t. a regular triangular set $\mathcal{A}$ iff there is a nonzero g in $K[u, y]$ such that $fg \in (\mathcal{A})$ and g is reduced w.r.t. $\mathcal{A}$.

Lemma 3.4 [17] Let $\mathcal{A}$ be an irreducible algebraic triangular set with a generic point η. Then for any polynomial f, the following facts are equivalent.

- g is invertible w.r.t. $\mathcal{A}$.
- $\mathbf{prem}(g,\mathcal{A}) \neq 0$, or equivalently $g \notin (\mathcal{A}) : I_{\mathcal{A}}$.
- $\bar{g} \neq 0$, where $\bar{g}$ is obtained by substituting η into g.
- $\mathrm{resl}(g,\mathcal{A}) \neq 0$. Let $\mathcal{A} = A_1, \cdots, A_m$, $\mathrm{resl}(g,\mathcal{A})$ is defined as follows: $\mathrm{resl}(g,\mathcal{A}) = \mathrm{resl}(\mathrm{resl}(g, A_m, \mathrm{lvar}(A_m)),\ A_1,\ \cdots,\ A_{m-1})$, and $\mathrm{resl}(g,\emptyset) = g$.

3.2 Proper irreducible chains

A chain $\mathcal{A}$ of the form(1) is said to be proper

- $\mathcal{A}^*$ as defined in (7) is an algebraic irreducible triangular set; and
- If $\sigma g \in \textbf{a-sat}(\mathcal{A}^*)$ then $g \in \textbf{a-sat}(\mathcal{A}^*)$.

Lemma 3.5 Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1) and V be the algebraic parameter set of $\mathcal{A}^*$. If $g \in \mathcal{K}[V]$, then σg is invertible w.r.t. $\mathcal{A}^*$.

Proof Since $\mathcal{A}^*$ is an algebraic irreducible chain, by Lemma 3.4, if σg is not invertible w.r.t. $\mathcal{A}^*$ then $\sigma g \in \textbf{a-sat}(\mathcal{A}^*)$. Since $\mathcal{A}$ is proper irreducible, we have $g \in \textbf{a-sat}(\mathcal{A}^*)$. But $g \in \mathcal{K}[V]$ and hence is invertible w.r.t. $\mathcal{A}$. Which is a contradiction.

The following is a key property of a proper irreducible chain.

Lemma 3.6 Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1). If f is invertible w.r.t. $\mathcal{A}$, then σf is invertible w.r.t. $\mathcal{A}$.

Proof We assume that $\mathcal{A}$ can be rewrited as (3). Let V be the parameter set of the algebraic chain $\mathcal{A}_f$ and Y other variables occurring in $\mathcal{A}_f$. By Lemma 2.8, V is also the parameter set of $\mathcal{A}^*$. Since f is invertible w.r.t. $\mathcal{A}$, there exist $\bar{f} \in \mathcal{K}[V,Y]$ and nonzero $g \in \mathcal{K}[V]$ such that $\bar{f} \cdot f \equiv g \bmod (\mathcal{A}_f)$, that is,

$$\bar{f} \cdot f = g + \sum_{A \in \mathcal{A}_f} B_A A. \tag{9}$$

Performing the transforming operator on the formula, we have

$$\sigma\bar{f} \cdot \sigma f \equiv \sigma g \ \bmod (\sigma\mathcal{A}_f). \tag{10}$$

If $\mathrm{ord}(f, y_i) \geq \mathrm{ord}(A_{i,k_i}, y_i)$ for all $i \leq p$, by Lemma 2.13, we can find a $J \in I_{\mathcal{A}^*}$ such that

$$J\sigma\bar{f} \cdot \sigma f \equiv J\sigma g \ \bmod (\mathcal{A}_{\sigma f}). \tag{11}$$

If $\mathrm{ord}(f, y_i) < \mathrm{ord}(A_{i,k_i}, y_i)$ for some $i \leq p$, we assume that for A in (9), $\mathrm{ord}(A, y_i) < \mathrm{ord}(A_{i,k_i}, y_i)$. Similar to Lemma 2.13, we can also find $J \in I_{\mathcal{A}^*}$ such that(11) is true. Since J is a product of powers of initials of $\mathcal{A}^*$, it is invertible w.r.t. $\mathcal{A}^*$. σg is invertible w.r.t. $\mathcal{A}^*$ by Lemma 3.5. As a consequence, there exist h and nonzero $r \in \mathcal{K}[V]$ such that

$$h \cdot J\sigma g \equiv r \ \bmod\ (\mathcal{A}^*).$$

Hence,

$$h \cdot J\sigma\bar{f} \cdot \sigma f \equiv h \cdot J \cdot \sigma g \equiv r \bmod (\mathcal{A}_{\sigma f}).$$

That is, σf is invertible w.r.t. $\mathcal{A}$.

The following theorem is one of the main properties of proper irreducible chains, which gives a constructive criterion for a chain to be regular.

Theorem 3.7 A coherent and proper irreducible chain is difference regular.

Proof Let $\mathcal{A} = A_1, \cdots, A_m$ and $I_j = \text{init}(A_j)$. Since $\mathcal{A}^*$ is an irreducible algebraic chain, by Lemma 3.4, I_i are invertible w.r.t. $\mathcal{A}^*$ and hence invertible w.r.t. $\mathcal{A}$. By Lemma 3.6, all $\sigma^j I_i$ are invertible w.r.t. $\mathcal{A}$.

3.3 Consistence of proper irreducible chains

In order to obtain a complete algorithm for difference polynomial systems, we need to show that a coherent and proper irreducible chain $\mathcal{A}$ is consistent, or equivalently, Zero($\mathbf{sat}(\mathcal{A})$) is not empty. The proof of Theorem 3.8 uses the theory of difference kernels established by Cohn [5]. It can also be considered as an extension of some of the results obtained by Cohn about one irreducible difference polynomial to certain chains.

