MM Research Preprints, 57–83
KLMM, AMSS, Academia Sinica
Vol. 25, December 2006

Characteristic Set Method for Differential-Difference Polynomial Systems

Xiao-Shan Gao[1], Joris van der Hoeven[2], Chunming Yuan[1], and Guilin Zhang[1]

Abstract. In this paper, we present a characteristic set method for mixed difference and differential polynomial systems. We introduce the concepts of coherent, regular, proper irreducible, and strong irreducible ascending chains and study their properties. We give an algorithm which can be used to decompose the zero set for a finitely generated difference and differential polynomial set into the union of the zero sets of regular ascending chains.

Keywords. Characteristic set, difference and differential polynomial, coherent ascending chain, regular ascending chain, irreducible ascending chain, zero decomposition algorithm.

1. Introduction

The characteristic set method is a tool for studying systems of polynomial or algebraic differential equations [9, 11]. Modern approaches to the characteristic set method, which are related to this paper, could be found in [1, 2, 3, 8, 17, 18]. The idea of the method is to priviledge systems which have been put in a special "triangular form", also called ascending chains. The zero-set of any finitely generated polynomial or differentially algebraic system of equations may be decomposed into the union of the zero-sets of ascending chains. With this method, solving an equation system can be reduced to solving univariate equations. We can also use the method to determine the dimension, the degree, and the order for a finitely generated polynomial or differential polynomial system, to solve the radical ideal membership problem, and to prove theorems from elementary and differential geometries.

The notion of characteristic set for difference polynomial systems was proposed by Ritt and Raudenbush [12, 13]. The general theory of difference algebra was established by Cohn [4]. Due to the major difference between the difference case and the differential case, algorithms and properties for difference ascending chains were studied only very recently [6, 7].

A natural problem is to consider the mixed difference and differential polynomial (DD-polynomial) systems. In [15], it was outlined how to generalize the characteristic set method to DD-polynomial systems. However, the author overlooked an additional difficulty in the proof of Rosenfeld's Lemma. Although all theoretical properties of differential algebra (dimension polynomials, finite generation of ideals, etc.; see also [10]) do generalize to the DD-setting, the algorithmic counterparts have to be redeveloped.

In this paper, we will present a characteristic set method for ordinary mixed DD-polynomial systems. The following results are established in this paper.

[1)]KLMM, Institute of Systems Science, AMSS, Academia Sinica, Beijing 100080, China.
[2)]Dpartement de Mathmatiques, Universit Paris-Sud 91405 Orsay Cedex, France.

1. Based on the concept of characteristic sets, we prove that DD-polynomial systems are Noetherian in the sense that the solutions for any set of DD-polynomials are the same as a finite set of DD-polynomials. This result is different from that in [10], because our assumption on the difference-differential structure is more general.

2. We introduce the concepts of coherent and regular ascending chains and prove that an ascending chain is coherent and regular if and only if it is the characteristic set for its saturation ideal (see Section 4 for details).

3. We define proper irreducible chains and prove that a proper irreducible chain is regular. This gives a constructive criterion for a chain to be regular. We further introduce the concept of strong irreducible chains and prove that an ideal is prime and reflexive if and only if its characteristic set is strong irreducible and coherent.

4. Based on the above results, we propose an algorithm which can be used to decompose the zero set for a finitely generated DD-polynomial set into the union of zero sets of proper irreducible chains.

The rest of the paper is organized as follows. In Section 2, we introduce notations. In Section 3, we prove the Noetherian property for DD-polynomial systems. In Section 4, we prove the properties for regular chains. In Section 5, we prove the properties for proper and strong irreducible chains. In Section 6, we give the zero decomposition algorithm.

2. DD-ring and DD-polynomials

2.1. DD-Polynomials

Let $\mathbb{K}$ be a computable field containing the field $\mathbb{Q}(x)$ of rational functions in an indeterminant x. A *differential operator* ∂ defined on $\mathbb{K}$ is a map $\partial : \mathbb{K} \to \mathbb{K}$ satisfying

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

for any $f, g \in \mathbb{K}$. A *difference operator* δ defined on $\mathbb{K}$ is a map $\delta : \mathbb{K} \to \mathbb{K}$ satisfying

$$\delta(f+g) = \delta(f) + \delta(g)$$
$$\delta(fg) = \delta(f)\delta(g)$$
$$\delta(f) = 0 \Longleftrightarrow f = 0$$

for any $f, g \in \mathbb{K}$. $\delta(f)$ is also called the *transform* of f. If all elements of $\mathbb{K}$ are functions in x, then the ordinary differentiation w.r.t. x is a differential operator. The shift operator $\delta(x) = x + 1$ and the q-difference operator $\delta(x) = qx$ are examples of difference operators.

A key fact to deal with the hybrid differential-difference case is to make an assumption on how both the differential and the difference operator interact. In this paper, we always assume that indeterminates should be considered as functions in x. This amounts to the requirement

$$\partial\delta(y) = h \cdot \delta\partial(y) \tag{1}$$

for some non-zero element $h \in \mathbb{K}$. It is easy to check that for a positive integer s, we have

$$\partial\delta^s(y) = \prod_{i=0}^{s-1} \delta^i(h) \cdot \delta^s\partial(y). \tag{2}$$

A product of the form $\prod_{i=0}^{k} \delta^i(h)^{n_i}$ is called an *h-product*.

When $h = 1$, (1) implies that the two operators are commutative, which is the case assumed in [10]. Also, (1) models most commonly used difference operators, such as the shift operator $\delta(x) = x + 1$ and the q-difference operator $\delta(x) = qx$, then (1) is valid. Intuitively, if we treat the difference operator as the right-composition with a non-trivial function. Indeed, if

$$\delta(f(x)) = f(\phi(x))$$

for any function $f(x)$ and a fixed function $\phi(x)$, then

$$\partial\delta(f(x)) = \partial(f(\phi(x))) = \frac{\partial\phi(x)}{\partial x}\,\delta\left(\frac{\partial f(x)}{\partial x}\right) = \frac{\partial\phi(x)}{\partial x}\delta\partial(f(x)),$$

whence (1) is satisfied for $h = \partial\phi(x)/\partial x$.

We denote $\Omega_0 = \{1\}, \Omega_1 = \{\delta, \partial\}$. For each $r \in \mathbb{N}$, we define $\Omega_{r+1} = \Omega_r \cup \delta\Omega_r \cup \partial\Omega_r$ inductively. These sets are subsets of Ω, with $\Omega = \bigcup_{r\in\mathbb{N}} \Omega_r$. An element of Ω is called a *word*. It is clear that

$$\Omega = \{\delta^{n_0}\partial^{m_0} \cdots \delta^{n_t}\partial^{m_t}\}$$

where n_i and m_i are non-negative integers and where we understand that $\delta^0 = \partial^0 = Id_{\mathbb{K}}$. Given $\omega \in \Omega$, we define its *total order* to be the smallest $r = \mathrm{ord}(\omega)$ with $\omega \in \Omega_r$. Let

$$\begin{aligned}\Theta &= \{\delta^\alpha\partial^\beta | \alpha, \beta \in \mathbb{N}\},\\ \Theta_{<[i,j]} &= \{\delta^k\partial^l | k \le i, l \le j, k + l < i + j\}.\end{aligned}$$

Note that Θ is a proper subset of Ω. A *shuffle* of a word with letters in $\{\delta, \partial\}$ is obtained by repeated transposition of these letters.

Lemma 2.1 *If $\omega = \delta^{n_1}\partial^{m_1} \cdots \delta^{n_t}\partial^{m_t}$ is a shuffle of $\delta^n\partial^m$, then $n = \sum_{i=1}^t n_i$, $m = \sum_{i=1}^t m_i$ and $\omega = g_\omega \cdot \delta^n\partial^m + P_\omega$, where g_ω is an h-product and P_ω is in $\mathbb{K}[\Theta_{<[n,m]}]$.*

Proof: We prove the lemma by induction on t. For $t = 1$, the result obviously holds. Assume that we proved the lemma for $t = i$. Then for $t = i + 1$,

$$\omega = \delta^{n_1}\partial^{m_1} \cdots \delta^{n_{i+1}}\partial^{m_{i+1}} = \delta^{n_1}\partial^{m_1}\left(g\delta^{n-n_1}\partial^{m-m_1} + \sum Q_jA_j\right),$$

where g is an h-product and $Q_j \in \mathbb{K}, A_j \in \Theta_{<[n-n_1,m-m_1]}$. Since $\delta^{n_1}\partial^{m_1}Q_jA_j \in \Theta_{<[n,m]}$ for any $A_j \in \Theta_{<[n-n_1,m-m_1]}$, we obtain

$$\delta^{n_1}\partial^{m_1}\left(g\delta^{n-n_1}\partial^{m-m_1} + \sum Q_jA_j\right) = \delta^{n_1}(g)\delta^{n_1}\partial^{m_1}\delta^{n-n_1}\partial^{m-m_1} + \sum Q'_kB_k,$$

where $Q'_k \in \mathbb{K}, B_k \in \Theta_{<[n,m]}$. By equation (2), we have

$$\partial^{m_1}\delta^{n-n_1} = g' \cdot \delta^{n-n_1}\partial^{m_1} + \sum Q_s C_s,$$

where g' is an h-product and $Q_s \in \mathbb{K}, C_s \in \Theta_{<[n-n_1,m_1]}$. We conclude that

$$\delta^{n_1}\partial^{m_1}\cdots\delta^{n_{i+1}}\partial^{m_{i+1}} = g'' \cdot \delta^n\partial^m + P,$$

where g'' is an h-product and P is in $\mathbb{K}[\Theta_{<[n,m]}]$. $\square$

Let $\mathbb{Y} = \{y_1, \ldots, y_n\}$ be a finite number of indeterminates, considered as functions of x. We denote

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

For convenience, we also denote

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

The set

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

is called the *DD-ring* of *DD-polynomials* over $\mathbb{K}$ in $\mathbb{Y}$. DD-polynomials in $\mathbb{K}\{\mathbb{Y}\}$ have a canonical representation as polynomials in $\mathbb{K}[\Theta\mathbb{Y}]$:

Proposition 2.2 $\mathbb{K}\{\mathbb{Y}\} = \mathbb{K}[\Theta\mathbb{Y}]$.

Proof: Any element in $\mathbb{K}\{\mathbb{Y}\}$ is a $\mathbb{K}$-linear combination of products of elements in $\Omega\mathbb{Y}$, so it suffices to prove that $\omega y_k \in \Theta\mathbb{Y}$ for $\omega y_k \subseteq \Omega\mathbb{Y}$. But this directly follows from Lemma 2.1. $\square$

Remark 2.3 When using a DD-polynomial P to form a triangular set $\{\theta P | \theta \in \Theta_{<[n,m]}\} \cup \{\delta^n\partial^m P\}$, Lemma 2.1 will imply that the saturation ideals of ωP and $\delta^n\partial^m P$ coincide.

A *DD-ideal*, or simply an ideal, is a subset I of $\mathbb{R}$, which is an algebraic ideal in $\mathbb{R}$ and is closed under ∂ and δ. An ideal I is called *reflexive* if $\delta P \in I$ implies $P \in I$, for all $P \in \mathbb{R}$. Let $\mathbb{P}$ be a set of elements of $\mathbb{R}$. The ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. Obviously, $[\mathbb{P}]$ is the set of all linear combinations of the DD-polynomials in $\mathbb{P}$ and their differentiations and transforms. An ideal I is called *perfect* if the presence in I of a product of powers of transforms of a DD-polynomial P implies $P \in I$. The perfect ideal generated by $\mathbb{P}$ is denoted as $\{\mathbb{P}\}$. A perfect ideal is always reflexive. An ideal I is called a *prime ideal* if for DD-polynomials P and Q, $PQ \in I$ implies $P \in I$ or $Q \in I$.

For a set of DD-polynomials $\mathbb{P}$, we write $(\mathbb{P})$ for the ordinary or algebraic ideal generated by $\mathbb{P}$, and $[\mathbb{P}]_\partial$ for the differential ideal generated by $\mathbb{P}$.

2.2. Admissible ordings

Consider a total ordering $\leq$ on $\Theta\mathbb{Y}$. Given $\mathbb{P} \subseteq \mathbb{K}[\Theta Y]$, we denote by $V_{\mathbb{P}} \subseteq \Theta\mathbb{Y}$ the set of elements of $\Theta\mathbb{Y}$ occurring in $\mathbb{P}$. For a DD-polynomial P, we let $V_P = V_{\{P\}}$. If $V_P \neq \emptyset$, then V_P has a maximal element for $\leq$, which is denoted by v_P or $v(P)$. We call it the *leader* of P.

The ordering $\leq$ is said to be *admissible* if

$$\begin{array}{lll} A1 & : & v(\theta y) < v(\delta\theta y), \quad \text{for any } \theta y \in \Theta Y; \\ & & v(\theta y) < v(\partial\theta y), \quad \text{for any } \theta y \in \Theta Y; \\ A2 & : & v(\delta\theta y) \leq v(\delta\theta' y'), \quad \text{for any } \theta y \leq \theta' y' \text{ in } \Theta Y; \\ & & v(\partial\theta y) \leq v(\partial\theta' y'), \quad \text{for any } \theta y \leq \theta' y' \text{ in } \Theta Y. \end{array}$$

Admissible orderings exist: one example is the ordering $\leq_l$ defined by:

$$\delta^{d_1}\partial^{s_1} y_{c_1} \leq_l \delta^{d_2}\partial^{s_2} y_{c_2} \Longleftrightarrow (c_1, d_1, s_1) \leq_{lex} (c_2, d_2, s_2),$$

where $\leq_{lex}$ stands for the pure lexicographical ordering. Another popular ordering is the *total order based* ordering:

$$\delta_1^d \partial_1^s y_i <_o \delta_2^d \partial_2^s y_j \Longleftrightarrow (d_1 + s_1, d_1, s_1, i) <_{lex} (d_2 + s_2, d_2, s_2, j).$$

In this paper, we will always assume that $\leq$ is admissible. We will also assume that $y_1 < \cdots < y_n$, which can always be made to hold after a permutation of indexes.

