Characteristic Set Method for Differential-Difference Polynomial Systems

Xiao-Shan Gao¹, Joris van der Hoeven², Chunming Yuan¹, and Guilin Zhang¹

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 privilege 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.

¹KLMM, Institute of Systems Science, AMSS, Academia Sinica, Beijing 100080, China.
²Département de Mathématiques, Université 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* $\partial$ defined on $\mathbb{K}$ is a map $\partial: \mathbb{K} \rightarrow \mathbb{K}$ 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* $\delta$ defined on $\mathbb{K}$ is a map $\delta: \mathbb{K} \rightarrow \mathbb{K}$ satisfying

\[
\delta(f + g) = \delta(f) + \delta(g) \\
\delta(fg) = \delta(f)\delta(g) \\
\delta(f) = 0 \iff f = 0
\]

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

\[
\partial\delta(y) = h \cdot \delta\partial(y)
\]

(1)
for some non-zero element $h \in \mathbb{K}$. It is easy to check that for a positive integer $s$, we have

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

A product of the form $\prod_{i=0}^{s} \delta^i(h)^{n_i}$ 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 $\Omega$, with $\Omega = \bigcup_{r \in \mathbb{N}} \Omega_r$. An element of $\Omega$ is called a word. It is clear that

$$\Omega = \{\delta^{n_0} \partial^{m_0} \cdots \delta^{n_l} \partial^{m_l}\}$$

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

$$\Theta = \{\delta^n \partial^\beta | \alpha, \beta \in \mathbb{N} \}, \quad \Theta_{<[i,j]} = \{\delta^k \partial^l | k \leq i, l \leq j, k + l < i + j \}.$$  

Note that $\Theta$ is a proper subset of $\Omega$. 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 $g_{\omega}$ is an $h$-product and $P_{\omega}$ 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 $t = i + 1$,

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

where $g$ is an $h$-product and $Q_j \in \mathbb{K}, A_j \in \Theta_{<[n_{i+1} - n_1, m_{i+1} - m_1]}$. Since $\delta^{n_1} \partial^{m_1} Q_j A_j \in \Theta_{<[n,m]}$ for any $A_j \in \Theta_{<[n_{i+1} - n_1, m_{i+1} - m_1]}$, we obtain

$$\delta^{n_1} \partial^{m_1} \left( g \delta^{n_{i+1} - n_1} \partial^{m_{i+1} - m_1} + \sum Q_j A_j \right) = \delta^{n_1} (g) \delta^{n_1} \partial^{m_1} \delta^{n_{i+1} - n_1} \partial^{m_{i+1} - m_1} + \sum Q'_k B_k,$$
where \( Q'_k \in \mathbb{K}, B_k \in \Theta_{< n,m} \). By equation (2), we have
\[
\delta^{n_1} \delta^{n-n_1} = g' \cdot \delta^{n-n_1} \delta^{m_1} + \sum Q_s C_s,
\]
where \( g' \) is an h-product and \( Q_s \in \mathbb{K}, C_s \in \Theta_{< n-n_1,m_1} \). We conclude that
\[
\delta^{n_1} \delta^{m_1} \cdots \delta^{n_{i+1}} \delta^{m_{i+1}} = g'' \cdot \delta^n \delta^m + P,
\]
where \( g'' \) is an h-product and \( P \) is in \( \mathbb{K}[\Theta_{< n,m}] \).

Let \( \mathbb{Y} = \{ y_1, \ldots, y_n \} \) be a finite number of indeterminates, considered as functions of \( x \). We denote
\[
\Omega\mathbb{Y} = \{ \omega y_i | \omega \in \Omega, y_i \in \mathbb{Y} \}
\]
\[
\Theta\mathbb{Y} = \{ \delta^d \delta^s y_i | d, s \in \mathbb{N}, y_i \in \mathbb{Y} \}.
\]
For convenience, we also denote
\[
y_{i,d,s} = \delta^d \delta^s (y_i).
\]
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 \( \{ \delta^d \delta^s P | d, s \in \mathbb{N} \} \cup \{ \delta^n \delta^m P \} \), Lemma 2.1 will imply that the saturation ideals of \( \omega P \) and \( \delta^n \delta^m P \) 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 \( \delta \) and \( \delta \). 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 \( [\mathbb{P}]_{\delta} \) for the differential ideal generated by \( \mathbb{P} \).
2.2. Admissible ordings

Consider a total ordering \( \leq \) on \( \Theta Y \). Given \( P \subseteq \mathbb{K}[\Theta Y] \), we denote by \( V_P \subseteq \Theta Y \) the set of elements of \( \Theta Y \) occurring in \( P \). For a DD-polynomial \( P \), we let \( V_P = V_P(P) \). 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

\[
\begin{align*}
A1 &: v(\theta y) < v(\delta y), \quad \text{for any } \theta y \in \Theta Y; \\
A2 &: v(\delta y) < v(\delta \theta y), \quad \text{for any } \theta y \in \Theta Y;
\end{align*}
\]

Admissible orderings exist: one example is the ordering \( \leq \), which can always be made to hold after a permutation of indexes.

An extended variable is an element of \( \Theta Y \) raised to some strictly positive power. The set of such variables will be denoted by \( (\Theta Y)^* \), and we use letters with star exponents \( v^* \) to denote extended variables. We extend the admissible ordering \( \leq \) on variables to extended variables by \( v^d \leq v^{d'} \) if and only if either \( v < v' \), or \( v = v' \) and \( d \leq d' \). 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 \( P_i \in \mathbb{K}[\Theta Y] \). 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 \( v^*(P_i) = (\delta^b \partial^c_y a_i)^{d_i} \).

Similarly, the ordering \( \leq \) on \( (\Theta Y)^* \) 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.

\[ \square \]

2.3. Pseudo-Remainder

We consider the DD-ring \( \mathbb{K}[\Theta Y] \), where \( Y = \{ y_1, \ldots, y_n \} \). Let \( Y_C = \{ y_1, \ldots, y_c \} \). For a DD-polynomial \( P \in \mathbb{K}[\Theta Y] \), we define the class of \( P \) to be the smallest \( c = \text{cls}(P) \) such that \( P \in \mathbb{K}[\Theta Y_c] \). 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 \( \text{ord}(P) = i + j \), \( \text{ord}_\theta(P, y_c) = i \), \( \text{ord}_Y(P, y_c) = j \).