Let $\mathbf{a}_i = (a_{i,1}, \cdots, a_{i,n}), i = 0, \cdots, r$ be n-tuples, where $a_{i,j}$ are elements from an extension field of $\mathcal{K}$. A difference kernel of length r, $\mathcal{R} = \mathcal{K}(\mathbf{a}_0, \mathbf{a}_1, \cdots, \mathbf{a}_r)$, over the difference field $\mathcal{K}$ is an algebraic field extension of $\mathcal{K}$ such that the difference operator σ of $\mathcal{K}$ can be extended to a field isomorphism from $\mathcal{K}(\mathbf{a}_0, \cdots, \mathbf{a}_{r-1})$ to $\mathcal{K}(\mathbf{a}_1, \cdots, \mathbf{a}_r)$ and $\sigma \mathbf{a}_i = \mathbf{a}_{i+1}, i = 0, \cdots, r-1$.

Theorem 3.8 Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then Zero($\mathbf{sat}(\mathcal{A})$) $\neq \emptyset$.

Proof Let $\mathcal{A}$ be of form (1). We rearrange $\mathcal{A}^*$ as follows

$$\mathcal{A}^* = B_{1,1}, \cdots, B_{1,c_1}, \cdots, B_{p,1}, \cdots, B_{p,c_p},$$

where $\text{lvar}(B_{i,j}) = y_i$. Let $o_i = \text{ord}(B_{i,c_i}, y_i), i = 1, \cdots, p$, $e = \max\limits_{A \in \mathcal{A}^*, p+1 \le j \le n} \{\text{ord}(A, y_j)\}$, $U_0 = \{\sigma^i y_j \,|\, p+1 \le j \le n, 0 \le i \le e\}$, $U_1 = \{\sigma^i y_j \,|\, p+1 \le j \le n, 1 \le i \le e+1\}$, $Y_0 = \{\sigma^i y_j \,|\, 1 \le j \le p, 0 \le i \le o_j - 1\}$, and $Y_1 = \{\sigma^i y_j \,|\, 1 \le j \le p, 1 \le i \le o_j\}$. Then $V_0 = U_0 \cup Y_0$ and $V_1 = U_1 \cup Y_1$ have the same number of elements. Since $\mathcal{A}$ is proper irreducible, $\mathcal{A}^*$ is an irreducible algebraic triangular set when $\sigma^i y_j$ are treated as independent variables. Hence, $I = \mathbf{a\text{-}sat}(\mathcal{A}^*)$ is a prime ideal in $\mathcal{K}[\hat{V}]$, where $\hat{V} = V_0 \cup V_1$. Let $\eta = (\eta_j^{(i)})$ be a generic zero of this prime ideal. Then $\sigma^j y_i = \eta_i^{(j)}$ annul every polynomial in $\mathcal{A}^*$ but not their initials.

We will construct a difference kernel of length one. Now, let $\mathbf{a}_0$ and $\mathbf{a}_1$ be obtained from V_0 and V_1 by replacing $\sigma^j y_i$ with $\eta_j^{(i)}$. The kernel is $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$. The difference operator σ introduces a map from $\mathcal{K}(\mathbf{a}_0)$ to $\mathcal{K}(\mathbf{a}_1)$ as follows $\sigma(\eta_j^{(i)}) = \eta_j^{(i+1)}$. We will prove that σ introduces an isomorphism between $\mathcal{K}(\mathbf{a}_0)$ and $\mathcal{K}(\mathbf{a}_1)$.

Let

$$\mathcal{B}_0 = \mathcal{A}^* - \{B_{1,c_1}, \cdots, B_{p,c_p}\}, \quad \mathcal{B}_1 = \{\sigma A \,|\, A \in \mathcal{B}_0\}.$$

From the definition of $\mathcal{A}^*$, the orders of y_k in $B_{i,j} \in \mathcal{B}_0$ are not exceeding $o_k - 1$. As a consequence, $\mathbf{a}_0$ is a generic zero of the algebraic prime ideal $\mathbf{a\text{-}sat}(\mathcal{A}^*) \cap \mathcal{K}[V_0] = \mathbf{a\text{-}sat}(\mathcal{B}_0)$ with $\mathcal{B}_0$ as a characteristic set.

Note that $\sigma \mathcal{B}_0 = \mathcal{B}_1$ and $\sigma \mathbf{a}_0 = \mathbf{a}_1$, by the nature of the difference operator, $\mathcal{B}_1$ is an irreducible triangular set in $\mathcal{K}[V_1]$ and $\mathbf{a}_1$ is a generic zero of the prime ideal $I_1 = \mathbf{a\text{-}sat}(\mathcal{B}_1)$ with $\mathcal{B}_1$ as a characteristic set. We will show that $I_1 = I \cap \mathcal{K}[V_1]$.

First of all, it is easy to see that $I_1 \subset I \cap \mathcal{K}[V_1]$. Let $I_0 = \mathbf{a\text{-}sat}(\mathcal{B}_0)$, W be the parametric set of I_0, then σW is the parametric set of I_1 by the difference operator. Now we will show that σW is the parametric set of $I \cap \mathcal{K}[V_1]$. If this is not true, then there exists a polynomial $P(\sigma W) \in I \cap \mathcal{K}[V_1]$ or $\sigma W' \cup \sigma W \subset V_1$ is the parametric set of $I \cap \mathcal{K}[V_1]$. For the first case, since $\mathcal{K}$ is inversive and $\mathcal{A}$ is proper irreducible, we have that $\sigma^{-1} P(\sigma W) \in I \cap \mathcal{K}[V_0] = I_0$, W is not the parametric set of I_0, a contradiction. For the second case, since W is the parametric set of I_0, there exists a polynomial $P(W', W) \in I_0$, hence $\sigma P(W', W) = Q(\sigma W', \sigma W) \in I_1$, which is impossible by the assumption. So, the two prime ideal $I_1, I \cap \mathcal{K}[V_1]$ have the same dimension and $I_1 \subset I \cap \mathcal{K}[V_1]$, then $I_1 = I \cap \mathcal{K}[V_1]$. Since $\sigma I_0 \rightarrow I_1$ is an isomorphism between two prime ideals, σ introduces an isomorphism between $\mathcal{K}(\mathbf{a}_0)$ and $\mathcal{K}(\mathbf{a}_1)$. As a consequence, $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$ is a difference kernel over $\mathcal{K}$.