An *extended variable* is an element of $\Theta\mathbb{Y}$ raised to some strictly positive power. The set of such variables will be denoted by $(\Theta\mathbb{Y})^*$, and we use letters with star exponents v^* to denote extended variables. We extend the admissible ordering $\leq$ on variables to extended variables by $v^d \leq (v')^e$, if and only if either $v < v'$, or $v = v'$ and $d \leq e$. The *extended leader* of a non ground DD-polynomial P is denoted by $v_P^* = v_P^{\deg(P, v_P)}$. The admissible ordering $\leq$ can be extended to DD-polynomials. For DD-polynomials P and Q, we will write $P \leq Q$ if $v_P^* \leq v_Q^*$. If $v_P^* = v_Q^*$, then we will write $P \sim Q$.

Lemma 2.4 *Let $P_i \in \mathbb{K}[\Theta\mathbb{Y}]$. Then any descending sequence $P_1 > P_2 > P_3 > \cdots$ is finite.*

Proof: The sequence $(P_i)_{i\in\mathbb{N}}$ induces a sequence $(a_i, b_i, c_i, d_i)_{i\in\mathbb{N}}$ with $v^*(P_i) = (\delta^{b_i}\partial^{c_i} y_{a_i})^{d_i}$. Similarly, the ordering $\leq$ on $(\Theta\mathbb{Y})^*$ induces a total ordering $\leq'$ on $\{1, \ldots, n\} \times \mathbb{N}^3$, which extends the canonical partial product ordering. Now for any a_i, the sequence $(b_i, c_i, d_i)_{i\in\mathbb{N}}$ is strictly decreasing for $\leq'$, whence its finiteness, by Dickson's Lemma. □

2.3. Pseudo-Remainder

We consider the DD-ring $\mathbb{K}[\Theta\mathbb{Y}]$, where $\mathbb{Y} = \{y_1, \ldots, y_n\}$. Let $\mathbb{Y}_c = \{y_1, \ldots, y_c\}$. For a DD-polynomial $P \in \mathbb{K}[\Theta\mathbb{Y}]$, we define the *class* of P to be the smallest $c = \text{cls}(P)$ such that $P \in \mathbb{K}[\Theta\mathbb{Y}_c]$. If $P \in \mathbb{K}$, then we set $\text{cls}(P) = 0$. If the leader of P is $\theta y_c = y_{c,i,j}$, then we define $\text{ord}(P) = i + j$, $\text{ord}_\delta(P, y_c) = i, \text{ord}_\partial(P, y_c) = j$.

If the leader of $P \in \mathbb{R} \setminus \mathbb{K}$ is $y_{c,d,s}$, then P has the following canonical representation:

$$P = P_t y_{c,d,s}^t + P_{t-1} y_{c,d,s}^{t-1} + \cdots + P_0. \tag{3}$$

$I_P = P_t$ is called the *initial* of P. $\text{ldeg}(P) = t$ is called the *leading degree* of P. Applying ∂ and δ to P, we have

Algorithm 1 — rprem(Q, P)

Input: DD-polynomials $P, Q \in \mathbb{R}$ 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 $\exists \omega^* \in V_R^*, v_P^* \preceq \omega^*$ do
  Choose the highest ω^* under $\leq$.
  Set $R := \text{aprem}(R, (\omega/v_P)P)$. /*/
Return R

/*/ aprem(P, Q) stands for the algebraic pseudo-remainder of P w.r.t. Q in variable v_Q.

Lemma 2.5 *Let P be of form (3). Then*

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

where

$$S_P = \prod_{i=0}^{d-1} \delta^i(h) \frac{\partial P}{\partial y_{c,d,s}}$$

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

Proof: The first equation is obvious. The second one is a consequence of (2). □

If the leader of $P \in \mathbb{R} \setminus \mathbb{K}$ is $y_{c,d,s}$, 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 $k \geq 0, l > 0$ and (2) $\deg(Q, y_{c,d+k,s}) < \deg(P, y_{c,d,s})$ for $k \geq 0$. If $P \in \mathbb{K} \setminus \{0\}$, then 0 is the only DD-polynomial which is reduced w.r.t. P.

We define a partial ordering $\preceq$ on Θ by

$$\theta = \delta^\alpha \partial^\beta \preceq \delta^{\alpha'} \partial^{\beta'} = \theta' \Longleftrightarrow \alpha \leq \alpha' \wedge \beta \leq \beta'.$$

If $\theta \preceq \theta'$, then we define

$$\theta'/\theta = \delta^{\alpha'-\alpha} \partial^{\beta'-\beta}$$

and notice that $(\theta'/\theta)\theta$ is a shuffle of θ'.

We define a *partial ordering* $\preceq$ on extended variables by $v^* = (\theta y_i)^d \preceq (\theta' y_i)^e = (v')^*$, if and only if $\theta \preceq \theta'$ and either $d \leq e$, or θ'/θ is not a pure difference operator. We remark that $\preceq$ is still a well-quasi-ordering.

Consider DD-polynomials $P, Q \in \mathbb{R}$ with $P \neq 0$. Then the algorithm **rprem** computes the *pseudo-remainder of Q w.r.t. P*. It is easily checked that rprem(Q, P) is reduced w.r.t. P.

Lemma 2.6 *Define*

$$\mathbf{H}_P = \{I_P^{a_0} \cdots \delta^k I_P^{a_k} S_P^{b_0} \cdots \delta^l S_P^{b_l} | a_0, \ldots, a_k, b_0, \ldots, b_l \in \mathbb{N}\}$$

and let $R = \mathrm{rprem}(Q, P)$*. Then there exists a* $J \in \mathbf{H}_P$ *such that* $v_J < v_Q$ *and*

$$JQ = R \mod [P],$$

where $[P]$ *denotes the ideal generated by* P*.*

Proof: For every step of the loop of the above procedure, the order of the initial of $v((\omega/v_P)P)$ is less than the order of $v(Q)$, so this is a direct consequence of the above procedure and Lemma 2.5. □

3. Characteristic Set of DD-Polynomial Ideals

3.1. Auto-reduced Sets

A subset $\mathcal{A} \subseteq \mathbb{K}\{\mathbb{Y}\} \setminus \mathbb{K}$ is said to be *auto-reduced*, if each $P \in \mathcal{A}$ is reduced w.r.t. each DD-polynomial in $\mathcal{A} \setminus \{P\}$. An auto-reduced set $\mathcal{A} = \{A_1, \ldots, A_r\}$ with $v_{A_1} < \cdots < v_{A_r}$ is called an *ascending chain* or simply a *chain*.

Lemma 3.1 *Any auto-reduced set is finite.*

Proof: Assume the contrary and consider an infinite auto-reduced set $\{P_1, P_2, \ldots\}$. The sequence $P_1, P_2, \ldots$ induces a sequence $(a_i, b_i, c_i, d_i)_{i\in\mathbb{N}}$ with $v^*(P_i) = (\delta^{b_i}\partial^{c_i} y_{a_i})^{d_i}$ and modulo the extraction of a subsequence, we may assume without loss of generality that $a_i = a_j$ for all i, j. If P_i is reduced w.r.t. P_j, then we cannot have $(b_i, c_i, d_i) \succeq (b_j, c_j, d_j)$ for the partial product ordering on $\mathbb{N}^3$. It follows that $(b_1, c_1, d_1), (b_2, c_2, d_2), \ldots$ are pairwise distinct and incomparable for $\preceq$. This contradicts Dickson's Lemma. □

Let $\mathcal{A} = \{A_1, \ldots, A_p\}$ and $\mathcal{B} = \{B_1, \ldots, B_q\}$ be chains. We define a partial ordering $\leq$ on chains by setting $\mathcal{A} \leq \mathcal{B}$ if there exists a j with $A_i \sim B_i$ for $1 \leq i < j$ and either $A_j < B_j$ or $j = q + 1 \leq p$. The ordering $\leq$ is also called a *ranking*.

Lemma 3.2 *Any descending chain* $\mathcal{A}_1 > \mathcal{A}_2 > \mathcal{A}_3 > \ldots$ *is finite.*

Proof: Assume the contrary. The first elements of the chains $\mathcal{A}_1, \mathcal{A}_2, \ldots$ satisfy $\mathcal{A}_{1,1} \geq \mathcal{A}_{2,1} \geq \cdots$. By Lemma 2.4, there exists an index j_1 with $A_{i,1} \sim A_{j_1,1}$ for all $i \geq j_1$. Similarly, there exists an index $j_2 > j_1$ with $A_{i,2} \sim A_{j_2,2}$ for all $i \geq j_2$. By induction, we get a sequence $j_1 < j_2 < \ldots$ with $A_{i,k} \sim A_{j_k,j}$ for all k and $i \geq j_k$. But then $\{A_{j_1,1}, A_{j_2,2}, \ldots\}$ is an infinite auto-reduced set, which contradicts Lemma 3.1. □

Let $\mathbb{P}$ be a set of DD-polynomials and consider the set of chains of DD-polynomials in $\mathbb{P}$. Among all those chains, the above lemma implies that there exists at least one chain with lowest rank. Such a 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 3.3 *If* $\mathcal{A}$ *is a characteristic set of* $\mathbb{P}$ *and* $\mathcal{A}'$ *a characteristic set of* $\mathbb{P} \cup \{P\}$ *for a DD-polynomial* P*, then we have* $\mathcal{A} \geq \mathcal{A}'$*. Moreover, if* P *is reduced w.r.t.* $\mathcal{A}$*, then* $\mathcal{A} > \mathcal{A}'$*.*

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 $L = \mathbb{L}_{\mathcal{A}}$, $\mathbb{Q} = \mathcal{A} \cup \mathbb{P}$, $\mathbb{H} = \{y_{c,d_{\mathbb{Q}}^{(c)},s_{\mathbb{Q}}^{(c)}}, c = 1, \ldots, n\}$, $V = \mathbb{V}_{\mathbb{H}} \setminus L$, and $\mathcal{A}_{\mathbb{P}} = \mathcal{A}$.

S1. If there exist ω, η and c with $\omega y_c \in V$, $\eta y_c \in L$ and $\eta \preceq \omega$, then choose ω and c such that ωy_c is largest for $\leq$. If there are no such ω, η and c, then return $\mathcal{A}_{\mathbb{P}}$.

S2. If for all the $\theta y_c \in L$ satisfying $\theta \preceq \omega$, ω/θ is a difference operator, let η be the largest of those θ under $\leq$, go to **S4**.

S3. If there exists a $\theta y_c \in L$ such that ω/θ is not a difference operator, let η be the one with largest in ord_δ. Go to **S4**.

S4. Let $A_i \in \mathcal{A}$ such that $v_{A_i} = \eta y_c$. Let $Q = (\omega/\eta)A_i$, $\mathcal{A}_{\mathbb{P}} = \mathcal{A}_{\mathbb{P}} \cup \{Q\}$, $V = V \cup (\mathbb{V}_Q \setminus \mathbb{L}_{\mathcal{A}_{\mathbb{P}}})$. Delete ωy_c from V and goto **S1**. Since all the variables in $\mathbb{V}_Q \setminus \mathbb{L}_{\mathcal{A}_{\mathbb{P}}}$ are less than ωy_c, this process will terminate.

Proof: The first statement is obviously true, since the characteristic set of $\mathbb{P}$ is in $\mathbb{P} \cup \{P\}$. As to the second statement, assume $\mathcal{A} = A_1, \ldots, A_p$ and $P \in \mathbb{P}$, with $\mathrm{cls}(P) = m$, is reduced w.r.t. $\mathcal{A}$. If $m > \mathrm{cls}(A_p)$, then the chain $A_1, \ldots, A_p, P$ is of rank lower than $\mathcal{A}$. If $\mathrm{cls}(A_{k-1}) < m \leq \mathrm{cls}(A_k) \leq \mathrm{cls}(A_p)$, then the chain $A_1, \ldots, A_{k-1}, P$ is of rank lower than $\mathcal{A}$. Hence $\mathcal{A} > \mathcal{A}'$. □

Lemma 3.4 *A chain $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ if and only if $\mathbb{P}$ does not contain a nonzero DD-polynomial which is reduced w.r.t. $\mathcal{A}$.*

Proof: By Lemma 3.3, we just need to prove the sufficiency. Assume $\mathcal{B} = B_1, \ldots, B_s$ is the characteristic set of $\mathbb{P}$, while $\mathcal{A}$ is not. We have $\mathcal{B} < \mathcal{A}$. If there exists a $k \leq \min\{s, p\}$ with $B_k < A_k$, then B_k is reduced w.r.t. $\mathcal{A}$. Otherwise $s > p$ and B_{p+1} is reduced w.r.t. $\mathcal{A}$. Both of the cases constradict the hypothesis and show that $\mathcal{A}$ is the characteristic set of $\mathbb{P}$. □

3.2. Extension of chains and pseudo-remainder

Let $\mathcal{A}$ be a chain. A variable $y_{c,d,s}$ is called a *principal variable* of $\mathcal{A}$ if there exists an $A \in \mathcal{A}$ such that $v_A \preceq y_{c,d,s}$. 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 $\mathbb{M}_{\mathcal{A}} \cup \mathbb{P}_{\mathcal{A}} = \Theta\mathbb{Y}$,

For a DD-polynomial set $\mathbb{P}$ and $1 \leq c \leq n$, let $d_{\mathbb{P}}^{(c)}$ be the largest d such that $y_{c,d,s}$ occurs in $\mathbb{P}$, $s_{\mathbb{P}}^{(c)}$ the largest s such that $y_{c,d,s}$ occurs in $\mathbb{P}$, and

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

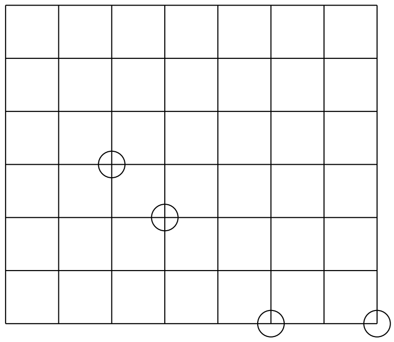

Fig. 1. The indices of chain $\mathcal{A}$ from (4)

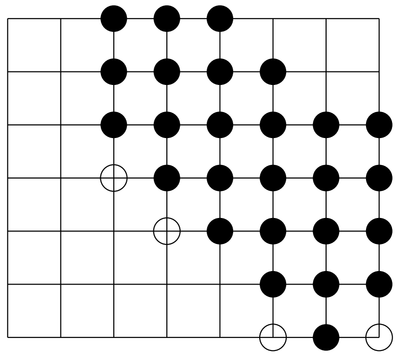

Fig. 2. The indices of chain $\mathcal{A}_P$

Given DD-polynomial set $\mathbb{P}$, the algorithm **Extension** shows how to compute the so called *extension of* $\mathcal{A}$ w.r.t. $\mathbb{P}$. This definition is motivated by the following result, which is clear from the construction algorithm.

