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 is 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 an 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[18] remains an interesting question. One of the problems in reflexive DD-polynomial systems is to find a proper term order that can help to define the reduction of DD-polynomials. 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. $\partial$ is a differential operator defined on $\mathbb{K}$ with $\partial : \mathbb{K} \to \mathbb{K}$

$$
\partial(f + g) = \partial(f) + \partial(g),
$$

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

for $f, g \in \mathbb{K}$. And difference operators $\partial$ and $\sigma$ 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 $\delta$ and $\partial$, $\sigma$ and $\delta$ commute according to the following rule:

$$
\partial \delta = h \cdot \partial \
$$

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

$$
\partial \delta^s = h^s \cdot \partial \
$$

$$
h_s = \prod_{i=0}^{s} \delta(h^i) 
$$

We denote

$$
\theta = [\delta^k]^i \in \mathbb{K}^i, \partial \sigma = h^{-1} \cdot \sigma,
$$

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

$$
\Omega = [\delta^j]^s \in \mathbb{K}^s, \theta \mathbb{Y} = [\delta^k]^i \mathbb{Y} \in \mathbb{Y},
$$

And for convenience, we denote

$$
\delta^k \mathbb{Y} = y_{i,d,s}
$$

We denote

$$
\mathbb{K} = \mathbb{K}[\mathbb{Y}] = \mathbb{K}[\theta \mathbb{Y}]
$$

$\mathbb{K}$ 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] $\mathbb{K}[\theta] = \mathbb{K}[\mathbb{Y}]$, and $\theta$ is a basis of the $\mathbb{K}$-vector space $\mathbb{K}[\theta]$. ($\mathbb{K}$ vector space $\mathbb{K}[\mathbb{Y}]$ over $\mathbb{K}$).

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:
Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013)

where decomposition of and of non-positive integers. The subset

paper, we always assume that the ordering

could deal with terms with negative exponents. In this

It is a weak admissible ordering

generalized term order is based on the orthant decomposition

variables in . For DD-polynomials

Lemma 3

where

_define_

and

Or

The concept of generalized term order was established by Zhou and Franz in 2008. It is a weak admissible ordering

generally called a orthant which can always be made to hold after a

permutation of indexes.

Let be the set of non-negative integers and be the set of non-positive integers. The subset and are called the orthant of . If and is a generalized order and , then we have . Without loss of generality, we always assume that generalized term order is based on the orthant decomposition

We denote the set of elements raised to strictly positive power in .

And denote the extended variables in by . The ordering is less than or equal to can be extended by , if and only if either or . The extended lexicographic order of a non-ground DD-polynomial is denoted by . For DD-polynomials P and Q, we will write

P ≤ Q if . We write P ≈ Q if either .

Lemma 3[5] Any descending sequence is finite with .

III. PSEUDO-REMAINDERS OF DD-POLYNOMIALS

Let , and is a DD-polynomial in . We define the class of to be the smallest

c = cls(P) such that . We set if and . Let the leader of a DD-polynomial P be denoted by . For a DD-polynomial P with

P = y_{c,d,s}^{i} + P_{t-1}y_{c,d,s}^{t-1} + \cdots + P_{0},

where

We call the initial of P. And is called the leading degree of P.

Applying and to we have


is called the separant of P. If P is a DD-polynomial with lower leading variable than

Then we say that Q is reduced w.r.t. P and if only if:

(1) does not occur in Q for k and d in the same orthant, k > 0;

(2) if and d in the same orthant.

If , then is the only DD-polynomial which is reduced w.r.t. P. In fact, we define a partial ordering ≤ on by

\[
\theta' \leq \theta \iff \theta' \preceq \theta, \text{ and } 0 \leq \alpha \leq \alpha' \text{ or } 0 \preceq \alpha \preceq \alpha'.
\]

For ≤, we define

The partial ordering ≤ on can be extended on extended variables by \( v' = (\theta y')^d \leq (\theta' y')^d = (\alpha')^d \), if and only if \( 0 \leq \theta' \) and either \( d \leq e \) or \( \theta' \theta \) is not a pure difference operator.

Let P, Q ∈ K be two DD-polynomials with P ≠ 0. Then the algorithm returns the pseudo-remainder of Q w.r.t. P. It is easily checked that returns it with P. Otherwise, the algorithm wouldn’t terminate.