By Lemma V on page 156 of [5], this kernel has a principal realization ψ corresponding to a series of kernels $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$, $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2), \cdots$. We will show that ψ is a zero of $\mathbf{sat}(\mathcal{A})$. From the construction of the kernel, for any $A \in \mathcal{A}^*$, we have $A(\psi) = A(\eta) = 0$. Hence ψ is a zero of the polynomials in $\mathcal{A}^*$ but does not annul any initials of $\mathcal{A}^*$. Then for any $A \in \mathcal{A}$, ψ is a zero of $\sigma^k A$ for any k, since σ is an isomorphism. Also, ψ does not annul any $J \in \mathbb{I}_{\mathcal{A}}$. As a consequence, $\psi \in \mathrm{Zero}(\mathbf{sat}(\mathcal{A}))$.

The following example shows that a coherent and regular chain could have no solutions.

Example 3.9 $f_1 = y_1^2 - 1, f_2 = y_{1,1} + y_1 \in \mathcal{K}\{y_1\}$. $\mathcal{A} = \{f_1, f_2\}$. $\mathcal{A}$ is coherent and regular difference. But $\mathcal{A}$ is not proper irreducible, since f_1 is not irreducible. We have $\mathrm{Zero}(\mathbf{sat}(\mathcal{A})) = \mathrm{Zero}(\mathcal{A}) = \mathrm{Zero}(y_1 - 1, y_{1,1} + y_1) \cup Z(y_1 + 1, y_{1,1} + y_1) = \emptyset$.

3.4 Characteristic sets of reflexive prime ideals

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

A proper irreducible chain $\mathcal{A}$ is called strong irreducible if for any nonnegative integers h_i, $\mathcal{A}_{(h_1,\cdots,h_n)}$ is an irreducible algebraic triangular set.

Theorem 3.10 Let $\mathcal{A}$ be a coherent and strong 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 Theorem 2.12, there exist nonnegative integers $h_1, \cdots, h_n$ such that $fg \in D = \mathbf{a\text{-}sat}(\mathcal{A}_{(h_1,\cdots,h_n)})$. Since $\mathcal{A}$ is strong irreducible, $\mathcal{A}_{(h_1,\cdots,h_n)}$ 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, that is, if $\sigma f \in \mathbf{sat}(\mathcal{A})$ then $f \in \mathbf{sat}(\mathcal{A})$. Suppose $f \notin \mathbf{sat}(\mathcal{A})$. By Lemma 2.12, $f \notin \mathbf{a\text{-}sat}(\mathcal{A}_f)$. Since $\mathcal{A}_f$ is an irreducible algebraic triangular set, f must be invertible w.r.t. $\mathcal{A}_f$. As a consequence, f is invertible w.r.t. $\mathcal{A}$. By Lemmas 3.6 and 2.6, σf is invertible w.r.t. $\mathcal{A}$ and hence $\sigma f \notin \mathbf{sat}(\mathcal{A})$, which contradicts the fact $\sigma f \in \mathbf{sat}(\mathcal{A})$.

Example 3.11 Consider $\mathcal{A} = \{A_1 = x_{1,0}^2 + t,\ A_2 = x_{2,0}^2 + t + k\ \}$ from [5] in $\mathcal{K}\{x_1, x_2\}$ where $\mathcal{K}$ is $Q(t)$ with the difference operator $\sigma t = t + 1$ and k is a positive integer. $\mathcal{A}^* = \{A_1, \sigma A_1, A_2, \sigma A_2\}$. If $k > 1$, $\mathcal{A}$ is proper irreducible. But $\mathbf{sat}(\mathcal{A})$ is not prime, because $A_2 - \sigma^k(A_1) = (x_{2,0} - x_{1,k})(x_{2,0} + x_{1,k})$.

Conversely, we have

Theorem 3.12 Let $\mathcal{I}$ be a reflexive prime difference ideal, $\mathcal{A}$ the characteristic sets of $\mathcal{I}$. Then $\mathcal{A}$ is coherent, strong irreducible, and $\mathcal{I} = \mathbf{sat}(\mathcal{A})$.

Proof By Lemma 3.13, for any characteristic set $\mathcal{A}$ of $\mathcal{I}$, we have $\mathcal{I} = \mathbf{sat}(\mathcal{A})$. By Theorem 2.11, $\mathcal{A}$ is coherent. By Lemma 3.14, we have for any nonnegative integers t_i, $\mathcal{A}_{(t_1,\cdots,t_p)}$ is algebraic irreducible. Also, if $\sigma g \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$, then $\sigma g \in \mathcal{I}$. Since $\mathcal{I}$ is reflexive, $g \in \mathcal{I}$. Then $g \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$.

Lemma 3.13 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 2.11, J is invertible w.r.t. $\mathcal{A}$ and hence not in $\mathcal{I}$ by Lemma 2.6. Since $\mathcal{I}$ is a prime ideal, $f \in \mathcal{I}$.

Lemma 3.14 Let $\mathcal{I}$ be a reflexive prime difference ideal, $\mathcal{A}$ its characteristic set. Then for any nonnegative integers t_i, $\mathcal{A}_{(t_1,\cdots,t_n)}$ is algebraic irreducible.

Proof Otherwise, we have nonnegative integers $t_1, \cdots, t_n$ such that $\mathcal{A}_{(t_1,\cdots,t_n)}$ is a reducible algebraic triangular set. By definition, there exist r-pols f and g which are reduced w.r.t. $\mathcal{A}_{(t_1,\cdots,t_n)}$ and with order not higher than those r-pols in $\mathcal{A}_{(t_1,\cdots,t_n)}$ such that $fg \in \mathcal{A}_{(t_1,\cdots,t_n)} \subset \mathbf{sat}(\mathcal{A}) = \mathcal{I}$. 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. $\mathcal{A}$.