Proposition 3.5 *For a chain $\mathcal{A}$ and a set of DD-polynomials $\mathbb{P}$, we have*

- *$\mathcal{A}_\mathbb{P}$ is an algebraic triangular set under the ordering $\leq$ when all $y_{c,n,m}$ are considered as independent variables.*
- *$\mathbb{L}_{\mathcal{A}_\mathbb{P}} = \mathbb{V}_{\mathcal{A}_\mathbb{P}}$.*
- *A DD-polynomial P is reduced w.r.t. $\mathcal{A}$ if and only if P is reduced w.r.t. $\mathcal{A}_P$ in the algebraic sense.*

Example 3.6 Consider the following chain for the ordering $\leq_l$ from Section 2.2.

$$\begin{array}{rcl} \mathcal{A} & = & \{A_1, A_2, A_3, A_4\} \\ A_1 & = & y_{1,2,3}^2 \\ A_2 & = & y_{1,3,2}^2 + y_{1,1,1} \\ A_3 & = & y_{1,5,0}^2 + y_{1,4,1} \\ A_4 & = & y_{1,7,0} + y_{1,4,0}. \end{array} \tag{4}$$

The DD-indices for the DD-polynomials in $\mathcal{A}$ are given in Figure 1. For $P = y_{1,7,4}^2 + y_{1,3,2}$, we have $d_{\mathbb{Q}}^{(1)} = 7$, $s_{\mathbb{Q}}^{(1)} = 4$, and

$$\begin{aligned} \mathcal{A}_P = \{ & A_1, \partial A_1, \partial^2 A_1, \partial^3 A_1, \\ & A_2, \partial A_2, \partial^2 A_2, \partial^3 A_2, \partial^4 A_2, \delta A_2, \delta\partial A_2, \delta\partial^2 A_2, \delta\partial^3 A_2, \delta\partial^4 A_2, \\ & A_3, \partial A_3, \partial^2 A_3, \partial^3 A_3, \partial^4 A_3, \partial^5 A_3, \delta A_3, \delta\partial A_3, \delta\partial^2 A_3, \delta\partial^3 A_3, \delta\partial^4 A_3, \\ & A_4, \partial A_4, \partial^2 A_4, \partial^3 A_4, \partial^4 A_4\}. \end{aligned}$$

Let $\omega y_1 = y_{1,5,4}$. Then for each of A_1, A_2, and A_3, its leader satisfies the condition in **S1**. The condition in **S2** is not satisfied. In **S3**, we choose the one with largest ord_δ, which is A_3.

As a consequence, we will add $\partial^4 A_3$ to $\mathcal{A}_{\mathbb{P}}$. Note that the DD-polynomial with the largest ord_δ will have the smallest ord_∂ for its leading variable.

Given $y_{i,d_j,s_j} \in \mathbb{L}_{\mathcal{A}}$, we define its *index* to be (d_j, s_j). The indices for the DD-polynomials in $\mathcal{A}_{\mathbb{P}}$ are given in Figure 2, where a solid dot represents the index of a newly added DD-polynomial. This figure is called the *index figure* of $\mathcal{A}_{\mathbb{P}}$.

Remark 3.7 For a chain $\mathcal{A}$ and a set of DD-polynomials $\mathbb{P}$, the DD-polynomial corresponding to the bottom index in each column in the index figure of $\mathcal{A}_{\mathbb{P}}$ is of form $\delta^d A$ for an $A \in \mathcal{A}$.

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

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

Let $\mathcal{A} = A_1, \ldots, A_p$ be a chain. We define

$$\begin{aligned} H_{\mathcal{A}} &= \{I_{A_1}^{i_1} S_{A_1}^{j_1} \cdots I_{A_p}^{i_p} S_{A_p}^{j_p} | i_1, j_1, \ldots, i_p, j_p \in \mathbb{N}\} \\ \mathbf{H}_{\mathcal{A}} &= \{H_1 \cdots H_p | H_1 \in \mathbf{H}_{A_1}, \ldots, H_p \in \mathbf{H}_{A_p}\} \end{aligned}$$

Lemma 3.8 *Let $R = \mathrm{rprem}(Q, \mathcal{A})$. Then R is reduced w.r.t. $\mathcal{A}$ and there exists a $J \in \mathbf{H}_{\mathcal{A}}$ such that $v_J < v_Q$ and*

$$\begin{aligned} JQ &\equiv R \mod [\mathcal{A}] \\ JQ &\equiv R \mod (\mathcal{A}_Q) \end{aligned}$$

Proof: This is a direct consequence of the procedure to compute $\mathcal{A}_Q$ and rprem. □

The *saturation ideal* of $\mathcal{A}$ is defined to be

$$\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbf{H}_{\mathcal{A}} = \{P \in \mathbb{K}[\Theta\mathbb{Y}] \mid \exists J \in \mathbf{H}_{\mathcal{A}} : JP \in [\mathcal{A}]\}.$$

Note that $\mathbf{H}_{\mathcal{A}}$ is closed under transforming and multiplication. Hence $\mathrm{sat}(\mathcal{A})$ is a DD-ideal. It is also clear that if $\mathrm{rprem}(P, \mathcal{A}) = 0$ then $P \in \mathrm{sat}(\mathcal{A})$. Conversely, $P \in \mathrm{sat}(\mathcal{A})$ generally does not imply $\mathrm{rprem}(P, \mathcal{A}) = 0$ and the condition for this to be valid will be given in Section 4.

3.3. Noetherian property of perfect ideals

As an application, we may prove that all perfect ideals in $\mathbb{K}[\Theta\mathbb{Y}]$ are finitely generated, or equivalently, the solutions for any set of DD-polynomials are the same as a finite set of DD-polynomials.

For a DD-polynomial set $\mathbb{P}$, let P be any element in $\mathbb{K}[\Theta\mathbb{Y}]$ with some product of positive powers of transforms of P in $\mathbb{P}$. The totality of such elements P will be denoted by $\mathbb{P}'$. Let $\mathbb{P}_1 = [\mathbb{P}]'$ and, continuing inductively, let $\mathbb{P}_n = [\mathbb{P}_{n-1}]'$ for every $n > 1$. We have $\mathbb{P}_0 \subseteq \mathbb{P}_1 \subseteq \mathbb{P}_2 \subseteq \cdots$ and $\bigcup_{k\in\mathbb{N}} \mathbb{P}_k = \{\mathbb{P}\}$.

Lemma 3.9 *Let $\mathbb{P}$ be any set of elements of $\mathbb{K}[\Theta\mathbb{Y}]$ and P and Q any two elements of $\mathbb{K}[\Theta\mathbb{Y}]$. If S is contained in $(\mathbb{P} \cup P)_n$ and T in $(\mathbb{P} \cup Q)_n, n \geq 1$, then ST is contained in $(\mathbb{P} \cup PQ)_{n+2}$.*

Proof: First, let $n = 1$, $S \in (\mathbb{P} \cup P)_1, T \in (\mathbb{P} \cup Q)_1$. There exists a product $\overline{S}$ of positive powers of transforms of S, and an $\overline{T}$ similarly related to T, which have expressions

$$\overline{S} = GA + \cdots + HB + k(\omega P) + \cdots + L(\theta P),$$
$$\overline{T} = G'A' + \cdots + H'B' + K'(\omega' Q) + \cdots + L'(\theta' Q),$$

where $A, \cdots, B, A', \cdots, B' \in \Theta\mathbb{P}, \omega, \cdots, \omega', \theta, \cdots, \theta' \in \Theta$ and the coefficients $G, G' \cdots, L, L' \in \mathbb{K}[\Theta\mathbb{Y}]$. Thus $\overline{ST}$ has an expression in which some terms are in $[\mathbb{P}]$ and the others are of the type $F \cdot \eta_1 P \cdot \eta_2 Q$ for some $\eta_1, \eta_2 \in \Theta$. Denote $\eta_1 = \delta^{r_1}\partial^{r_2}, \eta_2 = \delta^{s_1}\partial^{s_2}$, then by [11], Page 9, we have $\partial^{r_2} P \cdot \partial^{s_2} Q \in [PQ]'$, so we have $\delta^{r_1}\partial^{r_2} P \cdot \delta^{s_1}\partial^{s_2} Q \in [PQ]_2$. So we have $\overline{ST}$ is in $[(\mathbb{P} \cup PQ)_2]$. Some of product of powers of transforms of ST is a multiple of $\overline{ST}$. Thus ST is in $(\mathbb{P} \cup PQ)_3$.

Now, let $n = 2$. Let $\overline{S}$, described as above, be in $[(\mathbb{P} \cup P)_1]$. Then, $\overline{S}$ is a linear combination of elements of $[(\mathbb{P} \cup P)_1]$. We use an $\overline{T}$, described as above, which is linear in elements of $[(\mathbb{P} \cup Q)_1]$. Then $\overline{ST}$ has an expression in which each term is of type $F \cdot \eta A \cdot \omega B$, where $A, B \in (\mathbb{P} \cup Q)_1, \eta, \omega \in \Theta$. Now $\eta A \cdot \omega B$, by the case of $n = 1$, is in $(\mathbb{P} \cup PQ)_3$. Hence $\overline{ST}$ is in $[(\mathbb{P} \cup PQ)_3]$. This puts ST in $(\mathbb{P} \cup PQ)_4$.

The proof continues by induction. □

Lemma 3.10 *Let $\mathbb{P}$ be any set of elements of $\mathbb{K}[\Theta\mathbb{Y}]$ and P and Q any two elements of $\mathbb{K}[\mathbb{Y}]$. Then $\{\mathbb{P} \cup PQ\} = \{\mathbb{P} \cup P\} \cap \{\mathbb{P} \cup Q\}$.*

Proof: We need only to show that, S being any element in the intersection, S is contained in $\{\mathbb{P} \cup PQ\}$. Let n be such that S is contained in $(\mathbb{P} \cup P)_n$ and in $(\mathbb{P} \cup Q)_n$. Then by Lemma 3.9, S^2 is in $(\mathbb{P} \cup PQ)_{n+2}$. Thus S is also in $(\mathbb{P} \cup PQ)_{n+2}$. □

Lemma 3.11 *Let $\mathbb{P}, \mathbb{Q}$ be two sets of elements of $\mathbb{K}[\Theta\mathbb{Y}]$. Then $\{\mathbb{P}\} \cap \{\mathbb{Q}\} = \{\mathbb{P}\mathbb{Q}\}$.*

Proof: Similar to the proof of Lemma 3.9, we have $\mathbb{P}_n \cap \mathbb{Q}_n \subseteq (\mathbb{P}\mathbb{Q})_{n+2}$, the conclusion follows. □

Lemma 3.12 *Let $\mathbb{P}$ be a subset of $\mathbb{K}[\Theta\mathbb{Y}]$ and $P \in \{\mathbb{P}\}$. Then there exists a finite subset Σ of $\mathbb{P}$, such that $P \in \{\Sigma\}$.*

Proof: Since $\{\mathbb{P}\} = \bigcup_{n \in \mathbb{N}} \mathbb{P}_n$, we have $P \in \mathbb{P}_n$ for some n. Let us prove the Lemma by induction on n. The case $n = 0$ is trivial. Assume that we have proved the Lemma up to $n - 1$. We have $\prod_i (\delta^{t_i} P)^{s_i} \in [\mathbb{P}_{n-1}]$, for some $t_i, s_i \in \mathbb{N}$. Hence $\prod_i (\delta^{t_i} P)^{s_i} \in [Q_1, \ldots, Q_q]$ for some $Q_1, \ldots, Q_q \in \mathbb{P}_{n-1}$. For each $1 \leq j \leq q$, there exists a finite subset Σ_j of $\mathbb{P}$, such that $Q_j \in \{\Sigma_j\}$, by the induction hypothesis. Then we can taken $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_q$ and $P \in \{\Sigma\}$. □

Lemma 3.13 *If there exists a non finitely generated perfect DD-ideal, then the set of non finitely generated perfect DD-ideals admits a maximal element, and every such a maximal element is prime.*

Proof: The union of a totally ordered set of non finitely generated perfect DD-ideals is again a non finitely generated perfect DD-ideal. The existence of a maximal element follows therefore by Zorn's Lemma. Now let $\mathfrak{m}$ be any such maximal element. Clearly $\mathfrak{m} \neq \mathbb{K}$. Choose $P, Q \in \mathbb{K}[\Theta\mathbb{Y}] \setminus \mathbb{K}$. Then $\{\mathfrak{m}, P\}$ and $\{\mathfrak{m}, Q\}$ are finitely generated, say by $\mathbb{P}, \Sigma$ respectively. Thus by Lemma 3.10, $\{m, PQ\} = \{\mathbb{P}\} \cap \{\Sigma\}$. By Lemma 3.11, $PQ \notin \mathfrak{m}$, we have that $\mathfrak{m}$ is prime. □

Theorem 3.14 *The DD-ring* $\mathbb{K}[\Theta\mathbb{Y}]$ *is Noetherian in the sense that all perfect ideals in* $\mathbb{K}[\Theta\mathbb{Y}]$ *are finitely generated.*

Proof: First we fix some admissible ordering on $\Theta\mathbb{Y}$. Suppose that the conclusion of the theorem is false. By Lemma 3.13, there exists a maximal non finitely generated perfect DD-ideal $\mathfrak{m}$, which is prime. Let $\mathcal{C}$ be a characteristic set for $\mathfrak{m}$.

