Journal of Symbolic Computation 44 (2009) 242–260

Contents lists available at ScienceDirect

Journal of Symbolic Computation

journal homepage: www.elsevier.com/locate/jsc

A characteristic set method for ordinary difference polynomial systems☆

Xiao-Shan Gao, Yong Luo, Chunming Yuan

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

ARTICLE INFO

Article history:
Received 13 March 2005
Accepted 5 May 2007
Available online 26 September 2008

Keywords:
Difference polynomial
Ascending chain
Characteristic set
Coherence
Irreducibility
Zero decomposition theorem
Automated theorem proving

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.

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 (Ritt, 1950). The method was further extended by Kolchin, Rosenfeld, Seidenberg and other people (Kolchin, 1973; Rosenfeld, 1959; Seidenberg, 1956). But, studies of the algorithmic aspect of the characteristic set method was in stagnation for quite a long time, until Wu's work appeared in the late 1970s. Since then, theories and algorithms of the characteristic set methods were revived. In Wu (1978, 1987, 1984), Wu 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 (Aubry et al.,

☆ Partially supported by a National Key Basic Research Project of China and by a USA NSF grant CCR-0201253.
E-mail address: xgao@mmrc.iss.ac.cn (X.-S. Gao).

0747-7171/$ – see front matter
doi:10.1016/j.jsc.2007.05.005

1999; Kalkbrener, 1993; Lazard, 1991; Yang et al., 1996). The decomposition into simple systems was proposed by Wang (2000). The decomposition into unmixed varieties was proposed by Bouziane et al. and Gao–Chou (Bouziane et al., 2001; Gao and Chou, 1993). The concepts of invertibility, first introduced by Lazard (1991), was studied in detail by Kandry-Rody et al. and played an important rule in Bouziane et al. (2001). Efficient algorithms for decomposing differential polynomial systems were proposed in Boulier et al. (1995), Chou and Gao (1993), Hubert (2000), Li and Wang (1999), and Reid (1991). Lazard's Lemma plays an essential rule in Boulier et al. (1995). On the complexity issues, Gallo and Mishra gave an upper bound for the degrees of the polynomials in the characteristic set of an ideal (Gallo and Mishra, 1991). Dahan and Schost (2004) 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 Ritt and Doob (1933)) for difference polynomial systems was also proposed by Ritt (Ritt and Doob, 1933). The general theory of difference algebra was established mainly by Cohn and his students (Cohn, 1965). Cohn also introduced the theory of characteristic sequence, which plays an important rule in theoretical studies, but is not an algorithm in the general case (Cohn, 1965, 1948). More recently, elimination algorithms for linear difference or differential-difference operators are extensively studied (Chyzak and Salvy, 1998; Mansfield and Szanto, 2002; Takayama, 1990; van der Hoeven, 1996). But, we are not aware of the existence of 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 important problems in difference algebra, such as the intrinsic description of reflexive prime ideals, the perfect ideal membership problem, finding the dimension and order of prime ideals, and automated proof 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 no longer true in the difference case. This makes some of the key tools used in the algebraic and differential cases no longer available in the difference case. For instance, Rosenfeld's lemma and Lazard's lemma are not true in the difference case. As a consequence, we need to introduce new concepts and to develop new techniques.

We first consider the following question: "Let $\mathcal{A}$ be a difference ascending chain. Under what condition is $\mathcal{A}$ 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 $\mathcal{A}$ be regular (Aubry et al., 1999). This result is extended to the differential cases by Kandry-Rody et al. (Bouziane et al., 2001). In order to solve this problem in the difference case, we introduce two new properties for difference ascending chains. First, the concept of *coherent ascending chain* is introduced. In the differential case, coherent conditions are needed only in the partial differential case. But, in the 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 $\mathcal{A}$ be coherent and strong irreducible. In Cohn (1965), 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 Cohn (1965) 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 Cohn (1965). 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 Cohn (1965) and Ritt and Doob (1933).

2.1. Difference fields, difference polynomials, and difference ideals

A *difference field* $\mathcal{F}$ is a field with a unitary operation δ 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, δ is called the *transforming operator* of $\mathcal{F}$. If $a \in \mathcal{F}$, δa is called the transform of a. If $\delta^{-1}a$ is defined for all $a \in \mathcal{F}$, we say that $\mathcal{F}$ is *inversive*. Every difference field has an inversive closure (Cohn, 1965). In this paper, all difference fields are assumed to be inversive and of characteristic zero.

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

Let $\mathbb{Y} = \{y_1, y_2, \ldots, y_n\}$ be indeterminants. Then $\mathcal{R} = \mathcal{K}\{\mathbb{Y}\}$ is called an *n-fold difference polynomial ring* over $\mathcal{K}$. Any *difference polynomial* P (abbr. r-pol) in the ring $\mathcal{K}\{\mathbb{Y}\}$ 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 $P \in \mathcal{K}\{\mathbb{Y}\}$. The *class* of P, denoted by $\mathrm{cls}(P)$, is the least p such that $P \in \mathcal{K}\{y_1 \ldots, y_p\}$. If $P \in \mathcal{K}$, we set $\mathrm{cls}(P) = 0$. The *order* of P w.r.t. y_i, denoted by $\mathrm{ord}(P, y_i)$, is the largest j such that $y_i(x+j)$ appears in P. When y_i does not occur in P, we set $\mathrm{ord}(P, y_i) = 0$. If $\mathrm{cls}(P) = p$ and $\mathrm{ord}(P, y_p) = q$, we called y_p the *leading variable* and $y_p(x+q)$ the *lead* of P, denoted as $\mathrm{lvar}(P)$ and $\mathrm{lead}(P)$, respectively. The leading coefficient of P as a univariate polynomial in $\mathrm{lead}(P)$ is called the *initial* of P, and is denoted as $\mathrm{init}(P)$.

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

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

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

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

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 $P \in \mathcal{K}\{\mathbb{Y}\}$. 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 $\mathcal{K}\{\mathbb{Y}\}$. An n-tuple over $\mathcal{K}$ is called a *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

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

It is easy to check that $\mathrm{Zero}(P) = \mathrm{Zero}(\delta P)$. 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 *difference ideal* is a subset $\mathbb{I}$ of $\mathcal{R} = \mathcal{K}\{\mathbb{Y}\}$, which is an algebraic ideal in $\mathcal{R}$ and is closed under δ. 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 $\mathbb{I}$ is called *reflexive* if for an r-pol P, $\delta P \in \mathbb{I}$ implies $P \in \mathbb{I}$. A difference ideal $\mathbb{I}$ is called *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 $\mathrm{Zero}(\mathbb{P}) = \emptyset$ iff $1 \in \{\mathbb{P}\}$. A difference ideal $\mathbb{I}$ is called a *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 $\mathrm{lead}(P_1) = y_p(x+q)$ with $p > 0$. P_2 is said to be *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 $P_1 \in \mathcal{K}$ and nonzero, then P_2 is not reduced w.r.t. P_1.