Let $\mathcal{A} = A_1, \cdots, A_n$ be a sequence of the following form

$$A_1 = V_1\sigma x_1 - U_1, \cdots, A_n = V_n\sigma x_n - U_n, \tag{12}$$

where $V_i, U_i \in \mathcal{K}[x_1, \cdots, x_n]$ and $V_i \neq 0$. It is clear that under a total ordering, $\mathcal{A}$ is a chain. Furthermore, $\mathcal{A}$ is coherent since $\Delta(A_i, A_j)$ is always zero. Equations of form (12) are often used in control theory [9] and it is important to know whether $\mathbf{sat}(\mathcal{A})$ is a reflexive prime ideal. As an application of the method developed in this paper, we will give a new proof for the following result which is first given in [9].

Theorem 3.15 $\mathcal{A}$ is strong irreducible if and only if the determinant of the Jacobi matrix $Jac = \frac{\partial(\frac{U_1}{V_1},\cdots,\frac{U_n}{V_n})}{\partial(x_1,\cdots,x_n)}$ is not zero.

Proof By [9], we know that $|Jac| \neq 0$ if and only if $\{\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}\}$ is algebraically independent. Now, we will show that $|Jac| \neq 0$ if and only if $\mathcal{A}$ is strong irreducible.

To prove the theorem, we will show that the following conditions are equivalent:

(1) $\mathcal{A}^*$ is an algebraic irreducible triangular set and $\sigma f \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$ implies $f \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$.

(2) $\sigma f \in \mathbf{a\text{-}sat}(\mathcal{A})$ implies $f \in \mathbf{a\text{-}sat}(\mathcal{A})$.

(3) $|Jac| \neq 0$.

(4) $\mathcal{A}$ is strong irreducible.

First, we show (1) $\Leftrightarrow$ (2). Since $\mathcal{A}^*$ is a regular triangular set, it is evident that we only need to show (2) $\Rightarrow$ (1). Assume this is not true, there exists a $\sigma g \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$, but $g \notin \mathbf{a\text{-}sat}(\mathcal{A}^*)$. By (2), $\mathcal{A}^*$ is a regular triangular set since $V_i \notin \mathbf{a\text{-}sat}(\mathcal{A})$ and $\mathcal{A}$ is an algebraic irreducible triangular set. Let $\mathcal{A}_1 = \sigma\mathcal{A}$, and $\sigma h = \mathbf{a\text{-}prem}(\sigma g, \mathcal{A}_1)$. Then, $\sigma h \in \mathbf{a\text{-}sat}(\mathcal{A})$, but $h = \mathbf{a\text{-}prem}(g, \mathcal{A}) \neq 0$. This contradict to (2).

Second, we show that (2) $\Rightarrow$ (3). Assume that $|Jac| = 0$, then $\{\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}\}$ is algebraically dependent. Hence, there exists a polynomial $P(z_1, \cdots, z_n)$, such that $P(\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}) = 0$. Then $\mathbf{a\text{-}prem}(P(\sigma x_1, \cdots, \sigma x_n), \mathcal{A}) = V * P(\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}) = 0$, $P \in \mathbf{a\text{-}sat}(\mathcal{A})$, where V is a product of some V_i. But $\sigma^{-1}P \notin \mathbf{a\text{-}sat}(\mathcal{A})$, this contradict to (2).

Third, we show that (3) $\Rightarrow$ (2). Let $\sigma f(x_1, \cdots, x_n) = f'(\sigma x_1, \cdots, \sigma x_n)$. Since $\sigma f \in \mathbf{a\text{-}sat}(\mathcal{A})$, we have $\mathbf{a\text{-}prem}(\sigma f, \mathcal{A}) = \mathbf{a\text{-}prem}(f', \mathcal{A}) = V' * f'(\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}) = 0$, where V' is a product of some V_i. Hence, $f'(\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}) = 0$. Since $f \notin \mathbf{a\text{-}sat}(\mathcal{A})$, f' is a non-zero polynomial, hence $\{\frac{U_1}{V_1}, \cdots, \frac{U_n}{V_n}\}$ is algebraically dependent, which is contradict to (3).

At last, we show that (1) ⇔ (4). Since (4) ⇒ (1) is absolutely true by the definition of strong irreducible, we only need to show (1) ⇒ (4). It is sufficient to show that for any positive integer h, $\mathcal{A}_{(h,\cdots,h)}$ is an irreducible triangular set. We prove this by induction on h. When $h = 1, 2$, $\mathcal{A}_{(h,\cdots,h)} = \mathcal{A}^*$, the conclusion is true. Assume for any $l < h, h \geq 3$, $\mathcal{A}_{(l,\cdots,l)}$ is an irreducible triangular set, we show that $\mathcal{A}_{(h,\cdots,h)}$ is an irreducible triangular set. If this is not the case, there exists an i, such that $\sigma^h V_i \in \textbf{a-sat}(\mathcal{A}_{(h-1,\cdots,h-1)})$. Let $\sigma g = \textbf{a-prem}(\sigma^h V_i, \{\sigma^{h-1}\mathcal{A}, \cdots, \sigma\mathcal{A}\})$ be the successive pseudo-remainder of $\sigma^h V_i$ w.r.t. $\{\sigma^{h-1}\mathcal{A}, \cdots, \sigma\mathcal{A}\}$, then $g = \textbf{a-prem}(\sigma^h V_i, \{\sigma^{h-2}\mathcal{A}, \cdots, \mathcal{A}\})$. Since $\mathcal{A}_{(h-1,\cdots,h-1)}$ is a regular triangular set, we have $\sigma g \in \textbf{a-sat}(\mathcal{A})$ and $g \notin \textbf{a-sat}(\mathcal{A})$. which contradicts to (1).

