A characteristic set method for reflexive differential-difference polynomial systems

Gan Zhiwang
School of Mathematics and System Science
Beihang University
Beijing,China
ganzw@smss.buaa.edu.cn

Zhou Meng
School of Mathematics and System Science
Beihang University
Beijing,China
zhoumeng1613@hotmail.com

***Abstract*—In this paper, a zero decomposition algorithm based on characteristic set methods are developed in reflexive difference and differential polynomial systems. The "generalized term order" is used to deal with negative exponents of difference operators in DD-polynomials and the reduction of two DD-polynomials is discussed. We introduce the concept of characteristic set in reflexive DD-polynomial systems and propose a algorithm which can be used to decompose the zero set of a finitely generated reflexive DD-polynomial set into the union of zero sets of coherent chains.**

Keywords-Characteristic set; Reflexive difference and differential polynomials; Generalized term order; Zero decomposition algorithm

I. Introduction

Characteristic set method is an efficient method in studying polynomial systems or algebraic differential equations. The method is widely used in solving equations, solving the radical ideal membership problem, proving theorems in geometries, computer aided design, robotics, engineering and other fields, see[1,2,3,10,12,16].

The characteristic set method was generalized to the mixed difference and differential polynomial (simply called DD-polynomial) systems by Gao[17,18,19]. But a characteristic set method for reflexive DD-polynomial systems(DD-polynomial systems with inverse difference operators) remains an interesting question. One of the problems in reflexive DD-polynomial systems is to find a proper term order that can help to definite the reduction of DD-plolynomials. Zhou and Franz generalized the concept of term order to deal with negative exponents of terms in difference-differential modules[5].

In this paper, a part of the results based on Wu's characteristic set methods are extended to the reflexive difference and differential case. The "generalized term order" established by Zhou and Franz[5] is used to ordering terms of DD-polynomials. The problem with negative exponents of difference operators was solved by decompose $\mathbb{Z}^N$ into orthants. We introduce the concept of characteristic sets in reflexive DD-polynomial systems and propose a algorithms which can be used to decompose the zero set of a finitely generated reflexive DD-polynomial set into the union of zero sets of coherent chains based on Wu's method[11,12,13,14].

II. Preliminaries

Let $\mathbb{Q}(x)$ be the field of rational functions with an indeterminate x, and assume that $\mathbb{K} \supseteq \mathbb{Q}(x)$ is a computable field. ∂ is a differential operator defined on $\mathbb{K}$ with $\partial : \mathbb{K} \rightarrow \mathbb{K}$

$$\partial(f+g) = \partial(f) + \partial(g)$$
$$\partial(fg) = \partial(f)\cdot g + \partial(g)\cdot f$$

for $\forall f, g \in \mathbb{K}$. And difference operators δ and σ defined on $\mathbb{K}$ are isomorphic mappings satisfying $\sigma = \delta^{-1}$.

In this paper, we assume the existence of a non-zero element $h \in \mathbb{K}$, such that the operator δ and ∂ , σ and ∂ commute according to the following rule:

$$\partial\delta = h\cdot\delta\partial,$$
$$\partial\sigma = h^{-1}\cdot\sigma.$$

It is easy to check that for a non-zero integer s, we have

$$\partial\delta^s = h_s\delta^s\partial,$$
$$h_s = \prod_{i=0}^{s-\frac{s}{|s|}} \delta^i(h^{\frac{s}{|s|}}).$$

We denote

$$\Theta = \{\delta^d\partial^s | d \in Z, s \in N\},$$
$$\Omega = \{\delta^{d_1}\partial^{s_1}\cdots\delta^{d_t}\partial^{s_t}\}.$$

Let $\mathbb{Y} = \{y_1, \cdots, y_n\}$ be a finite number of indeterminates (y_i may be considered as functions of x).Let

$$\Omega\mathbb{Y} = \{\omega y_i | \omega \in \Omega, y_i \in \mathbb{Y}\},$$
$$\Theta\mathbb{Y} = \{\delta^d\partial^s y_i | d \in Z, s \in N, y_i \in \mathbb{Y}\}.$$

And for convenience, we denote

$$\delta^d\partial^s y_i = y_{i,d,s}.$$

We denote

$$\mathbb{R} = \mathbb{K}\{\mathbb{Y}\} = \mathbb{K}[\Omega\mathbb{Y}]$$

$\mathbb{R}$ is called the reflexive DD-ring of DD-polynomials over $\mathbb{K}$ in $\mathbb{Y}$ (In this paper, "DD" always means "reflexive difference-differential").

The following two lemmas hold in reflexive DD-polynomial system case.

Lemma 1[18] $\mathbb{K}[\Omega] = \mathbb{K}[\Theta]$,and Θ is a basis of the $\mathbb{K}$ -vector space $\mathbb{K}[\Omega]$].

Lemma 2[18] $\mathbb{K}\{\mathbb{Y}\} = \mathbb{K}[\Theta\mathbb{Y}]$, and $\Theta\mathbb{Y}$ is a transcendence basis of the $\mathbb{K}$-vector space $\mathbb{K}\{\mathbb{Y}\}$ over $\mathbb{K}$.