Let P be in $\mathfrak{m}$. We can write $J_P P = R \bmod [\mathcal{C}]$, where R is reduced w.r.t. $\mathcal{C}$, $J_P \in \mathbf{H}_{\mathcal{C}}$. By Lemma 3.4, $R = 0$. Hence $J_P P \in [\mathcal{C}]$, whence $H_{\mathcal{C}} P \in \{\mathcal{C}\}$. This proves that $H_{\mathcal{C}}\mathfrak{m} \subseteq \{\mathcal{C}\}$.

Since the initials and separants of $\mathcal{C}$ are reduced w.r.t. $\mathcal{C}$, they are not in $\mathfrak{m}$. Since $\mathfrak{m}$ is prime, we have $H_{\mathcal{C}} \notin \mathfrak{m}$. So the perfect DD-ideal $\{H_{\mathcal{C}}, \mathfrak{m}\}$ strictly contains $\mathfrak{m}$. Therefore, $\{H_{\mathcal{C}}, \mathfrak{m}\}$ is finitely generated by the maximality hypothesis. Applying Lemma 3.12, each generator is in a perfect DD-ideal generated by a finite subset of $\mathfrak{m} \cup \{H_{\mathcal{C}}\}$. Hence, we can write $\{H_{\mathcal{C}}, \mathfrak{m}\} = \{H_{\mathcal{C}}, \mathbb{P}\}$, for some $\mathbb{P} \subseteq \mathfrak{m}$ and $\mathbb{P}$ is a finite set. Finally, $\mathfrak{m}$ is finitely generated, since $\mathfrak{m} = \mathfrak{m} \cap \{H_{\mathcal{C}}, \mathfrak{m}\} = \mathfrak{m} \cap \{H_{\mathcal{C}}, \mathbb{P}\} = \{H_{\mathcal{C}}\mathfrak{m}, \mathbb{P}\} \subseteq \{\mathcal{C}, \mathbb{P}\}$. □

4. Coherent and regular chains

A key property for a chain $\mathcal{A}$ is that whether $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. In this section, we will give a necessary and sufficient condition for this to be true.

4.1. Coherent Chains

If we want to compute the pseudo-remainder of $P = y_{1,3,3}^3$ w.r.t. $\mathcal{A}$ in (4), we have two choices: we could either select A_1 and use δA_1 to eliminate $y_{1,3,3}$ from P, or select A_2 and use ∂A_2 to eliminate $y_{1,3,3}$ from P. To ensure that we obtain the same remainder with these two choices, we need to make sure that δA_3 and ∂A_1 satisfy some consistence conditions. This observation leads to the following definition.

Let $\mathcal{A}$ be a chain and $A_1, A_2 \in \mathcal{A}$. If $\mathrm{cls}(A_1) \neq \mathrm{cls}(A_2)$, define $\Delta(A_1, A_2) = 0$. If $\mathrm{cls}(A_1) = \mathrm{cls}(A_2) = c$, let $v_{A_1} = \theta_1 y_c$, $v_{A_2} = \theta_2 y_c$, and $\theta \in \Theta$ the smallest under $\leq$ such that $\theta_1 \preceq \theta, \theta_2 \preceq \theta$. If $\deg((\theta/\theta_1)A_1) \geq \deg((\theta/\theta_2)A_2)$, we define the Δ-*polynomial* of A_1 and A_2 to be

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

We denote by $\Delta(\mathcal{A})$ the set of non-zero Δ-polynomials $\Delta(A_1, A_2)$ for all $A_1, A_2 \in \mathcal{A}$. A chain $\mathcal{A}$ is said to be *coherent*, if for any $P \in \Delta(\mathcal{A})$, $\mathrm{rprem}(P, \mathcal{A}) = 0$.

Let $\mathcal{A} = A_1, \ldots, A_s$ be a chain. A linear combination $C = \sum_{\theta \in \Theta} Q_\theta \theta A_i$ is called *canonical* if θA_i in the expression are distinct elements in $\mathcal{A}_P$ for a DD-polynomial P. In other words, $C \in (\mathcal{A}_P)$.

Lemma 4.1 *Let $\mathcal{A}$ be a coherent chain, $A \in \mathcal{A}$, and $\theta \in \Theta$. Then there exist a DD-polynomial P and a $J \in \mathbf{H}_{\mathcal{A}}$ such that $v_J < v_{\theta A}$ and $J\theta A$ has a canonical representation:*

$$J\theta A = \sum_{v_B \leq v_A, B \in \mathcal{A}_P} Q_B B. \tag{5}$$

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

If $\theta A \in \mathcal{A}_{\theta A}$, the Lemma is true. Otherwise, we will prove this by induction on the ordering of $v_{\theta A}$. Let $A_{c,k}$ be largest w.r.t. $\leq$, such that $\text{ord}_\delta(A_{c,k}) \leq \text{ord}_\delta(\theta A)$. Then the canonical polynomial corresponding to $v_{\theta A}$ must be $\bar{\theta}_k A_{c,k}$ for a $\bar{\theta}_k \in \Theta$. We will form the Δ-polynomial for $A_{c,k}$ and $A_{c,i}$. Let $R = \Delta(A_{c,i}, A_{c,k})$. Then there exists $t \in \mathbb{N}$, $\theta_i \in \Theta$, and $\theta_k \in \Theta$, such that $v_{\theta_i A_{c,i}} = v_{\theta_k A_{c,k}}$ and

$$J_1^t \theta_i A = Q\theta_k A_{c,k} + R$$

where J_1 is either the initial or the separant of $A_{c,k}$ and $v_R < v_{\theta_i A}$. We have $v_{J_1} < v_{\theta_i A}$. Since $\mathcal{A}$ is a coherent chain, $\text{rprem}(R, \mathcal{A}) = \text{aprem}(R, A_R) = 0$. We have

$$J_2 R = \sum_{A \in A_R, v_A \leq v_R} B_A A$$

where $J_2 \in \mathbf{H}_{\mathcal{A}}$ such that $v_{J_2} < v_R < v_{\theta_i A}$ So we have

$$J_2 J_1^t \theta_i A = J_2 Q \theta_k A_{c,k} + \sum_{A \in A_R, v_A < v_{\theta_i A}} B_A A.$$

From the index diagram (Figure 2), we have $\theta_i \preceq \theta$. Let $\bar{\theta} = \theta/\theta_i = \delta^d \partial^s$ and $\bar{\theta}_k \in \Theta$ be a shuffle of $\bar{\theta}\theta_k$. Perform $\bar{\theta}$ on the above equation, by Lemma 2.1, we have

$$g\delta^d(J_2 J_1^t)\theta A = F\bar{\theta}_k A_{c,k} + \sum_{B \in \mathcal{A}, \eta \in \Theta, v_{\eta B} < v_{\theta A}} C_B \eta B,$$

where $g \in \mathbb{K}$. Use the induction hypothesis, we have that each ηB has a canonical representation. So there exist a DD-polynomial P' and a $J_3 \in \mathbf{H}_{\mathcal{A}}$ with $v_{J_3} < v_{\theta A}$ such that

$$J_3 \Big(\sum_{B \in \mathcal{A}, \eta \in \Theta, v_{\eta B} < v_{\theta A}} C_B \eta B \Big) = \sum_{v_C < v_{\theta A}, C \in \mathcal{A}'_P} Q_C C.$$

Let $J = J_3 g \delta^d (J_2 J_1^t)$. Then $v_J < v_{\theta A}, J \in \mathbf{H}_{\mathcal{A}}$ and $J\theta A$ has a canonical representation of form (5). □

Lemma 4.2 *Let $\mathcal{A} = A_1, \ldots, A_l$ be a coherent chain. For any $f = \sum g_{i,j} \eta_j A_i$, there is a $J \in \mathbf{H}_{\mathcal{A}}$ such that $J \cdot f$ has a canonical representation, and $v_J < \max\{v_{\eta_j A_i}\}$.*

Proof: This is a direct consequence of Lemma 4.1. □

4.2. Regular chains

We will introduce some notations and results about invertibility of algebraic polynomials with respect to an algebraic chain.

Let $\mathcal{A} = A_1, \ldots, A_p$ be a nontrivial triangular set in $\mathbb{K}[x_1, \ldots, x_n]$ over a field $\mathbb{K}$ of characteristic zero. Let y_i be the leading variable of A_i, $y = \{y_1, \ldots, y_p\}$ and $u = \{x_1, \ldots, x_n\} \setminus y$. u is called the *parameter set* of $\mathcal{A}$. We can denote $\mathbb{K}[x_1, \ldots, x_n]$ as $\mathbb{K}[u, y]$. For a triangular set $\mathcal{A}$, let $I_{\mathcal{A}}$ be the set of products of the initials of the polynomials in $\mathcal{A}$, and $H_{\mathcal{A}}$ the set of products of the initials and separants of the polynomials in $\mathcal{A}$. The quotient ideal $(\mathcal{A}) : I_{\mathcal{A}}$ is called the *algebraic saturation ideal* and is denoted by $\mathrm{asat}(\mathcal{A})$.

For a polynomial P and a triangular set $\mathcal{A} = A_1, A_2, \ldots, A_p$ in $\mathbb{K}[u, y]$ with u as the parameter set, let

$$P_p = P, P_{i-1} = \mathrm{Resl}(P_i, A_i, y_i), i = p, \ldots, 1$$

and define $\mathrm{Resl}(P, \mathcal{A}) = P_0$, where $\mathrm{Resl}(P, Q, y)$ is the resultant of P and Q w.r.t. y. We assume that if y does not appear in P, $\mathrm{Resl}(P, Q, y) = P$. It is clear that $\mathrm{Resl}(P, \mathcal{A}) \in \mathbb{K}[u]$.

A polynomial P is said to be *invertible* w.r.t. a chain $\mathcal{A}$ if $\mathrm{Resl}(P, \mathcal{A}) \neq 0$. $\mathcal{A} = A_1, \ldots, A_p$ is called *regular* if the initials of A_i are invertible w.r.t. $\mathcal{A}$. $\mathcal{A}$ is called *satured* if the initials and separants of A_i are invertible w.r.t. $\mathcal{A}$.

Lemma 4.3 *[1] Let $\mathcal{A}$ be a triangular set. Then $\mathcal{A}$ is a characteristic set of* $\mathrm{asat}(\mathcal{A}) = (\mathcal{A}) : I_{\mathcal{A}}$ *if and only if $\mathcal{A}$ is regular.*

Lemma 4.4 *[3] A polynomial g is not invertible w.r.t. a regular triangular set $\mathcal{A}$ if and only if there is a nonzero f in $\mathbb{K}[u, y]$ such that $fg \in (\mathcal{A})$ and g is reduced w.r.t. $\mathcal{A}$.*

Lemma 4.5 *[1, 3] Let $\mathcal{A}$ be a regular triangular set. Then a polynomial P is invertible w.r.t. $\mathcal{A}$ if and only if $(P, \mathcal{A}) \cap \mathbb{K}[u] \neq \{0\}$.*

Lemma 4.6 *[3] Let $\mathcal{A}$ be a satured triangular set. Then $(\mathcal{A}) : I_{\mathcal{A}} = (\mathcal{A}) : H_{\mathcal{A}}$ is a radical ideal.*

Let $\mathcal{A}$ be a chain and P a DD-polynomial. P is said to be *invertible* w.r.t. $\mathcal{A}$ if it is invertible w.r.t. $\mathcal{A}_P$ when P and $\mathcal{A}_P$ are treated as algebraic polynomials.

A chain $\mathcal{A}$ is said to be *regular* if any DD-polynomial in $\mathbf{H}_{\mathcal{A}}$ is invertible w.r.t. $\mathcal{A}$.

Lemma 4.7 *If a chain $\mathcal{A}$ is a characteristic set of* $\mathrm{sat}(\mathcal{A})$*, then for any DD-polynomial P, $\mathcal{A}_P$ is a regular algebraic triangular set.*

Proof: By Lemma 4.3, we need only to prove that $\mathcal{B} = \mathcal{A}_P$ is the characteristic set of $(\mathcal{B}) : I_{\mathcal{B}}$. Let W be the set of all the θy_j such that θy_j is of lower or equal ordering than a $\bar{\theta} y_j$ occurring in $\mathcal{B}$. Then $\mathcal{B} \subseteq \mathbb{K}[W]$. If $\mathcal{B}$ is not a characteristic set of $(\mathcal{B}) : I_{\mathcal{B}}$, then there is a $Q \in (\mathcal{B}) : I_{\mathcal{B}} \cap \mathbb{K}[W]$ which is reduced w.r.t. $\mathcal{B}$ and is not zero. Q does not contain θy_i which is of higher ordering than those in W. As a consequence, Q is also reduced w.r.t. $\mathcal{A}$. Since $Q \in (\mathcal{B}) : I_{\mathcal{B}} \subseteq \mathrm{sat}(\mathcal{A})$ and $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$, by Lemma 3.4, Q must be zero, a contradiction. $\square$

Lemma 4.8 *Let $\mathcal{A}$ be a coherent and regular chain, and R a DD-polynomial reduced w.r.t. $\mathcal{A}$. If $R \in \mathrm{sat}(\mathcal{A})$, then $R = 0$, or equivalently, $\mathcal{A}$ is the characteristic set of* $\mathrm{sat}(\mathcal{A})$.