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

Example 2.1. Let $P_1 = y(x+1)^2 - y^2(x) + 1$, $P_2 = y(x+2) + y(x+1) \in \mathcal{K}\{y\}$. 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 $\mathcal{A}$ be a chain and $\mathbb{I}_{\mathcal{A}}$ the set of all products of powers of the initials of the r-pols in $\mathcal{A}$ and their transforms. The *saturation ideal* of $\mathcal{A}$ is defined as follows

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

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

Let $\mathcal{B}$ be an algebraic chain and $I_{\mathcal{B}}$ the set of products of powers of initials of the polynomials in $\mathcal{B}$. Then we define

$$\mathbf{asat}(\mathcal{B}) = (\mathcal{B}) : I_{\mathcal{B}} = \{P \in \mathcal{K}[\mathbb{Y}] \mid \exists J \in I_{\mathcal{B}}, s.t.\, JP \in (\mathcal{B})\}.$$

A chain $\mathcal{A} = A_1, \ldots, A_p$ is said to be of *higher rank* than another chain $\mathcal{B} = B_1, \ldots, B_s$, denoted as $\mathcal{A} \succ \mathcal{B}$, if one of the following conditions holds:

(i) $\exists\, 0 < j \le \min\{p, s\}$, such that $\forall\, i < j$, $A_i \sim B_i$ and $A_j \succ B_j$, or

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

If no one has higher rank than the other for two chains, they have the same rank, and is denoted as $\mathcal{A} \sim \mathcal{B}$. $\mathcal{A}_1 \succeq \mathcal{A}_2$ means either $\mathcal{A}_1 \succ \mathcal{A}_2$ or $\mathcal{A}_1 \sim \mathcal{A}_2$. It is easy to see that $\succeq$ is a total order on the difference chain set.

Lemma 2.1 (*Ritt and Doob, 1933*). *Let $\mathcal{A}_i$ be a sequence of chains satisfying*

$$\mathcal{A}_1 \succeq \mathcal{A}_2 \succeq \ldots \succeq \mathcal{A}_k \succeq \ldots.$$

Then, there is an index i_0 such that for any $i > i_0$, $\mathcal{A}_i \sim \mathcal{A}_{i_0}$.

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

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

Lemma 2.3 (*Ritt and Doob, 1933*). *If $\mathcal{A}$ is a characteristic set of $\mathbb{P}$ and $\mathcal{A}'$ a characteristic set of $\mathbb{P} \cup \{P\}$ for an r-pol P, then we have $\mathcal{A} \succeq \mathcal{A}'$. Moreover, if P is reduced with respect to $\mathcal{A}$, we have $\mathcal{A} \succ \mathcal{A}'$.*

The difference pseudo-division is defined as follows.

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

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

From the above algorithm, it is easy to check that

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

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

where R, Q_i $(i = 1, \ldots, k+1)$ are r-pols and $J = \prod_{i=0}^{k}(\delta^i \mathrm{init}(P))^{s_i}$ 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 $\mathcal{A} = A_1, \ldots, A_p$ recursively as $\mathrm{rprem}(P, \mathcal{A})$ =rprem($\mathrm{rprem}(P, A_p)$, $A_1, \ldots, A_{p-1}$) and $\mathrm{rprem}(P, \{\}) = P$. As a direct consequence of Lemma 2.4, we have

Lemma 2.5. *Let $P, \mathcal{A}$ be as above. Then there is a $J \in \mathbb{I}_{\mathcal{A}}$ with $J \prec P$ such that $JP \equiv R \bmod [\mathcal{A}]$ and R is reduced w.r.t $\mathcal{A}$.*

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

Theorem 3.1 (*Aubry et al., 1999, Bouziane et al., 2001*). *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 (*Bouziane et al., 2001*). *A polynomial P is not invertible w.r.t. a regular triangular set $\mathcal{A}$ iff, there is a nonzero Q in $K[\mathbb{U}, \mathbb{Y}]$ such that $PQ \in (\mathcal{A})$ and Q is reduced w.r.t. $\mathcal{A}$.*

Lemma 3.2 (*Wu, 1984*). *Let $\mathcal{A}$ be an irreducible algebraic triangular set with parameters $\mathbb{U}$, leading variables $\mathbb{Y}$, and a generic point η. Then,* **asat**$(\mathcal{A})$ *is a prime ideal of dimension $|\mathbb{U}|$ and for any polynomial Q, the following facts are equivalent.*

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

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.

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

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

$$\mathcal{P}(\mathcal{A}) = \{y_i(x+j) | 1 \leq i \leq p, 0 \leq j \leq o_{i,1} - 1\} \tag{2}$$

and call $\mathrm{ord}(\mathcal{A}) = |\mathcal{P}(\mathcal{A})| = \sum_{i=1}^{p} o_{(i,1)}$ the *order* of $\mathcal{A}$.

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

$$\begin{aligned} &A_{1,1}, \delta A_{1,1}, \ldots, \delta^{o_{1,2}-o_{1,1}-1} A_{1,1}, A_{1,2}, \ldots, \quad A_{1,k_1}, \delta A_{1,k_1}, \ldots, \delta^{\hat{h}_1 - o_{1,k_1}} A_{1,k_1}, \\ &\ldots, \\ &A_{m,1}, \delta A_{m,1}, \ldots, \delta^{o_{m,2}-o_{m,1}-1} A_{m,1}, A_{m,2}, \ldots, \quad A_{m,k_m}, \delta A_{m,k_m}, \ldots, \delta^{\hat{h}_m - o_{m,k_m}} A_{m,k_m} \end{aligned} \tag{3}$$

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

$$\begin{aligned} \mathcal{A}^* &= \mathcal{A}_{(0,\ldots,0)} \\ \mathcal{A}_P &= \mathcal{A}_{(\mathrm{ord}(P,y_1),\ldots,\mathrm{ord}(P,y_p))}. \end{aligned} \tag{4}$$

With these notations, it is clear that

$$\mathrm{rprem}(P, \mathcal{A}) = \mathrm{prem}(P, \mathcal{A}_P) \tag{5}$$

where the variables and their transforms in $\mathrm{prem}(P, \mathcal{A}_P)$ 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* $\mathcal{A}_P$ *with* y_i *as leading variable.*
- *Let* $e_j = \max_{A \in \mathcal{A}_{(h_1,\ldots,h_m)}} \{\mathrm{ord}(A, u_j)\}$, $\mathbb{V} = \{\delta^i u_j \mid 1 \leq j \leq q, 0 \leq i \leq e_j\}$, $\mathbb{Z} = \{\delta^i y_j \mid 1 \leq j \leq m, 0 \leq i \leq \hat{h}_j\}$. *Then* $\mathcal{A}_{(h_1,\ldots,h_m)}$ *is an algebraic triangular set in* $\mathcal{K}[\mathbb{V}, \mathbb{Z}]$ *when the elements in* $\mathbb{V}$ *and* $\mathbb{Z}$ *are treated as independent variables.*
- *The parameters of* $\mathcal{A}_{(h_1,\ldots,h_m)}$ *as a triangular set are* $\mathbb{V} \cup \mathcal{P}(\mathcal{A})$.