Let $\leq$ be a total ordering on $\Theta\mathbb{Y}$. For a DD-polynomial set $\mathbb{P} \in \mathbb{K}[\Theta\mathbb{Y}]$, we define $V_{\mathbb{P}}$ to be the set of all elements of $\Theta\mathbb{Y}$ occurring in $\mathbb{P}$. We define the leader of $\mathbb{P}$ to be the maximal element of $V_{\mathbb{P}}$ under $\leq$ and denote it by $v_{\mathbb{P}}$ or $v(\mathbb{P})$. If $\mathbb{P} = \{P\}$, let $v_{\mathbb{P}} = v_P$.

A generalized term order is a total ordering $\leq$ satisfying the following conditions:

Published by Atlantis Press, Paris, France.

$$A_1\colon\begin{cases} v(\theta y) \le v(\delta\theta y), \forall\theta y \in \{\delta^d\partial^s y_i | \mathrm{d}, s \in N, y_i \in Y\}; \\ v(\theta y) \le v(\sigma\theta y), \forall\theta y \in \{\sigma^d\partial^s y_i | \mathrm{d}, s \in N, y_i \in Y\}; \\ v(\theta y) \le v(\partial\theta y), \forall\theta y \in \Theta Y; \end{cases}$$

$$A_2\colon\begin{cases} v(\delta\theta y) \le v(\delta\theta' y'), \forall\theta y \le \theta' y', \\ \theta\text{‘}y\text{’} \in \{\delta^d\partial^s y_i | \mathrm{d}, s \in N, y_i \in Y\}; \\ v(\sigma\theta y) \le v(\sigma\theta' y'), \forall\theta y \le \theta' y', \\ \theta' y' \in \{\sigma^d\partial^s y_i | \mathrm{d}, s \in N, y_i \in Y\}; \\ v(\partial\theta y) \le v(\partial\theta' y'), \forall\theta y \le \theta' y' \end{cases}$$

Generalized term orders exist: one example is the ordering $\le_l$ defined by:

$$\delta^{\alpha_1}\sigma^{\beta_1}\partial^{\gamma_1}y_{c_1} \le_l \delta^{\alpha_2}\sigma^{\beta_2}\partial^{\gamma_2}y_{c_2}$$
$$\Leftrightarrow (c_1, \alpha_1, \beta_1, \gamma_1) \le_{lex} (c_2, \alpha_2, \beta_2, \gamma_2),$$

where $\le_{lex}$ stands for the lexicographical ordering and $\alpha_1\beta_1 = 0, \alpha_2\beta_2 = 0$.

The concept of generalized term order was established by Zhou and Franz in 2008.It is a weak admissible ordering which could deal with terms with negative exponents. In this paper, we always assume that the ordering $\le$ is a generalized term order. We will also assume that $y_1 < y_2 < \cdots < y_n$, which can always be made to hold after a permutation of indexes.

Let $\mathbb{N}$ be set of non-negative integers and $\mathbb{E}$ be the set of non-positive integers. The subset $\mathbb{N}$ and $\mathbb{E}$ with $\mathbb{Z} = \mathbb{N} \cup \mathbb{E}$ and $\mathbb{N} \cap \mathbb{E} = \{0\}$ is called a orthant decomposition of $\mathbb{Z}$. $\mathbb{N}$ and $\mathbb{E}$ are called the orthant of $\mathbb{Z}$. If $\delta^{\alpha_1}\partial^{\gamma_1}y_c \le \delta^{\alpha_2}\partial^{\gamma_2}y_c$, where $\le$ is a generalized order and $\alpha_1, \alpha_2 \in \mathbb{Z}$, and β is an integer in the same orthant of $\mathbb{Z}$ with α_2, then we have $\delta^{\alpha_1+\beta}\partial^{\gamma_1}y_c \le \delta^{\alpha_2+\beta}\partial^{\gamma_2}y_c$. Without loss of generality, we always assume that generalized term order is based on the orthant decomposition $\mathbb{Z} = \mathbb{N} \cup \mathbb{E}$.

We denote $(\Theta\mathbb{Y})^*$ to be the set of elements raised to strictly positive power in $\Theta\mathbb{Y}$.And we denote the extended variables in $(\Theta\mathbb{Y})^*$ by v^*. The ordering $\le$ on variables can be extended by $v^d \le (v')^e$, if and only if either $v < v'$, or $v = v'$ and $d \le e$. The extended leader of a non-ground DD-polynomial P is denoted by $v_P^* = v_P^{\deg(P, v_P)}$. For DD-polynomials P and Q, we will write $P \le Q$ if $v_p^* \le v_Q^*$. We write $P \sim Q$ if $v_p^* = v_Q^*$.

Lemma 3[5] Any descending sequence $P_1 > P_2 > P_3 > \cdots$is finite with $P_i \in \mathbb{K}[\Theta\mathbb{Y}]$.

III. Pseudo-remainders of DD-polynomials

Let $\mathbb{Y}_c = \{y_1, \cdots, y_c\}$.And P is a DD-polynomial in $\mathbb{K}[\Theta\mathbb{Y}]$, we define the class of P to be the smallest $c = cls(P)$ such that $P \in \mathbb{K}[\Theta\mathbb{Y}_c]$.We set $cls(P) = 0$ if $P \in \mathbb{K}$. Let the leader of P to be $\theta y_c = y_{c,d,s}$, we define $ord_\delta(P, y_c) = ord_\delta(\theta) = d$.