Proof: Let $\mathcal{A} = A_1, A_2, \ldots, A_l$. Since $R \in \mathrm{sat}(\mathcal{A})$, there is a $J_1 \in \mathbf{H}_{\mathcal{A}}$ such that $J_1 \cdot R \equiv 0 \bmod [\mathcal{A}]$. Since $\mathcal{A}$ is regular, J_1 is difference invertible w.r.t. $\mathcal{A}$, that is, there exists a DD-polynomial $\bar{J}_1$ and a nonzero $N \in \mathbb{K}[V]$ such that

$$\bar{J}_1 \cdot J_1 = N + \sum_{v_B \le v_{J_1}, B \in \mathcal{A}_{J_1}} Q_B B$$

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

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

Or equivalently,

$$N \cdot R = \sum g_{i,j} \theta_{i,j} A_j. \tag{6}$$

Since $\mathcal{A}$ is a coherent chain, by Lemma 4.2, there is a $J_2 \in \mathbf{H}_{\mathcal{A}}$ such that $J_2 \cdot N \cdot R$ has a canonical representation, where $v_{J_2} < \max\{v_{\theta_{i,j} A_j}\}$ in equation (6). That is

$$J_2 \cdot N \cdot R = \sum_{ij} \bar{g}_{i,j} \rho_{i,j} A_j, \tag{7}$$

where, $v_{\rho_{i,j} A_j}$ are pairwisely different. If $\max\{v_{\rho_{i,j} A_j}\}$ in (7) is lower than $\max\{v_{\theta_{i,j} A_j}\}$ in (6), we have already reduced the highest ordering of $v_{\theta_{i,j} A_j}$ in (6). Otherwise, assume $v_{\rho_a A_b} = \max\{v_{\rho_{i,j} A_j}\}$ and $\rho_a A_b = I_b \cdot v_{\rho_a A_b}^{d_b} + R_b$. Substituting $v_{\rho_a A_b}^{d_b}$ by $-\frac{R_b}{I_b}$ in (7), the left side keeps unchanged since $v_{J_2} < v_{\rho_a A_b}$, N is free of $v_{\rho_a A_b}$ and $\deg(R, v_{\rho_a A_b}) < \deg(\rho_a A_b, v_{\rho_a A_b})$. In the right side, $\rho_a A_b$ becomes zero, i.e. the $\max\{v_{\rho_{i,j} A_j}\}$ decreases. Clearing denominators of the substituted formula of (7), we obtain a new equation:

$$I_b^t \cdot J_2 \cdot N \cdot R = \sum f_{ij} \tau_{i,j} A_j. \tag{8}$$

Note that in the right side of (8), the highest ordering of $\tau_{i,j} A_j$ and $I_b^t \cdot J_2$ are less than $v_{\rho_a A_b}$ and $I_b^t \cdot J_2$ is invertible w.r.t. $\mathcal{A}$. Then after multiplying a DD-polynomial, the right side of (8) can be represented as a linear combination of $\tau_{i,j} A_j$ all of which is strictly lower than $v_{\rho_a A_b}$. Repeating the above process, we can obtain a nonzero $\bar{N} \in \mathbb{K}[V]$, such that

$$\bar{N} \cdot R = 0.$$

Then $R = 0$. By Lemma 3.4, $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. □

The above lemma is a modified difference-differential version of Rosenfeld's Lemma [14]. The condition in this lemma is stronger than the one used in the differential version of Rosenfeld's Lemma. The conclusion is also stronger. The following example shows that the Rosenfeld's Lemma [14] cannot be extended to difference-differential case directly. As a consequence, the approach proposed in [2] cannot be extended to the DD-polynomials directly.

Example 4.9 Let us consider chain $\mathcal{A} = \{y_{1,1,0}^2 - 1, (y_{1,0,0} - 1)y_{2,0,0}^2 + 1\}$ in $\mathbb{K}\{y_1, y_2\}$. $\mathcal{A}$ is coherent and $y_{1,1,0}+1$ is reduced w.r.t. $\mathcal{A}$. $y_{1,1,0}+1 \in \mathrm{sat}(\mathcal{A})$, because $J = \mathrm{I}_{(y_{1,0,0}-1)y_{2,0,0}^2+1} = y_{1,0,0} - 1$ and $\delta(J)(y_{1,1,0} + 1) = y_{1,1,0}^2 - 1 \in [\mathcal{A}]$. On the other hand, $y_{1,1,0} + 1 \notin \mathrm{asat}(\mathcal{A})$.

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

Theorem 4.10 *A chain $\mathcal{A}$ is the characteristic set of* $\mathrm{sat}(\mathcal{A})$ *iff $\mathcal{A}$ is coherent and regular.*

Proof: If $\mathcal{A}$ is coherent and regular, then by Lemma 4.8, $\mathcal{A}$ is a characteristic set of $\mathrm{sat}(\mathcal{A})$. Conversely, let $\mathcal{A} = A_1, A_2, \ldots, A_l$ be a characteristic set of the saturation ideal $\mathrm{sat}(\mathcal{A})$ and $I_i = \mathrm{I}_{A_i}, S_i = \mathrm{S}_{A_i}$. For any $1 \le i < j \le l$, let $R = \mathrm{rprem}(\Delta_{i,j}, \mathcal{A})$, then R is in $\mathrm{sat}(\mathcal{A})$ and is reduced w.r.t. $\mathcal{A}$. Since $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$, $R = 0$. Then $\mathcal{A}$ is coherent. To prove that $\mathcal{A}$ is regular, we need to prove that any $P \in \mathbf{H}_{\mathcal{A}}$ is invertible w.r.t. $\mathcal{A}$. Assume this is not true. By definition, P is not invertible w.r.t. $\mathcal{A}_P$ when it is treated as algebraic equations. By Lemma 4.7, $\mathcal{A}_P$ is a regular algebraic triangular set. By Lemma 4.4, there is an $F \neq 0$ which is reduced w.r.t. $\mathcal{A}_P$ (and hence $\mathcal{A}$) such that $P \cdot F \in (\mathcal{A}_P) \subseteq [\mathcal{A}]$. Since $P \in \mathbf{H}_{\mathcal{A}}$, $F \in \mathrm{sat}(\mathcal{A})$ and F is reduced w.r.t. $\mathcal{A}$, $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$, we have $F = 0$, a contradiction. Hence, P is invertible w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is regular. □

As a Corollary, we have

Corollary 4.11 *Let $\mathcal{A}$ be a coherent and regular chain. Then* $\mathrm{sat}(\mathcal{A}) = \{P | \mathrm{rprem}(P, \mathcal{A}) = 0\}$.

Theorem 4.10 is significant because it provides an easy way to check whether a DD-polynomial is in $\mathrm{sat}(\mathcal{A})$. Unlike the algebraic and differential cases, if the initials and separants of $\mathcal{A}$ are invertible w.r.t. $\mathcal{A}$, we could have $\mathrm{sat}(\mathcal{A}) = [1]$. The main reason is the difference operator. See the following example.

Example 4.12 Let $\mathcal{A} = \{\delta y_1, y_1 y_2 + 1\}$. The initial of $y_1 y_2 + 1$, $I = y_1$, is invertible w.r.t. $\mathcal{A}$, but $\delta I \cdot 1 \in [\mathcal{A}]$ which implies $1 \in \mathrm{sat}(\mathcal{A})$.

Theorem 4.13 *If $\mathcal{A}$ is a coherent and regular chain, then*

$$\mathrm{sat}(\mathcal{A}) = \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P} = \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : I_{\mathcal{A}_P}.$$

Proof: It is easy to see that $\mathrm{sat}(\mathcal{A}) = [\mathcal{A}] : \mathbf{H}_{\mathcal{A}} \supset \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Let $f \in \mathrm{sat}(\mathcal{A})$. Since $\mathcal{A}$ is coherent and regular, $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. Then $\mathrm{rprem}(P, \mathcal{A}) = 0$, or $\mathrm{prem}(f, \mathcal{A}_P) = 0$. We have $P \in (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Hence $\mathrm{sat}(\mathcal{A}) \subseteq \bigcup_{P \in \mathbb{K}\{\mathbb{Y}\}} (\mathcal{A}_P) : H_{\mathcal{A}_P}$. Since $\mathcal{A}$ is regular, $\mathcal{A}_P$ is saturated, by Lemma 4.6, $(\mathcal{A}_P) : I_{\mathcal{A}_P} = (\mathcal{A}_P) : H_{\mathcal{A}_P}$, so we proved the theorem. □

5. Irreducible chains

There exist no direct methods to check whether a given chain is regular since we need to check that all possible transforms of the initials and separants are invertible. In this section, we will give a constructive criterion for a chain to be regular by introducing the concept of proper irreducible chains.

5.1. Index Set of a Chain

In this Section, we will use the ordering $\leq_l$ defined in Section 2.2. That is, $y_{i,d_1,s_1} \leq_l y_{j,d_2,s_2}$ iff (i, d_1, s_1) is less than (j, d_2, s_2) according to the lexicographical ordering.

Now we consider the structure of an auto-reduced set. For any chain $\mathcal{A}$, after a proper renaming of the variables, we could write it as the following form.

$$\mathcal{A} = \begin{cases} A_{1,1}(\mathbb{U}, y_1), \ldots, A_{1,k_1}(\mathbb{U}, y_1) \\ \ldots \\ A_{p,1}(\mathbb{U}, y_1, \ldots, y_p), \ldots, A_{p,k_p}(\mathbb{U}, y_1, \ldots, y_p) \end{cases} \tag{9}$$

where $\mathbb{U} = \{u_1, \ldots, u_q\}$ and $p+q = n$. For any i, we have $\mathrm{cls}(A_{i,j}) = \mathrm{cls}(A_{i,k})$. If $v_{A_{i,j}} = y_{c,d,s}$, let $d_{(d,s)}$ be the leading degree of $A_{i,j}$. We have

Lemma 5.1 *The set of all indices for a fixed class i will be denoted by IND_i. If we arrange $\mathrm{IND}_i = \{(a_1, b_1), \ldots, (a_s, b_s)\}$ such that $a_1 \leq a_2 \leq \cdots \leq a_s$. Then we have*

- *$a_1 < a_2 < \cdots < a_s$ and $b_1 \geq b_2 \geq \cdots \geq b_s$.*
- *If $b_j = b_{j+1}$, then $d_{(a_j,b_j)} < d_{(a_{j+1},b_{j+1})}$.*

Proof: Let A_1 and A_2 be the corresponding DD-polynomials of (a_1, b_1) and (a_2, b_2). We show that $a_1 = a_2$ cannot happen. Otherwise, consider b_1 and b_2. If $b_1 = b_2$, A_1 and A_2 will have the same leader which is impossible. If $b_1 < b_2$, A_2 is not reduced w.r.t. A_1, which is also impossible. Similarly, $b_1 > b_2$ cannot happen. This proves that $a_1 < a_2$. Similarly, we can prove that $a_i < a_{i+1}$. If $b_j = b_{j+1}$, since the corresponding DD-polynomials of $(a_j, b_j), (a_{j+1}, b_{j+1})$ are auto-reduced, we have $d_{(a_j,b_j)} < d_{(a_{j+1},b_{j+1})}$. □

Please refer to Figure 1 for an illustration of the above lemma.

Corollary 5.2 *Let $\mathcal{A}$ be a chain of form (9). Let $m_i = \max_j\{\mathrm{ord}_\delta(A_{i,j})\}$. Then $k_i \leq m_i$ and $|\mathcal{A}| \leq \sum_{i=1}^{p} m_i$.*

For any DD-polynomial set $\mathbb{P}$, the index set of the DD-polynomials in $\mathcal{A}_\mathbb{P}$ with class i is of the following form:

$$\begin{array}{llll} (a, s_1) & (a, s_1+1) & \ldots & (a, s_1+l_1) \\ (a+1, s_2) & (a+1, s_2+1) & \ldots & (a+1, s_2+l_2) \\ \ldots & \ldots & \ldots & \ldots \\ (a+r, s_r) & (a+r, s_r+1) & \ldots & (a+r, s_r+l_r) \end{array} \tag{10}$$

where $s_i, a, r, l_j \in \mathbb{N}$, and $s_1 \geq s_2 \geq \cdots \geq s_r$. Each row of (10) corresponds to a column in the index figure of $\mathcal{A}_\mathbb{P}$ (Figures 2 or 3).

To define the concept of proper irreducible chains, we need several properties of algebraic irreducible triangular sets. An algebraic triangular set $\mathcal{B}$ is called *irreducible* if $\mathcal{B}$ is regular and there exists no polynomials P and Q which are reduced w.r.t. $\mathcal{B}$ and $PQ \in \operatorname{asat}(\mathcal{B})$ [11, 16].

Lemma 5.3 *[17] Let $\mathcal{A}$ be an irreducible algebraic triangular set. Then* $\operatorname{asat}(\mathcal{A})$ *is a prime ideal and for any polynomial P, the following facts are equivalent.*

- *P is invertible w.r.t. $\mathcal{A}$.*
- *$P \notin \operatorname{asat}(\mathcal{A})$.*
- $\operatorname{aprem}(P, \mathcal{A}) \neq 0$*, where* aprem *is the algebraic pseudo-remainder.*

The above lemma was extended to the case of ordinary differential polynomials. Let $\mathcal{A}$ be a differential triangular set $\mathcal{A}$ [12, 17]. The *differential saturation ideal* of $\mathcal{A}$ is defined to be $\operatorname{dsat}(\mathcal{A}) = [\mathcal{A}]_\partial : H_\mathcal{A}$ where $[\mathcal{A}]_\partial$ is the differential ideal generated by $\mathcal{A}$.