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

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

(3)

\( I_P = P_t \) is called the initial of \( P \). \( \text{ideg}(P) = t \) is called the leading degree of \( P \). Applying \( \partial \) and \( \delta \) to \( P \), we have
Algorithm 1 — rprem(\(Q, P\))

\textbf{Input:} DD-polynomials \(P, Q \in \mathbb{R}\) with \(P \neq 0\).

\textbf{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 \(\omega^*\) 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 \(v_Q\).

\textbf{Lemma 2.5} Let \(P\) be of form (3). Then

\[\delta P = (\delta P_t)_{y_{c,d+1,s}} + (\delta P_{t-1})_{y_{c,d+1,s}} + \cdots + \delta P_0\]

\[\delta P = S_P y_{c,d,s+1} + R,\]

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 \(y_{c,d,s+1}\).

\textbf{Proof:} The first equation is obvious. The second one is a consequence of (2). \(\square\)

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. \(y_{c,d+k,s+1}\) 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 the \(\theta\) by

\[\theta = \delta^\alpha \delta^\beta \preceq \delta^\alpha' \delta^\beta' = \theta' \iff \alpha \leq \alpha' \land \beta \leq \beta'.\]

If \(\theta \preceq \theta'\), then we define

\[\theta'/\theta = \delta^{\alpha'-\alpha} \delta^{\beta'-\beta}\]

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

We define a partial ordering \(\leq\) 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 \(\theta'/\theta\) is not a pure difference operator. We remark that \(\leq\) is still a well-quasi-ordering.

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

\textbf{Lemma 2.6} Define

\[H_P = \{I_P^{a_0} \cdots \delta^k I_P^{a_k} S_P^{b_0} \cdots \delta^l S_P^{b_l} | a_0, \ldots, a_k, b_0, \ldots, b_l \in \mathbb{N}\}\]
and let $R = \text{rprem}(Q, P)$. Then there exists a $J \in H_P$ 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 $A \subseteq K[Y] \setminus K$ is said to be auto-reduced, if each $P \in A$ is reduced w.r.t. each DD-polynomial in $A \setminus \{P\}$. An auto-reduced set $A = \{A_1, \ldots, A_r\}$ 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 $v^*(P_i) = (\delta^b \delta^c y_{a_i})^{d_i}$ 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 $(b_i, c_i, d_i) \geq (b_j, c_j, d_j)$ 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 $\leq$. This contradicts Dickson’s Lemma. □

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

Lemma 3.2 Any descending chain $A_1 > A_2 > A_3 > \ldots$ is finite.

Proof: Assume the contrary. The first elements of the chains $A_1, A_2, \ldots$ satisfy $A_{1,1} \geq A_{2,1} \geq \cdots$. By Lemma 2.4, there exists an index $j_1$ with $A_{i,1} \sim A_{j_1,1}$ for all $i > j_1$. Similarly, there exists an index $j_2 > j_1$ with $A_{i,2} \sim A_{j_2,2}$ for all $i > j_2$. By induction, we get a sequence $j_1 < j_2 < \cdots$ with $A_{i,k} \sim A_{j_k,j}$ for all $k$ and $i > j_k$. But then $\{A_{j_1,1}, A_{j_2,2}, \ldots\}$ is an infinite auto-reduced set, which contradicts Lemma 3.1. □

Let $P$ be a set of DD-polynomials and consider the set of chains of DD-polynomials in $P$. 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 $P$.

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 $A$ is a characteristic set of $P$ and $A'$ a characteristic set of $P \cup \{P\}$ for a DD-polynomial $P$, then we have $A \succeq A'$. Moreover, if $P$ is reduced w.r.t. $A$, then $A > A'$. 

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

**Input:** A chain $A$ and a set $\mathcal{P}$ of DD-polynomials.

**Output:** The extension $A_P$ of $A$ w.r.t. $\mathcal{P}$.

1. Let $L = L_A$, $Q = A \cup \mathcal{P}$, $H = \{y_{c,d}^{(e)}e_{\omega}^{(e)}, c = 1, \ldots, n\}$, $V = \forall H \setminus L$, and $A_P = A$.

2. If there exist $\omega, \eta$ and $c$ with $\omega y_c \in V$, $\eta y_c \in L$ and $\eta \leq \omega$, then choose $\omega$ and $c$ such that $\omega y_c$ is largest for $\leq$. If there are no such $\omega, \eta$ and $c$, then return $A_P$.

3. If for all the $\theta y_c \in L$ satisfying $\theta \leq \omega$, $\omega/\theta$ is a difference operator, let $\eta$ be the largest of those $\theta$ under $\leq$, go to S4.

4. Let $A_k \in A$ such that $\eta y_c = \omega y_c$. Let $Q = (\omega/\eta)A_i$, $A_P = A_P \cup \{Q\}$, $V = V \cup (\forall Q \setminus L_{A_P})$.

Delete $\omega y_c$ from $V$ and go to S1. Since all the variables in $\forall Q \setminus L_{A_P}$ are less than $\omega y_c$, this process will terminate.

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

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

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

3.2. Extension of chains and pseudo-remainder

Let $A$ be a chain. A variable $y_{c,d,s}$ is called a principal variable of $A$ if there exists an $A \in A$ such that $v_A \leq y_{c,d,s}$. Otherwise, it is called a parametric variable of $A$. Denote the set of principal variables and the parametric variables of $A$ by $M_A$ and $P_A$ respectively. It is clear that $M_A \cup P_A = \Theta Y$.

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

\[ \forall_{\mathcal{P}} = \{y_{c,s,t} \in M_{\mathcal{A}} | \exists P \in \mathcal{P}, a, b : \deg(P, y_{c,a,b}) > 0, 1 \leq c \leq n, s \leq a, t \leq b\}, \]

\[ \ll_{\mathcal{P}} = \{y_{c,s,t} \in \mathcal{P} | \forall P \in \mathcal{P} : v_P = y_{c,s,t}\}. \]
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.
- \( L_{\mathcal{A}_\mathbb{P}} = \mathbb{V}_{\mathcal{A}_\mathbb{P}} \).
- A DD-polynomial \( P \) is reduced w.r.t. \( \mathcal{A} \) if and only if \( P \) is reduced w.r.t. \( \mathcal{A}_\mathbb{P} \) in the algebraic sense.