For a DD-ploynomial P with $cls(P) > 0$ and $v_p = y_{c,d,s}$, P can be written into the following canonical representation:

$$P = P_t {y_{c,d,s}}^t + P_{t-1}{y_{c,d,s}}^{t-1} + \cdots + P_0,$$

where $v_{P_i} < v_P (i = 0, \cdots, t)$.We call $I_p = P_t$ the initial of P. And $ldeg(P) = t$ is called the leading degree of P. Applying δ,σ and ∂ to P,we have

Lemma 4.

$$\delta P = \delta(P_t){y_{c,d+1,s}}^t + \delta(P_{t-1}){y_{c,d+1,s}}^{t-1} + \cdots + \delta(P_0)$$
$$\delta^{-1}P = \delta^{-1}(P_t){y_{c,d-1,s}}^t + \delta^{-1}(P_{t-1}){y_{c,d-1,s}}^{t-1} + \cdots + \delta^{-1}(P_0)$$
$$\partial P = S_p y_{c,d,s+1} + R$$

where

$$S_P = \prod_{i=0}^{d-\frac{d}{|d|}} \delta^i(h^{\frac{d}{|d|}}) \frac{\partial P}{\partial y_{c,d,s}}$$

is called the separant of P, R is a DD-polynomial with lower leading variable than $y_{c,d,s+1}$.

Let $P \in \mathbb{R}\backslash\mathbb{K}$ and $v_P = y_{c,d,s}$, then we say that Q is *reduced* w.r.t. P if and only if:

(1) $y_{c,d+k,s+l}$ does not occur in Q for k and d in the same orthant, $l > 0$;

(2) $\deg(Q, y_{c,d+k,s}) < \deg(P, y_{c,d,s})$ for k and d in the same orthant.

If $P \in \mathbb{K}\backslash\{0\}$, then 0 is the only DD-polynomial which is reduced w.r.t. P.

Let $\theta = \delta^\alpha\partial^\beta$,$\theta' = \delta^{\alpha'}\partial^{\beta'}$.We define a partial ordering $\le$ on Θ by

$$\theta \le \theta\text{’} \Leftrightarrow \beta \le \beta\text{‘}, and\ 0 \le \alpha \le \alpha\text{‘ or } 0 \ge \alpha \ge \alpha\text{‘}.$$

For $\theta \le \theta$’, we define

$$\theta\text{‘}/\theta = \delta^{\alpha\text{’}-\alpha}\partial^{\beta\text{‘}-\beta}$$

The partial ordering $\le$ on Θ can be extended on extended variables by $v^* = (\theta y_i)^d \le (\theta' y_i)^e = (v')^*$, if and only if $\theta \le \theta$’ and either $d \le e$,or θ'/θ is not a pure difference operator.

Let $\mathrm{P}, Q \in \mathbb{R}$ be two DD-polynomials with $P \neq 0$.Then the algorithm **rprem** returns the pseudo-remainder of Q w.r.t. P. It is easily checked that $rprem(Q, P)$ is reduced w.r.t. P. Otherwise, the algorithm wouldn’t terminate.

Algorithm 1-rprem(Q, P)

```
Input: Two DD-polynomials $P$ and $Q$ with $P \neq 0$.
Output: The pseudo remainder of $Q$ w.r.t $P$.
If $P \in \mathbb{K}$, then return 0.
Set $R = Q$.
While $\exists\omega^* \in V_R^*, v_P^* \le \omega^*$ do
    Choose the highest $\omega^*$ under $\le$.
    Set $R = aprem(R, (\omega/v_P)P)$.
Return $R$
/*/We denote $aprem(R, Q)$ to be the algebraic
    pseudo-remainder of $P$ w.r.t $Q$ in variable $v_Q$.
```

For polynomials P and Q, it’s easy to check that if $v_P < v_Q$, then P is reduced w.r.t. Q.

IV. Characteristic sets of DD-polynomial systems

A. Auto-reduced sets

$\mathcal{A}$ is a subset in $\mathbb{K}\{\mathbb{Y}\}\backslash\mathbb{K}$. If for each $P \in \mathcal{A}$, P is reduced w.r.t. each polynomial in $\mathcal{A}\backslash\{P\}$,then $\mathcal{A}$ is called a *auto-reduced set*. An auto-reduced set $\mathcal{A} = \{A_1, \cdots, A_r\}$

with $v_{A_1} < \cdots < v_{A_r}$ is called an *ascending chain* or simply a *chain*.

Let $y_{i,d,s}$ to be the leading variable of a polynomial in $\mathcal{A}$, we define its DD-index to be (d,s).

Let $\mathcal{A}$ be a chain. We denote IND_i the set of indices for the polynomials in $\mathcal{A}$ with a fixed class i.

We first recall two properties of auto-reduced sets in non-reflexive DD-polynomial case.

Proposition 5.(Gao et al.,2009) Let $\mathcal{A}$ be a chain. If we arrange $IND_i = \{(a_1,b_1),\cdots,(a_s,b_s)\}$ such that $a_1 \le a_2 \le \cdots \le a_s$.Then we have

- $a_1 < a_2 < \cdots < a_s$ and $b_1 \ge b_2 \ge \cdots \ge b_s$.
- If $b_j = b_{j+1}$,then $d(a_j,b_j) < d(a_{j+1},b_{j+1})$,where $d(a_j,b_j)$ is the leading degree of the polynomial with index (a_j,b_j).