Lemma 5.4 *[12, 16] Let $\mathcal{A}$ be a triangular set consisting of ordinary differential polynomials. If $\mathcal{A}$ is irreducible when considered as an algebraic triangular set, then* $\operatorname{dsat}(\mathcal{A})$ *is a prime differential ideal and for any differential polynomial P, $P \in \operatorname{dsat}(\mathcal{A})$ iff* $\operatorname{dprem}(P, \mathcal{A}) = 0$*, where* dprem *is the differential pseudo-remainder.*

5.2. Proper Irreducible Chain

We denote $\mathcal{A}^* = \mathcal{A}_\mathcal{A}$. Let $\mathcal{A}$ be the chain in (4), then the index set of $\mathcal{A}^*$ is given in Figure 3.

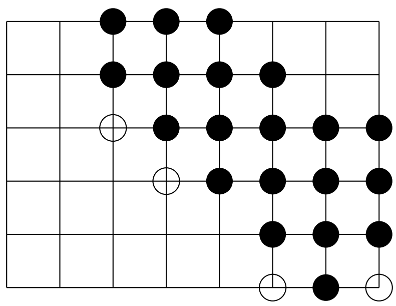

Fig. 3. The indices of chain $\mathcal{A}^*$

A chain $\mathcal{A}$ is said to be *proper irreducible* if

- $\mathcal{A}^*$ is an algebraic irreducible triangular set, and
- $\delta P \in \operatorname{dsat}(\mathcal{A}^*)$ implies $P \in \operatorname{dsat}(\mathcal{A}^*)$, where $\operatorname{dsat}(A^*)$ is the differential saturation ideal of $\mathcal{A}^*$.

Lemma 5.5 *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (9). If P is a nonzero DD-polynomial in $\mathbb{K}[\mathbb{P}_\mathcal{A}]$, then δP is invertible w.r.t. $\mathcal{A}$.*

Proof: Note that the indices of δP can be obtained by adding one to the δ-order of the indices of P, or equivalently by moving the indices of P to the right side by one in the index figure of $\mathcal{A}$. For an illustration, please consult Figure 3. As a consequence, the DD-polynomials $A \in \mathcal{A}_{\delta P}$ such that v_A appearing in δP must corresponds to the left most index on each row in the index figure of $\mathcal{A}_{\delta P}$. Let us denote these DD-polynomials by $\mathbb{H}$.

To test whether δP is invertible w.r.t. $\mathcal{A}_{\delta P}$, we need only consider those DD-polynomials in $\mathcal{A}_{\delta P}$ which will be needed when eliminating the leading variables of $\mathbb{H}$ with resultant computations. More precisely, these DD-polynomials $\mathcal{C}$ can be found recursively as follows:

- $\mathcal{C} = \mathbb{H}$, and
- if there exists an $A \in \mathcal{A}_{\delta P}$ such that $v_A \in \mathbb{V}_{\mathcal{C}} \setminus \mathbb{L}_{\mathcal{C}}$, then add A to $\mathcal{C}$.

From the definition of the invertibility, it is clear that δP is invertible w.r.t. $\mathcal{A}_{\delta P}$ iff δP is invertible w.r.t. $\mathcal{C}$. If $A \in \mathbb{H}$, there are two cases: $A \in \mathcal{A}^*$ or $A = \partial^s A_0, A_0 \in \mathcal{A}^*$. If $A \in \mathcal{A}^*$, then by Proposition 3.5, starting from A, all the DD-polynomials constructed in the above procedure are in $\mathcal{A}^*$. Let $A = \partial^s A_0, A_0 \in \mathcal{A}^*$. Due to the selection of the ordering $\leq_l$, for any class c, $d^c_{\{\partial^s A_0\}} \leq d^{(c)}_{\mathcal{A}^*}$. Therefore, starting from A, all the DD-polynomials constructed in the above procedure are in $\mathcal{A}^* \cup \mathbb{H}_1$ where $\mathbb{H}_1$ consists of DD-polynomials of the form $\partial^s A_0$ for $A_0 \in \mathcal{A}^*$. Since all DD-polynomials in $\mathbb{H}_1$ are linear in their leaders with their initials in $H_{\mathcal{A}^*}$ and A^* is irreducible, we know that $\mathcal{C}$ is an irreducible triangular set and $\mathrm{asat}(\mathcal{C}) \subseteq \mathrm{dsat}(\mathcal{A}^*)$.

Suppose that δP is not invertible w.r.t. $\mathcal{A}_{\delta P}$. Then, δP is not invertible w.r.t. $\mathcal{C}$. Since $\mathcal{C}$ is irreducible, by Lemma 5.3, we have $\delta P \in \mathrm{asat}(\mathcal{C}) \subseteq \mathrm{dsat}(\mathcal{A}^*)$. By the definition of the proper irreducible chain, $P \in \mathrm{dsat}(\mathcal{A}^*)$. By Lemma 5.4, $\mathrm{dprem}(P, \mathcal{A}^*) = 0$. On the other hand, since $P \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, we have $\mathrm{dprem}(P, \mathcal{A}^*) = P = 0$, a contradiction. □

The following example shows that if we replace dsat by asat in the definition of the proper irreducible chain, the above lemma will be false.

Let $A_1 = y_{1,2,0} - y_{0,0,0}$, $A_2 = y_{2,2,0} - y_{0,0,2}$, and $\mathcal{A} = A_1, A_2$. It is easy to see that $\mathcal{A}^* = A_1, A_2$ is an algebraic irreducible triangular set. Let $Q = y_{2,0,0} - y_{1,0,2} \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$. We have $\delta^2 Q = A_2 - \partial^2 A_1 \in \mathrm{sat}(\mathcal{A})$, but $Q \notin \mathrm{sat}(\mathcal{A})$.

The following is a key property for proper irreducible chains.

Lemma 5.6 *Let $\mathcal{A}$ be a coherent and proper irreducible chain of form (9). If P is invertible w.r.t. $\mathcal{A}$, then δP is invertible w.r.t. $\mathcal{A}$.*

Proof: We prove the lemma by induction on the order of P. By Lemma 5.5, if $P \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ then we are done. Assuming that the conclusion holds for any DD-polynomial Q such that $v_Q <_l v_P$, we will prove the lemma for P.

We first prove the following result.

$$\text{If } J \in \mathbf{H}_{\mathcal{A}} \text{ and } v_J <_l v_{\delta P}, \text{ then } J \text{ is invertible w.r.t. } \mathcal{A}. \tag{11}$$

Let I be the set of the initials and separants of the DD-polynomials in $\mathcal{A}^*$. By Lemma 5.3, any element in I is invertible w.r.t. $\mathcal{A}^*$ and hence invertible w.r.t. $\mathcal{A}$. Let $I_i = \delta^i I$ for $i \geq 0$. If $J \in I_1$ and $v_J <_l v_{\delta P}$, then $J = \delta L$, $L \in I$, and $v_L <_l v_P$. By the induction hypothesis,

J is invertible w.r.t. $\mathcal{A}$. Repeating the above procedure, we can prove that if $J \in I_i$ and $v_J <_l v_{\delta P}$, then J is invertible $\mathcal{A}$. Since $\mathbf{H}_{\mathcal{A}}$ is the set of products of elements in all I_i, each $J \in \mathbf{H}_{\mathcal{A}}$ satisfying $v_J <_l v_{\delta P}$ is invertible w.r.t. $\mathcal{A}$.

Let $\mathcal{B} = \{A \in \mathcal{A}_{\delta P} \,|\, v_A \leq v_{\delta P}\}$. By (11), $\mathcal{B}$ is a regular triangular set.

Since P is invertible w.r.t. $\mathcal{A}$, there exist a DD-polynomial Q and a non-zero DD-polynomial $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ such that $Q \cdot P \equiv G \bmod (\mathcal{A}_P)$, which can be represented by the following equation

$$Q \cdot P = G + \sum_{A \in \mathcal{A}_P, v_A \leq v_P} B_A A. \tag{12}$$

Since G is obtained from P by eliminating some variables using DD-polynomials in $\mathcal{A}_P$, we have $v_G \leq v_P$ and for each class c, $s^{(c)}_{\{G\}} \leq s^{(c)}_{\mathcal{A}_P}, d^{(c)}_{\{G\}} \leq d^{(c)}_{\mathcal{A}_P}$. Then $\mathbb{V}_{\delta G} \subseteq \mathbb{L}_{\mathcal{A}_P} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$. By Lemma 5.5, δG is invertible w.r.t. $\mathcal{A}_{\delta G}$. From $v_G \leq v_P$ and $\mathbb{V}_{\delta G} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$, δG is invertible w.r.t. $\mathcal{B}$.

Performing the transforming operator on (12), we have

$$\delta Q \cdot \delta P = \delta G + \sum_{\delta A \in \delta A_P, v_{\delta A} \leq v_{\delta P}} \delta B_A \delta A. \tag{13}$$

For any δA in the above equation, there are two cases. (1) $\delta A \in \mathcal{A}_{\delta P}$. (2) $\delta A \notin \mathcal{A}_{\delta P}$. Since $\mathcal{A}$ is coherent, by Lemma 4.1, there exists a $J \in \mathbf{H}_{\mathcal{A}}, v_J <_l v_{\delta A} \leq v_{\delta P}$ such that $J\delta A$ has a canonical representation. Then, there exists a $J \in \mathbf{H}_{\mathcal{A}}, v_J <_l v_{\delta P}$ and a DD-polynomial R such that

$$J\delta Q \cdot \delta P = J\delta G + \sum_{A \in \mathcal{A}_R, v_A \leq v_{\delta P}} C_A A.$$

Since $v_J <_l v_{\delta P}$, by (11), J is invertible w.r.t. $\mathcal{A}$. Since δG is invertible w.r.t. $\mathcal{B}$ and $v_{\delta G} \leq v_{\delta P}$, there exist DD-polynomials $P_1 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}], Q_1, T$ such that $P_1 \neq 0$ and

$$Q_1 J\delta G = P_1 + \sum_{A \in \mathcal{A}_T, v_A \leq v_{\delta P}} D_A A.$$

So there exists a DD-polynomial R_1 such that

$$Q_1 J\delta Q \cdot \delta P = P_1 + \sum_{A \in \mathcal{A}_{R_1}, v_A \leq v_{\delta P}} E_A A. \tag{14}$$

We write the summation of equation (14) as two parts:

$$Q_1 J\delta Q \cdot \delta P = P_1 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} E_A A + \sum_{B \notin \mathcal{A}_{\delta P}, B \in \mathcal{A}_{R_1}, v_B \leq v_{\delta P}} E_B B. \tag{15}$$

Let $B_1 = I_{B_1} v_{B_1}^{k_1} - U_1$ be the largest under the ordering $\leq_l$ in the third part of equation (15), where $I_{B_1} \in \mathbf{H}_{\mathcal{A}}$ is the initial of B_1. Since all the B in the third part of equation (15) are in $\mathcal{A}_{R_1}$, B_1 is determined uniquely. Replacing $v_{B_1}^{k_1}$ by U_1/I_{B_1}, we have

$$Q_1' \delta P = I_{B_1}^{t_1} P_1 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_{\delta P}} E_A' A + \sum_{A \notin \mathcal{A}_{\delta P}, A \in \mathcal{A}_{R_1}, v_B <_l v_{B_1}} E_B' B. \tag{16}$$

where $v_{I_{B_1}} <_l v_{B_1} \leq_l v_{\delta P}, t_1 \in \mathbb{N}$, and I_{B_1} is invertible w.r.t. $\mathcal{A}$. Since $\mathbb{V}_{\delta P} \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}, P_1 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ and for $A \in \mathcal{A}_{\delta P}$, $\mathbb{V}_A \subseteq \mathbb{L}_{\mathcal{A}_{\delta P}}$, for any $B \neq B_1$ in the third part of equation (14), $v_B <_l v_{B_1}$, they do not change under the above substitution.

Since I_{B_1} is invertible w.r.t. $\mathcal{A}$, similar to the above procedure, there exist DD-polynomials $Q_2, P_2 \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}], R_2$, such that $P_2 \neq 0$ and

$$Q_2\delta P = P_2 + \sum_{A\in\mathcal{A}_{\delta P}, v_A\leq v_{\delta P}} F_A A + \sum_{B\notin\mathcal{A}_{\delta P}, B\in\mathcal{A}_{R_2}, v_B<_l v_{B_1}\leq v_{\delta P}} F_B B. \tag{17}$$

The leaders of B in the above equation is less than that of v_{B_1}. Repeating the procedure for (17), by Lemma 3.2, after a finite number of steps, the third part of equation (17) will be eliminated. As a consequence, there is an H and a nonzero $R \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$ such that

$$H\delta P = R + \sum_{A\in\mathcal{A}_{\delta P}, v_A\leq v_{\delta P}} Q_A A = R + \sum_{A\in\mathcal{A}_{\mathcal{B}}} Q_A A.$$

Since $\mathcal{B}$ is a regular triangular set, by Lemma 4.5, δP is invertible w.r.t. $\mathcal{B} \subseteq \mathcal{A}_{\delta P}$. That is δP is invertible w.r.t. $\mathcal{A}$. □

The following result gives a constructive criterion to check whether a chain is regular.