4 Algorithms of Zero Decomposition

In this section, we will present two algorithms which can be used to decompose the zero set of a general r-pol set into the zero set of proper irreducible chains. Such algorithms are called zero decomposition algorithms.

4.1 The Zero decomposition algorithm

A chain $\mathcal{A}$ is called a Wu characteristic set of a set $\mathbb{P}$ of r-pols if $\mathcal{A} \subset [\mathbb{P}]$ and for all $P \in \mathbb{P}$, $\text{rprem}(P, \mathcal{A}) = 0$. As a direct consequence of the pseudo-remainder formula given in Lemma 2.10, we have

Lemma 4.1 Let $\mathbb{P}$ be a finite set of r-pols, $\mathcal{A} = A_1, \cdots, A_m$ a Wu characteristic set of $\mathbb{P}$, $I_i = \text{init}(A_i)$, and $J = \prod_{i=1}^{m} I_i$. Then

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\mathcal{A}/J) \bigcup \bigcup_{i=1}^{m} \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}),$$

$$\text{Zero}(\mathbb{P}) = \text{Zero}(\textbf{sat}(\mathcal{A})) \bigcup \bigcup_{i=1}^{m} \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}).$$

Now, we are ready to give the Ritt-Wu zero decomposition theorem.

Theorem 4.2 Let $\mathbb{P}$ be a finite set of r-pols in $\mathcal{K}\{y_1, \cdots, y_n\}$, then there exist a sequence of coherent and proper irreducible difference chains $\mathcal{A}_i$, $i = 1, \cdots, k$ such that

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \text{Zero}(\mathcal{A}_i/J_i), \qquad \text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \text{Zero}(\textbf{sat}(\mathcal{A}_i)). \tag{13}$$

$\text{Zero}(\mathbb{P}) = \emptyset$ iff $k = 1$ and $\mathcal{A}_1$ is trivial.

This is a quite straight forward extension of the procedure proposed in [17], except the procedure ProIrr to find a proper irreducible chain. The correctness of the algorithm is guaranteed by Lemma 4.1 and Lemma 4.5. The termination of it is guaranteed by Lemma 2.3.

In the algorithm RittWuZDT, we need to check whether a coherent difference chain is proper irreducible.

Example 4.3 Consider $\mathcal{B} = \{f_1 = x_{3,0}^2 + x_{1,0} + 1,\ f_2 = x_{3,2} + x_{2,0} + 1\ \} \subset \mathcal{K}\{x_1, x_2, x_3\}$, it is not coherent. Since $x_{3,2}^2 + x_{1,2} + 1 = (x_{3,2} + x_{2,0} + 1)(x_{3,2} - x_{2,0} - 1) + (x_{2,0} + 1)^2 + x_{1,2} + 1$. When we apply the above algorithm to $\mathcal{B}$, we get $\mathcal{A} = \{x_{2,0}^2 + 2x_{2,0} + x_{1,2} + 2,\ x_{3,0}^2 + x_{1,0} + 1,\ x_{3,2} + x_{2,0} + 1\}$, and $\mathcal{A}$ is coherent and proper irreducible difference chain. $\text{Zero}(\mathcal{B}) = \text{Zero}(\textbf{sat}(\mathcal{A}))$.

Algorithm 2 —RittWuZDT($\mathbb{P}$)

- **Input**: a finite set $\mathbb{P}$ of r-pols.
- **Output**: $W = \{\mathcal{A}_1, \cdots, \mathcal{A}_k\}$ such that $\mathcal{A}_i$ is coherent proper irreducible difference chain and $\text{Zero}(\mathbb{P}) = \bigcup\limits_{i=1}^{k} \text{Zero}(\mathbf{sat}(\mathcal{A}_i))$.

```
Begin
    $\mathcal{B} = C.S(\mathbb{P})$, $\mathcal{B} = B_1, \cdots, B_m$;
    If $\mathcal{B} = 1$ then
        $W = \{1\}$
    Else
        $\mathbb{R} = \{\mathbf{prem}(f, \mathcal{B}) \neq 0 \mid f \in (\mathbb{P} \setminus \mathcal{B}) \cup \triangle(\mathcal{B})\}$
        If $\mathbb{R} = \emptyset$ then (test, $\bar{\mathbb{P}}$) :=$\mathbf{ProIrr}(\mathcal{B})$
            If test then W=$\{\mathcal{B}\} \cup \mathbf{RittWuZDT}(\mathbb{P} \cup \mathcal{B} \cup \{I_i\})$
            Else W:= $\bigcup\limits_{i=1}^{k} \mathbf{RittWuZDT}(\mathbb{P}, \mathcal{B}, f_i) \cup$ $\mathbf{RittWuZDT}$ $(\mathbb{P}, \mathcal{B}, I_i)$
            where $I_i$ are the initials of the r-pols in $\mathcal{B}$
                and $\bar{\mathbb{P}} = \{f_i \mid i = 1, \cdots, k\}$
        Else $W$ :=$\mathbf{RittWuZDT}(\mathbb{P} \cup \mathbb{R})$
End.
```

4.2 Test of proper irreducible chain

In this section, we will give an algorithm to check whether a chain is proper irreducible, which is based on the following result.

Lemma 4.4 Let I be an algebraic ideal in $\mathcal{R}$, $\mathbb{X}_1 = \{x_{i,j} \,|\, 1 \leq i \leq n, j > 0\}$. Then the following conditions are equivalent

(a) For any polynomial g, $\sigma g \in I$ implies $g \in I$.

(b) $\sigma^{-1}(I \cap \mathcal{K}[\mathbb{X}_1]) \subset I$.

Proof (a) and (b) are different description of the same proposition of the ideal I.

The following lemma shows how to decompose the zero set of a polynomial set if its characteristic set is not proper irreducible.