Lemma 6. (Gao et al.,2009) Any auto-reduced set is finite.

Let $\mathcal{A}$ be a chain.We divide $\mathcal{A}$ into two parts by positive and negative exponent of δ in the leader of A_i, $\mathcal{A} = \mathcal{A}_\delta \cup \mathcal{A}_\sigma$. For $\forall P \in \mathcal{A}_\delta$, we have $ord_\delta(P, v_P) \ge 0$. $\mathcal{A}_\delta$ is a chain in non-reflexive DD-polynomial case, where all the term $y_{c,d,s}$ occur in $\mathcal{A}_\delta$ with $d < 0$ are treated as parameters. And similarly, $\mathcal{A}_\sigma$ is also a chain in non-reflexive DD-polynomial case.

Proposition 7. Let $\mathcal{A}$ be a chain. $IND_i = \{(a_{p_1},b_{p_1}),\cdots,(a_{p_s},b_{p_s}),(a_{n_1},b_{n_1}),\cdots,(a_{n_r},b_{n_r})\}$, where $0 \le a_{p_1} \le \cdots \le a_{p_s}$, $0 \ge a_{n_1} \ge \cdots \ge a_{n_s}$. Then we have

- $0 < a_{p_1} < \cdots < a_{p_s}$, $0 > a_{n_1} > \cdots > a_{n_s}$, and $b_{p_1} \ge \cdots \ge b_{p_s}$>0, $b_{n_1} \ge \cdots \ge b_{n_s}$>0.
- If $b_{p_j} = b_{p_{j+1}}$, then $d(a_{p_j},b_{p_j}) > d(a_{p_{j+1}},b_{p_{j+1}})$.
- If $b_{n_j} = b_{n_{j+1}}$, then $d(a_{n_j},b_{n_j}) > d(a_{n_{j+1}},b_{n_{j+1}})$.

Proof. Let $\mathcal{A} = \mathcal{A}_\delta \cup \mathcal{A}_\sigma$. $\mathcal{A}_\delta$ and $\mathcal{A}_\sigma$ is chains in non-reflexive DD-polynomial case, then the proposition is true according to Proposition 5.

Example 8 Set the ordering to be $\le_l$.The following set forms a chain.

$$\mathcal{A} = \{A_1, A_2, A_3, \mathrm{A}_4\}$$
$$A_1 = y_{1,-1,4}^2$$
$$A_2 = y_{1,-3,1} + y_{1,-2,2}$$
$$A_3 = y_{1,2,3}^2 + y_{1,-1,1}$$
$$A_4 = y_{1,4,3} + y_{1,-2,1}$$

From the DD-indices for $\mathcal{A}$ shows in Figure1, we can easy verify proposition 7.

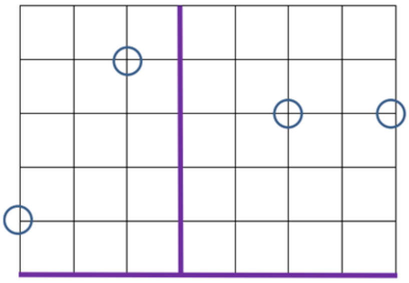

Figure 1. The indices of chain $\mathcal{A}$ from Example 8

Lemma 9. Any auto-reduced set is finite.

Proof. Let $\mathcal{A}$ be a chain. Let $\mathcal{A} = \mathcal{A}_\delta \cup \mathcal{A}_\sigma$. Since $\mathcal{A}_\delta$ and $\mathcal{A}_\sigma$ are finite according to Lemma 6, $\mathcal{A}$ is finite.

Let $\mathcal{A} = \{A_1,\cdots,A_m\}$ and $\mathfrak{B} = \{B_1,\cdots,B_n\}$ be chains. We consider the partial ordering $\le$ on chains. We $\mathcal{A} \le \mathfrak{B}$ if there exists a j with $A_i \sim B_i$ for $1 \le i < j$ and either $A_j < B_j$ or $j = n+1 \le m$. The ordering $\le$ is called a ranking.

Lemma 10. Any descending chain $\mathcal{A}_1 > \mathcal{A}_2 > \mathcal{A}_3 > \cdots$is finite.

Proof. Assume that the lemma is not ture. Then the first elements of the chains $\mathcal{A}_1$,$\mathcal{A}_2$,…satisfy $\mathcal{A}_{1,1} > \mathcal{A}_{2,1} > \cdots$. By Lemma 3, there exists an index j_1 with $\mathcal{A}_{i,1} \sim \mathcal{A}_{j_1,1}$ for $\forall i \ge j_1$. Similarly, there exists an index $j_2 > j_1$ with $\mathcal{A}_{i,2} \sim \mathcal{A}_{j_2,2}$ for $\forall i \ge j_2$. By induction, we get a sequence $j_1 < j_2 < \cdots$ with $\mathcal{A}_{i,k} \sim \mathcal{A}_{j_k,k}$ for $\forall i \ge j_k$ .But then $\{\mathcal{A}_{j_1,1}, \mathcal{A}_{j_2,2}, \cdots\}$ is an infinite auto-reduced set, which contradicts Lemma 9.

