A Characteristic Set Method For Ordinary Difference Polynomial Systems *

XIAO-SHAN GAO, YONG LUO, AND CHUNMING YUAN

Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS, Academia Sinica, Beijing, 100080, China

Abstract
We prove several basic properties for difference ascending chains including a necessary and sufficient condition for an ascending chain to be the characteristic set of its saturation ideal and a necessary and sufficient condition for an ascending chain to be the characteristic set of a reflexive prime ideal. Based on these properties, we propose an algorithm to decompose the zero set of a finite set of difference polynomials into the union of zero sets of certain ascending chains. This decomposition algorithm is implemented and used to solve the perfect ideal membership problem and to prove certain difference identities automatically.

Keywords: difference polynomial, ascending chain, characteristic set, coherence, irreducibility, zero decomposition theorem, automated theorem proving.

1. Introduction
A basic idea to deal with a system of algebraic or differential equations is to decompose its zero set into the union of the zero sets of algebraic or differential equations in certain triangular form, or to decompose the radical ideal generated by these equations into the intersection of prime or radical ideals represented by their characteristic sets. The theory of the characteristic set method was established by Ritt in the 1930s (19). The method is further extended by Kolchin, Rosenfeld, Seidenberg and other people (13; 21; 22). But, the study of the algorithmic aspect of the characteristic set method is in stagnation for quite a long time until Wu’s work appeared in the late 1970s. Since then, theories and algorithms of the characteristics set methods were revived. In (25; 26; 27), Wu

*Partially supported by a National Key Basic Research Project of China and by a USA NSF grant CCR-0201253.
introduced methods to decompose the zero set of a finitely generated polynomial or differential polynomial system into the union of quasi varieties represented by triangular sets. Aubry et al., Kalkbrener, Lazard, Zhang-Yang proposed decomposition methods without using the factorization of polynomials over algebraic extension fields (1; 12; 14; 29). The decomposition into simple systems was proposed by Wang (24). The decomposition into unmixed varieties was proposed by Bouziane et al and Gao-Chou (3; 10). The concepts of invertibility, first introduced by Lazard (14), was studied in detail by Kandry-Rody et al. and played an important role in (3). Efficient algorithms for decomposing differential polynomial systems were proposed in (2; 4; 11; 15; 18). Lazard’s Lemma plays an essential role in (2). On the complexity issues, Gallo and Mishra gave an upper bound for the degrees of the polynomials in the characteristic set of an ideal (9). Dahan and Schost proved that the height of the triangular set for a zero dimensional variety could be linear with respect to the height of the variety, which shows that triangular sets provide an efficient representation tool for varieties.

The notion of characteristic set (or basic set as named in (20)) for difference polynomial systems was also proposed by Ritt (20). The general theory of difference algebra was established mainly by Cohn and his students (6). Cohn also introduced the theory of characteristic sequence, which plays an important part in the theoretical study, but is not an algorithm in the general case (6; 7). More recently, elimination algorithms for linear difference or differential-difference operators are extensively studied (5; 16; 23; 28). But, we are not aware the existence for a zero decomposition algorithm for non-linear difference polynomial systems based on the characteristic set method.

In this paper, we will establish a characteristic set method for non-linear ordinary difference polynomial systems. We show that this method can be used to solve some of important problems in difference algebra, like the intrinsic description of reflexive prime ideals, the perfect ideal membership problem, finding the dimension and order of prime ideals, and automated proving of theorems about difference polynomials. The major difference between the differential case and the difference case is that the differentiation of a differential polynomial is always linear in its leading variable and this property is not true anymore in the difference case. This makes some of the key tools used in the algebraic and differential cases not available anymore in the difference case. For instance, Rosenfeld’s lemma and Lazard’s lemma are not true in difference case. As a consequence, we need to introduce new concepts and to develop new techniques.

We first consider the following question: “Let A be a difference ascending chain. Under what condition A is a characteristic set of its saturation ideal?” In the algebraic case, Aubry et al. proved that a sufficient and necessary condition for this to be valid is that A is regular (1). This result is extended to the differential cases by Kandry-Rody et al. (3). In order to solve this problem in difference case, we introduce two new properties for difference ascending chains. First, the concept of coherent ascending chain is introduced. In the differential
case, the coherent conditions are needed only in the partial differential case. But, in difference case, this property is needed even in the ordinary difference case. We prove that any element of the saturation ideal of a coherent ascending chain has a normal representation. Second, we introduce the concept of regular difference ascending chains. With these concepts, we proved that a difference ascending chain $\mathcal{A}$ is a characteristic set of its saturation ideal iff $\mathcal{A}$ is coherent and regular.

A new type of strong irreducibility is introduced. We prove that a sufficient and necessary condition for an ascending chain $\mathcal{A}$ to be the characteristic set of a reflexive prime ideal is that $\mathcal{A}$ is coherent and strong irreducible. In (6), Cohn also gave a necessary and sufficient condition for a reflexive prime ideal in terms of characteristic sequences. The condition given in this paper is intrinsic, that is, it only involves properties of the ascending chain itself, while the one in (6) does not have this property. We also show that the dimension and order of a reflexive prime ideal can be obtained directly from its characteristic set.

There is no direct method to check whether an ascending chain is regular. In order to develop an algorithm, we give a constructive criterion for the regularity test. This new criterion is called proper irreducibility. We proved that if an ascending chain is proper irreducible, then it is a regular chain and its saturation ideal has at least one solution over an extension field.

Based on the properties of ascending chains, we propose an algorithm which can be used to decompose the zero set of a finitely generated difference polynomials set into the union of the zero sets of the saturation ideals of coherent and proper irreducible ascending chains. As applications of the decomposition algorithm, we could solve the perfect ideal membership problem for difference polynomial systems and prove theorems which can be represented by difference polynomials automatically. This method to check the perfect ideal membership problem is different from the one proposed in (6). The algorithm is implemented in Maple and is used to prove certain difference identities.

The rest of this paper is organized as follows. In Section 2, we introduce some notations and preliminary results. In Section 3, the concepts of coherent and regular ascending chains are introduced. In Section 4, the concepts of strong and proper irreducible ascending chains are introduced. In Section 5, the algorithm of zero decomposition is introduced. In Section 6, conclusions are presented.

2. Preliminaries

We will introduce the notions and preliminary properties needed in this paper. Details on these concepts can be found in (6; 20).

2.1. Difference fields, difference polynomials, and difference ideals

A difference field $\mathcal{F}$ is a field with a unitary operation $\delta$ satisfying: for any $a, b \in \mathcal{F}$, $\delta(a + b) = \delta a + \delta b$, $\delta(ab) = \delta a \cdot \delta b$, and $\delta a = 0$ iff $a = 0$. Here, $\delta$ is
called the \textit{transforming operator} of $\mathcal{F}$. If $a \in \mathcal{F}$, $\delta a$ is called the transform of $a$. If $\delta^{-1} a$ is defined for all $a \in \mathcal{F}$, we say that $\mathcal{F}$ is \textit{inversive}. Every difference field has an inversive closure (6). In this paper, all difference fields are assumed to be inversive and of characteristic zero.

As an example, let $\mathcal{K} = \mathbb{Q}(x)$ be the set of rational functions in variable $x$ and with rational numbers as coefficients. Let $\delta$ be the mapping: $\delta f(x) = f(x+1)$, $f \in \mathcal{K}$. Then $\mathcal{K}$ is a difference field with transforming operator $\delta$. This is an inversive field. In all the examples in this paper, $\mathcal{K}$ is assumed to be this difference field.

Let $\mathcal{Y} = \{y_1, y_2, \ldots, y_n\}$ be indeterminants. Then $\mathcal{R} = \mathcal{K}\{\mathcal{Y}\}$ is called an $n$-fold difference polynomial ring over $\mathcal{K}$. Any difference polynomial $P$ (abbr. r-pol) in the ring $\mathcal{K}\{\mathcal{Y}\}$ is an ordinary polynomial in variables $\delta^k y_j (k = 0, 1, 2, \ldots, j = 1, \ldots, n)$. For convenience, we also denote $\delta^k y_j$ by $y_j(x+k)$.

Let $P \in \mathcal{K}\{\mathcal{Y}\}$. The class of $P$, denoted by $\text{cls}(P)$, is the least $p$ such that $P \in \mathcal{K}\{y_1, \ldots, y_p\}$. If $P \in \mathcal{K}$, we set $\text{cls}(P) = 0$. The \textit{order} of $P$ w.r.t. $y_i$, denoted by $\text{ord}(P, y_i)$, is the largest $j$ such that $y_i(x+j)$ appears in $P$. When $y_i$ does not occur in $P$, we set $\text{ord}(P, y_i) = 0$. If $\text{cls}(P) = p$ and $\text{ord}(P, y_p) = q$, we called $y_p$ the \textit{leading variable} and $y_p(x+q)$ the \textit{lead} of $P$, denoted as $\text{lvar}(P)$ and $\text{lead}(P)$, respectively. The leading coefficient of $P$ as a univariate polynomial in $\text{lead}(P)$ is called the \textit{initial} of $P$, and is denoted as $\text{init}(P)$.

An r-pol $P_1$ has \textit{higher rank} than an r-pol $P_2$, denoted as $P_1 \succ P_2$, if

i). $\text{cls}(P_1) > \text{cls}(P_2)$, or

ii). $c = \text{cls}(P_1) = \text{cls}(P_2)$ and $\text{ord}(P_1, y_c) > \text{ord}(P_2, y_c)$

iii). $c = \text{cls}(P_1) = \text{cls}(P_2)$, $o = \text{ord}(P_1, y_c) = \text{ord}(P_2, y_c)$, and $\text{deg}(P_1, y_c(x+o)) > \text{deg}(P_2, y_c(x+o))$.

If no one has higher rank than the other for two r-pols, they are said to have the same rank, denoted as $P_1 \sim P_2$. We use $P_1 \succeq P_2$ to denote the fact that either $P_1 \succ P_2$ or $P_1 \sim P_2$. It is easy to see that $\succeq$ is a total order on $\mathcal{R}$.

An $n$-tuple over $\mathcal{K}$ is of the form $\mathbf{a} = (a_1, \ldots, a_n)$, where the $a_i$ are selected from some difference extension field of $\mathcal{K}$. Let $P \in \mathcal{K}\{\mathcal{Y}\}$. To substitute an n-tuple $\mathbf{a}$ into $P$ means to replace each of the $y_i(x+j)$ occurring in $P$ with $\delta^j a_i$. Let $\mathbb{P}$ be a set of r-pols in $\mathcal{K}\{\mathcal{Y}\}$. An $n$-tuple over $\mathcal{K}$ is called a \textit{solution} of the equation set $\mathbb{P} = 0$ if the result of substituting the n-tuple into each r-pol of $\mathbb{P}$ is zero. Let

$$\text{Zero}(\mathbb{P}) = \{n$-tuples $\mathbf{a}$, s.t. $P(\mathbf{a}) = 0, \forall P \in \mathbb{P}\}.$$ 

It is easy to check that $\text{Zero}(P) = \text{Zero}(\delta P)$. For instance, let $P = y(x+1)y(x)+y(x+1) - y(x)$. Then $y = \frac{1}{x+c(x)}$ is a solution of $P = 0$, where $c(x)$ is any function satisfying $c(x+1) = c(x)$.