Theorem 5.7 *A coherent and proper irreducible chain is regular.*

Proof: Let $\mathcal{A}^* = A_1, \ldots, A_m$, $I_j = \mathrm{I}(A_j)$, and $S_j = S_{A_j}$. Since $\mathcal{A}^*$ is an irreducible triangular set, by Lemma 5.3, I_j and S_j are invertible w.r.t. $\mathcal{A}^*$ and hence invertible w.r.t. $\mathcal{A}$. By Lemma 5.6, all $\delta^i I_j, \delta^i S_j$ are invertible w.r.t. $\mathcal{A}$. As a consequence, the products of $\delta^i I_j, \delta^i S_j$ are invertible w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is regular. □

Theorem 5.8 *Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then* $\mathrm{sat}(\mathcal{A})$ *is reflexive.*

Proof: For any $\delta P \in \mathrm{sat}(\mathcal{A})$, if $P \notin \mathrm{sat}(\mathcal{A})$. Let $R = \mathrm{rprem}(P, \mathcal{A}) \neq 0$. Then $\delta R \in \mathrm{sat}(\mathcal{A})$. So we can assume that $\delta P \in \mathrm{sat}(\mathcal{A})$ and P is reduced w.r.t. $\mathcal{A}$. By Theorem 5.7, $\mathcal{A}$ is regular, by Theorem 4.10, $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. Since $\delta P \in \mathrm{sat}(\mathcal{A})$ we have $\mathrm{rprem}(\delta P, \mathcal{A}) = 0$. So there exists a $J \in I_{\mathcal{A}_{\delta P}}$ such that $J\delta P \in (\mathcal{A}_{\delta P})$ and J is invertible w.r.t. $\mathcal{A}_{\delta P}$. So there exists a nonzero $G \in \mathbb{K}[\mathbb{P}_{\mathcal{A}}]$, such that

$$G\delta P = \sum_{A\in\mathcal{A}_{\delta P}} B_A A. \tag{18}$$

Let $\mathcal{C} = \mathcal{A}_{\delta P} \cap \{\delta^d\partial^s A \,|\, \delta^d A \in \mathcal{A}^*\}$. We have $[\mathcal{C}] \subseteq \mathrm{dsat}(\mathcal{A}^*)$. Since each DD-polynomial $A \in \mathcal{A}_{\delta P} \setminus \mathcal{C}$ must be the transforms for a DD-polynomial B which corresponds to the last index of a row in the index diagram for $\mathcal{C}$, the leading degree of A is the same as that of B. As a consequence, δP is reduced w.r.t. $\mathcal{A}_{\delta P} \setminus \mathcal{C}$. We can write the right hand side of the equation (18) as two parts:

$$G\delta P = \sum_{A\in\mathcal{C}} D_A A + \sum_{B\in\mathcal{A}_{\delta P}\setminus\mathcal{C}} D_B B.$$

Let $B = I_B v_B^k - U$, where $I_B \in \mathbf{H}_\mathcal{A}$ is the initial of B. Replacing v_B^k by U/I_B, we have

$$JG\delta P = \sum_{A\in\mathcal{C}} C_A A \in [\mathcal{C}] \subseteq \mathrm{dsat}(\mathcal{A}^*),$$

where $J \in \mathbf{H}_\mathcal{A}$ and is invertible w.r.t. $\mathcal{A}$. Since $G \in \mathbb{K}[\mathbb{P}_\mathcal{A}]$ and δP is reduced w.r.t. $\mathcal{A}_{\delta P} \setminus \mathcal{C}$, $G\delta P$ does not change under the above substitution. Let $B \in \mathcal{A}_{\delta P} \setminus \mathcal{C}$ with class c. For any $A \in \mathcal{C}$, by the construction of $\mathcal{A}^*$, $d_{\{A\}}^{(c)} <_l d_{\{B\}}^{(c)}$ and hence A will not change under the above substitution. Since $\mathcal{A}^*$ is irreducible, $G \in \mathbb{K}[\mathbb{P}_\mathcal{A}]$, J is invertible w.r.t. $\mathcal{A}$, and $JG\delta P \in \mathrm{dsat}(\mathcal{A}^*)$, by Lemma 5.4, we have $JG \notin \mathrm{dsat}(\mathcal{A}^*)$ and $\delta P \in \mathrm{dsat}(\mathcal{A}^*)$. Since $\mathcal{A}$ is proper irreducible, we have $P \in \mathrm{dsat}(\mathcal{A}^*) \subseteq \mathrm{sat}(\mathcal{A})$, a contradiction. □

Example 5.9 Consider $\mathcal{A} = \{A_1 = y_{1,0,0}^2 + t,\ A_2 = x_{2,0,0}^2 + t + k\ \}$ from [5] in $\mathbb{K}\{y_1, y_2\}$ where $\mathbb{K}$ is $Q(t)$ with the difference operator $\partial t = t+1$ and k is a positive integer. $\mathcal{A}^* = \{A_1, A_2\}$. If $k > 1$, $\mathcal{A}$ is proper irreducible. But $\mathrm{sat}(\mathcal{A})$ is not prime, because $A_2 - \delta^k(A_1) = (y_{2,0,0} - y_{1,k,0})(y_{2,0,0} + y_{1,k,0})$.

A proper irreducible chain $\mathcal{A}$ is said to be *strong irreducible* if for any DD-polynomial P $\mathcal{A}_P$ is an algebraic irreducible triangular set. In this section, we will prove that any reflexive prime ideal can be described with strong irreducible chains.

The following theorem gives a description for prime ideals with strong irreducible chains.

Theorem 5.10 *Let $\mathcal{A}$ be a coherent and strong irreducible chain. Then* $\mathrm{sat}(\mathcal{A})$ *is a reflexive prime ideal. On the other side, if I is a reflexive prime ideal and $\mathcal{A}$ the characteristic set for I, then $I = \mathrm{sat}(\mathcal{A})$ and $\mathcal{A}$ is a coherent and strong irreducible chain.*

Proof: "$\Longrightarrow$" Since $\mathcal{A}$ is a coherent and proper irreducible chain, by Theorem 4.10, $\mathcal{A}$ is regular and $\mathcal{A}$ is the characteristic set of $\mathrm{sat}(\mathcal{A})$. For two DD-polynomials P and Q such that $PQ \in \mathrm{sat}(\mathcal{A})$, by Theorem 4.13, there exists a DD-polynomial R, such that $PQ \in \mathrm{asat}(\mathcal{A}_R)$. Since $\mathcal{A}_R$ is an irreducible triangular set, by Lemma 5.3, we have $P \in \mathrm{asat}(\mathcal{A}_R)$ or $Q \in \mathrm{asat}(\mathcal{A}_R)$. Therefore, $\mathrm{sat}(A)$ is a prime ideal. By Theorem 5.8, $\mathrm{sat}(\mathcal{A})$ is reflexive. Then $\mathrm{sat}(\mathcal{A})$ is a reflexive prime ideal.

"$\Longleftarrow$" Since $\mathcal{A}$ is the characteristic set of I, by Theorem 4.10, $\mathcal{A}$ is coherent, regular, and $I \subseteq \mathrm{sat}(\mathcal{A})$. On the other hand, for $P \in \mathrm{sat}(\mathcal{A})$, there exists a $J \in \mathbf{H}_\mathcal{A}$, such that $JP \in [\mathcal{A}]$. Since I is a reflexive prime ideal, the initials and separants of $\mathcal{A}$ are not in I, so are their transforms. Then, we have $P \in I$, and hence $I = \mathrm{sat}(\mathcal{A})$. For any DD-polynomial P, $\mathcal{A}_P$ is an irreducible triangular set. Otherwise there exist DD-polynomials G, H, such that $GH \in \mathrm{asat}(\mathcal{A}_P) \subseteq \mathrm{sat}(\mathcal{A})$, G, H are reduced w.r.t. $\mathcal{A}_P$. Hence G, H are reduced w.r.t. $\mathcal{A}$. As a consequence, $G, H \notin I = \mathrm{sat}(\mathcal{A})$ but $GH \in I$, which contradicts to the fact that I is a prime ideal. If $\delta P \in \mathrm{dsat}(\mathcal{A}^*)$, we have $\delta P \in \mathrm{sat}(\mathcal{A}) = I$, and then $P \in \mathrm{sat}(\mathcal{A})$. Since $\mathcal{A}$ is coherent and regular, we have $P \in \mathrm{asat}(\mathcal{A}_P)$. Since $\mathcal{A}^*$ is irreducible, $\mathrm{dsat}(\mathcal{A}^*)$ is a prime differential ideal. Without loss of generality, we may assume that $d_{\{\delta P\}}^{(c)} \le d_{\mathcal{A}^*}^{(c)}$ for all c. As a consequence $\mathcal{A}_P \subseteq \mathrm{dsat}(\mathcal{A}^*)$ and $P \in \mathrm{asat}(\mathcal{A}_P) \subseteq \mathrm{dsat}(\mathcal{A}^*)$. □

6. Zero Decomposition Algorithms

In this section, we will present two algorithms which can be used to decompose the zero set of a finite DD-polynomial system into the union of the zero sets of proper irreducible chains. Such algorithms are called *zero decomposition algorithms*.

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

Lemma 6.1 *Let $\mathbb{P}$ be a finite set of DD-polynomials, $\mathcal{A} = A_1, \ldots, A_m$ a Wu characteristic set of $\mathbb{P}$, $I_i = \mathrm{I}(A_i), S_i = S_{A_i}$, and $J = \prod_{i=1}^m I_i S_i$. Then*

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

Proof: Since for any $P \in \mathbb{P}$, $\mathrm{rprem}(P, \mathcal{A}) = 0$, $\mathrm{Zero}(\mathbb{P}) \supset \mathrm{Zero}(\mathrm{sat}(\mathcal{A}))$. Therefore $\mathrm{Zero}(\mathbb{P}) \supset \mathrm{Zero}(\mathrm{sat}(\mathcal{A})) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$. Conversely, since $\mathcal{A} \subseteq [\mathbb{P}]$, $\mathrm{Zero}(\mathbb{P}) \subseteq \mathrm{Zero}(\mathcal{A})$. Let η be a solution of $\mathbb{P}$ in some extension field of $\mathbb{K}$. If η annuls some I_i, S_i, it is a solution of $\mathbb{P} \cup \{I_i\}$ or $\mathbb{P} \cup \{S_i\}$. If η annuls no I_i, S_i, then by Lemma 3.8 η is a solution of $\mathrm{sat}(\mathcal{A})$. Hence, $\mathrm{Zero}(\mathbb{P}) \subseteq \mathrm{Zero}(\mathrm{sat}(\mathcal{A})) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$. Thus, $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathrm{sat}(\mathcal{A})) \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\} \bigcup \cup_{i=1}^m \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$. Since $\mathcal{A}$ is the Wu characteristic set of $\mathbb{P}$, we have $\mathrm{Zero}(\mathbb{P} \cup \mathcal{A}) = \mathrm{Zero}(\mathbb{P})$. The second equation is proved. The first equation can be proved similarly. □

Lemma 6.2 *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 $P_1, P_2, \ldots, P_h$ which are reduced w.r.t. $\mathcal{A}$ such that*

$$\mathrm{Zero}(\mathbb{P}) = \cup_{i=1}^h \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{P_i\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$$

where I_i, S_i are the initials and separants of the DD-polynomials in $\mathcal{A}$.

Proof: Denote $\mathcal{B} = \mathcal{A}^* = B_1, \ldots, B_p$. Then the initials of $\mathcal{B}$ are the initials and separants of $\mathcal{A}$ and their transforms. First, if $\mathcal{A}^*$ is not algebraic irreducible, by Lemma 3 in Section 4.5 of [17], there are $P_1, \ldots, P_h$ which are reduced w.r.t. $\mathcal{A}^*$ such that

$$P = \prod_{i=1}^p I_i^{v_i} P_1^{t_1} \ldots P_h^{t_h} = \sum_{i=1}^{k+1} g_i B_i, \tag{19}$$

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 $\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{P} \cup \{P\}) = \cup_{i=1}^h \mathrm{Zero}(\mathbb{P}, P_i) \bigcup \cup_i \mathrm{Zero}(\mathbb{P}, I_i)$. If I_i is the initial of $\delta^d A$ for some $A \in \mathcal{A}$, then $\mathrm{Zero}(\mathbb{P}, I_i) = \mathrm{Zero}(\mathbb{P}, I_A)$. If I_i is the initial of $\delta^d \partial^t A$ for some $A \in \mathcal{A}$, then $\mathrm{Zero}(\mathbb{P}, I_i) = \mathrm{Zero}(\mathbb{P}, S_A)$. In other words, we need only to include the initials and separants of the DD-polynomials in $\mathcal{A}$.

If $\mathcal{A}^*$ is algebraic irreducible. Let $f = \delta g \in \mathrm{dsat}(\mathcal{A}^*)$ which satisfying $\mathrm{dprem}(g, \mathcal{A}^*) \neq 0$. $P_1 = \mathrm{dprem}(g, \mathcal{A}^*)$, we have $P_1 \neq 0$, P_1 is reduced w.r.t. $\mathcal{A}$, and

$$P_1 = \prod_{i=1}^p I_i^{v_i} S_i^{u_i} g - \sum_{i,j} g_{i,j} \partial^j B_i.$$

Algorithm 3 — ZDT($\mathbb{P}$)

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

Output: $W = \{\mathcal{A}_1, \ldots, \mathcal{A}_k\}$ such that $\mathcal{A}_i$ is a coherent and proper irreducible chain and $\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i))$.