Algorithm 1-rrrem(\( R, Q \))

Input: Two DD-polynomials P and Q with P ≠ 0.

Output: The pseudo remainder of Q w.r.t. P.

If P ∈ K, then return 0.

Set R = Q.

While \( \exists \omega' \in V_{R} \), \( v_{P} \leq \omega' \) do

Choose the highest \( \omega' \) under ≤.

Set R = \( \text{aprem}(R, (\omega / v_{P})) \).

Return R

We denote \( \text{aprem}(R, Q) \) 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

A is a subset in K[Y]\K. If for each P ∈ A, P is reduced w.r.t. each polynomial in A\{P\}, then A is called a auto-reduced set. An auto-reduced set is \( \{ A_{1}, \cdots, A_{r} \} \)
with \( v_{A_1} < \cdots < v_{A_r} \) is called an ascending chain or simply a chain.

Let \( y_{1,\delta} \) to be the leading variable of a polynomial in \( \mathcal{A} \), we define its DD-index to be \( (d, \delta) \).

Let \( \mathcal{A} \) be a chain. We denote \( IND \) 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 \( IND = \{(a_1, b_1), \cdots, (a_n, b_n)\} \) such that \( a_1 \leq a_2 \leq \cdots \leq a_n \). Then we have

1. \( a_i = a_k = \cdots = a_n \), and \( b_1 \geq b_2 \geq \cdots \geq b_l \).
2. \( b_i = b_{i+1}, \) then \( d(a_i, b_i) < d(a_{i+1}, b_{i+1}) \), where \( d(a_i, b_i) \) is the leading degree of the polynomial with index \( (a_i, b_i) \).

**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 \( \delta \) in the leader of \( A_i \), \( \mathcal{A} = \mathcal{A}_\delta \cup \mathcal{A}_\sigma \). For \( \forall \mathbf{P} \in \mathcal{A}_\delta \), we have \( ord_{\delta} (P, v_P) \geq 0 \). \( \mathcal{A}_\delta \) is a chain in non-reflexive DD-polynomial case, where all the term \( y_{c,d} \) 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.

\( IND = \{(a_{p_1}, b_{p_1}), \cdots, (a_{p_n}, b_{p_n}), (a_{n_1}, b_{n_1}), \cdots, (a_{n_t}, b_{n_t})\} \), where \( 0 \leq a_{p_1} \leq \cdots \leq a_{n_1} \geq \cdots \geq a_{n_t} \). Then we have

1. \( 0 < a_{p_1} < \cdots < a_{p_n} \), and \( b_{p_1} \geq \cdots \geq b_{p_n} \).
2. If \( b_{p_j} = b_{p_{j+1}} \), then \( d(a_{p_j}, b_{p_j}) > d(a_{p_{j+1}}, b_{p_{j+1}}) \).
3. If \( b_{p_j} = b_{p_{j+1}} \), 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 \( \leq_1 \). The following set forms a chain.

\[
\mathcal{A} = \{A_1, A_2, A_3, A_4\} \\
A_1 = y_{1,1}^2 \\
A_2 = y_{1,3} + y_{1,2} \\
A_3 = y_{1,2} + y_{1,1} \\
A_4 = y_{1,4} + y_{1,3} \\
\]

From the DD-indices for \( \mathcal{A} \) shows in Figure 1, we can easy verify proposition 7.
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 $\theta P$ 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 $\mathbb{M}_\mathcal{A} = \{y_{c,d,s} | A \in \mathcal{A}, y_d = y_{c,d,s}, s \geq s', d$ and $\text{ord}_\mathcal{A}$ are in the same orthant $\}$. So $\mathbb{M}_\mathcal{A}$ is the set of all possible lifted variables by the leader in $\mathcal{A}$. For a DD-polynomial set $\mathbb{P}$, let $d_{P_1}$ be the largest $d$ such that $y_{c,d,s}$ occurs in $\mathbb{P}$, $d_{P_2}$ be the smallest $d$ such that $y_{c,d,s}$ occurs in $\mathbb{P}$, and $s_P$ be the largest $s$ such that $y_{c,d,s}$ occurs in $\mathbb{P}$. And

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

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

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

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

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

$$\mathcal{A}_P = \{A_1, \sigma\partial^2 A_1, \sigma\partial A_1, A_1, \partial^2 A_1, \partial A_1, A_2, \partial^2 A_2, \partial A_2, A_3, \partial^2 A_3, \partial A_3, A_4, \partial^2 A_4, \partial A_4, A_5\}$$