A \textit{difference ideal} is a subset $\mathcal{I}$ of $\mathcal{R} = \mathcal{K}\{\mathcal{Y}\}$, which is an algebraic ideal in $\mathcal{R}$ and is closed under $\delta$. Let $\mathbb{P}$ be a set of elements of $\mathcal{R}$. The difference ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. Obviously, $[\mathbb{P}]$ is the set of all linear combinations of the r-pols in $\mathbb{P}$ and their transforms. The (ordinary or algebraic) ideal generated by $\mathbb{P}$ is denoted as $(\mathbb{P})$. A difference ideal $\mathcal{I}$ is called \textit{reflexive} if
Let \( P \in \mathbb{I} \) implies \( P \in \mathbb{I} \). A difference ideal \( \mathbb{I} \) is called \textit{perfect} if the presence in \( \mathbb{I} \) of a product of powers of transforms of an r-pol \( P \) implies \( P \in \mathbb{I} \). The perfect difference ideal generated by \( \mathbb{P} \) is denoted as \( \{ \mathbb{P} \} \). A perfect ideal is always reflexive. It is clear that \( \text{Zero}(\mathbb{P}) = \emptyset \) iff \( 1 \in \{ \mathbb{P} \} \). A difference ideal \( \mathbb{I} \) is called a \textit{prime ideal} if for r-pols \( P \) and \( Q \), \( PQ \in \mathbb{I} \) implies \( P \in \mathbb{I} \) or \( Q \in \mathbb{I} \).

2.2. Difference ascending chains

Let \( P_1, P_2 \) be two r-pols and \( \text{lead}(P_1) = y_p(x + q) \) with \( p > 0 \). \( P_2 \) is said to be \textit{reduced} w.r.t. \( P_1 \) if \( \deg(P_2, y_p(x + q + i)) < \deg(P_1, y_p(x + q)) \) for any nonnegative integer \( i \). If \( P_1 \in \mathbb{K} \) and nonzero, then \( P_2 \) is not reduced w.r.t. \( P_1 \).

A finite sequence of nonzero r-pols \( \mathbb{A} = A_1, \ldots, A_p \) is called an \textit{ascending chain}, or simply a \textit{chain}, if either \( p = 1 \) or \( p > 1 \), \( 0 < \text{cls}(A_i) \), \( A_i \prec A_j \), and \( A_j \) is reduced w.r.t. \( A_i \) for \( 1 \leq i < j \leq p \). \( \mathbb{A} \) is called \textit{trivial} if \( \text{cls}(A_1) = 0 \).

**Example 2.1:** Let \( P_1 = y(x + 1)^2 - y^2(x + 1), P_2 = y(x + 2) + y(x + 1) \in \mathbb{K}\{y\} \).

Since \( P_1 \prec P_2, \deg(P_2, y(x + 1)) = \deg(P_1, y(x + 1)) \) and \( \deg(P_2, y(x + 2)) < \deg(P_1, y(x + 1)) \), \( P_2 \) is reduced w.r.t. \( P_1 \). Hence, \( P_1, P_2 \) is a chain.

From this example, we can see that even in ordinary difference case, a chain could contain more than one r-pol in the same leading variable. This is different from the differential case.

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

\[
\text{sat}(\mathbb{A}) = \text{sat}(\mathbb{A}) = \{ P \in \mathbb{K}\{Y\} | \exists J \in \mathbb{I}_\mathbb{A}, s.t. JP \in [\mathbb{A}] \}.
\]

Note that \( \mathbb{I}_\mathbb{A} \) is closed under transforming and multiplication. Then \( \text{sat}(\mathbb{A}) \) is a difference ideal.

Let \( \mathbb{B} \) be an algebraic chain and \( \mathbb{I}_\mathbb{B} \) the set of products of powers of initials of the polynomials in \( \mathbb{B} \). Then we define

\[
\text{asat}(\mathbb{B}) = (\mathbb{B}) : \mathbb{I}_\mathbb{B} = \{ P \in \mathbb{K}[Y] | \exists J \in \mathbb{I}_\mathbb{B}, s.t. JP \in (\mathbb{B}) \}
\]

A chain \( \mathbb{A} = A_1, \ldots, A_p \) is said to be of \textit{higher rank} than another chain \( \mathbb{B} = B_1, \ldots, B_s \), denoted as \( \mathbb{A} \succeq \mathbb{B} \), if one of the following conditions holds:

i). \( 0 < j \leq \min\{p, s\} \), such that \( \forall i < j, A_i \sim B_i \) and \( A_j \gtrsim B_j \), or

ii). \( s > p \) and \( A_i \sim B_i \) for \( i \leq p \).

If no one has higher rank than the other for two chains, they have the same rank, and is denoted as \( \mathbb{A} \succeq \mathbb{B} \). \( \mathbb{A}_1 \succeq \mathbb{A}_2 \succeq \ldots \succeq \mathbb{A}_k \succeq \ldots \). It is easy to see that \( \succeq \) is a total order on the difference chain set.

**Lemma 2.1:** (20) Let \( \mathbb{A}_i \) be a sequence of chains satisfying

\[
\mathbb{A}_1 \succeq \mathbb{A}_2 \succeq \ldots \succeq \mathbb{A}_k \succeq \ldots
\]
Then there is an index $i_0$ such that for any $i > i_0, A_i \sim A_{i_0}$.

Let $\mathbb{P}$ be a set of r-pols. It is possible to form chains with r-pols in $\mathbb{P}$. Among all those chains, by the above lemma, there are some which have a lowest rank. Any chain in $\mathbb{P}$ with the lowest rank is called a characteristic set of $\mathbb{P}$.

An r-pol is said to be reduced w.r.t. a chain if it is reduced to every r-pol in the chain. The following result is evident from the definitions.

**Lemma 2.2:** $A \subset \mathbb{P}$ is a characteristic set of $\mathbb{P}$ iff there is no nonzero r-pol in $\mathbb{P}$ which is reduced w.r.t. $A$.

**Lemma 2.3:** (20) If $A$ is a characteristic set of $\mathbb{P}$ and $A'$ a characteristic set of $\mathbb{P} \cup \{P\}$ for an r-pol $P$, then we have $A \succeq A'$. Moreover, if $P$ is reduced with respect to $A$, we have $A \succ A'$.

The difference pseudo-division is defined as follows.

**Algorithm 2.1:** $\text{rprem}(G, P)$. Input: $G, P \in \mathcal{K}\{\mathcal{Y}\}$. Output: an r-pol $R$ which is the pseudo remainder of $G$ w.r.t. $P$.

\[ p := \text{cls}(P); \]
\[ \text{If } p = 0 \text{ or } \text{ord}(G, y_p) < \text{ord}(P, y_p) \text{ then return } G; \]
\[ \text{else} \]
\[ R := G; \]
\[ \text{for } i \text{ from } \text{ord}(G, y_p) - \text{ord}(P, y_p) \text{ to } 0 \text{ by } -1 \text{ do } \]
\[ R := \text{prem}(R, P, y_p(x + \text{ord}(P, y_p) + i)); \]  // (*)
\[ \text{If } R = 0 \text{ then return}(0); \]
\[ \text{return}(R); \]
\[ \text{end}; \]

In (*), $\text{prem}(P, Q, v)$ is the pseudo-remainder of $P$ w.r.t $Q$ in variable $v$, where the variables $y$ and their transforms are treated as independent algebraic variables.

From the above algorithm, it is easy to check that

**Lemma 2.4:** Let $R = \text{rprem}(G, P)$, $\text{lead}(P) = y_p(x + q)(p > 0)$, $h = \text{ord}(G, y_p)$, and $k = h - q \geq 0$. Then $R$ is reduced w.r.t. $P$ and we have the remainder formula

\[ JG = Q_1\delta^kP + Q_2\delta^{k-1}P + \cdots + Q_{k+1}P + R, \]

where $R, Q_i(i = 1, \ldots, k + 1)$ are r-pols and $J = \prod_{i=0}^{k}(\delta^{\text{init}(P)})^{s_i}$ for non-negative integers $s_i$. Note that $J \prec P$.

We define the pseudo-remainder of an r-pol $P$ w.r.t. a chain $A = A_1, \ldots, A_p$ recursively as $\text{rprem}(P, A) = \text{rprem}(\text{rprem}(P, A_p), A_1, \ldots, A_{p-1})$ and $\text{rprem}(P, \{\}) = P$. As a direct consequence of Lemma 2.4, we have

**Lemma 2.5:** Let $P, A$ be as above. Then there is a $J \in \mathbb{I}_A$ with $J \prec P$ such that $JP \equiv R \mod [A]$ and $R$ is reduced w.r.t $A$. 
3. Coherent and regular difference chains

3.1. Invertibility of algebraic polynomials

We will introduce some notations and results about invertibility of algebraic polynomials w.r.t. an algebraic chain.

A sequence of polynomials $\mathcal{A} = A_1, \ldots, A_m$ in $K[x_1, \ldots, x_n]$ is called a triangular set if $\text{cls}(A_1) < \text{cls}(A_2) < \cdots < \text{cls}(A_m)$. Let $y_i$ be the leading variable of $A_i$, $\mathcal{Y} = \{y_1, \ldots, y_p\}$ and $\mathcal{U} = \{x_1, \ldots, x_n\} \setminus \mathcal{Y}$. $\mathcal{U}$ and $\mathcal{Y}$ are called the parameter set and the leading variable set of $\mathcal{A}$ respectively. We can denote $K[x_1, \ldots, x_n]$ as $K[\mathcal{U}, \mathcal{Y}]$. A polynomial $P$ is said to be invertible w.r.t. $\mathcal{A}$ if either $P \in K[\mathcal{U}]$ or $(P, A_1, \ldots, A_s) \cap K[\mathcal{U}] \neq \{0\}$ where $\text{lvar}(P) = \text{lvar}(A_s)$. $\mathcal{A}$ is called regular if the initials of $A_i$ are invertible w.r.t. $\mathcal{A}$.

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

Lemma 3.1: (3) A polynomial $P$ is not invertible w.r.t. a regular triangular set $\mathcal{A}$ iff there is a nonzero $Q$ in $K[\mathcal{U}, \mathcal{Y}]$ such that $PQ \in (\mathcal{A})$ and $Q$ is reduced w.r.t. $\mathcal{A}$.

Lemma 3.2: (27) Let $\mathcal{A}$ be an irreducible algebraic triangular set with parameters $\mathcal{U}$, leading variables $\mathcal{Y}$, and a generic point $\eta$. Then $\text{asat}(\mathcal{A})$ is a prime ideal of dimension $|\mathcal{U}|$ and for any polynomial $Q$, the following facts are equivalent.

- $Q$ is invertible w.r.t. $\mathcal{A}$.
- $\text{prem}(Q, \mathcal{A}) \neq 0$, or equivalently $Q \notin (\mathcal{A}) : I_\mathcal{A}$.
- $Q(\eta) \neq 0$.
- $\text{resl}(Q, \mathcal{A}) \neq 0$. Let $\mathcal{A} = A_1, \ldots, A_m$, $\text{resl}(Q, \mathcal{A})$ is defined as follows: $\text{resl}(Q, \mathcal{A}) = \text{resl}(\text{resl}(P, A_m, \text{lvar}(A_m)), A_1, \ldots, A_{m-1})$ and $\text{resl}(Q, \{\}) = Q$.

3.2. Extension of a chain

For any chain $\mathcal{A}$, after a proper renaming of the variables, we could write it as the following form.

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

where $\text{lvar}(A_{i,j}) = y_i$ and $\mathcal{U} = \{u_1, \ldots, u_q\}$ such that $p + q = n$. Let $a_{i,j} = \text{ord}(A_{i,j}, y_i)$. $\mathcal{U}$ is called the parameter set of $\mathcal{A}$ and $\text{dim}(\mathcal{A}) = |\mathcal{U}|$ is called the dimension of $\mathcal{A}$. Denote

$$\mathcal{P}(\mathcal{A}) = \{y_i(x+j)|1 \leq i \leq p, 0 \leq j \leq a_{i,1} - 1\}$$
and call $\text{ord}(A) = |P(A)| = \sum_{i=1}^{p} o_{(i,1)}$ the order of $A$.