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

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

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

Let $\mathcal{A} = A_1, \ldots, A_s$ 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 $\mathcal{A}_{(h_1,\ldots,h_p)}$ for some nonnegative integers $h_1, \ldots, h_p$. In other words, $C \in (\mathcal{A}_{(h_1,\ldots,h_p)})$.

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

Proof. Let $\Delta_{ij} = \mathrm{prem}(\delta^{o_j-o_i}A_i, A_j, y_t(x+o_j))$, $I_j = \mathrm{init}(A_j)$. 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, $\mathrm{prem}(\Delta_{ij}, \mathcal{A}^*) = 0$. 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 $l_i \geq \mathrm{ord}(A_{i,o_i}, y_i)$. Then $\exists J \in I_{\mathcal{A}^*}$ s.t. $J \prec \delta P$ and $J\delta P \in (\mathcal{A}_{(l_1+1,\ldots,l_p+1)})$.*

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 $\mathrm{lvar}(B_{i,j}) = y_i$. Then we have $P = \sum_{i,j} P_{i,j}B_{i,j}$ and $\delta P = \sum_{i,j} \delta P_{i,j}\delta B_{i,j}$. Since $B_{i,c_i} \in \mathcal{A}_{(l_1,\ldots,l_p)}$ and $l_i \geq \mathrm{ord}(A_{i,o_i}, y_i)$, $\delta B_{i,c_i}$ must be in $\mathcal{A}_{(l_1+1,\ldots,l_p+1)}$. 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 $J \in \mathbb{I}_{\mathcal{A}}$ such that $J \prec \delta^m A$ and $J \cdot \delta^m A$ has a normal representation.*

Proof. Let $f_i = \mathrm{ord}(\delta^m A, y_i)$, $c = \mathrm{cls}(A)$. We divide the proof into three cases. First, if $\delta^m A \in \mathcal{A}_{(f_1,\ldots,f_p)}$, the result is obvious. Second, if there exists a $B \in \mathcal{A}$ such that $\mathrm{ord}(B, y_c) = \mathrm{ord}(\delta^m A, y_c)$, 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 $\mathrm{ord}(\delta^g B, y_c) = \mathrm{ord}(\delta^m A, y_c)$. 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 $J_1 \in \mathbb{I}_{\mathcal{A}}$ such that $\mathrm{lead}(J_1) < \mathrm{lead}(\delta^{m-g}A)$ and

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

Perform g transformations, we have

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

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

$$\delta^g J_1 \cdot J_2 \cdot \delta^m A \equiv 0 \bmod (\mathcal{A}_{(h_1+g,\ldots,h_c+g)}).$$

The condition $\mathrm{lead}(J) \prec \mathrm{lead}(\delta^m A)$ 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 $P = \sum Q_{ij}\delta^j A_i$, there is a $J \in \mathbb{I}_{\mathcal{A}}$ such that $J \cdot P$ has a normal representation, and $J \prec \max\{\delta^j A_i\}$.*

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 $I_i = \mathrm{init}(A_i)$. $\mathcal{A}$ 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 $J \in \mathbb{I}_{\mathcal{A}}$ 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 $\mathbb{U}$ 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 $N \in \mathcal{K}\{\mathbb{U}\}$ such that $QP = N \bmod [\mathcal{A}]$. If $P \in I$, then $N \in I$. Since 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* **sat**(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 **asat**$(\mathcal{B})$. Let $\mathbb{X}$ be the set of all the $\delta^i y_j \preceq \delta^u y_v$ such that $\delta^u y_v$ occurs in $\mathcal{B}$. Then $\mathcal{B} \subset \mathcal{K}[\mathbb{X}]$. If $\mathcal{B}$ is not the characteristic set of **asat**$(\mathcal{B})$, then there is a $P \in$ **asat**$(\mathcal{B}) \cap \mathcal{K}[\mathbb{X}]$ which is reduced w.r.t. $\mathcal{B}$ and is not zero. By Lemma 3.3, P does not contain $\delta^i y_j$ which is of higher rank than those in $\mathbb{X}$. As a consequence, P is also reduced w.r.t. $\mathcal{A}$. Since $P \in$ **asat**$(\mathcal{B}) \subset$ **sat**$(\mathcal{A})$ and $\mathcal{A}$ is the characteristic set of **sat**(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 $R \in$* **sat**$(\mathcal{A})$*, then $R = 0$.*

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

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

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

$$\widetilde{J} \cdot N \cdot R = \sum Q_{ij} \delta^j A_i, \tag{8}$$

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 $\delta^u A_v$ in (7), we already reduce the rank of $\delta^u A_v$ in (7). Otherwise, assume $y_k(x+q) = \max\{\mathrm{lead}(\delta^j A_i)\}$ and $\mathrm{lead}(\delta^{j_0} A_{i_0}) = y_k(x+q)$. Let us assume $A_{i_0} = I_{i_0} y_k(x+s)^{d_{i_0}} + R_{i_0}$. Then, $\delta^{j_0} A_{i_0} = \delta^{j_0} I_{i_0} y_k(x+q)^{d_{i_0}} + \delta^{j_0} R_{i_0}$. Substituting $y_k(x+q)^{d_{i_0}}$ by $-\frac{\delta^{j_0} R_{i_0}}{\delta^{j_0} I_{i_0}}$ in (8), the left hand side keeps unchanged since $\mathrm{lead}(\widetilde{J}) \prec y_k(x+q)$, N is free of $y_k(x+q)$, and R is reduced w.r.t. $\mathcal{A}$. In the right hand side, the $\delta^{j_0} A_{i_0}$ becomes zero, i.e. the $\max\{\mathrm{lead}(\delta^j A_i)\}$ decreases. Clearing denominators of the substituted formula of (8), we obtain a new equation:

$$(\delta^{j_0} I_{i_0})^t \cdot \widetilde{J} \cdot N \cdot R = \sum \hat{Q}_{ij} \delta^j A_i. \tag{9}$$

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 $(\delta^{j_0} I_{i_0})^t \cdot \widetilde{J}$ is invertible w.r.t. $\mathcal{A}$ and wit rank lower than that of $y_k(x+q)$. Repeating the process starting from the proof, we will finally obtain a nonzero $\widehat{N} \in \mathcal{K}[\mathbb{V}]$, such that $\widehat{N} \cdot R = 0$. Then $R = 0$. By Lemma 2.2, $\mathcal{A}$ is the characteristic set of **sat**$(\mathcal{A})$. ∎

The above lemma is a difference version of the Rosenfeld Lemma (Rosenfeld, 1959). 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 (Rosenfeld, 1959) is not valid in the difference case.