**Example 3.6** Consider the following chain for the ordering \( \leq_I \) from Section 2.2.

\[
\mathcal{A} = \{ A_1, A_2, A_3, A_4 \} \\
A_1 = y_{\frac{7}{3},2,3} \\
A_2 = y_{\frac{7}{3},3,2} + y_{1,1,1} \\
A_3 = y_{\frac{5}{4},5,0} + y_{1,4,1} \\
A_4 = y_{1,7,0} + y_{1,4,0}.
\]

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

\[
\mathcal{A}_P = \{ A_1, \partial A_1, \partial^2 A_1, \partial^3 A_1, \\
A_2, \partial A_2, \partial^2 A_2, \partial^3 A_2, \partial^4 A_2, \partial A_2, \partial A_2, \partial \partial^2 A_2, \partial \partial^3 A_2, \partial \partial^4 A_2, \\
A_3, \partial A_3, \partial^2 A_3, \partial^3 A_3, \partial^4 A_3, \partial^5 A_3, \partial A_3, \partial A_3, \partial \partial A_3, \partial \partial^2 A_3, \partial \partial^3 A_3, \partial \partial \partial A_3, \\
A_4, \partial A_4, \partial^2 A_4, \partial^3 A_4, \partial^4 A_4 \}.
\]

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 \( \text{ord}_4 \), which is \( A_3 \).
As a consequence, we will add $\partial^4 A_3$ to $A_P$. Note that the DD-polynomial with the largest $\text{ord}_{\delta}$ will have the smallest $\text{ord}_{\partial}$ for its leading variable.

Given $y_i, d_j, s_j \in L_A$, we define its index to be $(d_j, s_j)$. The indices for the DD-polynomials in $A_P$ 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 $A_P$.

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

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

$$r_{\text{prem}}(P, A) = \text{aprem}(P, A_P).$$

**Lemma 3.8** Let $R = r_{\text{prem}}(Q, A)$. Then $R$ is reduced w.r.t. $A$ and there exists a $J \in H_A$ such that $v_J < v_Q$ and

$$JQ \equiv R \mod [A]$$

**Proof:** This is a direct consequence of the procedure to compute $A_Q$ and $\text{r prem}$. □

The saturation ideal of $A$ is defined to be

$$\text{sat}(A) = [A] : H_A = \{ P \in \mathbb{K}[\Theta Y] \mid \exists J \in H_A : J P \in [A] \}.$$

Note that $H_A$ is closed under transforming and multiplication. Hence $\text{sat}(A)$ is a DD-ideal. It is also clear that if $r_{\text{prem}}(P, A) = 0$ then $P \in \text{sat}(A)$. Conversely, $P \in \text{sat}(A)$ generally does not imply $r_{\text{prem}}(P, A) = 0$ 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 $\mathbb{K}[\Theta Y]$ 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 $P$, let $P$ be any element in $\mathbb{K}[\Theta Y]$ with some product of positive powers of transforms of $P$ in $P$. The totality of such elements $P$ will be denoted by $P'$. Let $P_1 = [P]'$ and, continuing inductively, let $P_n = [P_{n-1}]'$ for every $n > 1$. We have $P_0 \subseteq P_1 \subseteq P_2 \subseteq \cdots$ and $\bigcup_{k \in \mathbb{N}} P_k = \{P\}$.

**Lemma 3.9** Let $P$ be any set of elements of $\mathbb{K}[\Theta Y]$ and $P$ and $Q$ any two elements of $\mathbb{K}[\Theta Y]$. If $S$ is contained in $(P \cup P)_n$ and $T$ in $(P \cup Q)_n$, $n \geq 1$, then $ST$ is contained in $(P \cup PQ)_{n+2}$.
Proof: First, let \( n = 1 \), \( S \in \langle \mathbb{P} \cup P \rangle_1 \), \( T \in \langle \mathbb{P} \cup Q \rangle_1 \). 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 \( A, \ldots, B, A', \ldots, B' \in \Theta \mathbb{P}, \omega, \ldots, \omega', \theta, \ldots, \theta' \in \Theta \) and the coefficients \( G, G' \cdots, L, L' \in \mathbb{K} \{ \Theta \mathbb{Y} \} \). Thus \( ST_\overline{} \) has an expression in which some terms are in \( \mathbb{P} \) and the others are of the type \( F \cdot \eta P \cdot \eta Q \) for some \( \eta_1, \eta_2 \in \Theta \). Denote \( \eta_1 = \delta_{\pi_1} \partial \delta_{\pi_2}, \eta_2 = \delta_{\pi_1} \partial \delta_{\pi_2} \), then by [11], Page 9, we have \( \partial \delta_{\pi_2} P \cdot \partial \delta_{\pi_2} Q \in [PQ]' \), so we have \( \partial \delta_{\pi_2} P \cdot \delta_{\pi_1} \partial \delta_{\pi_2} Q \in [PQ]_2 \). So we have \( ST_\overline{} \) is in \([\mathbb{P} \cup PQ]_2\). Some of product of powers of transforms of \( ST \) is a multiple of \( ST_\overline{} \). 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 \( ST_\overline{} \) 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 \( ST_\overline{} \) is in \([\mathbb{P} \cup PQ]_3\). This puts \( ST \) in \([\mathbb{P} \cup PQ]_4\).