Lemma 4.5 Let $\mathcal{A}$ be a Wu characteristic set of a finite set $\mathbb{P}$. If $\mathcal{A}$ is not a proper irreducible chain, then we can find $f_1, f_2, \cdots, f_h$ which are reduced w.r.t. $\mathcal{A}$ and some initials I_i of $\mathcal{A}$ such that $\text{Zero}(\mathbb{P}) = \bigcup\limits_{i=1}^{h} \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \cup\{f_i\}) \bigcup \cup_i \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \cup\{I_i\})$.

Proof Denote $\mathcal{B} = \mathcal{A}^* = B_1, \cdots, B_m$. First, if $\mathcal{A}^*$ is not algebraic irreducible, by Lemma 3 in Section 4.5 of [17], there are $f_1, \cdots, f_h$ which are reduced w.r.t. $\mathcal{A}^*$ such that

$$f = \prod_{i=1}^{m} I_i^{v_i} f_1^{t_1} \cdots f_h^{t_h} = \sum_{i=1}^{k+1} g_i B_i,$$

where I_i is the initial of B_i. Since $\mathcal{A}$ is a Wu characteristic set of $\mathbb{P}$, $f \in [\mathbb{P}]$. Then $\text{Zero}(\mathbb{P}) = \text{Zero}(\mathbb{P} \cup \{f\}) = \bigcup\limits_{i=1}^{h} \text{Zero}(\mathbb{P}, f_i) \bigcup \cup_i \text{Zero}(\mathbb{P}, I_i)$. If I_i is the initial of $\sigma^d A$ for some $A \in \mathcal{A}$, then

$\mathrm{Zero}(\mathbb{P}, I_i) = \mathrm{Zero}(\mathbb{P}, \mathrm{init}(A))$. In other words, we need only to include the initials of the r-pols in $\mathcal{A}$.

If $\mathcal{A}^*$ is algebraic irreducible, let $f \in \mathbf{a\text{-}sat}(\mathcal{A}^*)$ be the lowest rank such that $f = \sigma g$, $\mathbf{a\text{-}prem}(g, \mathcal{A}^*) \neq 0$. Let $f_1 = \mathbf{a\text{-}prem}(g, \mathcal{A}^*)$, we have $f_1 \neq 0$, f_1 is reduced w.r.t. $\mathcal{A}$,

$$f_1 = \prod_{i=1}^{m} I_i^{v_i} g - \sum_{i=1}^{k+1} g_i B_i,$$

then $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{f\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) = \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{g\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) = \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{f_1\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\})$.

Algorithm 3 —ProIrr($\mathcal{A}$)

- **Input**: a difference coherent chain $\mathcal{A}$ of the form(1).
- **Output**:

(true,$\emptyset$) if $\mathcal{A}$ is proper irreducible

(false,$\bar{\mathbb{P}}$) otherwise. $\bar{\mathbb{P}}$ consists of the difference polynomials in Lemma 4.5.

```
Begin
    test:=ture
    If $\mathcal{A}^*$ is algebraic irreducible then
        $G$ :=GBasis(a-sat($\mathcal{A}^*$))/*/
            $G_1 := G \cap \mathcal{K}[V_1]$ where $V_1$ are the
            variables in $G$ minus those $y_{j,0}$ with order zero.
            $G_1 := \sigma^{-1}G$
        If $G_1 \subset G$
            test:=true; Return.
        Else $\bar{\mathbb{P}} := \{\mathbf{prem}(g, A) \mid g \in G_1 \mid g \notin G\}$, test:= false; Return.
    Else
      test:=false, $\bar{\mathbb{P}}$ consists of the difference polynomials
      which we get in the first case of Lemma 4.5.
End.
```

/*/$G :=$ **GBasis**(**a-sat**($\mathcal{A}^*$)) compute the Groebner basis w.r.t. the eliminating ordering $y_{n,0} > y_{n-1,0} > \cdots > y_{1,0} > y_{n,1} > \cdots > y_{1,1} > \cdots$ In [7], it is proved that for any chain $\mathcal{A} \subset \mathcal{K}[x_1, \cdots, x_n]$, we have $\mathbf{a\text{-}sat}(\mathcal{A}) = (\mathcal{A}, zI_{\mathcal{A}} - 1) \cap \mathcal{K}[x_1, \cdots, x_n]$, where z is a new variable. Based on this result, we can compute a finite basis for $\mathbf{a\text{-}sat}(\mathcal{A}^*)$ and its Groebner basis.

The procedure ProIrr, when it applied to a coherent difference chain $\mathcal{B}$, returns two argument: test, $\bar{\mathbb{P}}$. If $\mathcal{B}^*$ is proper irreducible, then test is true and $\bar{\mathbb{P}} = \emptyset$; else test is false, $\bar{\mathbb{P}}$ consists of some difference polynomials $f_1, \cdots, f_k$ mentioned in Lemma 4.5.

5 A Modified Cohn's Algorithm

In [5], Cohn gave an algorithm to solve the nullstellensatz test of perfect difference ideals. The idea is to transform the problem to a difference ideal with order less than or equal to one and then use zero decomposition algorithms in algebraic case to construct a difference kernel. This certainly simplifies the problem. On the other hand, reduce the order of r-pols to one by introducing new auxiliary variables destroy the structure of the ideal itself. In this section, by combining the idea of Cohn and the concept of algebraic irreducible chains, we will give another algorithm of zero decomposition for difference polynomial systems.

We give some notations at first. Let $\mathcal{X}=\{x_{i,e_i}1\leq i\leq n, d_i\leq e_i\leq o_i\}$, $\mathcal{X}_0=\{x_{i,e_i}1\leq i\leq n, d_i\leq e_i\leq o_i-1\}$, $\mathcal{X}_1=\{x_{i,e_i}1\leq i\leq n, d_i+1\leq e_i\leq o_i\}$.