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

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

Theorem 3.3. *A chain $\mathcal{A}$ is the characteristic set of* **sat**(A) *iff $\mathcal{A}$ is coherent and regular.*

Proof. If $\mathcal{A}$ is coherent and regular, then by Lemma 3.9, $\mathcal{A}$ is a characteristic set of $\mathbf{sat}(A)$. Conversely, let $\mathcal{A} = A_1, \ldots, A_m$ be a characteristic set of $\mathbf{sat}(A)$ and $I_i = \mathrm{init}(A_i)$. For any $1 \le i < j \le p$, let $R = \mathrm{rprem}(\Delta_{ij}, \mathcal{A})$ where Δ_{ij} is defined in (6). Then, R is in $\mathbf{sat}(A)$ and is reduced w.r.t. $\mathcal{A}$. Since $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(A)$, $R = 0$. Then, $\mathcal{A}$ is coherent. To prove that $\mathcal{A}$ is regular, for any $i \ge 0$, $1 \le j \le m$, we need to prove that $P = \delta^i I_j$ is invertible w.r.t. $\mathcal{A}$. Assume this is not true. By definition, P is not invertible w.r.t. $\mathcal{A}_P$ when they are treated as algebraic equations. By Lemma 3.8, $\mathcal{A}_P$ is a regular algebraic chain. By Lemma 3.1, there is a nonzero Q which is reduced w.r.t. $\mathcal{A}_P$ (and hence $\mathcal{A}$) such that $PQ = \delta^i I_j Q \in (A_P) \subset [A]$. Then $Q \in \mathbf{sat}(A)$ and Q is reduced w.r.t. $\mathcal{A}$. Since $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(A)$, this is impossible. Hence, $P = \delta^i I_j$ is invertible w.r.t. $\mathcal{A}$ and $\mathcal{A}$ is regular. ∎

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

Theorem 3.4. *If $\mathcal{A}$ is a coherent and regular chain of form (1), then*

$$\mathbf{sat}(\mathcal{A}) = \bigcup_{h_1 \ge 0, \ldots, h_p \ge 0} (\mathbf{asat}(\mathcal{A}_{(h_1, \ldots, h_p)})).$$

Proof. It is easy to see that $\mathbf{sat}(\mathcal{A}) \supset \bigcup_{h_1 \ge 0, \ldots, h_m \ge 0} (\mathbf{asat}(\mathcal{A}_{(h_1, \ldots, h_p)}))$. Let $P \in \mathbf{sat}(\mathcal{A})$. Since $\mathcal{A}$ is coherent and regular, by Theorem 3.3, $\mathcal{A}$ is the characteristic set of $\mathbf{sat}(\mathcal{A})$, and hence $\mathrm{rprem}(P, \mathcal{A}) = \mathrm{prem}(P, \mathcal{A}_f) = 0$. That is $P \in \mathbf{asat}(\mathcal{A}_P)$. Hence $\mathbf{sat}(\mathcal{A}) \subset \bigcup_{h_1 \ge 0, \ldots, h_m \ge 0} \mathbf{asat}(\mathcal{A}_{(h_1, \ldots, h_p)}))$. ∎

4. Proper and strong irreducible chains

Note that there is no direct method to check wether 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 $\mathcal{A}$ of the form (1) is said to be *proper irreducible* if

- $\mathcal{A}^*$ 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 $\mathcal{K}(\eta_{c-1})[y_c(x), \ldots, y_c(x + f_c)]$, where $f_c = \mathrm{ord}(A_{c,1}, y_c)$, $\mathcal{B}_c = \mathcal{A}^* \cap \mathcal{K}\{\mathbb{U}, y_1, \ldots, y_c\}$ ($\mathcal{B}_0 = \emptyset$), η_c is a generic point for the algebraic irreducible chain $\mathcal{B}_c$, and $\hat{A}_{c,1}$ is obtained by substituting η_{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 $\mathcal{A} = A_1, \ldots, A_m$ and $I_j = \mathrm{init}(A_j)$. Since $\mathcal{A}^*$ is an irreducible algebraic triangular set, by Lemma 3.2, I_i are invertible w.r.t. $\mathcal{A}^*$ and hence invertible w.r.t. $\mathcal{A}$. By Lemma 4.2, all $\delta^j I_i$ are invertible w.r.t. $\mathcal{A}$. ∎

We need to prove several lemmas.

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

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 $\mathrm{resl}(P, \mathcal{A}^*) \neq 0$. If $p = 1$, $P \in \mathcal{K}[\mathbb{V}, y_1(x+1), \ldots, y_1(x+f_1)]$, where $\mathbb{V}$ is the set of $\delta^i u_j$ occurring in P and $\mathcal{A}^*$. Variable $y_1(x+f_1)$ must occur in P effectively. Otherwise P is already invertible w.r.t. $\mathcal{A}^*$. Note that the lead of any r-pol in $\mathcal{A}$ other than $A_{1,1}$ is of higher rank than $y_1(x+f_1)$. Then $R = \mathrm{resl}(P, \mathcal{A}^*) = \mathrm{resl}(P, A_{1,1}, y_1(x+f_1))$. If $R = 0$, then $A_{1,1}|P$, since $A_{1,1}$ is irreducible. This is impossible, since $y_1(x)$ occurs in $A_{1,1}$ ($\mathcal{A}$ 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 $\mathrm{resl}(P, \mathcal{B}_{p-1}) \neq 0$. Since $\mathcal{A}$ is proper irreducible, $\mathcal{B}_{p-1}$ is an algebraic irreducible triangular set. For any polynomial Q, let $\hat{Q}$ be obtained from Q by substituting $\mathbb{U}, y_i$ with η_{p-1}. Substituting η_{p-1} into P and $A_{p,1}$ we get two polynomials in $\hat{P} \in \mathcal{K}(\eta)[y_p(x+1), \ldots, y_p(x+f_p)]$ and $\hat{A}_{p,1} \in \mathcal{K}(\eta)[y_p(x), \ldots, y_p(x+f_p)]$. Since $\mathrm{resl}(P, \mathcal{B}_{p-1}) \neq 0$, $\hat{P} \neq 0$. Furthermore, $\hat{A}_{p,1}$ involves $y_p(x)$ effectively. This is because $A_{p,1}$ is reduced w.r.t. $\mathcal{B}_{p-1}$, and hence by Lemma 3.2, the term containing $y_p(x)$ does not vanish after the substitution. Let $R = \mathrm{resl}(P, A_{p,1}, y_p(x+f_p))$. We will show that $\hat{R} \neq 0$. Since $\mathcal{A}$ is proper irreducible, $\hat{A}_{p,1}$ is an irreducible polynomial. If $\hat{R} = 0$, then $\hat{A}_{p,1}|\hat{P}$, which is impossible, since $y_m(x)$ occurs in $\hat{A}_{p,1}$ effectively but not in P. Since $\mathcal{B}_{p-1}$ is irreducible, by Lemma 3.2, $\hat{R} \neq 0$ is equivalent to the fact that R is invertible w.r.t. $\mathcal{B}_{p-1}$. Therefore, P is invertible w.r.t. $\mathcal{A}^*$. ∎

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

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

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

$$\delta\hat{P} \cdot \delta P - \delta N = \sum_{A \in \mathcal{A}_P} Q_A \delta A. \tag{10}$$

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

$$J\delta\bar{P} \cdot \delta P \equiv J\delta g \bmod (\mathcal{A}_{\delta P}). \tag{11}$$

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

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

$$T \cdot J\delta N \equiv R \bmod (\mathcal{A}^*) \equiv R \bmod (\mathcal{A}_{\delta P}).$$

The last equality is valid because $\mathcal{A}^* \subset \mathcal{A}_{\delta P}$. Hence,

$$T \cdot J\delta\hat{P} \cdot \delta P \equiv T \cdot J \cdot \delta N \equiv R \bmod (\mathcal{A}_{\delta P}).$$

That is, δP is invertible w.r.t. $\mathcal{A}$. ∎

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 δQ is not, which implies that Lemma 4.2 is not true without this assumption.