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

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

Let $\mathbb{P} \subseteq \mathbb{K}\{Y\}$ be a finite system of DD-polynomials and let $\mathbb{K}$ be a DD-superfield of $\mathbb{K}$. A zero of $\mathbb{P}$ in $\mathbb{K}$ is a tuple $\bar{y} = (y_1, \ldots, y_n) \in \mathbb{K}^n$ with $P(y_1, \ldots, y_n) = 0$ for all $P$ in $\mathbb{P}$. We use $\text{Zero}(\mathbb{P})$ to denote the set of all zeros of $\mathbb{P}$. Let $D$ be a polynomial. We use $\text{Zero}(\mathbb{P}/D)$ 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, $\mathcal{A} = \{A_1, \ldots, A_m\}$ is a Wu characteristic set of $\mathbb{P}$. $I_1 = I_A, S_1 = S_A$, and $H = \prod_{i=1}^{m} I_i S_i$. Then

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

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 $\mathbb{K}\{y_1, \ldots, y_n\}$. Then the algorithm $\text{ZDT}$ computes sequence of coherent Wu characteristic sets $\mathcal{A}_1, \ldots, \mathcal{A}_k$, such that

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

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

**Algorithm 3 – ZDT**

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

**Output:** $W = \{A_{11}, \ldots, A_{kk}\}$, such that $A_{ii}$ is a coherent chain and

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

Let $\mathbb{S} := \text{CS}(\mathbb{P})$, $\mathbb{B} := B_1, \ldots, B_p$. If $\mathbb{S} = 1$ then return $\{\}$. Else

Let $\mathbb{R} := \{r\text{prem}(f, \mathbb{S}) \neq 0 \mid f \in (\mathbb{P} \setminus \mathbb{S}) \cup \Delta(\mathbb{S})\}$. If $\mathbb{R} = \emptyset$ then $W = \{\mathbb{S}\} \cup \text{ZDT}(\mathbb{P} \cup \mathbb{S} \cup \{I_1\}) \cup \text{ZDT}(\mathbb{P} \cup \mathbb{S} \cup \{S_1\})$.

Else $W' := \text{ZDT}(\mathbb{P} \cup \mathbb{R})$.

/* $\text{CS}(\mathbb{P})$ returns the characteristic set of $\mathbb{P}$. It is easy to find $\text{CS}(\mathbb{P})$ since $\mathbb{P}$ is a finite set.**

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

**Example 17.** Let $A_1 = y_{1,2,1} + y_{1,0,0}$, $A_2 = y_{2,0,2}$, $A_3 = y_{2,1,1} + y_{1,1,0}$, $\mathbb{P} = \{A_1, A_2, A_3\}$. The generalized term order is $\leq_1$. The difference operator $\delta$ satisfies $\delta(f(x)) = f(x + 1)$ for any $f \in \mathbb{K}$. We have $\partial \delta = \partial \partial = \partial \delta$. First we have $\mathbb{B} = \text{CS}(\mathbb{P}) = \{A_1, A_2, A_3\}$, $\delta(\mathbb{B}) = \Delta(\mathbb{A}_2, A_3) = \text{aprem}(\partial \delta A_3, A_3) = y_{1,1,2}$, then $\text{rprem}(A_4, \mathbb{B}) = -y_{0,0,0}$. Let $A_5 = -y_{0,0,0}$, $\mathbb{P} = \mathbb{P} \cup \{A_5\}$, then we have $W = \text{ZDT}(\mathbb{P}_2)$.

We have $\mathbb{B}_1 = \text{CS}(\mathbb{P}_2) = \{A_2, A_3\}$. Then $\mathbb{B}_1 = \emptyset$, $A_4 = S_A = 2y_{1,2,1} \mathbb{P}_2 = \emptyset$, $A_4 = S_A = 2y_{1,2,1}$. Let $\mathbb{P}_3 = \mathbb{P}_2 \cup \{A_4\}$. We have $W = \{\mathbb{B}_2\} \cup \text{ZDT}(\mathbb{P}_3)$.

And similarly, $\text{ZDT}(\mathbb{P}_3)$ returns $\{A_5, A_7, A_4, A_2, A_4\}$, where $A_7 = 2y_{1,1,0}$.

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

**Acknowledgment**

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

**References**