Let $\mathbb{P}$ be a set of DD-polynomials and consider the set of chains of DD-polynomials in $\mathbb{P}$. By Lemma 10, there exists at least one chain with lowest rank among all chains. And the least chain is called a *characteristic set* of $\mathbb{P}$.

A DD-polynomial is said to be *reduced w.r.t. a chain* if it is reduced to every DD-polynomial in the chain.

Lemma 11. If $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ and $\mathcal{A}'$ a characteristic set of $\mathbb{P} \cup \{\mathrm{P}\}$ for a DD-polynomial P, then we have $\mathcal{A} \ge \mathcal{A}'$. Moreover, if P is reduced w.r.t. $\mathcal{A}$, then $\mathcal{A} > A'$.

Proof. The first statement is obviously true, since the characteristic set of $\mathbb{P}$ is in $\mathbb{P} \cup \{\mathrm{P}\}$. As to the second statement, assume $\mathcal{A} = \{A_1,\cdots,A_r\}$. If $v_P > v_{A_r}$, then chain $A_1,\cdots,A_r,P$ is of rank lower than $\mathcal{A}$. If $v_{A_{k-1}} < v_P \le v_{A_k} \le v_{A_p}$, then chain $A_1,\cdots,A_{k-1},P$ is of rank lower than $\mathcal{A}$. Hence $\mathcal{A} > A'$.

Lemma 12. A chain $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ if and only if $\mathbb{P}$ does not contain a non-zero DD-polynomial which is reduced w.r.t. $\mathcal{A}$.

Proof. By Lemma 11, we just need to prove the sufficiency. Assume $\mathfrak{B} = \{B_1,\cdots,B_s\}$ is the characteristic set of $\mathbb{P}$, while $\mathcal{A}$ is not. We have $\mathfrak{B} < \mathcal{A}$. If there exists a $k \le \min\{s,p\}$ with $B_k < A_k$, then B_k is reduced w.r.t. $\mathcal{A}$ by the definition of auto-reduced chain. Otherwise $s > p$ and B_{p+1} is reduced w.r.t. $\mathcal{A}$. Both of the cases contradict the hypothesis and show that $\mathcal{A}$ is the characteristic set of $\mathbb{P}$.

B. Extension of chains

In the process of computing the pseudo-remainder of Q w.r.t P, we need to lift the difference and differential orders of P by considering θP for certain $\theta \in \Theta$. Similarly, in order to compute the pseudo-remainder of a DD-polynomial w.r.t. a chain, we also need to select a DD-polynomial in the chain and to lift its orders. But the selection of the DD-polynomial is not unique. Different choice might lead to different result. In order to give a proper definition for pseudo-remainders, Gao Xiaoshan[18] introduced the concept of extension for chains, which could be extended to the reflexive DD-polynomial case.

Let $\mathcal{A}$ be a chain.We denote

$\mathbb{M}_{\mathcal{A}} = \{y_{c,d,s} | \exists A \in \mathcal{A}, v_A = y_{c,d',s'}, s' \geq s, d' and\ ord_\delta\ are\ in\ the\ same\ orthant\}$. So $\mathbb{M}_{\mathcal{A}}$ is the the set of all possible lifted variables by the leader in $\mathcal{A}$. For a DD-polynomial set $\mathbb{P}$, let $d^c_{\mathbb{P},1}$ be the largest d such that $y_{c,d,s}$ occurs in $\mathbb{P}$, $d^c_{\mathbb{P},2}$ be the smallest d such that $y_{c,d,s}$ occurs in $\mathbb{P}$, and $s^c_{\mathbb{P}}$ be the largest s such that $y_{c,d,s}$ occurs in $\mathbb{P}$. And

$$\mathbb{V}_{\mathbb{P}} = \{y_{c,s,t} \in \mathbb{M}_{\mathcal{A}} | \exists P \in \mathbb{P}, a, b: \deg(P, y_{c,a,b}) > 0, 1 \leq c \leq n, t \leq b, 0 \leq s \leq a\ or\ 0 \geq s \geq a\}$$

$$\mathbb{L}_{\mathbb{P}} = \{y_{c,s,t} | \exists P \in \mathbb{P}: v_P = y_{c,s,t}\}$$

So $\mathbb{L}_{\mathbb{P}}$ is the set of leading variables of $\mathbb{P}$ and $\mathbb{V}_{\mathbb{P}}$ implicitly depends on $\mathcal{A}$.

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

- For any $P \in \mathcal{A}_{\mathbb{P}}$, there exist a $\theta \in \Theta$ and an $A \in \mathcal{A}$ such that $P = \theta A$. So $\mathcal{A}_{\mathbb{P}}$ is the set of lifted polynomials.
- $\mathcal{A}_{\mathbb{P}}$ is an algebraic triangular set under the ordering $\leq$ when all $y_{c,m,n}$ are considered as independent variables.
- $\mathbb{L}_{\mathcal{A}_{\mathbb{P}}} = \mathbb{V}_{\mathbb{P} \cup \mathcal{A}_{\mathbb{P}}}$.
- A DD-polynomial P is reduced w.r.t $\mathcal{A}$ if and only if P is algebraic reduced w.r.t $\mathcal{A}_P$ when all $y_{c,m,n}$ are considered as independent variables.