4.2. Consistence 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, Zero($\mathbf{sat}(A)$) is not empty. The proof of Theorem 4.2 uses the theory of difference kernels established by Cohn (1965). 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.

Let $\mathbf{a}_i = (a_{i,1}, \ldots, a_{i,n})$, $i = 0, \ldots, r$ be n-tuples, where $a_{i,j}$ are elements from an extension field of $\mathcal{K}$. A *difference kernel* of length r, $\mathcal{R} = \mathcal{K}(\mathbf{a}_0, \mathbf{a}_1, \ldots, \mathbf{a}_r)$, over the difference field $\mathcal{K}$ is an algebraic field extension of $\mathcal{K}$ such that the difference operator δ of $\mathcal{K}$ can be extended to a field isomorphism from $\mathcal{K}(\mathbf{a}_0, \ldots, \mathbf{a}_{r-1})$ to $\mathcal{K}(\mathbf{a}_1, \ldots, \mathbf{a}_r)$ and $\delta\mathbf{a}_i = \mathbf{a}_{i+1}$, $i = 0, \ldots, r-1$.

Theorem 4.2. *Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then* Zero($\mathbf{sat}(A)$) $\neq \emptyset$, *or equivalently,* $1 \notin \{\mathbf{sat}(\mathcal{A})\}$.

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 $\mathrm{lvar}(B_{i,j}) = y_i$. Let $o_i = \mathrm{ord}(B_{i,c_i}, y_i)$, $i = 1, \ldots, p$, $e = \max_{A\in\mathcal{A}^*, 1\le j\le q}\{\mathrm{ord}(A, u_j)\}$, $\mathbb{U}_0 = \{\delta^i u_j \mid 1 \le j \le q, 0 \le i \le e\}$, $\mathbb{U}_1 = \{\delta^i u_j \mid 1 \le j \le q, 1 \le i \le e+1\}$, $\mathbb{Y}_0 = \{\delta^i y_j \mid 1 \le j \le p, 0 \le i \le o_j - 1\}$, and $\mathbb{Y}_1 = \{\delta^i y_j \mid 1 \le j \le p, 1 \le i \le o_j\}$. Then $\mathbb{V}_0 = \mathbb{U}_0 \cup \mathbb{Y}_0$ and $\mathbb{V}_1 = \mathbb{U}_1 \cup \mathbb{Y}_1$ 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, $I = \mathbf{sat}(\mathcal{A}^*)$ is a prime ideal in $\mathcal{K}[\hat{\mathbb{V}}]$, where $\hat{\mathbb{V}} = \mathbb{U}_0 \cup \mathbb{Y}_0 \cup \{\delta^{o_1} y_1, \ldots, \delta^{o_p} y_p\}$. Let $\eta = (\alpha_j^{(i)}, \beta_j^{(i)})$ be a generic zero of this prime ideal. Then $\delta^j u_i = \alpha_i^{(j)}$, $\delta^j y_i = \beta_i^{(j)}$ annul every polynomial in $\mathcal{A}^*$ but not their initials.

We will construct a difference kernel of length one. Now, let $\mathbf{a}_0$ and $\mathbf{a}_1$ be obtained from $\mathbb{V}_0$ and $\mathbb{V}_1$ by replacing $\delta^j u_i$ and $\delta^j y_i$ with the corresponding $\alpha_j^{(i)}$ and $\beta_j^{(i)}$. The kernel is $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$. The difference operator δ introduces a map from $\mathcal{K}(\mathbf{a}_0)$ to $\mathcal{K}(\mathbf{a}_1)$ as follows $\delta(\alpha_j^{(i)}) = \alpha_j^{(i+1)}$ and $\delta(\beta_j^{(i)}) = \beta_j^{(i+1)}$. We will prove that δ introduces an isomorphism between $\mathcal{K}(\mathbf{a}_0)$ and $\mathcal{K}(\mathbf{a}_1)$. Let

$$\mathcal{B}_0 = \mathcal{A}^* - \{B_{1,c_1}, \ldots, B_{p,c_p}\},\ \mathcal{B}_1 = \{\delta A \mid A \in \mathcal{B}_0\}.$$

From the definition of $\mathcal{A}^*$, the orders of y_k in $B_{i,j} \in \mathcal{B}_0$ are not exceeding $o_k - 1$. As a consequence, $\mathbf{a}_0$ is a generic zero of the algebraic prime ideal I_0 with $\mathcal{B}_0$ as a characteristic set.

Note that $\delta\mathcal{B}_0 = \mathcal{B}_1$ and $\delta\mathbf{a}_0 = \mathbf{a}_1$, by the nature of the difference operator, $\mathcal{B}_1$ is an irreducible triangular set in $\mathcal{K}[\mathbb{V}_1]$ and $\mathbf{a}_1$ is a generic zero of the prime ideal I_1 with $\mathcal{B}_1$ as a characteristic set. We will show that $I_1 = (\mathcal{B}_1) : I_{\mathcal{B}_1} = I \cap \mathcal{K}[\mathbb{V}_1]$. Let $t_i = \mathrm{ord}(B_{i,1})$, $\mathbb{U}^* = \mathbb{U}_0 \cup \mathbb{U}_1$, $\mathbb{Y}^* = \mathbb{Y}_0 \cup \mathbb{Y}_1$. Since each $B_{i,1}$ is effective, we can choose $\mathbb{U}^*$ and $\{y_{i,j} | 1 \le i \le p, 1 \le j \le t_i\}$ as the parametric set of $I \cap \mathcal{K}[\mathbb{U}^*, \mathbb{Y}^*]$. Then the number of parameters in I_0 is the same as that of $I \cap \mathcal{K}[\mathbb{V}_1]$. I_1 has the same number of parameters as I_0. Hence I_1 also has the same number of parameters as $I \cap \mathcal{K}[\mathbb{V}_1]$. Since these two prime ideals I_1 and $I \cap \mathcal{K}[\mathbb{V}_1]$ have the same parameter set and $I_1 \subset I \cap \mathcal{K}[\mathbb{V}_1]$, we have $I_1 = I \cap \mathcal{K}[\mathbb{V}_1]$. Since $\delta I_0 \to I_1$ is an isomorphism between two prime ideals, $\delta\mathcal{K}(\mathbf{a}_0) \to \mathcal{K}(\mathbf{a}_1)$ is a field isomorphism. As a consequence, $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$ is a difference kernel over $\mathcal{K}$.