Let $\mathcal{B} := C.S(\mathbb{P})$, $\mathcal{B} := B_1, \ldots, B_p$. /*/
If $\mathcal{B} = 1$ then return $\{\}$.
Else
  Let $\mathbb{R} := \{\mathrm{rprem}(f, \mathcal{B}) \neq 0 \mid f \in (\mathbb{P} \setminus \mathcal{B}) \cup \Delta(\mathcal{B})\}$.
  If $\mathbb{R} = \emptyset$ then
    Let $(test, \bar{\mathbb{P}})$:=**ProIrr**($\mathcal{B}$).
    If test then W = $\{\mathcal{B}\}\cup$**ZDT**$(\mathbb{P} \cup \mathcal{B} \cup \{I_i\})\cup$**ZDT**$(\mathbb{P} \cup \mathcal{B} \cup \{S_i\})$.
    Else W:= $\cup_{i=1}^k$**ZDT**$(\mathbb{P}, \mathcal{B}, P_i)\cup$ **ZDT** $(\mathbb{P}, \mathcal{B}, I_i)\cup$ **ZDT** $(\mathbb{P}, \mathcal{B}, S_i)$,
      where I_i, S_i are the initials and separants of the DD-polynomials in $\mathcal{B}$
      and $\bar{\mathbb{P}} = \{P_i \mid i = 1, \ldots, k\}$.
  Else W :=**ZDT**$(\mathbb{P} \cup \mathbb{R})$.

/*/ $C.S(\mathbb{P})$ gives the characteristic set of $\mathbb{P}$. Since $\mathbb{P}$ is finite, it is easy to find $C.S(\mathbb{P})$.

Then $\mathrm{Zero}(\mathbb{P}/\mathbf{H}_{\mathcal{A}}) = \mathrm{Zero}(\mathbb{P} \cup \{f\}/\mathbf{H}_{\mathcal{A}}) = \mathrm{Zero}(\mathbb{P} \cup \{g\}/\mathbf{H}_{\mathcal{A}}) = \mathrm{Zero}(\mathbb{P} \cup \{P_1\}/\mathbf{H}_{\mathcal{A}})$.

Combining these two conditions, we have that if $\mathcal{A}$ is not a proper irreducible chain, then we can find $P_1, P_2, \ldots, P_h$ which are reduced w.r.t. $\mathcal{A}$ such that

$$\mathrm{Zero}(\mathbb{P}) = \cup_{i=1}^h \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{P_i\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}) \bigcup \cup_i \mathrm{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{S_i\})$$

where I_i, S_i are the initials and separants of $\mathcal{A}$. □

Now, we can give the *zero decomposition theorem* for finite DD-polynomial sets.

Theorem 6.3 *Let $\mathbb{P}$ be a finite set of DD-polynomials in $\mathbb{K}\{y_1, \ldots, y_n\}$. Then there exist a sequence of coherent and proper irreducible chains $\mathcal{A}_i$, $i = 1, \ldots, k$ such that*

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \mathrm{Zero}(\mathcal{A}_i/J_i)$$
$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i)) \tag{20}$$

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

The correctness of the above theorem follows from the correctness of the algorithm **ZDT**. This is a quite straight forward extension of the algebraic and differential zero decomposition algorithms in [12, 17], except for the algorithm **ProIrr** to find a proper irreducible chain. The correctness of the algorithm is guaranteed by Lemma 6.1 and Lemma 6.2. The termination of it is guaranteed by Lemmas 3.2 and 3.3.

Indeed, in **ZDT**, we need to check whether a coherent chain is proper irreducible. The procedure **ProIrr**, when it applied to a coherence chain $\mathcal{B}$, returns two argument: test, $\bar{\mathbb{P}}$.

Algorithm 4 — ProIrr($\mathcal{A}$)

Input: A coherent chain $\mathcal{A}$ of the form (9).
Output: (true,$\emptyset$), if $\mathcal{A}$ is proper irreducible.
(false,$\bar{\mathbb{P}}$), otherwise, where $\bar{\mathbb{P}}$ is the set of DD-polynomials mentioned in Lemma 6.2.

If $\mathcal{A}^*$ is algebraic irreducible then
  $G := \mathbf{DCS}(\mathcal{A}^*)$ /*/
    $G_1 := G \cap \mathbb{K}[U_1, Y_1]$ where U_1, Y_1 are the
    variables in G, except for those $u_{i,0,j}, y_{i,0,k}$ with zero ord_δ.
    $G_1 := \delta^{-r} G_1$, where r is the largest s, such that δ^{-s} is a DD-polynomial.
  If $\mathrm{rprem}(g, \mathcal{A}^*) = 0$ for all $g \in G_1$, then return (true,$\emptyset$).
  Else return (false,$\{\mathrm{rprem}(g, \mathcal{A}^*) \neq 0 \mid g \in G_1\}$).
Else
  Let $\bar{\mathbb{P}}$ be the set of DD-polynomials in (19).
  Return (false,$\bar{\mathbb{P}}$)

/*/ $G := \mathbf{DCS}(\mathcal{A}^*)$ computes a differential characteristic set of $\mathrm{dsat}(\mathcal{A}^*)$ w.r.t. the elimination ordering $y_{c,0,i} > y_{c,0,i-1} > \cdots y_{c-1,0,t} > \cdots > y_{1,0,s} > u_{d,0,l} > \cdots > u_{1,0,k} > \cdots$. So this is an algorithm for differential ideals. We treat $y_{c,i,0}, u_{t,i,0}$ as differential indeterminates and $y_{c,i,k}, u_{t,i,k}$ as differentiations of $y_{c,i,0}, u_{t,i,0}$.

If $\mathcal{B}^*$ is proper irreducible, then test is true and $\bar{\mathbb{P}} = \emptyset$; else test is false, $\bar{\mathbb{P}}$ consists of the DD-polynomials $P_1, \ldots P_k$ mentioned in Lemma 6.2.

Lemma 6.4 *Algorithm* **DCS** *is correct.*

Proof: By the definition of dsat, we have

$$\mathrm{Zero}(\mathrm{dsat}(\mathcal{A})/J) = \mathrm{Zero}(\mathcal{A}/J) = \cup_i \mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_i)/J). \tag{21}$$

Since $\mathcal{A}$ is irreducible, by Lemma 5.4, $\mathrm{dsat}(\mathcal{A})$ is a prime ideal. Then $\mathrm{dsat}(\mathcal{A}) \subseteq \mathrm{dsat}(\mathcal{A}_i)$ for any i. Due to (21), a generic zero of $\mathrm{dsat}(\mathcal{A})$ must be in some $\mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_k))$. For this k, we have $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$. We will show that $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_k)$. For any

Algorithm 5 — DCS($\mathcal{A}$)

Input: $\mathcal{A}$ an irreducible differential triangular set in $\mathbb{K}\{u, y\}$.
Output: A differential characteristic set $\mathcal{B}$ of $\mathrm{dsat}(\mathcal{A})$ under the variable ordering $y_{c_1,0,i} > y_{c_2,k,j}$ for any $k \neq 0$.

Let J be the product of the initials and separants of $\mathcal{A}$.
Compute a zero decomposition $\mathrm{Zero}(\mathcal{A}/J) = \cup_i \mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_i)/J)$ with method from [16], where $\mathcal{A}_i$ are irreducible differential chains.
Find a k such that $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$.
Return A_k.

$P \in \mathrm{dsat}(\mathcal{A}_k)$, there exists a $J_1 \in H_{\mathcal{A}_k}$ such that $J_1 P \in [\mathcal{A}_k]$. We say that $J_1 \notin \mathrm{dsat}(\mathcal{A})$. Otherwise, $J_1 \in \mathrm{dsat}(\mathcal{A}) \subseteq \mathrm{dsat}(\mathcal{A}_k)$, a contradiction. Since $\mathrm{dprem}(P, \mathcal{A}) = 0$ for all $P \in \mathcal{A}_k$, there exists a $J_2 \in H_{\mathcal{A}}$ such that $J_1 J_2 P \in [\mathcal{A}]$. Since $J_1 J_2 \notin \mathrm{dsat}(\mathcal{A})$, we have $P \in \mathrm{dsat}(\mathcal{A})$. So $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_k)$. □

Lemma 6.5 *Algorithm* **ProIrr** *is valid.*

Proof: If **ProIrr($\mathcal{A}$)** returns $(true, \emptyset)$, we will show that for any $\delta P \in \mathrm{dsat}(\mathcal{A}^*)$, $P \in \mathrm{dsat}(\mathcal{A}^*)$. Since $\mathrm{dsat}(\mathcal{A}^*) = \mathrm{dsat}(\mathcal{A}_k)$, where $\mathcal{A}_k$ is obtained form **DCS**($\mathcal{A}^*$), we have $\delta P \in \mathrm{dsat}(\mathcal{A}_k)$. Since $\mathcal{A}_k$ is an irreducible differential chain, $\mathrm{dprem}(\delta P, \mathcal{A}_k) = 0$. We denote $G_1 = \mathcal{A}_k \cap \mathbb{K}[U_1, Y_1], G_0 = \delta^{-1} G_1$, where $\mathbb{K}[U_1, Y_1]$ is described in algorithm **ProIrr**. Then $\mathrm{dprem}(\delta P, \mathcal{A}_k) = \mathrm{dprem}(\delta P, G_1) = 0$. So there exists a $J \in H_{G_1}$, such that $J \delta P = \sum_{i \in \mathbb{N}, B \in G_1} Q_{i,B} \partial^i B$, where $J, B, Q_{i,B} \in \mathbb{K}[U_1, Y_1]$. Perform δ^{-1} on this equation, we have $(\delta^{-1} J) P \in [G_0]_\partial$. Since for any $G \in G_0$, $d^{(c)}_{\{G\}} \leq d^{(c)}_{\{\mathcal{A}^*\}}$ for all c, we have $\mathcal{A}_G \subseteq [\mathcal{A}^*]_\partial$ and $\mathrm{rprem}(G, \mathcal{A}) = \mathrm{aprem}(G, \mathcal{A}_G) = \mathrm{dprem}(G, \mathcal{A}^*) = 0$. Then we have $(\delta^{-1} J) P \in \mathrm{dsat}(\mathcal{A}^*)$. Since $\mathcal{A}_k$ is an irreducible differential chain, J is invertible w.r.t. $\mathcal{A}_k$, then it is invertible w.r.t. $\mathcal{A}_J \subset [\mathcal{A}^*]_\partial$. Hence $\delta^{-1} J$ must be invertible w.r.t. $\mathcal{A}_{\delta^{-1} J} \subset [\mathcal{A}^*]_\partial$. Otherwise, we have $\delta^{-1} J \in \mathrm{asat}(\mathcal{A}_{\delta^{-1} J})$. Since $\mathcal{A}$ is coherent and regular, by Theorem 4.10, it is the characteristic set of $\mathrm{sat}(\mathcal{A})$ and $J \in \mathrm{sat}(\mathcal{A})$. Then $\mathrm{rprem}(J, \mathcal{A}) = \mathrm{aprem}(J, \mathcal{A}_J) = \mathrm{dprem}(J, \mathcal{A}^*) = 0$, a contradiction. Then we have $P \in \mathrm{dsat}(\mathcal{A}^*)$. □

Example 6.6 Let $A_1 = y_{1,2,0} - y_{0,0,0}$, $A_2 = y_{2,2,0} - y_{0,0,2}$, and $\mathcal{A} = A_1, A_2$. Then $\mathcal{A}$ is already a coherent chain and algorithm ZDT will call ProIrr($\mathcal{A}$) directly. In the algorithm ProIrr, since $\mathcal{A}^* = A_1, A_2$ is an algebraic irreducible triangular set, algorithm DCS($\mathcal{A}^*$) will be called. In the algorithm DCS, we have $J = 1$ and under the new variable order $y_{0,0,0} > y_{0,0,2} > y_{1,2,0} > y_{2,2,0}$, we have

$$\mathrm{Zero}(\mathcal{A}^*) = \mathrm{Zero}(\mathrm{dsat}(A_1, A_3)) = \mathrm{Zero}(A_1, A_3)$$

where $A_3 = y_{2,2,0} - y_{1,2,2}$. Algorithm DCS returns A_1, A_3. Now we back to algorithm ProIrr and $G_1 = \delta^{-2}\{A_3\} = \{A_4 = y_{2,0,0} - y_{1,0,2}\}$. Algorithm ProIrr returns $(false, , \{A_4\})$. Now we back to algorithm ZDT with input $\{A_1, A_2, A_4\}$. Since $\mathcal{B} = A_1, A_4$ is a coherent and proper irreducible chain, the algorithm returns $\mathcal{B}$ and we have $\mathrm{Zero}(\mathcal{A}) = \mathrm{Zero}(\mathrm{sat}(\mathcal{B})) = \mathrm{Zero}(\mathcal{B})$.

References

[1] P. Aubry, D. Lazard, and M.M. Maza, On the Theory of Triangular Sets, *Journal of Symbolic Computation*, **28**, 105-124, 1999.

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

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

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

[5] R.M. Cohn, Manifolds of Difference Polynomials, *Trans. of AMS*, **64**, 133-172, 1948.

[6] X.S. Gao and Y. Luo, A Characteristic Set Method for Difference Polynomial Systems, *Proc. ICPSS*, 28-30, Nov. 24-26, Paris, 2004. Full version in *MM Research Preprints*, **23**, 66-91, 2004.

[7] X.S. Gao and C. Yuan, Resolvent Systems of Difference Polynomial Ideals, *Proc. ISSAC 2006*, 101-108, ACM Press, New York, 2006.

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

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

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

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

[12] J.F. Ritt and J.L. Doob, Systems of Algebraic Difference Equations, *American Journal of Mathematics*, 55, 505-514, 1933.

[13] J.F. Ritt and H.W. Raudenbush, Ideal Theory and Algebraic Difference Equations, *Trans. of AMS*, 46, 445-452, 1939.

[14] A. Rosenfeld, Specialization in Differential Algebra, *Trans. Am. Math. Soc.*, 90, 394-407, 1959.

[15] J. van der Hoeven, *Differential and Mixed Differential-difference Equations from the Effetive Viewpoint*, Preprints, 1996.

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

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

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