Given a DD-polynomial set $\mathbb{P}$, the algorithm **Extension** shows how to compute an extension of $\mathcal{A}$ w.r.t. $\mathbb{P}$, which is satisfying the above properties. The algorithm is similar but different from[18].We will give an example of $\mathcal{A}_P$.

Example 13. Let $\mathcal{A}$ be the chain in Example 9, and $P = y_{1,5,5} + y_{1,-2,3}$, we have

$$\mathcal{A}_P = \{A_1, \sigma\partial^2 A_1, \sigma\partial A_1, \sigma A_1, \partial^2 A_1, \partial A_1, A_2, \partial^4 A_2, \partial^3 A_2, \partial^2 A_2, \partial A_2, A_3, \delta\partial^2 A_3, \delta\partial A_3, \delta A_3, \partial^2 A_3, \partial A_3, A_4, \delta\partial^2 A_4, \delta\partial A_4, \delta A_4, \partial^2 A_4, \partial A_4\}$$

The DD-indices for the DD-polynomials in $\mathcal{A}_P$ are given in Figure 2,where a solid dot represents the index of a newly added DD-polynomial.

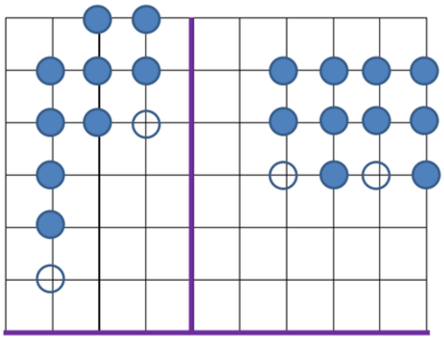

Figure 2. The DD-indices for $\mathcal{A}_P$ in Example 13.

Algorithm 2-Extension($\mathcal{A}$, $\mathbb{P}$)

```
Input: A chain $\mathcal{A}$ and a set $\mathbb{P}$ of DD-polynomials.
Output: The extension $\mathcal{A}_{\mathbb{P}}$ of $\mathcal{A}$ w.r.t. $\mathbb{P}$.
S0. Let $L = \mathbb{L}_{\mathcal{A}}, \mathbb{Q} = \mathcal{A} \cup \mathbb{P}, \mathbb{H} = \{y_{c,d^c_{\mathbb{P},1},s^c_{\mathbb{P}}}, y_{c,d^c_{\mathbb{P},2},s^c_{\mathbb{P}}}, c = 1, \cdots, n\}, V = \mathbb{V}_{\mathbb{H}} \backslash L$,and $\mathcal{A}_{\mathbb{P}} = \mathcal{A}$.
S1. If there exist$\omega$,c and $\eta$ with $\omega y_c \in V, \eta y_c \in L$ and $\eta \leq \omega$, then choose $\omega$ and c such that $\omega y_c$ is largest for $\leq$. If there are no such $\omega, \eta$ and c, then return $\mathcal{A}_{\mathbb{P}}$
S2. If for all the $\theta y_c \in L$ satisfying $\theta \leq \omega$, $\omega/\theta$ is a difference operator. Let $\eta$ be the largest one of those $\theta$ under $\leq$, go to S4.
S3. If there exist a $\theta y_c \in L$, $\omega/\eta$ is not a difference operator. Let $\eta$ be the one with largest in $|ord_\delta|$.Go to S4.
S4.Let $A_i \in \mathcal{A}$ such that $v_{A_i} = \eta y_c$. Let $Q = (\omega/\eta)A_i$, $\mathcal{A}_{\mathbb{P}} = \mathcal{A}_{\mathbb{P}} \cup \{Q\}, V = V \cup (\mathbb{V}_Q \backslash \mathbb{L}_{\mathcal{A}_{\mathbb{P}}})$. Delete $\omega y_c$ from V and go to S1. Since all the variables in $\mathbb{V}_Q \backslash \mathbb{L}_{\mathcal{A}_{\mathbb{P}}}$ are less than $\omega y_c$, this process will terminate.
```

For a DD-polynomial P.The pseudo-remainder of a polynomial P w.r.t. a chain $\mathcal{A}$ is defined to be the algebraic pseudo-remainder of P w.r.t. the algebraic triangular set $\mathcal{A}_P$:

$$rprem(P, \mathcal{A}) = aprem(P, \mathcal{A}_P).$$

Lemma 14. Let $R = rprem(P, \mathcal{A})$. Then R is reduced w.r.t. $\mathcal{A}$ and there exists an $H \in \mathbf{H}_{\mathcal{A}}$ such that $v_H < v_Q$ and

$$HQ \equiv R \bmod [\mathcal{A}],$$
$$HQ \equiv R \bmod (\mathcal{A}_Q).$$

Where $[\mathcal{A}]$ stands for the differential-difference ideal generated by $\mathcal{A}$ and $(\mathcal{A}_Q)$ is the algebraic ideal generated by $\mathcal{A}_Q$.