By Lemma V on page 156 of Cohn (1965), the kernel $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$ has a principal realization ψ corresponding to a series of kernels $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1)$, $\mathcal{K}(\mathbf{a}_0, \mathbf{a}_1, \mathbf{a}_2)$, ... We will show that ψ is a zero of $\mathbf{sat}(\mathcal{A})$. From the construction of the kernel, for any $A \in \mathcal{A}^*$, we have $A(\psi) = A(\eta) = 0$. Hence, ψ is a zero of the polynomials in $\mathcal{A}^*$ but does not annul any initials of $\mathcal{A}^*$. Then for any $A \in \mathcal{A}$, η is a zero of $\delta^k A$ for any k, since δ is an isomorphism. Also, η does not annul any $J \in \mathbb{I}_{\mathcal{A}}$. As a consequence, $\eta \in$ Zero($\mathbf{sat}(A)$). ∎

The following example, due to Cohn through private communication, shows that a coherent and regular chain could have no solutions.

Example 4.2. Let $A_1 = y_1^2 + 1, A_2 = y_1(x+1) - y_1, A_3 = y_2^2 + 1, A_4 = y_2(x+1) + y_2$, and $\mathcal{A} = \{A_1, A_2, A_3, A_4\}$. $\mathcal{A}$ is coherent and regular. But $\mathcal{A}$ is not proper irreducible, since $A_3 - A_1 = (y_2 - y_1)(y_2 + y_1)$. We have Zero($\mathbf{sat}(\mathcal{A})$) = Zero($\mathcal{A}$) = Zero($\mathcal{A} \cup \{y_2 - y_1\}$) $\cup$ Zero($\mathcal{A} \cup \{y_2 - y_1\}$) = $\emptyset$.

4.3. Characteristic sets of reflexive prime ideals

The following example shows that for a coherent and proper irreducible chain $\mathcal{A}$, $\mathbf{sat}(\mathcal{A})$ does not necessarily need to be a perfect or prime ideal. It also shows that Lazard's lemma cannot be generalized to the difference case.

Example 4.3. Let $A = y_1^2 + 1$ and $\mathcal{A} = A$. Then $\mathcal{A}$ is coherent and proper irreducible over $\mathcal{K} = \mathbb{O}(x)$. We will show that $\mathbf{sat}(\mathcal{A}) = [A]$ is not a perfect ideal. $\delta A - A = PQ$ where $P = y_1(x+1) - y_1$, $Q = y_1(x+1) + y_1$. If $[A]$ is a perfect ideal, from $PQ \in [A]$, we have

$$P\delta Q\delta(P\delta Q) = P\delta^2 Q\delta(PQ) \in [A].$$

Hence, $P\delta Q \in [A]$. By Theorem 4.1, $\mathcal{A}$ is a regular chain and $\mathrm{rprem}(P\delta Q, A) = 0$. But, a direct computation shows that $\mathrm{rprem}(P\delta Q, \mathcal{A}) \neq 0$, 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_i, $\mathcal{A}_{(h_1,\ldots,h_p)}$ is an irreducible algebraic triangular set.

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

Proof. Let P, Q be two r-pols such that $PQ \in \mathbf{sat}(A)$. 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, $P \in \mathbf{sat}(A)$ or $Q \in \mathbf{sat}(A)$. Hence, $\mathbf{sat}(A)$ is a prime ideal. We still need to show that $\mathbf{sat}(A)$ is reflexive, that is, if $\delta P \in \mathbf{sat}(A)$ then $P \in \mathbf{sat}(A)$. Suppose $P \notin \mathbf{sat}(A)$. By Theorem 3.4, $P \notin (\mathcal{A}_P) : I_{\mathcal{A}_P}$. Since $\mathcal{A}_P$ is an irreducible algebraic triangular set, P must be invertible w.r.t. $\mathcal{A}_P$. As a consequence, P is invertible w.r.t. $\mathcal{A}$. By Lemmas 3.7 and 4.2, δP is invertible w.r.t. $\mathcal{A}$ and hence $\delta P \notin \mathbf{sat}(A)$, which contradicts the fact $\delta P \in \mathbf{sat}(A)$. We proved that $\mathbf{sat}(\mathcal{A})$ is a reflexive prime ideal.

We will prove that $\mathbb{U}$ is a *complete parameter set* of $\mathbf{sat}(\mathcal{A})$, that is $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}\} = \{0\}$ and $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}, y_i\} \neq \{0\}$ for every i. By Theorems 4.1 and 3.3, $\mathcal{A}$ is a characteristic set of $\mathbf{sat}(\mathcal{A})$. Then, $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}\} = \emptyset$, since every non-zero r-pol in $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}\}$ is reduced w.r.t to $\mathcal{A}$ and hence must be zero. If there exists an i, such that $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}, y_i\} = \{0\}$, let $h = |\mathcal{P}(\mathcal{A})|$ (see (2)) and $\mathcal{C} = \mathcal{A}_{(0,\ldots,0,h,0,\ldots,0)}$, where h is at the i-th place. Let $\mathbb{Y}'$ and $\mathbb{U}'$ be the set of all $y_i(x+j)$ and $u_k(x_l)$ occurring in $\mathcal{C}$ and $\mathbb{Y}'' = \mathbb{Y}' \cup \mathcal{P}(\mathcal{A})$. By Lemma 3.2, $\mathbf{asat}(\mathcal{C})$ is a prime ideal of dimension $\dim(A) = h$ in $\mathcal{K}(\mathbb{U}')[\mathbb{Y}'']$. On the other hand, $\mathbf{asat}(\mathcal{C}) \cap \mathcal{K}(\mathbb{U}')[y_{i,0}, \ldots, y_{i,h}] \subset \mathbf{sat}(\mathcal{A}) \cap \mathcal{K}(\mathbb{U}')[y_{i,0}, \ldots, y_{i,h}] = \{0\}$. From this, we have $\dim(\mathbf{asat}(\mathcal{C})) \geq h+1$, a contradiction. This proves that $\mathbb{U}$ is a complete parameter set of $\mathbf{sat}(\mathcal{A})$. Then, by Theorem IV on page 127 of Cohn (1965), $\dim(\mathbf{sat}(\mathcal{A})) = \dim(\mathcal{A})$.

The relative order of $\mathbf{sat}(\mathcal{A})$ w.r.t. $\mathbb{U}$ is defined to be the number of $y_i(x+h)$ which are algebraically independent module $\mathbf{sat}(\mathcal{A})$ in $\mathcal{K}(\mathbb{U})\{\mathbb{Y}\}$ (page 128 of Cohn (1965)). By Lemma 3.3, this is just the dimension of the algebraic prime ideal $\mathbf{asat}(\mathcal{A}^*)$ in $\mathcal{K}(\mathbb{U})\{\mathbb{Y}\}$, which is $|\mathcal{P}(\mathcal{A})| = \mathrm{ord}(\mathcal{A})$ 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 $I = \mathbf{sat}(A)$.*

Proof. By Lemma 4.3, for any characteristic set $\mathcal{A}$ of I, we have $I = \mathbf{sat}(A)$. 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 $\mathcal{B}_c = \mathcal{A}^* \cap \mathcal{K}\{\mathbb{U}, y_1, \ldots, y_c\}$ ($\mathcal{B}_0 = \emptyset$) and η_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 $\mathcal{K}(\eta_{c-1})[y_c(x), \ldots, y_c(x+f_c)]$, where $f_c = \mathrm{ord}(A_{c,1}, y_c)$. It is obvious that the u_i and y_i in (1) satisfy the conditions in Lemma 4.5.