Let $A$ be a chain of form (1) and $h_1, \ldots, h_m$ ($m \leq p$) nonnegative integers. The extension of $A$, denoted as $A_{(h_1, \ldots, h_m)}$, is the following sequence of r-pols

$$ A_{1,1}, \delta A_{1,1}, \ldots, \delta^{a_{1,2} - a_{1,1} - 1} A_{1,1}, A_{1,2}, \ldots, A_{1,k_1}, \delta A_{1,k_1}, \ldots, \delta^{h_{1,1} - a_{1,1} - 1} A_{1,k_1}, $$

$$ \ldots, $$

$$ A_{m,1}, \delta A_{m,1}, \ldots, \delta^{a_{m,2} - a_{m,1} - 1} A_{m,1}, A_{m,2}, \ldots, A_{m,k_m}, \delta A_{m,k_m}, \ldots, \delta^{h_{m,1} - a_{m,1} - 1} A_{m,k_m} \tag{3} $$

where $\hat{h}_i$ is defined as follows: $\hat{h}_m = \max\{h_m, o_{m,k_m}\} + 1$, and for $i = m-1, \ldots, 1$, $o_i = \max\{\text{order of} \ y_i(x) \text{ appears in} \ A_{i+1,1}, \delta A_{i+1,1}, \ldots, \delta^{h_{m,1} - a_{m,1} - 1} A_{m,k_m}\}$, $\hat{h}_i = \max\{h_i, o_i, o_{i,k_i}\} + 1$. For a chain $A$ and an r-pol $P$, let

$$ A^* = A_{(0,\ldots,0)} $$

$$ A_P = A_{(\text{ord}(P,y_1),\ldots,\text{ord}(P,y_p))} \tag{4} $$

With these notations, it is clear that

$$ \text{rprem}(P, A) = \text{prem}(P, A_P) \tag{5} $$

where the variables and their transforms in $\text{prem}(P, A_P)$ are treated as independent variables. The following fact is clearly true.

**Lemma 3.3:** Use the notations in (3).

- For each $i$, there exist at least two r-pols in $A_P$ with $y_i$ as leading variable.
- Let $e_j = \max_{A \in A_{(h_1, \ldots, h_m)}} \{\text{ord}(A, u_j)\}$, $V = \{\delta^i u_j \mid 1 \leq j \leq q, 0 \leq i \leq e_j\}$, $Z = \{\delta^i y_j \mid 1 \leq j \leq m, 0 \leq i \leq \hat{h}_j\}$. Then $A_{(h_1, \ldots, h_m)}$ is an algebraic triangular set in $K[\mathcal{V}, \mathcal{Z}]$ when the elements in $V$ and $Z$ are treated as independent variables.
- The parameters of $A_{(h_1, \ldots, h_m)}$ as a triangular set are $V \cup P(A)$.

### 3.3. Coherent chains

Note that in Example 2.1, we have $\delta P_1 - (y(x + 2) + y(x + 1))P_2 = 1$, i.e. $1 \in [P_1, P_2]$. This fact leads to the following concept.

Let $A = A_1, \ldots, A_m$ be a chain and $o_i = \text{ord}(A_i, \text{iav}(A_i))$, $i = 1, \ldots, m$. For any $1 \leq i < j \leq m$, if $\text{cls}(A_i) = \text{cls}(A_j) = t$, let

$$ \Delta_{ij} = \text{prem}(\delta^{o_j - o_i} A_i, A_j, y_t(x + o_j)) \tag{6} $$

otherwise, let $\Delta_{ij} = 0$. If $\text{rprem}(\Delta_{ij}, A) = \text{prem}(\Delta_{ij}, A^*) = 0$, we call $A$ a coherent chain.

Let $A = A_1, \ldots, A_s$ be a chain. A linear combination $C = \sum_{i,j} Q_{ij} \delta^j A_i$ is called normal if $\delta^j A_i$ in the expression are distinct elements in $A_{(h_1, \ldots, h_p)}$ for some nonnegative integers $h_1, \ldots, h_p$. In other words, $C \in (A_{(h_1, \ldots, h_p)})$. 

Lemma 3.4: Let $\mathcal{A} = A_1, \ldots, A_m$ be a coherent chain, $\text{cls}(A_i) = \text{cls}(A_j) = t, i < j$, and $o_i = \text{ord}(A_i, \text{lvar}(A_i)), i = 1, \ldots, m$. Then, there is a $J \in I_{\mathcal{A}^*}$ satisfying $J \prec A_j$ such that $J \cdot \delta^{o_j-o_i}A_i = 0 \mod (\mathcal{A}^*)$.

Proof: Let $\Delta_{ij} = \text{prem}(\delta^{o_j-o_i}A_i, A_j, y_i(x + o_j)), I_j = \text{init}(A_j)$. Then there is a nonnegative integer $v$ such that $I_j^v \cdot \delta^{o_j-o_i}A_i = QA_j + \Delta_{ij}$. Since $\mathcal{A}$ is coherent, $\text{prem}(\Delta_{ij}, \mathcal{A}^*) = 0$. Now, the result is a consequence of the remainder formula for the algebraic pseudo-remainder.

Lemma 3.5: Let $\mathcal{A}$ be a coherent chain of form (1), $P \in (\mathcal{A}(l_1,\ldots,l_p))$ and $l_i \geq \text{ord}(A_{i,c_i}, y_j)$. Then $\exists J \in I_{\mathcal{A}^*}$ s.t. $J \prec P$ and $J\delta P \in (\mathcal{A}(l_{i+1},\ldots,l_{p+1}))$.

Proof. Let $\mathcal{A}(l_1,\ldots,l_p) = B_{1,1}, \ldots, B_{1,c_1}, \ldots, B_{p,1}, \ldots, B_{p,c_p}$ with lvar($B_{i,j}$) = $y_i$. Then we have $P = \sum_{i,j} P_{i,j}B_{i,j}$ and $\delta P = \sum_{i,j} \delta P_{i,j}B_{i,j}$. Since $B_{i,c_i} \in \mathcal{A}(l_1,\ldots,l_p)$ and $l_i \geq \text{ord}(A_{i,c_i}, y_j)$, $\delta B_{i,c_i}$ must be in $\mathcal{A}(l_{i+1},\ldots,l_{p+1})$. For $j < c_i$, $\delta B_{i,j}$ is either in $\mathcal{A}(l_1,\ldots,l_p)$ or fall in the situation considered in Lemma 3.4. This proves the Lemma.

Lemma 3.6: Let $\mathcal{A}$ be a coherent chain of form (1), $A \in \mathcal{A}$, and $m$ a non-negative integer. Then there is a $J \in I_{\mathcal{A}}$ such that $J \prec \delta^mA$ and $J \cdot \delta^mA$ has a normal representation.

Proof: Let $f_i = \text{ord}(\delta^mA, y_j), c = \text{cls}(A)$. We divide the proof into three cases. First, if $\delta^mA \in \mathcal{A}(f_1,\ldots,f_p)$, the result is obvious. Second, if there exists a $B \in \mathcal{A}$ such that $\text{ord}(B, y_c) = \text{ord}(\delta^mA, y_c)$, then this is Lemma 3.4. Third, if there exists a $B \in \mathcal{A}$ with a higher lead than that of $A$ and an integer $g > 0$ such that $\text{ord}(\delta^gB, y_c) = \text{ord}(\delta^{m-g}A, y_c)$. It is clear that $g < m$. We will prove the lemma by induction on $m$. We already proved the case for $m=0$. Now, suppose that the lemma is correct for $m=1, \ldots, k-1$ and we will prove the case for $m=k$. By Lemma 3.4, there is a $J_1 \in I_{\mathcal{A}}$ such that $\text{lead}(J_1) < \text{lead}(\delta^{m-g}A)$ and

$$J_1 \cdot \delta^{m-g}A \equiv 0 \mod (\mathcal{A}(h_1,\ldots,h_c)).$$

Perform $g$ transformations, we have

$$\delta^gJ_1 \cdot \delta^mA \equiv 0 \mod (\delta^g\mathcal{A}(h_1,\ldots,h_c)).$$

Each element in $\delta^g\mathcal{A}(h_1,\ldots,h_c)$ must satisfy the induction hypothesis. Then there is a $J_2 \in I_{\mathcal{A}}$ such that $\text{lead}(J_2) < \text{lead}(\delta^mA)$ and

$$\delta^gJ_1 \cdot J_2 \cdot \delta^mA \equiv 0 \mod (\mathcal{A}(h_1+g,\ldots,h_c+g)).$$

The condition $\text{lead}(J) < \text{lead}(\delta^mA)$ is clearly valid.

As a direct consequence of Lemma 3.6, we now have the main property of a coherent chain.

Theorem 3.2: If $\mathcal{A} = A_1, \ldots, A_s$ is a coherent chain, for any $P = \sum Q_{ij} \delta^jA_i$, there is a $J \in I_{\mathcal{A}}$ such that $J \cdot P$ has a normal representation, and $J \prec \max \{\delta^jA_i\}$. 
3.4. Regular chains

Let $\mathcal{A}$ be a chain of form (1) and $P$ an r-pol. $P$ 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.

Let $\mathcal{A} = A_1, \ldots, A_m$ be a difference chain and $I = \text{init}(A_i)$. $\mathcal{A}$ is said to be (difference) regular if $\delta^i I_j$ is invertible w.r.t. $\mathcal{A}$ for any non-negative integer $i$ and $1 \leq j \leq m$, or equivalently, every $J \in \mathbb{I}_A$ is invertible w.r.t. $\mathcal{A}$.

**Lemma 3.7:** Let $\mathcal{A}$ be a characteristic set of an ideal $I$. If an r-pol $P$ is invertible w.r.t. $\mathcal{A}$, then $P \notin I$.

*Proof.* Let $\mathcal{U}$ be the parameter set of $\mathcal{A}$. Since $P$ is invertible w.r.t $\mathcal{A}$, there exist an r-pol $Q$ and a nonzero $N \in K\{\mathcal{U}\}$ such that $Q P = N \mod [\mathcal{A}]$. If $P \in I$, then $N$ is reduced w.r.t. $\mathcal{A}$, by Lemma 2.2 $N = 0$, a contradiction. \[\]

**Lemma 3.8:** If a chain $\mathcal{A}$ of form (1) is the characteristic set of $\text{sat}(\mathcal{A})$, then for any integers $h_i \geq 0$, $\mathcal{A}_{(h_1,\ldots,h_p)}$ is a regular algebraic triangular set.

*Proof.* By Theorem 3.1, we need only to prove that $\mathcal{B} = \mathcal{A}_{(h_1,\ldots,h_p)}$ is the characteristic set of $\text{asat}(\mathcal{B})$. Let $\mathcal{X}$ be the set of all the $\delta^i y_j \leq \delta^i y_k$, which is of higher rank than those in $\mathcal{X}$. As a consequence, $P$ is also reduced w.r.t. $\mathcal{A}$. Since $P \in \text{asat}(\mathcal{B}) \subset \text{sat}(\mathcal{A})$ and $\mathcal{A}$ is the characteristic set of $\text{sat}(\mathcal{A})$, $P$ must be zero, a contradiction. \[\]

The following result shows that a coherent and regular chain is regular.

**Lemma 3.9:** Let $\mathcal{A}$ be a coherent and regular chain, and $R$ an r-pol reduced w.r.t. $\mathcal{A}$. If $R \in \text{sat}(\mathcal{A})$, then $R = 0$.