V. Coherent Chains and Zero Decomposition Algorithm

Consider two DD-polynomials A_1, $A_2 \in \mathbb{R} \backslash \mathbb{K}$. If $ord_\delta(v(A_1))ord_\delta(v(A_2)) < 0$ or $cls(A_1) \neq cls(A_2)$, then we define $\Delta(A_1, A_2) = 0$. Else, let $v(A_1) = \theta_1 y_c$, $v(A_2) = \theta_2 y_c$, and $\theta \in \Theta$ be the smallest under $\leq$ such that $\theta_1 \leq \theta$, $\theta_2 \leq \theta$. Ordering A_1 and A_2 such that $\deg((\theta/\theta_1)A_1) \geq \deg((\theta/\theta_2)A_2)$, we define the $\Delta - polynomial$ of A_1 and A_2 to be

$$\Delta(A_1, A_2) = aprem_{\theta y_c}((\theta/\theta_1)A_1, (\theta/\theta_2)A_2).$$

Given a chain $\mathcal{A} = \{A_1, \cdots, A_p\}$, we denote by $\Delta(\mathcal{A})$ the set of non-zero Δ-polynomials $\Delta\left(A_i, A_j\right)$ for all $A_i, A_j \in \mathcal{A}$. A chain is said to be *coherent* if $rprem(P, \mathcal{A}) = 0$ for all $P \in \Delta(\mathcal{A})$.

A chain $\mathcal{A}$ is called a *Wu characteristic set* of a DD-polynomial set $\mathbb{P}$ if $\mathcal{A} \subseteq \mathbb{P}$ and $rprem(P, \mathcal{A}) = 0$ for all $P \in \mathbb{P}$.

Let $\mathbb{P} \subset \mathbb{K}\{\mathbb{Y}\}$ be a finite system of DD-polynomials and let $\widehat{\mathbb{K}}$ be a DD-superfield of $\mathbb{K}$. A zero of $\mathbb{P}$ in $\widehat{\mathbb{K}}$ is a tuple $\hat{y}_1, \cdots, \hat{y}_n \in \widehat{\mathbb{K}}^n$ with $P(\hat{y}_1, \cdots, \hat{y}_n) = 0$ for all P in $\mathbb{P}$. We use $Zero(\mathbb{P})$ to denote the set of all zeros of $\mathbb{P}$. Let D be a polynomial. We use $Zero(\mathbb{P}/D)$ to denote the set of zeros of $\mathbb{P}$ which do not annul D.

Lemma 15. Let $\mathbb{P}$ be a finite set of DD-polynomials, $\mathcal{A} = \{A_1, \cdots, A_m\}$ is a Wu characteristic set of $\mathbb{P}$. $I_i = I_{A_i}$,$S_i = S_{A_i}$,and $H = \prod_{i=1}^{m} I_i S_i$. Then

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathcal{A}/H) \cup \bigcup_{i=1}^{m} \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\})$$

$$\cup \bigcup_{i=1}^{m} \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$$

Proof. This is a direct consequence of Lemma 14.

Now we have the zero decomposition theorem as follow.

Theorem 16. Let $\mathbb{P}$ be a finite set of DD-polynomials in $\mathbb{K}\{y_1, \cdots, y_n\}$. Then the algorithm **ZDT** computes sequence of coherent Wu characteristic sets $\mathcal{A}_1, \cdots, \mathcal{A}_k$, such that

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathcal{A}_i/H_i).$$

where H_i is a product of the initials and separants of $\mathcal{A}_i$.

Algorithm 3 –ZDT$(\mathbb{P})$

Input: A finite set $\mathbb{P}$ of reflexive DD-polynomials.

Output: $W = \{\mathcal{A}_1, \cdots, \mathcal{A}_k\}$,such that $\mathcal{A}_i$ is a coherent chain and

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathcal{A}_i/H_i).$$

```
Let $\mathfrak{B} := CS(\mathbb{P}), \mathfrak{B} := B_1, \cdots, B_p$.
If $\mathfrak{B} = 1$ then return $\{\}$.
Else
    Let $\mathbb{R} := \{rprem(f, \mathfrak{B}) \neq 0 | f \in (\mathbb{P} \backslash \mathfrak{B}) \cup \Delta(\mathfrak{B})\}$.
    If $\mathbb{R} = \emptyset$ then $W = \{\mathfrak{B}\} \cup \mathbf{ZDT}(\mathbb{P} \cup \mathfrak{B} \cup \{I_i\}) \cup \mathbf{ZDT}(\mathbb{P} \cup \mathfrak{B} \cup \{S_i\})$
    Else $W := \mathbf{ZDT}(\mathbb{P} \cup \mathbb{R})$.
/*/ $CS(\mathbb{P})$ returns the characteristic set of $\mathbb{P}$. It is easy to find $CS(\mathbb{P})$ since $\mathbb{P}$ is finite.
```

Proof. If $\mathbb{R} = \emptyset$, then $\mathfrak{B}$ is a coherent Wu characteristic set of $\mathbb{P}$. BY Lemma 5.2, we have $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathfrak{B}/H) \cup \bigcup_{i=1}^{m} \mathrm{Zero}(\mathbb{P} \cup \mathfrak{B} \cup \{I_i\}) \cup \bigcup_{i=1}^{m} \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$. If $\mathbb{R} \neq \emptyset$, we have $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{P} \cup \mathbb{R})$ by the Lemma 14. By Lemma 10 and Lemma 11, the algorithm terminates after finite steps.