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

Since I is a prime ideal, there exists a non-zero $P_i \in I_i = I \cap \mathcal{K}\{U, y_i\}$ 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_1 is not effective in y_1, we may assume that P_1 is effective in one of the u_i, say u_1. Otherwise, P_1 is not effective in all the variables P_1 and hence $P_1 = \delta Q_1$ for some r-pol Q_1. Since I is reflexive, $Q_1 \in I$, which contradicts the fact that P_1 has the lowest order in y_1. 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 $\mathbb{V} = \{u_2, \ldots, u_q, y_i\}$ as the parameter set. Let $P'_j, j = 1, \ldots, i-1$ be the irreducible r-pols which have the lowest rank and total degree in $I \cap \mathcal{K}\{\mathbb{V}, y_j\}$ and P'_i the irreducible r-pol which has the lowest rank and total degree in $I \cap \mathcal{K}\{\mathbb{V}, u_1\}$. We will show that $P'_j, 1 \leq j < i$ 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 $I \cap \mathcal{K}\{\mathbb{V}, u_1\}$ 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, $\mathrm{prem}(P_i, \mathcal{B}_{P_i}) = 0$ implies $\mathrm{prem}(Q_k, \mathcal{B}_{P_i}) = 0$ 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'_j is effective in y_j. Otherwise, we choose the characteristic set $\mathcal{B}'$ of $I \cap \mathcal{K}\{u_2, \ldots, u_q, y_i, u_1, y_j\}$ 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'_j 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, $\mathrm{prem}(P_i, \mathcal{B}'_{P_j}) = 0$ implies $\mathrm{prem}(Q_k, \mathcal{B}'_{P_j}) = 0$ 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 $I = \mathbf{sat}(A)$.*

Proof. It is clear that $I \subset \mathbf{sat}(A)$. Let $P \in \mathbf{sat}(\mathcal{A})$. Then, there is a $J \in \mathbb{I}_{\mathcal{A}}$ such that $JP \in [A] \subset I$. 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_i, $\mathcal{A}_{(h_1,\ldots,h_p)}$ 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 $PQ \in \mathcal{A}_{(h_1,\ldots,h_p)} \subset \mathbf{sat}(A) = I$. 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 $\mathcal{K}\{u_1, \ldots, u_q, y_1, \ldots, y_p\}$ such that $I \cap \mathcal{K}\{u_1, \ldots, u_q\} = \{0\}$, for each y_i, $I_i = I \cap \mathcal{K}\{u_1, \ldots, u_q, y_i\} \neq \{0\}$, 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 $u_i < y_1 < y_2 < \cdots < y_p$ 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 $\mathrm{ord}(P_c, y_c) = \mathrm{ord}(A_{c,1}, y_c)$. As a consequence, when computing $\mathrm{prem}(P_c, \mathcal{A}_{P_c})$, 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, $\mathrm{prem}(P_c, \mathcal{A}_{P_c}) = 0$ implies $\mathrm{prem}(Q_k, \mathcal{A}_{P_c}) = 0$ and hence $Q_k \in I$ which contradicts the fact the 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 $\mathrm{lord}(P, y_i)$). Now the transformation of variables is $y_i(x) = z_i(x + h_{i+1} + \cdots + h_n)$, $i = 1, \ldots, n-1$ 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 $\mathrm{lord}(\hat{P}, z_j) = \mathrm{lord}(P, y_j) + h_{j+1} + \cdots + h_n \geq \mathrm{lord}(P, y_i) + h_{i+1} + \cdots + h_n = \mathrm{lord}(\hat{P}, z_i)$, for $j = 1, \ldots, i-1$. Since $\mathcal{K}$ is inversive, we get an effective r-pol $\bar{P} = \delta^{-\mathrm{lord}(\hat{P}, z_i)}\hat{P}$ in $\mathcal{K}\{z_1, \ldots, z_n\}$. We obtain a set of effective r-pols $\bar{\mathbb{P}}$ from $\mathbb{P}$. If $\mathbf{a} = (a_1, \ldots, a_n)$, $a_i \in \mathcal{F}$ is a solution of $\mathbb{P}$. Then in the inversive 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 $\mathbf{b} = (b_1, \ldots, b_n)$ is a solution of $\bar{\mathbb{P}}$. On the other hand, for any solution $\mathbf{b} = (b_1, \ldots, b_n)$ of $\bar{\mathbb{P}}$. 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 $\mathbf{a} = (a_1, \ldots, a_n)$ of $\mathbb{P}$. ∎

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

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 $\bar{\mathbb{P}}$.

```
Begin
    h_i := 0, i = 1, ..., n; P̄ := { };
    For P in P do
        if i := cls(P) then h_i := max(h_i, lord(P, y_i));
    T := {y_i(x) = z_i(x + h_{i+1} + ··· + h_n), i = 1, ..., n};
    P̂ := subs(T, P); (Do a variable change as in Lemma 5.1)
    For P in P̂ do
        let k := cls(P);
        P̄ := P̄ ∪ {δ^{-lord(P, z_k)} P};
    return(T, P̄);
end.
```

Example 5.1. Let

$$\mathbb{P} = \begin{Bmatrix} y_1(x+1) + xy_1(x),\ y_1(x)y_2(x+3) + y_2(x+2), \\ y_2(x+4) + y_1(x)y_2(x+1),\ y_3(x+3) + y_2(x)y_3(x+1) \end{Bmatrix}.$$

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

$$\hat{\mathbb{P}} = \begin{Bmatrix} z_1(x+4) + xz_1(x+3),\ z_1(x+3)z_2(x+4) + z_2(x+3), \\ z_2(x+5) + z_1(x+3)z_2(x+2),\ z_3(x+3) + z_2(x+1)z_3(x+1) \end{Bmatrix}.$$

Hence $\bar{\mathbb{P}} = \{z_1(x+1) + (x-3)z_1(x),\ z_1(x)z_2(x+1) + z_2(x),\ z_2(x+3) + z_1(x+1)z_2(x),\ z_3(x+2) + z_2(x)z_3(x)\}$. Note that each r-pol in $\bar{\mathbb{P}}$ is effective.

It is easy to verify the following properties.