The proof continues by induction. \( \square \)

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 \( \langle \mathbb{P} \cup P \rangle_n \) and in \( \langle \mathbb{P} \cup Q \rangle_n \). Then by Lemma 3.9, \( S^2 \) is in \( \langle \mathbb{P} \cup PQ \rangle_{n+2} \). Thus \( S \) is also in \( \langle \mathbb{P} \cup PQ \rangle_{n+2} \). \( \square \)

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

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

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 \( \Sigma \) 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 \( \prod_{i}(\delta_{ti} P)^{si} \in \mathbb{P}_{n-1} \), for some \( t_i, s_i \in \mathbb{N} \). Hence \( \prod_{i}(\delta_{ti} P)^{si} \in \{ Q_1, \ldots, Q_q \} \) for some \( Q_j, Q_q \in \mathbb{P}_{n-1} \). For each \( 1 \leq j \leq q \), there exists a finite subset \( \Sigma_j \) 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 \( P \in \{ \Sigma \} \). \( \square \)

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 \( m \) be any such maximal element. Clearly \( m \neq \mathbb{K} \). Choose \( P, Q \in \mathbb{K}[\Theta \mathcal{Y}] \setminus \mathbb{K} \). Then \( \{ m, P \} \) and \( \{ m, Q \} \) are finitely generated, say by \( \mathcal{P}, \mathcal{Q} \) respectively. Thus by Lemma 3.10, \( \{ m, PQ \} = \{ \mathcal{P} \} \cap \{ \mathcal{Q} \} \). By Lemma 3.11, \( PQ \notin m \), we have that \( m \) is prime.

\[ \square \]

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

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

Let \( P \) be in \( m \). We can write \( J_P P = R \mod \{ C \} \), where \( R \) is reduced w.r.t. \( C \), \( J_P \in \mathcal{H}_C \). By Lemma 3.4, \( R = 0 \). Hence \( J_P P \in \{ C \} \), whence \( \mathcal{H}_C P \in \{ C \} \). This proves that \( \mathcal{H}_C m \subseteq \{ C \} \).

Since the initials and separants of \( C \) are reduced w.r.t. \( C \), they are not in \( m \). Since \( m \) is prime, we have \( \mathcal{H}_C \notin m \). So the perfect DD-ideal \( \{ \mathcal{H}_C, m \} \) strictly contains \( m \). Therefore, \( \{ \mathcal{H}_C, m \} \) 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 \( m \cup \{ \mathcal{H}_C \} \). Hence, we can write \( \{ \mathcal{H}_C, m \} = \{ \mathcal{H}, \mathcal{P} \} \), for some \( \mathcal{P} \subseteq m \) and \( \mathcal{P} \) is a finite set. Finally, \( m \) is finitely generated, since \( m = m \cap \{ \mathcal{H}_C, m \} = m \cap \{ \mathcal{H}_C, \mathcal{P} \} = \{ \mathcal{H}_C m, \mathcal{P} \} \subseteq \{ \mathcal{C}, \mathcal{P} \} \).

\[ \square \]

4. Coherent and regular chains

A key property for a chain \( \mathcal{A} \) is that whether \( \mathcal{A} \) is the characteristic set of 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 \( \partial A_1 \) to eliminate \( y_{1,3,3} \) from \( P \), or select \( A_2 \) and use \( \partial A_2 \) 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 \( \partial A_3 \) and \( \partial A_1 \) 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 \( \text{cls}(A_1) \neq \text{cls}(A_2) \), define \( \Delta(A_1, A_2) = 0 \). If \( \text{cls}(A_1) = \text{cls}(A_2) = c \), 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 \( \theta_1 \leq \theta, \theta_2 \leq \theta \). If \( \text{deg}(((\theta/\theta_1)A_1) \geq \text{deg}((\theta/\theta_2)A_2) \), we define the \( \Delta \)-polynomial of \( A_1 \) and \( A_2 \) to be

\[ \Delta(A_1, A_2) = \text{aprem}((\theta/\theta_1)A_1, (\theta/\theta_2)A_2, \theta y_c). \]

We denote by \( \Delta(\mathcal{A}) \) the set of non-zero \( \Delta \)-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 \( P \in \Delta(\mathcal{A}) \), \( \text{rprem}(P, \mathcal{A}) = 0 \).

Let \( \mathcal{A} = A_1, \ldots, A_s \) be a chain. A linear combination \( C = \sum_{\theta \in \Theta} Q_\theta A_i \) is called canonical if \( \theta A_i \) 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 $J \in H_{\mathcal{A}}$ such that $v_J < v_{\theta A}$ and $J\theta A$ has a canonical representation:

$$J\theta A = \sum_{v_B \leq v_{\theta A}, B \in A_P} Q_B B.$$  \hspace{1cm} (5)

Proof: Let $c = \text{cls}(A)$. The DD-polynomials in $A$ with class $c$ are $A_{c,1}, \ldots, A_{c,k}$, 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 $\text{ord}_d(A_{c,k}) \leq \text{ord}_d(\theta A)$. Then the canonical polynomial corresponding to $v_{\theta A}$ must be $\bar{\theta}A_{c,k}$ for a $\bar{\theta} \in \Theta$. We will form the $\Delta$-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 $v_R < v_{\theta_i A}$. Since $\mathcal{A}$ is a coherent chain, $\text{rprem}(R, A) = \text{aprem}(R, A_R) = 0$. We have

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

where $J_2 \in H_{\mathcal{A}}$ such that $v_{J_2} < v_R < v_{\theta A}$. 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 $\theta_i \preccurlyeq \theta$. Let $\bar{\theta} = \theta / \theta_i = \delta^d \theta^g$ and $\bar{\theta} \in \Theta$ be a shuffle of $\theta_k$. Perform $\bar{\theta}$ on the above equation, by Lemma 2.1, we have

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

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

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

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

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 $J \in H_{\mathcal{A}}$ 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. \hfill $\square$
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 \( \text{asat}(\mathcal{A}) \).

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
\[
    P_p = P, P_{p-1} = \text{Resl}(P_i, A_i, y_i), i = p, \ldots, 1
\]
and define \( \text{Resl}(P, \mathcal{A}) = P_0 \), where \( \text{Resl}(P, Q, y) \) is the resultant of \( P \) and \( Q \) w.r.t. \( y \). We assume that if \( y \) does not appear in \( P \), \( \text{Resl}(P, Q, y) = P \). It is clear that \( \text{Resl}(P, \mathcal{A}) \in \mathbb{K}[u] \).

A polynomial \( P \) is said to be invertible w.r.t. a chain \( \mathcal{A} \) if \( \text{Resl}(P, \mathcal{A}) \neq 0 \). \( \mathcal{A} = A_1, \ldots, A_p \) is called regular if the initials of \( A_i \) are invertible w.r.t. \( \mathcal{A} \). \( \mathcal{A} \) is called saturated 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 \( \text{asat}(\mathcal{A}) = (\mathcal{A}) : I_{\mathcal{A}} \) 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 saturated 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 \( H_{\mathcal{A}} \) is invertible w.r.t. \( \mathcal{A} \).