Example 17. Let $A_1 = y_{1,-2,1} + y_{0,0,0}$, $A_2 = y_{2,0,2}$, $A_3 = y_{2,1,1}^2 + y_{1,-2,0}$, $\mathbb{P} = \{A_1, A_2, A_3\}$. The generalized term order is $\leq_l$. The difference operator δ satisfys $\delta\left(f(x)\right) = f(x+1)$ for any $f \in \mathbb{K}$. We have $\partial\delta = \delta\partial$,$\partial\sigma = \sigma\partial$.

First we have $\mathfrak{B} = CS(\mathbb{P}) = \{A_1, A_2, A_3\}$, $A_4 = \Delta(\mathfrak{B}) = \Delta(A_2, A_3) = aprem(\partial A_3, \delta A_2) = y_{1,-2,1}$, then $rprem(A_4, \mathfrak{B}) = -y_{0,0,0}$. Let $A_5 = -y_{0,0,0}$, $\mathbb{P}_1 = \mathbb{P} \cup \{A_5\}$, then we have $W = \mathbf{ZDT}(\mathbb{P}_1)$.

We have $\mathfrak{B}_1 = CS(\mathbb{P}_1) = \{A_5, A_2, A_3\}$, $\Delta(\mathfrak{B}_1) = A_4$,$rprem(A_4, \mathfrak{B}_1) = rprem(A_1, \mathfrak{B}_1) = A_4$.Let $\mathbb{P}_2 = \mathbb{P}_1 \cup \{A_4\}$, then $W = \mathbf{ZDT}(\mathbb{P}_2)$.

The algorithm goes on. We have $\mathfrak{B}_2 = CS(\mathbb{P}_2) = \{A_5, A_4, A_2, A_3\}$ .Then $\mathbb{R} = \emptyset$, $A_6 = S_{A_3} = 2y_{2,1,1}$ .Let $\mathbb{P}_3 = \mathbb{P}_2 \cup \{A_6\}$.We have $W = \{\mathfrak{B}_2\} \cup \mathbf{ZDT}(\mathbb{P}_3)$.

And similarly, $\mathbf{ZDT}(\mathbb{P}_3)$ returns $\{A_5, A_7, A_2, A_6\}$,where $A_7 = 2y_{1,-2,0}$.

Finally we have $W = \{A_5, A_4, A_2, A_3\} \cup \{A_5, A_7, A_2, A_6\}$.

ACKNOWLEDGMENT

The reported work was supported by NSFC project 11271040 and the Natural Science Foundation of Beijing(1102026).

REFERENCES

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

[2] J.F. Ritt. Differential Algebra, American Mathematical Society, 1950.

[3] J.F. Ritt., J.L. Doob. Systems of algebraic difference equations. Amer. J. Math, 1933. 55, 505-514.

[4] Mansfield,E.L., Szanto,A. Elimination theory for differential difference polynomials. In: Proc. ISSAC,02. ACM Press, New York, 2002, pp.191-198.

[5] Meng Zhou,Franz Winkler.Computing difference-differential dimension polynomials by relative Gr$\ddot{o}$bner bases in difference-differential modules. Journal of Symbolic Computation,2008,43,726-745

[6] R.M. Cohn. Difference Algebra, Interscience Publishers, 1965.

[7] Rosenfeld, A. Specialization in differential algebra, Trans, 1959. AMS 90, 394-407.

[8] Seidenberg, A.. An elimination theory for differential algebra., Univ. California Publication in Math, 1956. 3, 31-65.

[9] van der Hoeven, J. Differential and mixed differential-difference equations from the effective viewpoint, Preprints, 1996.

[10] Wang,D..Elimination Methods.Springer,Berlin,2000.

[11] W.T. Wu. On the decision problem and the mechanization of theorem in elementary geometry. Scientia Sinica ,1978,21, 159-172.

[12] W.T. Wu. Mechanical derivation of Newton's gravitational laws from Kepler's laws. MM Researche Preprints,1987,53-61.

[13] W.T. Wu. On the Foundation of Algebraic Differential Polynomial Geometry, Sys. Sci. & Math.Sci., 1989, 2(4) , 289-312.

[14] W.T. Wu. Basic Principle of Mechanical Theorem Proving in Geometries, Science Press, Beijing,1984; English translation, Springer, Wien, 1994.

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

[16] W.T. Wu,X.S. Gao.Mathematics mechanization and applications after thirty years, Frontiers of Computer Science in China,2007,vol 1,Issue 1,1-8.

[17] X.S. Gao,Y. Luo,G. Zhang.A characteristic set method for ordinary difference polynomial systems.In:MM-preprints,2006, vol.25.pp.84-102.

[18] X.S. Gao, J. Van der Hoeven, C.M. Yuan, G.L. Zhang.Characteristic set method for differential-difference polynomial systems.Journal of Symbolic Computation ,2009.44,1137-1163

[19] X.S. Gao, Luo,Y., Yuan,C.M..A characteristic set method for ordinary difference polynomial systems.Journal of Symbolic Computation,2009.44,242-260

[20] X.S. Gao, Z.M. Li.Mechanized methods for differential and difference equations.Journal of System Science and Mathematics Science ,2009.29,1222-123