*Proof.* Let $\mathcal{A} = A_1, \ldots, A_m$. Since $R \in \text{sat}(\mathcal{A})$, there is a $J \in \mathbb{I}_A$ such that $J \cdot R \equiv 0 \mod [\mathcal{A}]$. Since $\mathcal{A}$ is regular, $J$ is invertible w.r.t. $\mathcal{A}$, i.e. there is an r-pol $\tilde{J}$ and a nonzero $N \in K[\mathcal{V}]$ such that $\tilde{J} \cdot J \equiv N \mod [\mathcal{A}]$ where $\mathcal{V}$ is the set of parameters of $A^*$ as an algebraic triangular set (see Lemma 3.3). Hence, $NR \equiv \tilde{J} \cdot J \cdot R \equiv 0 \mod [\mathcal{A}]$. Or equivalently,

$$N \cdot R = \sum R_{u,v} \delta^u A_v. \quad (7)$$

Since $\mathcal{A}$ is coherent, by Theorem 3.2, there is a $\tilde{J} \in \mathbb{I}_A$ such that $\tilde{J} NR$ has a normal representation in $[\mathcal{A}]$, where lead($\tilde{J}$) $\prec \max \{\text{lead}(\delta^\mu A_v)\}$ in (7). That is

$$\tilde{J} \cdot N \cdot R = \sum Q_{ij} \delta^j A_i, \quad (8)$$

where, each $\delta^j A_i$ has a different lead. If the leads of $\delta^j A_i$ in (8) are of lower rank than that of $\delta^\mu A_v$ in (7), we already reduce the rank of $\delta^\mu A_v$ in (7). Otherwise, assume $y_k(x + q) = \max \{\text{lead}(\delta^j A_i)\}$ and lead($\delta^{j_0} A_w$) = $y_k(x + q)$. Let us
assume  \( A_{ij} = I_{ij}y_k(x + s)^{d_{ij}} + R_{ij} \). Then \( \delta^{j_0} A_{ij} = \delta^{j_0} I_{ij}y_k(x + q)^{d_{ij}} + \delta^{j_0} R_{ij} \). Substituting \( y_k(x + q)^{d_{ij}} \) by \( -\frac{\delta^{j_0} R_{ij}}{\delta^{j_0} I_{ij}} \) in (8), the left hand side keeps unchanged since \( \text{lead}(\tilde{J}) < y_k(x + q) \), \( N \) is free of \( y_k(x + q) \), and \( R \) is reduced w.r.t. \( A \). In the right hand side, the \( \delta^{j_0} A_{ij} \) becomes zero, i.e. the \( \max\{\text{lead}(\delta^j A_i)\} \) decreases. Clearing denominators of the substituted formula of (8), we obtain a new equation:

\[
(\delta^{j_0} I_{ij})^{\dagger} \cdot \tilde{J} \cdot N \cdot R = \sum \tilde{Q}_{ij} \delta^j A_i.
\]

In the right hand side of (9), the lead of \( \delta^j A_i \) with highest rank is less than \( y_k(x + q) \) and \( (\delta^{j_0} I_{ij})^{\dagger} \cdot \tilde{J} \) is invertible w.r.t. \( A \) and with rank lower than that of \( y_k(x + q) \). Repeating the process starting from the proof, we will finally obtain a nonzero \( \tilde{N} \in \mathbb{K}[\mathbb{V}]^\dagger \), such that \( \tilde{N} \cdot R = 0 \). Then \( R = 0 \). By Lemma 2.2, \( A \) is the characteristic set of \( \text{sat}(A) \).

The above lemma is a difference version of the Rosenfeld Lemma (21). The condition in this lemma is stronger than that used in the differential Rosenfeld Lemma. The conclusion is also stronger. The following example shows that the Rosenfeld Lemma (21) is not valid in the difference case.

Example 3.1: Let \( A = \{y_1(x + 1)^2 - 1, (y_1 - 1)y_2^2 + 1\} \). \( A \) is coherent and \( y_1(x + 1) + 1 \) is reduced w.r.t. \( A \). \( y_1(x + 1) + 1 \in \text{sat}(A) \), because \( (\delta(y_1 - 1))(y_1(x + 1) + 1) = y_1(x + 1)^2 - 1 \). On the other hand, \( y_1(x + 1) + 1 \notin \text{asat}(A) \).

The following is the key property for a regular and coherent chain.

**Theorem 3.3:** 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 3.9, \( A \) is a characteristic set of \( \text{sat}(A) \). Conversely, let \( A = A_1, \ldots, A_m \) be a characteristic set of \( \text{sat}(A) \) and \( I_j = \text{init}(A_j) \). For any \( 1 \leq i < j \leq p \), let \( R = \text{rpre}(\Delta_{ij}, A) \) where \( \Delta_{ij} \) is defined in (6). 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, for any \( i \geq 0, 1 \leq j \leq m \), we need to prove that \( P = \delta^i I_j \) is invertible w.r.t. \( A \). Assume this is not true. By definition, \( P \) is not invertible w.r.t. \( A_P \) when they are treated as algebraic equations. By Lemma 3.8, \( A_P \) is a regular algebraic chain. By Lemma 3.1, there is a nonzero \( Q \) which is reduced w.r.t. \( A_P \) (and hence \( A \)) such that \( PQ = \delta^i I_j Q \in (A_P) \subset [A] \). Then \( Q \in \text{sat}(A) \) and \( Q \) is reduced w.r.t. \( A \). Since \( A \) is the characteristic set of \( \text{sat}(A) \), this is impossible. Hence, \( P = \delta^i I_j \) is invertible w.r.t. \( A \) and \( A \) is regular.

We have the following normal representation for the saturation ideal of a coherent and regular chain.

**Theorem 3.4:** If \( A \) is a coherent and regular chain of form (1), then

\[
\text{sat}(A) = \bigcup_{h_1 \geq 0, \ldots, h_p \geq 0} (\text{asat}(A_{[h_1, \ldots, h_p]}))
\]
Proof. It is easy to see that \( \text{sat}(A) \supset \bigcup_{h_1 \geq 0, \ldots, h_m \geq 0} \text{asat}(A(h_1, \ldots, h_p)) \). Let \( P \in \text{sat}(A) \). Since \( A \) is coherent and regular, by Theorem 3.3, \( A \) is the characteristic set of \( \text{sat}(A) \), and hence \( \text{rprem}(P, A) = \text{prem}(P, A_f) = 0 \). That is \( P \in \text{asat}(A_P) \). Hence \( \text{sat}(A) \subset \bigcup_{h_1 \geq 0, \ldots, h_m \geq 0} \text{asat}(A(h_1, \ldots, h_p)) \).

4. Proper and strong irreducible chains

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

4.1. Proper irreducible chains

An r-pol \( P \) is called effective in variable \( y_i \) if \( y_i(x) \) occurs in \( P \). \( P \) is called effective if \( P \) is effective in its leading variable.

A chain \( A \) of the form (1) is said to be proper irreducible if

- \( A^* \) as defined in (4) is an algebraic irreducible triangular set; and
- For \( c = 1, \ldots, p \), \( A_{c,1} \) is effective and \( \hat{A}_{c,1} \) is irreducible in \( \mathbb{K}(\eta_{c-1})[y_c(x), \ldots, y_c(x+f_c)] \), where \( f_c = \text{ord}(A_{c,1}, y_c) \), \( B_c = A^* \cap \mathbb{K}\{U, y_1, \ldots, y_c\} (B_0 = \emptyset) \), \( \eta_c \) is a generic point for the algebraic irreducible chain \( B_c \), and \( \hat{A}_{c,1} \) is obtained by substituting \( \eta_{c-1} \) into \( A_{c,1} \).

The following result is a key property of proper irreducible chains, which gives a constructive criterion to check whether a given chain is regular.

**Theorem 4.1:** A coherent and proper irreducible chain is regular.

**Proof.** Let \( A = A_1, \ldots, A_m \) and \( I_j = \text{init}(A_j) \). Since \( A^* \) is an irreducible algebraic triangular set, by Lemma 3.2, \( I_i \) are invertible w.r.t. \( A^* \) and hence invertible w.r.t. \( A \). By Lemma 4.2, all \( \delta^i I_i \) are invertible w.r.t. \( A \).

We need to prove several lemmas.

**Lemma 4.1:** Use the notations in the definition of proper irreducible chains. Let \( A \) be proper irreducible, and \( P \) an r-pol satisfying \( 1 \leq \text{ord}(P, y_i) \leq f_i \). Then \( P \) is algebraic invertible w.r.t. \( A^* \).

**Proof.** This lemma only involves algebraic properties. Hence all statements should be understood to be algebraic. We prove the lemma by induction on \( p \). By Lemma 3.7, we need to prove \( \text{resl}(P, A^*) \neq 0 \). If \( p = 1 \), \( P \in \mathbb{K}[V, y_1(x+1), \ldots, y_1(x+f_1)] \), where \( V \) is the set of \( \delta^i u_j \) occurring in \( P \) and \( A^* \). Variable \( y_1(x+f_1) \) must occur in \( P \) effectively. Otherwise \( P \) is already invertible w.r.t. \( A^* \). Note that the lead of any r-pol in \( A \) other than \( A_{1,1} \) is of higher rank than \( y_1(x+f_1) \). Then \( R = \text{resl}(P, A^*) = \text{resl}(P, A_{1,1}, y_1(x+f_1)) \). If \( R = 0 \), then \( A_{1,1} \mid P \), since \( A_{1,1} \).
is irreducible. This is impossible since \( y_1(x) \) occurs in \( A_{1,1} \) (\( A \) is effective) but not in \( P \). Now, suppose that the result is true for \( 1, \ldots, p - 1 \). We are going to show that it is also true for \( p \). By the induction hypothesis, we may assume that \( \text{resl}(P, B_{p-1}) \neq 0 \). Since \( A \) is proper irreducible, \( B_{p-1} \) is an algebraic irreducible triangular set. For any polynomial \( Q \), let \( \tilde{Q} \) be obtained from \( Q \) by substituting \( \mathbb{U}, y_i \) with \( \eta_{p-1} \). Substituting \( \eta_{p-1} \) into \( P \) and \( A_{p,1} \) we get two polynomials in \( \tilde{P} \in \mathcal{K}(\eta)[y_p(x + 1), \ldots, y_p(x + f_p)] \) and \( \tilde{A}_{p,1} \in \mathcal{K}(\eta)[y_p(x), \ldots, y_p(x + f_p)] \). Since \( \text{resl}(P, B_{p-1}) \neq 0 \), \( \tilde{P} \neq 0 \). Furthermore, \( \tilde{A}_{p,1} \) involves \( y_p(x) \) effectively. This is because \( A_{p,1} \) is reduced w.r.t. \( B_{p-1} \), and hence by Lemma 3.2, the term containing \( y_p(x) \) does not vanish after the substitution. Let \( R = \text{resl}(P, A_{p,1}, y_p(x + f_p)) \).

We will show that \( \tilde{R} \neq 0 \). Since \( A \) is proper irreducible, \( \tilde{A}_{p,1} \) is an irreducible polynomial. If \( R = 0 \), then \( \tilde{A}_{p,1}|\tilde{P} \), which is impossible since \( y_m(x) \) occurs in \( A_{p,1} \) effectively but not in \( P \). Since \( B_{p-1} \) is irreducible, by Lemma 3.2, \( \tilde{R} \neq 0 \) is equivalent to the fact that \( R \) is invertible w.r.t. \( B_{p-1} \). Therefore, \( P \) is invertible w.r.t. \( A^* \).

The following result is a key lemma for proper and strong irreducible chains.