**Lemma 4.7** If a chain \( \mathcal{A} \) is a characteristic set of \( \text{sat}(\mathcal{A}) \), 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 \( \theta y_j \) such that \( \theta y_j \) is of lower or equal ordering than a \( \theta y_j \) 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 \( \theta y_i \), which is of higher ordering than those in \( W \). As a consequence, \( Q \) is also reduced w.r.t. \( \mathcal{A} \). Since \( Q \in (\mathcal{B}) : I_{\mathcal{B}} \subseteq \text{sat}(\mathcal{A}) \) and \( \mathcal{A} \) is the characteristic set of \( \text{sat}(\mathcal{A}) \), 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 $R \in \text{sat}(\mathcal{A})$, then $R = 0$, or equivalently, $\mathcal{A}$ is the characteristic set of $\text{sat}(\mathcal{A})$.

Proof: Let $\mathcal{A} = A_1, A_2, \ldots, A_l$. Since $R \in \text{sat}(\mathcal{A})$, there is a $J_1 \in H_{\mathcal{A}}$ such that $J_1 \cdot R \equiv 0 \mod [A]$. 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

$$\bar{J}_1 \cdot J_1 = N + \sum_{v_B \leq v_{J_1}, B \in A_{J_1}} Q_B B$$

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

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

Or equivalently,

$$N \cdot R = \sum_{i,j} g_{i,j} \theta_{i,j} A_j.$$  \hspace{1cm} (6)

Since $\mathcal{A}$ is a coherent chain, by Lemma 4.2, there is a $J_2 \in H_{\mathcal{A}}$ 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

$$J_2 \cdot N \cdot R = \sum_{i,j} g_{i,j} \rho_{i,j} A_j,$$  \hspace{1cm} (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 $v_{\rho_{A_b}} = \max \{v_{\rho_{i,j}} A_j\}$ and $\rho_{A_b} = I_b \cdot v_{\rho_{A_b}} + R_b$. Substituting $v_{\rho_{A_b}}$ by $-R_b$ in (7), the left side keeps unchanged since $v_{J_2} < v_{\rho_{A_b}}$, $N$ is free of $v_{\rho_{A_b}}$ and $\deg(R, v_{\rho_{A_b}}) < \deg(\rho_{A_b}, v_{\rho_{A_b}})$. In the right side, $\rho_{A_b}$ 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:

$$I_b^I \cdot J_2 \cdot N \cdot R = \sum_{i,j} f_{i,j} \tau_{i,j} A_j.$$  \hspace{1cm} (8)

Note that in the right side of (8), the highest ordering of $\tau_{i,j} A_j$ and $I_b^I \cdot J_2$ are less than $v_{\rho_{A_b}}$ and $I_b^I \cdot J_2$ 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 $v_{\rho_{A_b}}$. 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 $\text{sat}(\mathcal{A})$. \hfill $\square$

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 $A = \{y_{1,0}^2 - 1, (y_{1,0} - 1)y_{2,0}^2 + 1\}$ in $\mathbb{K}\{y_1, y_2\}$. $A$ is coherent and $y_{1,0} + 1$ is reduced w.r.t. $A$. $y_{1,0} + 1 \in \text{sat}(A)$, because $J = I_{(y_{1,0} - 1)y_{2,0}^2 + 1} = y_{1,0} - 1$ and $\delta(J)(y_{1,0} + 1) = y_{1,0}^2 - 1 \in [A]$. On the other hand, $y_{1,1,0} + 1 \notin \text{asat}(A)$.

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

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

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

As a Corollary, we have

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

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

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

Theorem 4.13 If $A$ is a coherent and regular chain, then

$$\text{sat}(A) = \bigcup_{P \in \mathbb{K}\{Y\}} (A_P) : H_{A_P} = \bigcup_{P \in \mathbb{K}\{Y\}} (A_P) : I_{A_P}.$$ 

Proof: It is easy to see that $\text{sat}(A) = [A] : H_A = \bigcup_{P \in \mathbb{K}\{Y\}} (A_P) : H_{A_P}$. Let $f \in \text{sat}(A)$. Since $A$ is coherent and regular, $A$ is the characteristic set of $\text{sat}(A)$. Then $\text{rprem}(P, A) = 0$, or $\text{prem}(f, A_P) = 0$. We have $P \in (A_P) : H_{A_P}$. Hence $\text{sat}(A) \subseteq \bigcup_{P \in \mathbb{K}\{Y\}} (A_P) : H_{A_P}$. Since $A$ is regular, $A_P$ is saturated, by Lemma 4.6, $(A_P) : I_{A_P} = (A_P) : H_{A_P}$, 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 separators 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, \( y_{i,d_i,s_i} \leq_l y_{j,d_j,s_j} \) iff \((i,d_i,s_i)\) is less than \((j,d_j,s_j)\) according to the lexicographical ordering.

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

\[
A = \left\{ A_{1,1}(U, y_1), \ldots, A_{1,k_1}(U, y_1) \right\} \ldots \left\{ A_{p,1}(U, y_1, \ldots, y_p), \ldots, A_{p,k_p}(U, y_1, \ldots, y_p) \right\}
\]

(9)

where \( U = \{u_1, \ldots, u_q\} \) and \( p+q = n \). For any \( i \), we have \( \text{cls}(A_{i,j}) = \text{cls}(A_{i,k}) \). 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 \( \text{IND}_i \). If we arrange \( \text{IND}_i = \{(a_1, b_1), \ldots, (a_s, b_s)\} \) 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 \( a_1 < a_{i+1} \). 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 \( d_{(a_j,b_j)} < d_{(a_{j+1},b_{j+1})} \). \( \square \)

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

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

For any DD-polynomial set \( \mathcal{P} \), the index set of the DD-polynomials in \( A_\mathcal{P} \) with class \( i \) is of the following form:

\[
(a, s_1) \quad (a, s_1+1) \quad \cdots \quad (a, s_1+l_1) \\
(a+1, s_2) \quad (a+1, s_2+1) \quad \cdots \quad (a+1, s_2+l_2) \\
\cdots \\
(a+r, s_r) \quad (a+r, s_r+1) \quad \cdots \quad (a+r, s_r+l_r)
\]

(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 \( A_\mathcal{P} \) (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 $B$ is called irreducible if $B$ is regular and there exists no polynomials $P$ and $Q$ which are reduced w.r.t. $B$ and $PQ \in \text{asat}(B)$ [11, 16].