An algebraic ideal I in $\mathcal{K}[\mathcal{X}]$ satisfies left (right) consistent condition w.r.t. $\{d_i\ ;o_i\}$, if $\forall f\in I\cap\mathcal{K}[\mathcal{X}_1](\mathcal{K}[\mathcal{X}_0])$, $\sigma^{-1}f\in I$ $(\sigma f\in I)$. In the above definition, if for any $i, o_i=d_i$, we assume that $\mathcal{K}[\mathcal{X}_1](\mathcal{K}[\mathcal{X}_0])=\emptyset$. If I satisfies left and right consistent condition w.r.t. $\{d_i\ ;o_i\}$, we say that I satisfies consistent condition w.r.t. $\{d_i\ ;o_i\}$.

Lemma 5.1 Let $\mathbb{P}\subset\mathcal{K}\{x_1,\cdots,x_n\}$, and d_i, o_i the minimal and maximal orders of x_i appearing in $\mathbb{P}$ respectively. Suppose that $\mathbb{P}$ generates a prime algebraic ideal I in $\mathcal{K}[\mathcal{X}]$, and η be the generic zero of I. Then η can be extended to a difference zero of $\mathbb{P}$ iff I satisfies the consistent condition w.r.t. $\{d_i\ ;\ o_i\}$.

Proof Suppose that I satisfies the consistent condition w.r.t. $\{d_i\ ;\ o_i\}$. We will extend η to be a difference kernel of length one. Let $\mathcal{A}=A_1,\cdots,A_p$ be a characteristic set of I. Then $I=\textbf{a-sat}(\mathcal{A})$. Let $I_1=\sigma I$. Since σ is an isomorphism, I_1 is an algebraic prime ideal in $\mathcal{K}[\mathcal{X}_1,x_{1,o_1+1},\cdots,x_{n,o_n+1}]$ and $I_1=\textbf{a-sat}(\sigma\mathcal{A})$. Let $\eta_d=\{\eta_{i,d_i},1\leq i\leq n\}$, $\eta_o=\{\eta_{i,e_i},1\leq i\leq n, d_i+1\leq e_i\leq o_i\}$.

We claim that $I\cap\mathcal{K}[\mathcal{X}_1]=I_1\cap\mathcal{K}[\mathcal{X}_1]$. Since for any $f\in I\cap\mathcal{K}[\mathcal{X}_1]$, $\sigma^{-1}f\in I\cap\mathcal{K}[\mathcal{X}_0]$ by the left consistent condition, then $f\in I_1\cap\mathcal{K}[\mathcal{X}_1]$. For any $f\in I_1\cap\mathcal{K}[\mathcal{X}_1]$, $\sigma^{-1}f\in I\cap\mathcal{K}[\mathcal{X}_0]$, then $f\in I\cap\mathcal{K}[\mathcal{X}_1]$ by the right consistent condition. So, $I\cap\mathcal{K}[\mathcal{X}_1]=I_1\cap\mathcal{K}[\mathcal{X}_1]$ and η_o is the generic zero of $I_1\cap\mathcal{K}[\mathcal{X}_1]$, then η_o can be extended to a generic zero of I_1.

Let $I_2'=\{f(\eta_o,x_{1,o_1+1},\cdots,x_{n,o_n+1})\mid f\in I_1\}$. Then, I_2' generated a prime algebraic ideal denoted by I_2 in $\mathcal{K}(\eta_o)[x_{1,o_1+1},\cdots,x_{n,o_n+1}]$. If we denote by η' a generic zero of I_2, then $\{\eta_o,\eta'\}$ is the generic zero of I_1.

Let I_3 be an ideal generated by I_2 in $\mathcal{K}(\eta_d)(\eta_o)[x_{1,o_1+1},\cdots,x_{n,o_n+1}]$. If P is an essential prime divisor of I_3, then $P\cap\mathcal{K}(\eta_o)[x_{1,o_1+1},\cdots,x_{n,o_n+1}]=I_2$ by the Corollary in the page 32 of [5]. Let the generic zero of P be $\eta_{o+1}=\{\eta_{i,o_i+1},1\leq i\leq n\}$. Then (η_d,η_o) and (η_o,η_{o+1}) is the generic zero of I and I_1, respectively. η,η_{o+1} is a difference kernel of length one and $\{\eta,\eta_{o+1}\}$ is a zero of $\mathbb{P}$.

Hence, by Lemma V on Page 156 of [5], η can be extended to a difference zero of $\mathbb{P}$.

If $\forall i, o_i-d_i>0$, then the generic zero of I is difference kernel of length one. This is the same as Cohn's theory.

The process Consistent (I) where I is the same as in Lemma 5.1 works as follows: Let GL be the Grobner bases of I w.r.t. the eliminating ordering $x_{1,d_1}>x_{2,d_2}>\cdots>x_{n,d_n}>\cdots$. $G_1=GL\cap\mathcal{K}[\mathcal{X}_1]$. Let GR be the Grobner bases of I w.r.t. the eliminating ordering $x_{1,o_1}>x_{2,o_2}>\cdots>x_{n,o_n}>\cdots$. $G_2=GR\cap\mathcal{K}[\mathcal{X}_0]$. If $\sigma^{-1}G_1\subset I$ and $\sigma G_2\subset I$, then test=true,

$\bar{I} = \emptyset$; else test=false, $\bar{I} = \{\sigma^{-1}f, \sigma g \mid f \in G_1\ \sigma^{-1}f \notin I, g \in G_2\ \sigma g \notin I\}$.