**Lemma 4.2:** Let \( A \) be a coherent and proper irreducible chain of the form (1). If \( P \) is invertible w.r.t. \( A \), then \( \delta P \) is invertible w.r.t. \( A \).

**Proof:** Let \( f_i = \text{ord}(A_{i,1}, y_i), V \) the parameter set of the algebraic triangular set \( A_P \), and \( Y \) the leading variables of \( A_P \). By Lemma 3.3, \( V \) is also the parameter set of \( A^* \). Since \( P \) is invertible w.r.t. \( A \), there are \( \tilde{P} \in \mathcal{K}[V, Y] \) and a nonzero \( N \in \mathcal{K}[V] \) such that \( \tilde{P} \cdot P \equiv N \mod (A_P) \). Performing the transforming operator on the above formula, we have

\[
\delta \tilde{P} \cdot \delta P - \delta N = \sum_{A \in A_P} Q_A \delta A \quad (10)
\]

If \( \text{ord}(P, y_i) \geq \text{ord}(A_{i,k_i}, y_i) \) for all \( i \), by Lemma 3.5, there is a \( J \in I_{A^*} \) such that

\[
J \delta \tilde{P} \cdot \delta P \equiv J \delta g \mod (A_{\delta P}) \quad (11)
\]

If \( \text{ord}(P, y_i) < \text{ord}(A_{i,k_i}, y_i) \) for some \( i \), we may assume that for \( A \) in (10), \( \text{ord}(A, y_i) < \text{ord}(A_{i,k_i}, y_i) \). Similar to Lemma 3.5, we can also find a \( J \in I_{A^*} \) such that (11) is true.

Since \( J \) is a product of powers of initials of \( A^* \) and \( A^* \) is irreducible, by Lemma 3.2, it is invertible w.r.t. \( A^* \). Note that \( \delta N \) satisfies \( 1 \leq \delta N \leq f_i \). Then by Lemma 4.1, \( \delta N \) is also invertible w.r.t. \( A^* \). Then, \( J \delta N \) is invertible w.r.t. \( A^* \). As a consequence, there is a \( T \) and a nonzero \( R \in \mathcal{K}[V] \) such that

\[
T \cdot J \delta N \equiv R \mod (A^*) \equiv R \mod (A_{\delta P})
\]

The last equality is valid because \( A^* \subset A_{\delta P} \). Hence,

\[
T \cdot J \delta \tilde{P} \cdot \delta P \equiv T \cdot J \cdot \delta N \equiv R \mod (A_{\delta P})
\]

That is, \( \delta P \) is invertible w.r.t. \( A \).
4.2. Consistency of proper irreducible chains

In order to obtain a complete algorithm for difference polynomial systems, we need to show that a coherent and proper irreducible chain $\mathcal{A}$ is consistent, or equivalently, $\text{Zero}(\text{sat}(\mathcal{A}))$ is not empty. The proof of Theorem 4.2 uses the theory of difference kernels established by Cohn (6). It can also be considered as an extension of some of the results obtained by Cohn about one irreducible difference polynomial to proper irreducible chains.

Example 4.1: This example explains why $A_{c,1}$ has to be effective in the definition of proper irreducible chains. Let $\mathcal{A} = A_1, A_2$, where $A_1 = y_1(x + 1) - y_1(x), A_2 = y_2(x + 1) - y_1(x)$. Then $\mathcal{A}$ satisfies all the properties in the definition of proper irreducible chains except that $A_2$ is not effective. Let $P = A_2 - A_1 = \delta(y_2(x) - y_1(x))$. It is easy to check that $Q = y_2(x) - y_1(x)$ is invertible w.r.t $\mathcal{A}$, but $\delta Q$ is not, which implies that Lemma 4.2 is not true without this assumption.

Theorem 4.2: Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then $\text{Zero}(\text{sat}(\mathcal{A})) \neq \emptyset$, or equivalently, $1 \notin \{\text{sat}(\mathcal{A})\}$. Proof: Let $\mathcal{A}$ be of form (1). Denote $\mathcal{A}^*$ as follows

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

where $\text{lvar}(B_{i,j}) = y_i$. Let $a_i = \text{ord}(B_{i,c_i}, y_i), i = 1, \ldots, p, e = \max_{A \in \mathcal{A}^*, 1 \leq j \leq q}{\text{ord}(A, u_j)}$, $U_0 = \{\delta^i u_j | 1 \leq j \leq q, 0 \leq i \leq e\}, U_1 = \{\delta^i u_j | 1 \leq j \leq q, 1 \leq i \leq e + 1\}, Y_0 = \{\delta^i y_j | 1 \leq j \leq p, 0 \leq i \leq o_j - 1\},$ and $Y_1 = \{\delta^i y_j | 1 \leq j \leq p, 1 \leq i \leq o_j\}$. Then $V_0 = U_0 \cup Y_0$ and $V_1 = U_1 \cup Y_1$ have the same number of elements. Since $\mathcal{A}$ is proper irreducible, $\mathcal{A}^*$ is an irreducible algebraic triangular set when $\delta^i u_j$ and $\delta^i y_j$ are treated as independent variables. Hence, $I = \text{sat}(\mathcal{A}^*)$ is a prime ideal in $\mathcal{K}[\hat{\mathcal{V}}]$, where $\hat{\mathcal{V}} = U_0 \cup Y_0 \cup \{\delta^{o_1} y_1, \ldots, \delta^{o_p} y_p\}$. Let $\eta = (\alpha^{(i)}_j, \beta^{(i)}_j)$ be a generic zero of this prime ideal. Then $\delta^i u_i = \alpha^{(i)}_i, \delta^i y_i = \beta^{(i)}_i$ annihilate every polynomial in $\mathcal{A}^*$ but not their initials.

We will construct a difference kernel of length one. Now, let $a_0$ and $a_1$ be obtained from $V_0$ and $V_1$ by replacing $\delta^i u_i$ and $\delta^i y_i$ with the corresponding $\alpha^{(i)}_j$ and $\beta^{(i)}_j$. The kernel is $\mathcal{K}(a_0, a_1)$. The difference operator $\delta$ introduces a map from $\mathcal{K}(a_0)$ to $\mathcal{K}(a_1)$ as follows $\delta(\alpha^{(i)}_j) = \alpha^{(i+1)}_j$ and $\delta(\beta^{(i)}_j) = \beta^{(i+1)}_j$. We will prove that $\delta$ introduces an isomorphism between $\mathcal{K}(a_0)$ and $\mathcal{K}(a_1)$. Let

$$B_0 = \mathcal{A}^* - \{B_{1,c_1}, \ldots, B_{p,c_p}\}, B_1 = \{\delta A | A \in B_0\}.$$
Let $\delta A$ be an ideal. As a consequence, $PQ$ is an irreducible triangular set in $K[V_1]$. Hence, perfect ideal, from Lazard’s lemma cannot be generalized to the difference case. The following example shows that for a coherent and proper irreducible chain $A$, sat $(A) = 0$. By Theorem 4.1, $A$ is a regular chain and rprem$(P\delta Q, A) = 0$. But, a direct computation shows that rprem$(P\delta Q, A) \neq 0$, a contradiction.
In order to describe prime ideals with chains, we introduce the following concept. A proper irreducible chain $\mathcal{A}$ is called strong irreducible if for any nonnegative integers $h_1, \ldots, h_p$ is an irreducible algebraic triangular set.

**Theorem 4.3:** Let $\mathcal{A}$ be a coherent and strong irreducible chain of form (1). Then $\text{sat}(\mathcal{A})$ is a reflexive prime ideal whose dimension is $\dim(\mathcal{A})$ and whose relative order w.r.t. $\mathcal{U}$ is $\text{ord}(\mathcal{A})$.

**Proof:** Let $P, Q$ be two r-pols such that $PQ \in \text{sat}(\mathcal{A})$. By Theorem 3.4, there exist nonnegative integers $h_1, \ldots, h_p$ such that $PQ \in D = (\mathcal{A}_{(h_1, \ldots, h_p)} : I_{\mathcal{A}_{(h_1, \ldots, h_p)}})$. Since $\mathcal{A}$ is strong irreducible, $\mathcal{A}_{(h_1, \ldots, h_p)}$ is an irreducible algebraic triangular set and hence $D$ is a prime ideal. We thus have $P \in D$ or $Q \in D$. In other words, $P \in \text{sat}(\mathcal{A})$ or $Q \in \text{sat}(\mathcal{A})$. Hence, $\text{sat}(\mathcal{A})$ is a prime ideal. We still need to show that $\text{sat}(\mathcal{A})$ is reflexive, that is, if $\delta P \in \text{sat}(\mathcal{A})$ then $P \in \text{sat}(\mathcal{A})$. Suppose $P \not\in \text{sat}(\mathcal{A})$. By Lemma 3.4, $P \not\in (A_P) : I_{A_P}$. Since $A_P$ is an irreducible algebraic triangular set, $P$ must be invertible w.r.t. $A_P$. As a consequence, $P$ is invertible w.r.t. $\mathcal{A}$. By Lemmas 4.2 and 3.7, $\delta P$ is invertible w.r.t. $\mathcal{A}$ and hence $\delta P \not\in \text{sat}(\mathcal{A})$, which contradicts the fact $\delta P \in \text{sat}(\mathcal{A})$. We proved that $\text{sat}(\mathcal{A})$ is a reflexive prime ideal.

We will prove that $\mathcal{U}$ is a complete parameter set of $\text{sat}(\mathcal{A})$, that is $\text{sat}(\mathcal{A}) \cap K\{\mathcal{U}\} = \{0\}$ and $\text{sat}(\mathcal{A}) \cap K\{\mathcal{U}, y_i\} \neq \{0\}$ for every $i$. By Theorems 4.1 and 3.3, $\mathcal{A}$ is a characteristic set of $\text{sat}(\mathcal{A})$. Then, $\text{sat}(\mathcal{A}) \cap K\{\mathcal{U}\} = \emptyset$, since every non-zero r-pol in $\text{sat}(\mathcal{A}) \cap K\{\mathcal{U}\}$ is reduced w.r.t. $\mathcal{A}$ and hence must be zero. If there exists an $i$, such that $\text{sat}(\mathcal{A}) \cap K\{\mathcal{U}, y_i\} = \{0\}$, let $h = |P(\mathcal{A})|$ (see (2)) and $\mathcal{C} = \mathcal{A}_{[0, \ldots, 0, h, 0, \ldots, 0]}$, where $h$ is at the $i$-th place. Let $\mathcal{Y}$ and $\mathcal{U}'$ be the set of all $y_i(x + j)$ and $u_k(x_l)$ occurring in $\mathcal{C}$ and $\mathcal{Y}' = \mathcal{Y} \cup P(\mathcal{A})$. By Lemma 3.2, $\text{asat}(\mathcal{C})$ is a prime ideal of dimension $\dim(\mathcal{A}) = h$ in $K(\mathcal{U})[\mathcal{Y}']$. On the other hand, $\text{asat}(\mathcal{C}) \cap K(\mathcal{U})[y_0, \ldots, y_h] \subset \text{sat}(\mathcal{A}) \cap K(\mathcal{U})[y_0, \ldots, y_h] = \{0\}$. From this, we have $\dim(\text{asat}(\mathcal{C})) \geq h + 1$, a contradiction. This proves that $\mathcal{U}$ is a complete parameter set of $\text{sat}(\mathcal{A})$. Then, by Theorem IV on page 127 of (6), $\dim(\text{sat}(\mathcal{A})) = \dim(\mathcal{A})$.