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

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

The above lemma was extended to the case of ordinary differential polynomials. Let $A$ be a differential triangular set $A$ [12, 17]. The differential saturation ideal of $A$ is defined to be $\text{dsat}(A) = \left[ A \right]_H A$ where $\left[ A \right]_H$ is the differential ideal generated by $A$.

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

5.2. Proper Irreducible Chain

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

![Fig. 3. The indices of chain $A^*$](image)

A chain $A$ is said to be proper irreducible if

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

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

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

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

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

From the definition of the invertibility, it is clear that $\delta P$ is invertible w.r.t. $A_{\delta P}$ iff $\delta P$ is invertible w.r.t. $C$. If $A \in \mathbb{H}$, there are two cases: $A \in A^{*}$ or $A = \delta^* A_0, A_0 \in A^{*}$. If $A \in A^{*}$, then by Proposition 3.5, starting from $A$, all the DD-polynomials constructed in the above procedure are in $A^{*}$. Let $A = \delta^* A_0, A_0 \in A^{*}$. Due to the selection of the ordering $\leq_{1}$, for any class $c$, $d^{(c)}_{\delta(A)} \leq d^{(c)}_{A}$. Therefore, starting from $A$, all the DD-polynomials constructed in the above procedure are in $A^{*} \cup \mathbb{H}_1$ where $\mathbb{H}_1$ consists of DD-polynomials of the form $\delta^* A_0$ for $A_0 \in A^{*}$. Since all DD-polynomials in $\mathbb{H}_1$ are linear in their leaders with their initials in $H_{A^{*}}$ and $A^{*}$ is irreducible, we know that $C$ is an irreducible triangular set and $\text{asat}(C) \subseteq \text{dsat}(A^{*})$.

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

The following example shows that if we replace $\text{dsat}$ by $\text{asat}$ 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 $A = A_1, A_2$. It is easy to see that $A^{*} = A_1, A_2$ is an algebraic irreducible triangular set. Let $Q = y_{2,0,0} - y_{1,0,2} \in K[P_{A}]$. We have $\delta^* Q = A_2 - \delta^* A_1 \in \text{sat}(A)$, but $Q \notin \text{sat}(A)$.

The following is a key property for proper irreducible chains.

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

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

We first prove the following result.

If $J \in H_{A}$ and $v_J < v_{\delta P}$, then $J$ is invertible w.r.t. $A$. \hfill (11)

Let $I$ be the set of the initials and separants of the DD-polynomials in $A^{*}$. By Lemma 5.3, any element in $I$ is invertible w.r.t. $A^{*}$ and hence invertible w.r.t. $A$. Let $I_i = \delta^i I$ for $i \geq 0$. If $J \in I_1$ and $v_J < v_{\delta P}$, then $J = \delta L, L \in I$, and $v_L < v_P$. By the induction hypothesis,
$J$ is invertible w.r.t. $A$. Repeating the above procedure, we can prove that if $J \in I$, and $v_J \leq v_{\delta P}$, then $J$ is invertible $A$. Since $H_A$ is the set of products of elements in all $I$, each $J \in H_A$ satisfying $v_J \leq v_{\delta P}$ is invertible w.r.t. $A$.

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

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

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

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 $c$, $s^{(c)}_{\delta G} \leq s^{(c)}_{\delta P}$, $q^{(c)}_{\delta G} \leq q^{(c)}_{\delta P}$. Then $V_{\delta G} \subseteq L_{\mathcal{A}_P} \subseteq L_{\mathcal{A}_{\delta P}}$. By Lemma 5.5, $\delta G$ is invertible w.r.t. $\mathcal{A}_{\delta G}$. From $v_G \leq v_P$ and $V_{\delta G} \subseteq L_{\mathcal{A}_{\delta P}}$, $\delta G$ is invertible w.r.t. $\mathcal{B}$.

Performing the transforming operator on (12), we have

$$\delta Q \cdot \delta P = \delta G + \sum_{A \in \mathcal{A}_P, v_A \leq v_P} \delta B_A \delta A. \quad (13)$$

For any $\delta A$ 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 $J \in H_A$, $v_J < l v_{\delta A} \leq v_{\delta P}$ such that $J \delta A$ has a canonical representation. Then, there exists a $J \in H_A$, $v_J < l v_{\delta P}$ and a DD-polynomial $R$ such that

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

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

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

So there exists a DD-polynomial $R_1$ such that

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

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

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

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 $I_{B_1} \in H_A$ 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 $v_{B_1}$ by $U_1/I_{B_1}$, we have

$$Q_1' \delta P = I_{B_1}^{k_1} P_1 + \sum_{A \in \mathcal{A}_{\delta P}, v_A \leq v_P} E_A A + \sum_{A \in \mathcal{A}_{\delta P}, A \in \mathcal{A}_{R_1}, v_B \leq v_{B_1}} E_B B. \quad (16)$$
A coherent and proper irreducible chain is regular. Let $A$ w.r.t. equation (18) as two parts: $B$ index of a row in the index diagram for $r_{prem(A)}$. By Theorem 4.10, So we can assume that $A$ are invertible w.r.t. set, by Lemma 5.3, $\delta P$ is invertible w.r.t. $v$. Proof: For any $A \in A$, the third part of equation (14), $v_B < v_{B_1}$, they do not change under the above substitution.