Algorithm 4 — Cohn($\mathbb{P}$)

- **Input**: a finite set $\mathbb{P}$ of r-pols.
- **Output**:

  ($\Sigma = \emptyset$) if Zero($\mathbb{P}$) $= \emptyset$

  ($\Sigma = \{\mathcal{B}_i\}$) otherwise, Zero($\mathbb{P}$) $= \cup$Zero($\mathcal{B}_i$) and Zero($\mathcal{B}_i$) $\neq \emptyset$

```
Begin
    $\Sigma = \emptyset$
    $\sqrt{[\mathbb{P}]} = \cap\textbf{a-sat}(\mathcal{A}_i)$ // $\mathcal{A}_i$ is algebraic irreducible
    If $\sqrt{[\mathbb{P}]} = \{1\}$, Return
    Else For all $\mathcal{A}_i$
        $I = \textbf{a-sat}(\mathcal{A}_i)$
        $(test, \bar{I}) = \textbf{Consistent}(I)$
        If $test$ $\Sigma = \Sigma \cup \{\mathcal{A}_i\}$
        Else Cohn$(I \cup \bar{I})$
End.
```

Algorithm 5 —-Consistent($I = \textbf{a-sat}(\mathcal{A})$)

- **Input**: an algebraic irreducible chain $\mathcal{A}$, and d_i, o_i the minimal and maximal order of x_i appearing in $\mathcal{A}$.
- **Output**:

  (true,$\emptyset$) if $I = \textbf{a-sat}(\mathcal{A})$ is consistent w.r.t. $\{d_i\ ; o_i\}$.

  (false,$\bar{I}$) Otherwise.

```
Begin
    test:=ture
    $GL$ :=LGBasis(a-sat($\mathcal{A}$))/*/
    $GR$ :=RGBasis(a-sat($\mathcal{A}$))/*/
    $G_1 = GL \cap \mathcal{K}[\mathcal{X}_1]$.
    $G_2 = GR \cap \mathcal{K}[\mathcal{X}_0]$.
    If $\sigma^{-1}G_1 \subset I$ and $\sigma G_2 \subset I$
        then test=true; Return.
    Else
        test:=false, $\bar{I} = \{\sigma^{-1}f, \sigma g \mid f \in G_1\ \sigma^{-1}f \notin I, g \in G_2\ \sigma g \notin I\}$.
End.
```

/*/**LGBasis**(**RGBasis**) (**a-sat**($\mathcal{A}$)) compute the Groebner bases of **a-sat**($\mathcal{A}$) w.r.t. the eliminating ordering $x_{1,d_1} > x_{2,d_2} > \cdots x_{n,d_n} > \cdots$ $(x_{1,o_1} > x_{2,o_2} > \cdots x_{n,o_n} > \cdots)$.

Example 5.2 $\mathbb{P} = f_1, f_2$ where f_1, f_2 are the same as Example 3.9. when we apply Cohn{} to $\mathbb{P}$, we have $\sqrt{[\mathbb{P}]} = \textbf{a-sat}(\mathcal{A}_1) \cap \textbf{a-sat}(\mathcal{A}_2)$, where $\mathcal{A}_1 = y_1 - 1, y_{1,1} + 1$ and $\mathcal{A}_2 = y_1 + 1, y_{1,1} - 1$. For $\mathcal{A}_1$, since $\sigma(y_1 - 1) = y_{1,1} - 1$ and $y_{1,1} + 1$, the procedure return Null. So is $\mathcal{A}_2$. Hence, Zero($\mathbb{P}$) = $\emptyset$.

References

[1] Aubry P, Lazard D, Maza M M. On the Theory of Triangular Sets. Journal of Symbolic Computation, 1999, **25**: 105–124

[2] Boulier F, Lazard D, Ollivier F, Petitiot M. Representation for the Radical of a Finitely Generated Differential Ideal. Proc of ISSAC'95, 158-166, ACM Press, 1995

[3] Bouziane D, Kandri Rody A, Maârouf H. Unmixed-dimensional Decomposition of a Finitely Generated Perfect Differential Ideal. Journal of Symbolic Computation, 2001, **31**: 631–649

[4] Chai F, Gao X S, Yuan C M. A characteristic set method for solving boolean equations and applications in cryptanalysis of stream ciphers. Journal of Systems Science & Complexity, 2008, **21**(2): 191–208

[5] Cohn R M. Difference Algebra. Interscience Pbulishers, 1965

[6] Gallo G, Mishra B. Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets, in Effective Methods in Algebraic Geometry, Progress in Mathematics, **94**, 119-142, Birkhauser, Boston, 1991

[7] Gao X S, Luo Y., Yuan C M. A characteristic set method for ordinary difference polynomial systems. Journal of Symbolic Computation, 2009, **44**: 242–260

[8] Gao X S, Luo Y, Yuan C M. A Characteristic Set Method for Difference Polynomial Systems. Journal of Symbolic Computation, 2009, **44**: 242–260

[9] Halas M, Kotta U, Li Z, Wang H, Yuan C M. Submersive Rational Difference Systems and Formal Accessibility. submitted to ISSAC 2009

[10] Hubert E. Factorization-free Decomposition Algorithms in Differential Algebra. Journal of Symbolic Computation, 2000, **29**: 641–662

[11] Kolchin E. Differential Algebra and Algebraic Groups. New York: Academic Press, 1973

[12] Kondratieva M V, Levin A B, Mikhalev A V, Pankratiev E V. Differential and Difference Dimension Polynomials. Kluwer Academic Publishers, 1999

[13] Ritt J F. Differential Algebra. Amer Math Soc Colloquium, 1950

[14] Ritt J F, Doob J L. Systems of Algebraic Difference Equations. American Journal of Mathematics, 1933, **55**: 505–514

[15] Wu W T. On the Decision Problem and the Mechanization of Theorem in Elementary Geometry. Scientia Sinica, 1978, **21**: 159–172

[16] Wu W T. A constructive Theorey of Differential Algebraic Algebraic Geometry. Lect Notes in Math, No. 1255, 173-189, Springer, 1987

[17] Wu W T. Basic Principle of Mechanical Theorem Proving in Geometries (in Chinese). Beijing: Science Press, 1984; English Version, Wien: Springer, 1994

[18] Wu W T. Mathematics Machenization. Beijing: Science Press/Kluwer, 2001

[19] Yang L, Zhang J Z, Hou X R. Non-linear Algebraic Equations and Automated Theorem Proving (in Chinese). Shanghai: Shanghai Science and Education Pub, 1996