The relative order of $\text{sat}(\mathcal{A})$ w.r.t. $\mathcal{U}$ is defined to be the number of $y_i(x + h)$ which are algebraically independent module $\text{sat}(\mathcal{A})$ in $K(\mathcal{U})\{\mathcal{Y}\}$ (page 128 of (6)). By Lemma 3.3, this is just the dimension of the algebraic prime ideal $\text{asat}(\mathcal{A}^*)$ in $K(\mathcal{U})\{\mathcal{Y}\}$, which is $|P(\mathcal{A})| = \text{ord}(\mathcal{A})$ by Lemma 3.2.

Conversely, not every characteristic set of a reflexive prime ideal is strong irreducible. For instance, a characteristic set of $[y_2(x + 1) + y_1(x)]$ under the variable order $y_1 < y_2$ is not effective and hence not strong irreducible. But, we have the following result.

**Theorem 4.4:** Let $I$ be a reflexive prime ideal. We may choose a proper order of variables such that among the characteristic sets of $I$ under this variable order, there exists one $\mathcal{A}$ which is coherent, strong irreducible, and $I = \text{sat}(\mathcal{A})$.

**Proof:** By Lemma 4.3, for any characteristic set $\mathcal{A}$ of $I$, we have $I = \text{sat}(\mathcal{A})$. By Theorem 3.3, $\mathcal{A}$ is coherent.
Assume that $\mathcal{A}$ is of the form (1). Since $I$ is a prime ideal, we may choose $A_{1,1}$ to be irreducible. For $c = 1, \ldots, p$, let $\mathcal{B}_c = \mathcal{A}^* \cap \mathcal{K}\{U, y_1, \ldots, y_c\}$ ($\mathcal{B}_0 = \emptyset$) and $\eta_c$ a generic point for the algebraic irreducible triangular set $\mathcal{B}_c$. Since $I$ is prime, we may choose $\mathcal{A}$ such that $A_{c,1}$ is an irreducible polynomial in $\mathcal{K}\{y_{c-1}(x), \ldots, y_c(x + f_c)\}$, where $f_c = \text{ord}(A_{c,1}, y_c)$. It is obvious that the $u_1$ and $y_{c_i}$ in (1) satisfy the conditions in Lemma 4.5.

We will show that there exist r-pol $P_i \in \mathcal{K}\{U, y_i\}, i = 1, \ldots, p$ satisfying the conditions of Lemma 4.5 where $U = \{u_1, \ldots, u_q\}$.

Since $I$ is a prime ideal, there exists a non-zero $P_i \in I = I \cap \mathcal{K}\{U, y_i\}$ which is of lowest order in $y_i$ and lowest total degree. $P_i$ must be an irreducible r-pol. We will prove that $P_i$ is effective in $y_i$ by induction. If $P_i$ is not effective in $y_i$, we may assume that $P_i$ is effective in one of the $u_i$, say $u_1$. Otherwise, $P_i$ is not effective in all the variables $P_i$ and hence $P_i = \delta Q_1$ for some r-pol $Q_1$. Since $I$ is reflexive, $Q_1 \in I$, which contradicts the fact that $P_i$ has the lowest order in $y_i$. Suppose that $P_j, j = 1, \ldots, i - 1$ is effective in $y_j$ and $P_i$ is not effective in $y_i$. Similar to the case of $i = 1$, we may assume that $P_i$ is effective in one of the $u_i$, say $u_1$. We may exchange $u_1$ and $y_i$ and treat $y_i$ as a parameter and $u_1$ as the leading variable of $P_i$. We choose $\mathcal{V} = \{u_2, \ldots, u_q, y_i\}$ as the parameter set. Let $P_i', j = 1, \ldots, i - 1$ be the irreducible r-pol which have the lowest rank and total degree in $I \cap \mathcal{K}\{\mathcal{V}, y_j\}$ and $P_i'$ the irreducible r-pol which has the lowest rank and total degree in $I \cap \mathcal{K}\{\mathcal{V}, y_i\}$. We will show that $P_i', 1 \leq j < i$ is effective in $y_j$ and $P_i'$ is effective in $u_1$.

First, $P_i'$ is effective in $u_1$. Otherwise, we choose a characteristic set $\mathcal{B}$ of $I \cap \mathcal{K}\{\mathcal{V}, u_1\}$ under the variable order $u_2 < \cdots < u_q < y_i < u_1$. Write $P_i$ as an r-pol in $u_1(x)$:

$$P_i = \sum_j Q_j u_1(x)^j.$$ 

By Lemma 4.4, $\mathcal{B}_{P_i}$ is an irreducible triangular set and $u_1(x)$ does not occur in any polynomial in $\mathcal{B}$. Then by Lemma 3.2, prem($P_i, \mathcal{B}_{P_i}$) = 0 implies prem($Q_k, \mathcal{B}_{P_i}$) = 0 and hence $Q_k \in I$ which contradicts the fact the $P_i$ has the lowest total degree.

Second, for any $j, 1 \leq j < i$, we will show that $P_i'$ is effective in $y_j$. Otherwise, we choose the characteristic set $\mathcal{B}'$ of $I \cap \mathcal{K}\{u_2, \ldots, u_q, y_j, u_1, y_j\}$ under the variable order $u_2 < \cdots < u_q < y_i < y_j < u_1$. Then by Lemma 4.4, $\mathcal{B}'_{P_j}$ is an irreducible triangular set. Since $P_i'$ does not contain $y_j(x), y_j(x)$ does not occur in each polynomial in $\mathcal{B}'_{P_j}$. Write $P_j$ as a polynomial in $y_j(x)$:

$$P_j = \sum_k Q_k y_j(x)^k.$$ 

Then by Lemma 3.2, prem($P_j, \mathcal{B}'_{P_j}$) = 0 implies prem($Q_k, \mathcal{B}'_{P_j}$) = 0 and hence $Q_k \in I$ which contradicts the fact the $P_j$ has the lowest total degree.

In this way, we have selected the $P_i$ satisfying the conditions in Lemma 4.5.
By Lemma 4.5, \( \mathcal{A} \) is effective. Together with Lemma 4.4, we know that \( \mathcal{A} \) is strong irreducible.

**Lemma 4.3:** Let \( I \) be a reflexive prime difference ideal, \( \mathcal{A} \) its characteristic set. Then \( I = \text{sat}(\mathcal{A}) \).

**Proof:** It is clear that \( I \subset \text{sat}(\mathcal{A}) \). Let \( P \in \text{sat}(\mathcal{A}) \). Then there is a \( J \in \mathbb{I}_\mathcal{A} \) such that \( JP \in [\mathcal{A}] \subset I \). By Theorem 3.3 and Lemma 3.7, \( J \) is invertible w.r.t. \( \mathcal{A} \) and hence not in \( I \). Since \( I \) is a prime ideal, \( P \in I \).

**Lemma 4.4:** Let \( I \) be a reflexive prime difference ideal, \( \mathcal{A} \) its characteristic set. Then for any nonnegative integers \( h_1, \ldots, h_p \), \( \mathcal{A}(h_1, \ldots, h_p) \) is algebraic irreducible.

**Proof:** Otherwise, we have nonnegative integers \( h_1, \ldots, h_p \) such that \( \mathcal{A}(h_1, \ldots, h_p) \) is a reducible algebraic triangular set. By definition, there exist r-pols \( P \) and \( Q \) which are reduced w.r.t. \( \mathcal{A}(h_1, \ldots, h_p) \) and with order not higher than those r-pols in \( \mathcal{A}(h_1, \ldots, h_p) \) such that \( PQ \in \mathcal{A}(h_1, \ldots, h_p) \subset \text{sat}(\mathcal{A}) = I \). From this we have \( P \in I \) or \( Q \in I \), which is impossible since \( P \) and \( Q \) are reduced w.r.t. \( \mathcal{A} \).

**Lemma 4.5:** Let \( I \) be a reflexive prime difference ideal in \( \mathbb{K}\{u_1, \ldots, u_q, y_1, \ldots, y_p\} \) such that \( I \cap \mathbb{K}\{u_1, \ldots, u_q\} = \{0\} \), for each \( y_i \), \( I_i = I \cap \mathbb{K}\{u_1, \ldots, u_q, y_i\} \neq \{0\} \), and \( P_i \in I_i \) a non-zero irreducible r-pol of lowest order in \( y_i \) and of lowest total degree. If \( P_i \) is effective in \( y_i \) then a characteristic set of \( I \) under the variable order \( u_i < y_1 < y_2 < \ldots < y_p \) is effective.

**Proof:** Assume that the characteristic set of \( I \) is of form (1). We need only to show that \( A_{c,1} \) is effective in \( y_c \). Assume that there is a \( c \) such that \( A_{c,1} \) is not effective. Write \( P_c \) as a polynomial in \( y_c(x) \):

\[
P_c = \sum_i Q_i y_c(x)^i.
\]

Since \( P_c \) has the lowest order in \( y_c \), we have \( \text{ord}(P_c, y_c) = \text{ord}(A_{c,1}, y_c) \). As a consequence, when computing \( \text{prem}(P_c, \mathcal{A}_{P_c}) \), all \( A_{c,i}, i > 1 \) are not needed. By Lemma 4.4, \( \mathcal{A}_{P_c} \) is an irreducible algebraic triangular set and \( y_c(x) \) does not occur in \( A_{c,1} \). Then by Lemma 3.2, \( \text{prem}(P_c, \mathcal{A}_{P_c}) = 0 \) implies \( \text{prem}(Q_k, \mathcal{A}_{P_c}) = 0 \) and hence \( Q_k \in I \) which contradicts the fact that \( P_c \) has the lowest total degree.

### 5. A zero decomposition algorithm

We will give an algorithm to decompose the zero set of a finitely generated r-pol systems into the union of zero sets of regular and proper irreducible chains.

#### 5.1. Effective characteristic sets

Note that an r-pol is called effective if it is effective in its leading variable. A set of r-pols \( \mathbb{P} \) is called **effective** if any r-pol in \( \mathbb{P} \) is effective.
Lemma 5.1: Let $\mathbb{P}$ be a finite set of r-pols in $\mathcal{K}\{y_1, \ldots, y_n\}$ and $k_i, i = 1, \ldots, n$ integers. By a proper transformation of variables $z_i(x + k_i) = y_i(x)$, there is a set of r-pols $\hat{\mathbb{P}} \in \mathcal{K}\{z_1, \ldots, z_n\}$ which is effective and there is a one to one correspondence between the solutions of $\mathbb{P}$ and $\hat{\mathbb{P}}$.

Proof: First, let us divide $\mathbb{P}$ into $\mathbb{P}_1, \ldots, \mathbb{P}_n$ according to their classes. Let $h_i$ be the largest one among the lowest orders of $P \in \mathbb{P}_i$ in $y_i$ (denoted by lord$(P, y_i)$). Now the transformation of variables is $y_i(x) = z_i(x + h_i + \cdots + h_n), i = 1, \ldots, n - 1$ and $y_n(x) = z_n(x)$. Under such a transformation, an r-pol $P \in \mathbb{P}_i$ becomes $\hat{P}$. It is easy to see lord$(\hat{P}, z_j) = \text{lord}(P, y_j) + h_{j+1} + \cdots + h_n \geq \text{lord}(P, y_i) + h_{i+1} + \cdots + h_n = \text{lord}(\hat{P}, z_i)$, for $j = 1, \ldots, i - 1$. Since $\mathcal{K}$ is inverse, we get an effective r-pol $\hat{P} = \delta^{-\text{lord}(\hat{P}, z_i)} P$ in $\mathcal{K}\{z_1, \ldots, z_n\}$. We obtain a set of effective r-pols $\hat{\mathbb{P}}$ from $\mathbb{P}$. If $a = (a_1, \ldots, a_n), a_i \in \mathcal{F}$ is a solution of $\mathbb{P}$. Then in the inverse closure of $\mathcal{F}$, let $b_i = \delta^{-(h_{i+1} + \cdots + h_n)} a_i$, $1 \leq i < n$ and $b_n = a_n$. We can check that $b = (b_1, \ldots, b_n)$ is a solution of $\hat{\mathbb{P}}$. On the other hand, for any solution $b = (b_1, \ldots, b_n)$ of $\hat{\mathbb{P}}$. Let $a_i = \delta^{h_{i+1} + \cdots + h_n} b_i$, $1 \leq i < n$ and $a_n = b_n$. We get a solution $a = (a_1, \ldots, a_n)$ of $\mathbb{P}$.