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

$$Q_2 \delta P = P_2 + \sum_{A \in A_{v_1}, v_A \leq v_2, B} F_A A + \sum_{B \notin A_{v_1}, B \in A_{v_2}, v_B < v_{B_1} \leq v_2} F_B B. \quad (17)$$

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 $R \in K[\mathbb{P}_A]$ such that

$$H \delta P = R + \sum_{A \in A_{v_1}, v_A \leq v_2} Q_A A = R + \sum_{A \in A_{v_1}} Q_A A.$$ 

Since $B$ is a regular triangular set, by Lemma 4.5, $\delta P$ is invertible w.r.t. $B \subseteq A_{v_1}$. That is $\delta P$ is invertible w.r.t. $A$. □

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 $A = A_1, \ldots, A_m, I_j = I(A_j)$, and $S_j = S(A_j)$. Since $A$ is an irreducible triangular set, by Lemma 5.3, $I_j$ and $S_j$ are invertible w.r.t. $A$ and hence invertible w.r.t. $A$. By Lemma 5.6, all $\delta I_j, \delta S_j$ are invertible w.r.t. $A$. As a consequence, the products of $\delta I_j, \delta S_j$ are invertible w.r.t. $A$ and $A$ is regular. □

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

**Proof:** For any $\delta P \in \text{sat}(A)$, if $P \notin \text{sat}(A)$. Let $R = \text{rprem}(P, A) \neq 0$. Then $R \in \text{sat}(A)$. So we can assume that $\delta P \in \text{sat}(A)$ and $P$ is reduced w.r.t. $A$. By Theorem 5.7, $A$ is regular, by Theorem 4.10, $A$ is the characteristic set of $\text{sat}(A)$. Since $\delta P \in \text{sat}(A)$ we have $\text{rprem}(\delta P, A) = 0$. So there exists a $J \in I_{A_{v_1}}$, such that $J\delta P \in (A_{v_1})$ and $J$ is invertible w.r.t. $A_{v_1}$. So there exists a nonzero $G \in K[\mathbb{P}_A]$, such that

$$G \delta P = \sum_{A \in A_{v_1}} B_A A. \quad (18)$$

Let $C = A_{v_1} \cap \{\delta^i \delta^s A \mid \delta^i A \in A\}$. We have $|C| \subseteq \text{dsat}(A)$. Since each DD-polynomial $A \in A_{v_1} \setminus C$ must be the transforms for a DD-polynomial $B$ which corresponds to the last index of a row in the index diagram for $C$, the leading degree of $A$ is the same as that of $B$. As a consequence, $\delta P$ is reduced w.r.t. $A_{v_1} \setminus C$. We can write the right hand side of the equation (18) as two parts:

$$G \delta P = \sum_{A \in C} D_A A + \sum_{B \in A_{v_1} \setminus C} D_B B.$$
Let $B = I_B v_B^k - U$, where $I_B \in H_A$ is the initial of $B$. Replacing $v_B^k$ by $U/I_B$, we have

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

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

**Example 5.9** Consider $A = \{A_1 = y_1^2 + t, A_2 = x_2^2 y_0^2 + t + k\}$ from [5] in $K\{y_1, y_2\}$ where $K$ is $Q(t)$ with the difference operator $\delta t = t + 1$ and $k$ is a positive integer. $A^* = \{A_1, A_2\}$. If $k > 1$, $A$ is proper irreducible. But $\text{sat}(A)$ is not prime, because $A_2 - \delta^k(A_1) = (y_2^2 - y_1)(y_2 + k)$.

A proper irreducible chain $A$ is said to be **strong irreducible** if for any DD-polynomial $P \not\in A_P$ 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 $A$ be a coherent and strong irreducible chain. Then $\text{sat}(A)$ is a reflexive prime ideal. On the other side, if $I$ is a reflexive prime ideal and $A$ the characteristic set for $I$, then $I = \text{sat}(A)$ and $A$ is a coherent and strong irreducible chain.

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

$\Leftarrow$ Since $A$ is the characteristic set of $I$, by Theorem 4.10, $A$ is coherent, regular, and $I \subseteq \text{sat}(A)$. On the other hand, for $P \in \text{sat}(A)$, there exists a $J \in H_A$, such that $JP \in [A]$. Since $I$ is a reflexive prime ideal, the initials and separators of $A$ are not in $I$, so are their transforms. Then, we have $P \in I$, and hence $I = \text{sat}(A)$. For any DD-polynomial $P$, $A_P$ is an irreducible triangular set. Otherwise there exist DD-polynomials $G, H$, such that $GH \in \text{asat}(A_P) \subseteq \text{sat}(A)$, $G, H$ are reduced w.r.t. $A_P$. Hence $G, H$ are reduced w.r.t. $A$. As a consequence, $G, H \notin I = \text{sat}(A)$ but $GH \in I$, which contradicts to the fact that $I$ is a prime ideal. If $\delta P \in \text{dsat}(A^*)$, we have $\delta P \in \text{sat}(A^*) = I$, and then $P \in \text{sat}(A)$. Since $A$ is coherent and regular, we have $P \in \text{asat}(A_P)$. Since $A^*$ is irreducible, $\text{dsat}(A^*)$ is a prime differential ideal. Without loss of generality, we may assume that $d^{(c)}_{\delta P} \leq d^{(c)}_A$ for all $c$. As a consequence $A_P \subseteq \text{dsat}(A^*)$ and $P \in \text{asat}(A_P) \subseteq \text{dsat}(A^*)$. \qed
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 $A$ is called a Wu characteristic set of a set $P$ of DD-polynomials if $A \subseteq [P]$ and for all $P \in P$, rprem$(P, A) = 0$.

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

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

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

**Lemma 6.2** Let $A$ be a Wu characteristic set of a finite set $P$. If $A$ is not a proper irreducible chain, then we can find $P_1, P_2, \ldots, P_h$ which are reduced w.r.t. $A$ such that

$$\text{Zero}(P) = \bigcup_{i=1}^h \text{Zero}(P \cup A \cup \{P_i\}) \bigcup \bigcup_{i=1}^k \text{Zero}(P \cup A \cup \{I_i\}) \bigcup \bigcup_{i=1}^k \text{Zero}(P \cup A \cup \{S_i\})$$

where $I_i, S_i$ are the initials and separatants of the DD-polynomials in $A$.

**Proof:** Denote $B = A^* = B_1, \ldots, B_p$. Then the initials of $B$ are the initials and separatants of $A$ and their transforms. First, if $A^*$ 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. $A^*$ such that

$$P = \prod_{i=1}^p I_i^{p_i} P_1^{i_1} \ldots P_h^{i_h} = \sum_{i=1}^{k+1} g_i B_i,$$

where $I_i$ is the initial of $B_i$. Since $A$ is a Wu characteristic set of $P$, $f \in [P]$. Then Zero$(P) =$ Zero$(P \cup \{P\}) = \bigcup_{i=1}^p \text{Zero}(P, P_i) \bigcup \bigcup_{i=1}^h \text{Zero}(P, I_i)$. If $I_i$ is the initial of $\delta^d A$ for some $A \in A$, then Zero$(P, I_i) =$ Zero$(P, A)$. If $I_i$ is the initial of $\delta^d \overline{A}$ for some $A \in A$, then Zero$(P, I_i) =$ Zero$(P, S_A)$. In other words, we need only to include the initials and separatants of the DD-polynomials in $A$.