We have the following procedure to find a set of effective r-pols.

Algorithm 5.1: Effective$(\mathbb{P})$ Input: a finite set of r-pols $\mathbb{P}$. Output: variables transformation $y_i(x) = z_i(x + k_i)$ and a set of effective r-pols $\hat{\mathbb{P}}$.

Begin

\begin{itemize}
  \item $h_i := 0, i = 1, \ldots, n; \hat{\mathbb{P}} := \{ \}$;
  \item For $P$ in $\mathbb{P}$ do
    \begin{itemize}
      \item if $i := \text{cls}(P)$ then $h_i := \text{max}(h_i, \text{lord}(P, y_i))$;
      \item $T := \{ y_i(x) = z_i(x + h_{i+1} + \cdots + h_n), i = 1, \ldots, n \}$;
      \item $\hat{\mathbb{P}} := \text{subs}(T, \mathbb{P})$; (Do a variable change as in Lemma 5.1)
    \end{itemize}
  \item For $P$ in $\hat{\mathbb{P}}$ do
    \begin{itemize}
      \item let $k := \text{cls}(P)$;
      \item $\hat{\mathbb{P}} := \hat{\mathbb{P}} \cup \{ \delta^{-\text{lord}(P, z_k)} P \}$;
      \item return($T, \hat{\mathbb{P}}$);
    \end{itemize}
\end{itemize}

End.

Example 5.1: Let

$$
\mathbb{P} = \left\{ y_1(x + 1) + xy_1(x), y_1(x)y_2(x + 3) + y_2(x + 2), y_2(x + 4) + y_1(x)y_2(x + 1), y_3(x + 3) + y_2(x)y_3(x + 1) \right\}
$$

Then $h_1 = 0, h_2 = \max\{2, 1\} = 2, h_3 = 1$. Let $z_1(x + 2 + 1) = y_1(x), z_2(x + 1) = y_2(x), z_3(x) = y_3(x)$. Then

$$
\hat{\mathbb{P}} = \left\{ z_1(x + 4) + xz_1(x + 3), z_1(x + 3)z_2(x + 4) + z_2(x + 3), z_2(x + 5) + z_1(x + 3)z_2(x + 2), z_3(x + 3) + z_2(x + 1)z_3(x + 1) \right\}
$$
Under the variable transformation

\[ E \text{CharSet}(A) \]

Let \( E \) be a finite set of \( r \)-pols \( A \) and chains \( A_1, A_2 \) in \( K \{ y_1, \ldots, y_n \} \) become the \( r \)-pols \( \bar{A}_1, \bar{A}_2 \), \( P, Q \) and chains \( \bar{A}_1, \bar{A}_2 \) in \( K \{ z_1, \ldots, z_n \} \) respectively. Then, we have \( A_1 \prec A_2 \iff \bar{A}_1 \prec \bar{A}_2 \), \( A_1 \prec A_2 \iff \bar{A}_1 \prec \bar{A}_2 \), and Zero(\( P \)) = Zero(\( Q \)) \iff Zero(\( P \)) = Zero(\( Q \)).

**Lemma 5.2**: Under the variable transformation \( y_i(x) = z_i(x + k_i), i = 1, \ldots, n \), \( r \)-pols \( A_1, A_2, P, Q \) and chains \( A_1, A_2 \) in \( K \{ y_1, \ldots, y_n \} \) become the \( r \)-pols \( \bar{A}_1, \bar{A}_2 \), \( P, Q \) and chains \( \bar{A}_1, \bar{A}_2 \) in \( K \{ z_1, \ldots, z_n \} \) respectively. Then, we have \( A_1 \prec A_2 \iff \bar{A}_1 \prec \bar{A}_2 \), \( A_1 \prec A_2 \iff \bar{A}_1 \prec \bar{A}_2 \), and Zero(\( P \)) = Zero(\( Q \)) \iff Zero(\( P \)) = Zero(\( Q \)).

**Lemma 5.3**: A finite set \( \mathbb{P} \) of \( r \)-pols becomes \( \bar{\mathbb{P}} \) by the effective algorithm, the variable transformation is \( T = \{ y_i(x) = z_i(x + k_i), i = 1, \ldots, n \} \). If \( \mathcal{A} \) is a characteristic set of \( \mathbb{P} \), \( \mathcal{A} \) becomes \( \bar{\mathcal{A}} \) under the variable transformation \( T \). Let \( \bar{\mathcal{A}} \) be a characteristic set of \( \bar{\mathbb{P}} \). Then \( \bar{\mathcal{A}} \succeq \bar{\mathcal{A}} \).

**Proof**: By Lemma 5.2, \( \bar{\mathcal{A}} \) is a chain in \( K \{ z_1, \ldots, z_n \} \). If \( \bar{\mathcal{A}} \) is effective, \( \bar{\mathcal{A}} \subset \bar{\mathbb{P}} \). Hence it has a higher or equal rank than that of \( \bar{\mathcal{A}} \). Otherwise, there is an \( A_i \in \bar{\mathcal{A}} \) which is not effective, that is, there is an \( \bar{A}_i \in \bar{\mathbb{P}} \), \( t > 0 \), such that \( \delta^t \bar{A}_i = A_i \). It is clear that \( A_i \prec A_i \). Hence \( \bar{\mathcal{A}} \succ \bar{\mathcal{A}} \).

**Algorithm 5.2**: \( \text{ECharSet}(\mathbb{P}) \) Input: a finite set \( \mathbb{P} \) of \( r \)-pols. Output: a variable transformation \( y_i(x) = z_i(x + k_i), i = 1, \ldots, n \), \( \bar{\mathbb{P}} = \text{Effective}(\mathbb{P}) \), and an effective chain \( \mathcal{B} \) which is a characteristic set of \( \bar{\mathbb{P}} \).

Begin
\[
\begin{align*}
[T, \bar{\mathbb{P}}] &= \text{Effective}(\mathbb{P}), \mathcal{B} = \{ \}; \\
\text{while } \bar{\mathbb{P}} &\neq \{ \} \text{ do}
\quad \bar{\mathbb{P}} &= \text{the } r \text{-pols in } \bar{\mathbb{P}} \text{ which are reduced w.r.t. } \mathcal{B}; \\
\quad \mathcal{B} &= \mathcal{B} \cup \{ \text{one of } r \text{-pols with the lowest rank in } \bar{\mathbb{P}} \}; \\
\quad \text{return}(T, \bar{\mathbb{P}}, \mathcal{B})
\end{align*}
\]
end.

**5.2. A zero decomposition algorithm for difference polynomial systems**

A chain \( \mathcal{A} \) is called a **Wu characteristic set** of a set \( \mathbb{P} \) of \( r \)-pols if \( \mathcal{A} \subset [\mathbb{P}] \) and for all \( P \in \mathbb{P} \), \( \text{rprem}(P, \mathcal{A}) = 0 \).

**Lemma 5.4**: Let \( \mathbb{P} \) be a finite set of \( r \)-pols, \( \mathcal{A} = A_1, \ldots, A_m \) a Wu characteristic set of \( \mathbb{P} \), \( I_i = \text{init}(A_i) \), and \( J = \prod_{i=1}^m I_i \).

Then
\[
\begin{align*}
\text{Zero}(\mathbb{P}) &= \text{Zero}(\text{sat}(\mathcal{A})) \bigcup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{ I_i \}) \\
\text{Zero}(\mathbb{P}) &= \text{Zero}(\mathcal{A}/J) \bigcup \bigcup_{i=1}^m \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{ I_i \})
\end{align*}
\]

**Proof**: This is a direct consequence of the remainder formula in Lemma 2.5.

The following algorithm is a modification of a standard algorithm to compute the Wu characteristic set of a finite polynomials set (27).
Algorithm 5.3: **ECohWuCharSet**$(\mathcal{P})$ Input: a finite set $\mathcal{P}$ of r-pols. Output: a variable transformation $\mathcal{T} = \{y_i(x) = z_i(x + k_i), i = 1, \ldots, n\}$, an effective r-pol set $\mathcal{P'}$, and a coherent and effective chain $\mathcal{A} \subset \mathcal{P}'$ such that

- $\text{Zero}(\mathcal{P'}) = \text{Zero}(\hat{\mathcal{P}})$ where $\hat{\mathcal{P}} = \text{Effective}(\mathcal{P})$ under $\mathcal{T}$.
- For any $P \in \mathcal{P'}$, we have $\text{rprem}(P, \mathcal{A}) = 0$. Hence, $\mathcal{A}$ is a Wu characteristic set of $\mathcal{P'}$.

Begin

$\mathcal{P'} := \mathcal{P}$, $\mathcal{R} := \mathcal{P}$, $\mathcal{T} = \mathcal{I}$ is the identity variable transformation;

while $\mathcal{R} \neq \{\}$ do

- $[\mathcal{T}, \mathcal{P'}, \mathcal{A}] := \text{ECharSet}(\mathcal{P'})$;
- $\mathcal{R} := \{\text{rprem}(f, \mathcal{B}) \mid f \in \Delta(\mathcal{A})\} \setminus \{0\}$;
- $\mathcal{R} := \mathcal{R} \cup \{\text{rprem}(P, \mathcal{A}) \mid P \in \mathcal{P'}\} \setminus \{0\}$;
- $\mathcal{P} = \mathcal{P'} \cup \mathcal{R}$;
- $\mathcal{T} = \mathcal{T} \circ \mathcal{T}$ (compositions of variable transformation))

return($\mathcal{T}, \mathcal{P'}, \mathcal{A}$)

end.

In Algorithm 5.3, $\Delta(\mathcal{A})$ is the set of $\Delta$ r-pols defined in (6). The r-pols in $\mathcal{R}$ are reduced w.r.t. $\mathcal{A}$ by Lemma 2.5. By Lemmas 2.3, 5.2 and 5.3, the rank of $\mathcal{A}$ is decreasing after each iteration. Then by Lemma 2.1, the algorithm terminates.

Lemma 5.5: Let $\mathcal{A}$ be a Wu characteristic set of a finite set $\mathcal{P}$. If $\mathcal{A}^*$ is not an algebraic irreducible triangular set, then we can find $P_1, P_2, \ldots, P_h$ which are reduced w.r.t. $\mathcal{A}$ and some initials $I_i$ of $\mathcal{A}$ such that

$$\text{Zero}(\mathcal{P}) = \bigcup_{i=1}^h \text{Zero}(\mathcal{P}, P_i) \bigcup \bigcup_{i=1}^h \text{Zero}(\mathcal{P}, I_i).$$

Proof: Denote $\mathcal{B} = \mathcal{A}^* = B_1, \ldots, B_p$. Since $\mathcal{A}^*$ is not irreducible, by Lemma 3 in Section 4.5 of (27), there are $P_1, \ldots, P_h$ which are reduced w.r.t. $\mathcal{A}^*$ such that

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

where $I_i$ is the initial of $B_i$. Since $\mathcal{A}$ is a Wu characteristic set of $\mathcal{P}$, $P \in [\mathcal{P}]$. Then $\text{Zero}(\mathcal{P}) = \text{Zero}(\mathcal{P} \cup \{P\}) = \bigcup_{i=1}^h \text{Zero}(\mathcal{P}, P_i) \bigcup \bigcup \text{Zero}(\mathcal{P}, I_i)$. \hfill $\Box$

Now, we can give the Ritt-Wu zero decomposition algorithm.