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

$$P_1 = \prod_{i=1}^p I_i^{p_i} S_i^{m_i} g - \sum_{i,j} g_{i,j} \delta^j B_i.$$
Algorithm 3 — ZDT($\mathbb{P}$)

Input: A finite set $\mathbb{P}$ of DD-polynomials.
Output: $W = \{A_1, \ldots, A_k\}$ such that $A_i$ is a coherent and proper irreducible chain and $\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \text{Zero}(<sat(A_i)>)$.

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

/* $C.S(\mathbb{P})$ gives the characteristic set of $\mathbb{P}$. Since $\mathbb{P}$ is finite, it is easy to find $C.S(\mathbb{P})$. */
Algorithm 4 — ProIrr(\(A\))

Input: A coherent chain \(A\) of the form (9).

Output: 
- (true, \(\emptyset\)), if \(A\) is proper irreducible.
- (false, \(\overline{P}\)), otherwise, where \(\overline{P}\) is the set of DD-polynomials mentioned in Lemma 6.2.

If \(A^*\) is algebraic irreducible then

\[
G := \text{DCS}(A^*) \quad */\parsestyle{*/}
\]

- \(G_1 := G \cap \mathbb{K}[U_1, Y_1]\) where \(U_1, Y_1\) are the variables in \(G\), except for those \(u_{i,0,j}, y_{i,0,k}\) with zero ord.<br>
- \(G_1 := \delta^{-r}G_1\), where \(r\) is the largest \(s\), such that \(\delta^{-s}\) is a DD-polynomial.

If \(\text{rprem}(g, A^*) = 0\) for all \(g \in G_1\), then return (true, \(\emptyset\)).
Else return (false, \(\{\text{rprem}(g, A^*) \neq 0 \mid g \in G_1\}\)).
Else

Let \(\overline{P}\) be the set of DD-polynomials in (19).
Return (false, \(\overline{P}\))

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

If \(B^*\) is proper irreducible, then test is true and \(\overline{P} = \emptyset\); else test is false, \(\overline{P}\) 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

\[
\text{Zero}(\text{dsat}(A)/J) = \text{Zero}(A/J) = \bigcup_i \text{Zero}(\text{dsat}(A_i)/J).
\] (21)

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

Algorithm 5 — DCS(\(A\))

Input: \(A\) an irreducible differential triangular set in \(\mathbb{K}\{u, y\}\).

Output: A differential characteristic set \(B\) of \(\text{dsat}(A)\) under the variable ordering \(y_{c_{1,0,i}} > y_{c_{2,0,j}}\) for any \(k \neq 0\).

Let \(J\) be the product of the initials and separants of \(A\).
Compute a zero decomposition \(\text{Zero}(A/J) = \bigcup_i \text{Zero}(\text{dsat}(A_i)/J)\) with method from [16],
where \(A_i\) are irreducible differential chains.
Find a \(k\) such that \(\text{dprem}(P, A) = 0\) for all \(P \in A_k\).
Return \(A_k\).
$P \in \text{dsat}(A_k)$, there exists a $J_1 \in H_{A_k}$ such that $J_1 P \in [A_k]$. We say that $J_1 \not\in \text{dsat}(A)$. Otherwise, $J_1 \in \text{dsat}(A) \subseteq \text{dsat}(A_k)$, a contradiction. Since $\text{dprem}(P, A) = 0$ for all $P \in A_k$, there exists a $J_2 \in H_{A}$ such that $J_1 J_2 P \in [A]$. Since $J_1 J_2 \not\in \text{dsat}(A)$, we have $P \in \text{dsat}(A)$. So $\text{dsat}(A) = \text{dsat}(A_k)$.

**Lemma 6.5** Algorithm ProIrr is valid.

**Proof:** If ProIrr$(A)$ returns $(true, \emptyset)$, we will show that for any $\delta P \in \text{dsat}(A^*)$, $P \in \text{dsat}(A^*)$. Since $\text{dsat}(A^*) = \text{dsat}(A_k)$, where $A_k$ is obtained from DCS$(A^*)$, we have $\delta P \in \text{dsat}(A_k)$. Since $A_k$ is an irreducible differential chain, $\text{dprem}(\delta P, A_k) = 0$. We denote $G_1 = A_k \cap \mathbb{K}[U_1, Y_1], G_0 = \delta^{-1}G_1$, where $\mathbb{K}[U_1, Y_1]$ is described in algorithm ProIrr. Then $\text{dprem}(\delta P, A_k) = \text{dprem}(\delta P, G_1) = 0$. So there exists a $J \in G_1$, such that $J^\delta P = \sum_{i \in \mathbb{N}, B \in G_1} Q_{i,B} d^i B$, where $J, B, Q_{i,B} \in \mathbb{K}[U_1, Y_1]$. Perform $\delta^{-1}$ on this equation, we have $\delta^{-1}J P \in [G_0]^\delta$. Since for any $G \in G_0$, $d^{(c)}_{G} \leq d^{(c)}_{A^*}$ for all $c$, we have $A_G \subseteq [A^*]^\delta$ and $\text{rprem}(G, A) = \text{aprem}(G, A_G) = \text{dprem}(G, A^*) = 0$. Then we have $(\delta^{-1}J P) \in \text{dsat}(A^*)$.

**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 $A = A_1, A_2$. Then $A$ is already a coherent chain and algorithm ZDT will call ProIrr$(A)$ directly. In the algorithm ProIrr, since $A^* = A_1, A_2$ is an algebraic irreducible triangular set, algorithm DCS$(A^*)$ 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

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

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 $G_1 = \delta^{-2}\{A_3\} = \{A_1 = y_{2,0.0} - y_{1,0.2}\}$. Algorithm ProIrr returns $(false, \{A_3\})$. Now we back to algorithm ZDT with input $\{A_1, A_2, A_4\}$. Since $B = A_1, A_4$ is a coherent and proper irreducible chain, the algorithm returns $B$ and we have $\text{Zero}(A) = \text{Zero}(\text{sat}(B)) = \text{Zero}(B)$.

**References**