Algorithm 5.4: **RittWuDec**$(\mathcal{P})$ Input: a finite set $\mathcal{P}$ of r-pols. Output: Either $\text{Zero}(\mathcal{P}) = \emptyset$, or a sequence of variable transformations $\mathcal{T}_i = \{y_j(x) = z_{ij}(x + k_{ij}), j = 1, \ldots, t\}$ and a sequence of coherent and proper irreducible difference chains $\mathcal{A}_i \subset K\{z_{i1}, \cdots, z_{in}\}$, $i = 1, \ldots, t$ such that

$$\text{Zero}(\mathcal{P}) = \bigcup_{i=1}^t \text{Zero}(\text{sat}(\mathcal{A}_i))$$
where \( \hat{P} \) and \( \hat{A}_i \) in \( K\{z_1, \ldots, z_n\} \) are obtained from \( \mathbb{P} \) and \( A_i \) under the variable transformation \( \mathbf{T} = \{y_j(x) = z_j(x + k_j), j = 1, \ldots, n\} \), where \( k_j = \max\{k_{ij}, i = 1, \ldots, l\} \).

Begin
\[
[T, \mathbb{P'}, A] := \text{ECohCharSet}(\mathbb{P});
\]
If \( A \) is trivial then return \( \{\} \); If \( A \) is proper irreducible then
\[
\text{return}(\{[A, T]\} \cup \cup_i \text{RittWuDec}(\mathbb{P'} \cup A \cup \{I_i\})));
\]
else by Lemma 5.5, we can find \( P_i, i = 1, \ldots, h \) and
\[
\text{return}(\cup_i \text{RittWuDec}(\mathbb{P'} \cup \{F_i\}) \cup \cup_i \text{RittWuDec}(\mathbb{P'} \cup \{I_i\}));
\]
end.

**Proof of the correctness of the Algorithm.** In algorithm \( \text{ECohCharSet} \), since \( \text{Zero}(\mathbb{P'}) = \text{Zero}(\mathbb{P}) \) and \( A \subset \mathbb{P'} \), it is clear that if \( A \) is trivial \( \text{Zero}(\mathbb{P}) = \emptyset \). Note that \( A \) is already coherent. If \( A \) is proper irreducible, then we have an output. The correctness of the return value is due to Lemma 5.4 and the fact \( \text{Zero}(\mathbb{P'}) = \text{Zero}(\mathbb{P}) \). If \( A \) is not proper irreducible, the correctness of the return value is due to Lemma 5.5. In all the recursive cases, the added r-pols \( I_i \) or \( P_i \) are reduced w.r.t to \( A \). Then by Lemmas 2.3, 5.2 and 5.3, the rank of \( A \) obtained from \( \text{RittWuDec}(\mathbb{P'} \cup A \cup \{I_i\}) \) or \( \text{RittWuDec}(\mathbb{P'} \cup A \cup \{P_i\}) \) has lower rank. Then by Lemma 2.1, the algorithm terminates. Note that for each \( A_i \), we have a variable transformation \( T_i \) to ensure that \( A_i \) is effective. In order to obtain a decomposition for \( \mathbb{P} \), we need to have a “maximal” variable transformation such that all \( A_i \) can be represented explicitly in terms of these variables. \( \blacksquare \)

**Example 5.2:** Let
\[
P_1 = (y_1(x + 1) - y_1(x))^2 - (y_1(x + 1) + y_1(x))
\]
\[
P_2 = (y_1(x + 3) - y_1(x + 1)) \cdot y_2(x + 1) + (y_1(x + 2) - y_1(x)) \cdot y_2(x).
\]
\( \text{RittWuDec}(P_1) \) returns \( \{P_1\} \). \( \text{RittWuDec}(P_1, P_2) \) returns two chains:
\[
\begin{align*}
P_1, y_1(x + 2) - y_1(x) \\
P_1, y_1(x + 2) - 2y_1(x + 1) + y_1(x) - 1, P_3
\end{align*}
\]
where \( P_3 = (2y_1(x + 1) - 2y_1(x + 3)y_2(x + 1) + (2y_1(x + 1) - 2y_1(x) + 1)y_2(x). \)
There is no variables transformations.

As an application of Ritt-Wu’s zero decomposition algorithm, we can solve the membership problem of perfect difference ideals.

**Theorem 5.1:** Let \( \mathbb{P} \) be a finite set of r-pols in \( K\{y_1, \ldots, y_n\} \) and the Ritt-Wu zero decomposition of \( \mathbb{P} \) is \( \{[A_1, T_1], \ldots, [A_k, T_k]\} \). Then \( \text{Zero}(\mathbb{P}) = \emptyset \) iff \( k = 0 \). **Proof:** By Lemma 5.1, \( \mathbb{P} = 0 \) has solutions iff \( \mathbb{P} = 0 \) has solutions under a variable transformation. Now the result is a direct consequence of Theorem 4.2. \( \blacksquare \)

The membership problem of perfect difference ideals can be solved as follows. An r-pol \( Q \in \{\mathbb{P}\} \) iff \( \text{Zero}(\mathbb{P} \cup \{Qz + 1\}) = \emptyset \) where \( z \) is a new variable. Now the problem can be solved with Theorem 5.1.
5.3. Automated proving of certain difference identities

If a sequence of numbers \( \{f_n\}_{n \geq 0} \) satisfies a linear homogenous r-pol equation whose coefficients are algebraic polynomials, it can be regard as a solution of an r-pol equation under certain initial values. If the order of the r-pol is \( k \) and the initial of the r-pol is not zero, we need only to verify that \( f_0, f_1, \ldots, f_{k-1} \) are zero in order to show that for all \( i \), \( f_i = 0 \). Algorithms to prove identities of this type can be found, for instance, in (5; 17; 23; 30). Since Ritt-Wu’s zero decomposition algorithm proposed in this paper provides an elimination tool for non-linear difference equations, it is possible to prove identities for number sequences defined by non-linear difference equations. In what below, we use two examples to show how to prove difference identities with Ritt-Wu’s zero decomposition algorithm.

The first example is about Gauss’ hypergeometric function which can be regarded as a power series solution to the hypergeometric equation

\[
z(1-z)w'' + [r - (a + b + 1)]w' - aw = 0.
\]

It is denoted as \( F(a, b, r; z) = \sum_{n=0}^{\infty} c_n z^n \), where \( c_n \) satisfies

\[
(n + 1)(n + r)c_{n+1} - (n + a)(n + b)c_n = 0, \quad c_0 = 1.
\]

To prove

\[
(r - 1)F(a, b, r - 1; z) - aF(a + 1, b, r; z) - (r - a - 1)F(a, b, r; z) = 0, \quad (12)
\]

let us denote \( F(a, b, r - 1; z) = \sum_{k=0}^{\infty} a_k z^k \). Then \( a_k \) satisfies \( (n+1)(n+r-1)a_{n+1} - (n+a)(n+b)a_n = 0, a_0 = 1 \). Denote \( F(a+1, b, r; z) = \sum_{k=0}^{\infty} b_k z^k \). Then \( b_k \) satisfies \( (n+1)(n+r)b_{n+1} - (n+a+1)(n+b)b_n = 0, b_0 = 1 \). With these notations, identity (12) becomes

\[
\sum_{k=0}^{\infty} ((r - 1)a_k - ab_k - (r - a - 1)c_k)z^k = 0.
\]

That is, we need to show: \( \forall k, \ (r - 1)a_k - ab_k - (r - a - 1)c_k = 0 \). Let

\[
\begin{align*}
P_1 &= (n + 1)(n + r - 1)a_{n+1} - (n + a)(n + b)a_n, \\
P_2 &= (n + 1)(n + r)b_{n+1} - (n + a + 1)(n + b)b_n, \\
P_3 &= (n + 1)(n + r)c_{n+1} - (n + a)(n + b)c_n, \\
P_4 &= h_n - (r - 1)a_n - ab_n - (r - a - 1)c_n.
\end{align*}
\]

Using RittEuDec under the variable order \( h_n < a_n < b_n < c_n \) (in our implementation, the command is RittWuDec([\( P_1, P_2, P_3, P_4 \), [\( h_n, a_n, b_n, c_n \)]]), we obtain a trivial chain and a coherent proper irreducible chain whose first r-pol is:

\[
A_1 = (b + 1 + n) (n + b) (n + 1 + a) (n + a) h_n - 2 (n + r) (n + 1) (b + 1 + n) (n + 1 + a) h_{n+1} + (n + 2) (n + 1) (n + r + 1) (n + r) h_{n+2}.
\]
Since $P_i$ are linear, $h_n$ satisfies the difference equation $A_1 = 0$ of order two. We need only to verify that $h_0 = h_1 = 0$, then $h_n = 0$ for any $n$. It is clear that $h_0 = (r - 1)a_0 - ab_0 - (r - a - 1)c_0 = (r - 1) - a - (r - a - 1) = 0$, $h_1 = (r - 1)a_1 - ab_1 - (r - a - 1)c_1 = 0$. We proved the identity.

The second example is to prove the Cassini identity about Fibonacci numbers. The Fibonacci number $F_n$ satisfies

$$F_{n+2} - F_{n+1} - F_n = 0, F_0 = 0, F_1 = 1.$$ 

We will prove the Cassini identity:

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}, n = 0, 1, 2, \ldots.$$ 

The number sequence $(-1)^n$ can be represented by difference relations $a_{n+1} + a_n = 0$ with initial value $a_0 = 1$. Let $P_1 = F_{n+2} - F_{n+1} - F_n$, $P_2 = h_n - (F_{n+2}F_n - F_{n+1}^2 + a_n)$, $P_3 = a_{n+1} + a_n$. Using RittEuDec to $\{P_1, P_2, P_3\}$ under the variable order $h_n < a_n < F_n$, we obtain a coherent proper irreducible chain:

$$h_{n+1} + h_n, a_{n+1} + a_n, F_nF_{n+1} + F_n^2 - h_n - F_{n+1}^2 + a_n, F_{n+2} - F_{n+1} - F_n.$$ 

From the computation procedure, we know that $C = h_{n+1} + h_n$ is a linear combination of $P_1, P_2,$ and $P_3$ and their transformations. Then $h_n$ satisfies $C = 0$. Since $h_0 = F_2F_0 - F_1^2 + a_0 = 0$, $h_n = 0$ for any $n$. Cassini’s identity is proved. In (17), a difference equation of order three $F_{n+3} - 2F_{n+2} - 2F_{n+1} - F_n$ is obtained with linear algebraic tools. In (5), the same difference equation as the one in this paper is obtained with an elimination procedure over Ore algebras.

6. Conclusion

In this paper, we developed a characteristic set method for nonlinear ordinary difference polynomial systems. The method could be used to decompose the zero set of a finitely generated difference polynomial system into the union of the zero sets of coherent and proper irreducible chains. We further proved that a coherent and proper irreducible chain has the following nice properties: it is the characteristic set of its saturation ideal and it has at least one solution. These two properties make us possible to solve the membership problem for perfect difference ideals and to prove difference identities.

We also established several basic properties of difference chains. In particular, we proved that an chain is the characteristic set of its saturation ideal iff it is coherent and regular; a chain is the characteristic set of a reflexive prime ideal iff it is coherent and strongly irreducible. This last criterion gives an intrinsic criterion for a chain to be the characteristic set for a reflexive prime ideal.
References