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 $\mathcal{A}_1, \mathcal{A}_2$ in $\mathcal{K}\{y_1, \ldots, y_n\}$ become the r-pols $\bar{A}_1, \bar{A}_2, \bar{P}, \bar{Q}$ and chains $\bar{\mathcal{A}}_1, \bar{\mathcal{A}}_2$ in $\mathcal{K}\{z_1, \ldots, z_n\}$ respectively. Then, we have $A_1 \prec A_2 \iff \bar{A}_1 \prec \bar{A}_2$, $\mathcal{A}_1 \prec \mathcal{A}_2 \iff \bar{\mathcal{A}}_1 \prec \bar{\mathcal{A}}_2$, and $\mathrm{Zero}(P) = \mathrm{Zero}(Q) \iff \mathrm{Zero}(\bar{P}) = \mathrm{Zero}(\bar{Q})$.*

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

Proof. By Lemma 5.2, $\hat{\mathcal{A}}$ is a chain in $\mathcal{K}\{z_1, \ldots, z_n\}$. If $\hat{\mathcal{A}}$ is effective, $\hat{\mathcal{A}} \subset \bar{\mathbb{P}}$. Hence, it has a higher or equal rank than that of $\bar{\mathcal{A}}$. Otherwise, there is an $A_i \in \hat{\mathcal{A}}$ 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 $\bar{A}_i \prec A_i$. Hence $\hat{\mathcal{A}} \succ \bar{\mathcal{A}}$. ∎

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

```
Begin
    [T, P̂] = Effective(P), B = { };
    while P̂ ≠ { } do
        P̂ =the r-pols in P̂ which are reduced w.r.t. B;
        B = B ∪ {one of r-pols with the lowest rank in P̂};
    return(T, P̂, B)
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 $P \in \mathbb{P}$, $\mathrm{rprem}(P, \mathcal{A}) = 0$.

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 $\mathbb{P}$, $I_i = \mathrm{init}(A_i)$, and $J = \prod_{i=1}^m I_i$. Then*

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

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

ECohWuCharSet($\mathbb{P}$) Input: a finite set $\mathbb{P}$ of r-pols. Output: a variable transformation $\mathbf{T} = \{y_i(x) = z_i(x + k_i), i = 1, \ldots, n\}$, an effective r-pol set $\mathbb{P}'$, and a coherent and effective chain $\mathcal{A} \subset \mathbb{P}'$ such that

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

The following algorithm is a modification of a standard algorithm to compute the Wu characteristic set of a finite polynomials set (Wu, 1984).

Begin
  $\mathbb{P}' := \mathbb{P}, \mathbb{R} := \mathbb{P}, \mathbf{T} = \mathbf{I}$ is the identity variable transformation;
  while $\mathbb{R} \neq \{\}$ do
    $[\bar{\mathbf{T}}, \mathbb{P}', \mathcal{A}] := \text{ECharSet}(\mathbb{P}')$;
    $\mathbb{R} := \{\text{rprem}(f, \mathcal{B}) \mid f \in \Delta(\mathcal{A})\} \setminus \{0\}$;
    $\mathbb{R} := \mathbb{R} \cup \{\text{rprem}(P, \mathcal{A}) \mid P \in \mathbb{P}'\} \setminus \{0\}$;
    $\mathbb{P}' = \mathbb{P}' \cup \mathbb{R}$;
    $\mathbf{T} = \bar{\mathbf{T}} \circ \mathbf{T}$; (compositions of variable transformation))
  return($\mathbf{T}, \mathbb{P}', \mathcal{A}$)
end.

In Algorithm **ECohWuCharSet($\mathbb{P}$)**, $\Delta(\mathcal{A})$ is the set of Δ r-pols defined in (6). The r-pols in $\mathbb{R}$ 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 $\mathbb{P}$. 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*

$$\text{Zero}(\mathbb{P}) = \cup_{i=1}^{h}\text{Zero}(\mathbb{P}, P_i) \bigcup \cup_i \text{Zero}(\mathbb{P}, I_i).$$

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 Wu (1984), 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 $\mathbb{P}$, $P \in [\mathbb{P}]$. Then $\text{Zero}(\mathbb{P}) = \text{Zero}(\mathbb{P} \cup \{P\}) = \cup_{i=1}^{h}\text{Zero}(\mathbb{P}, P_i) \bigcup \cup_i \text{Zero}(\mathbb{P}, I_i)$. ∎

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

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

$$\text{Zero}(\hat{\mathbb{P}}) = \bigcup_{i=1}^{t} \text{Zero}(\textbf{sat}(\hat{\mathcal{A}}_i))$$

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

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

Proof of the correctness of the Algorithm. In algorithm **ECohCharSet**, since $\text{Zero}(\mathbb{P}') = \text{Zero}(\hat{\mathbb{P}})$ and $\mathcal{A} \subset \mathbb{P}'$, it is clear that if $\mathcal{A}$ is trivial $\text{Zero}(\mathbb{P}) = \emptyset$. Note that $\mathcal{A}$ is already coherent. If $\mathcal{A}$ is proper irreducible, then we have an output. The correctness of the return value is due to Lemma 5.4 and the fact $\text{Zero}(\mathbb{P}') = \text{Zero}(\hat{\mathbb{P}})$. If $\mathcal{A}$ 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 $\mathcal{A}$. Then by Lemmas 2.3, 5.2 and 5.3, the rank of $\mathcal{A}$ obtained from $\text{RittWuDec}(\mathbb{P}' \cup \mathcal{A} \cup \{I_i\})$ or $\text{RittWuDec}(\mathbb{P}' \cup \mathcal{A} \cup \{P_i\})$ has lower rank. Then by Lemma 2.1, the algorithm terminates. Note that for each $\mathcal{A}_i$, we have a variable transformation $\mathbf{T}_i$ to ensure that $\mathcal{A}_i$ is effective. In order to obtain a decomposition for $\mathbb{P}$, we need to have a "maximal" variable transformation such that all $\mathcal{A}_i$ can be represented explicitly in terms of these variables. ∎

Example 5.2. Let

$$\begin{aligned} P_1 &= (y_1(x+1) - y_1(x))^2 - (y_1(x+1) + y_1(x)) \\ P_2 &= (y_1(x+3) - y_1(x+1)) * y_2(x+1) + (y_1(x+2) - y_1(x)) * y_2(x). \end{aligned}$$

$\textbf{RittWuDec}(P_1)$ returns $\{P_1\}$. $\textbf{RittWuDec}(P_1, P_2)$ returns two chains:

$$\begin{cases} P_1, y_1(x+2) - y_1(x) \\ P_1, y_1(x+2) - 2y_1(x+1) + y_1(x) - 1, P_3 \end{cases}$$

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 $\mathcal{K}\{y_1, \ldots, y_n\}$ and the Ritt–Wu zero decomposition of $\mathbb{P}$ is $\{[\mathcal{A}_1, \mathbf{T}_1], \ldots, [\mathcal{A}_k, \mathbf{T}_k]\}$. 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. ∎

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 regarded 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 Chyzak and Salvy (1998), Mallinger (1996), Takayama (1990) and Zeilberger (1990). 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. We use two examples to show how to prove difference identities with Ritt–Wu's zero decomposition algorithm, given below.

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

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

It is denoted as $F(a, b, r; z) = \sum_0^\infty c_k z^k$, where c_k satisfies

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

To prove

$$(r-1)F(a, b, r-1; z) - aF(a+1, b, r; z) - (r-a-1)F(a, b, r; z) = 0, \tag{12}$$

let us denote $F(a, b, r-1; z) = \sum_0^\infty a_k z^k$. Then a_k satisfies $(n+1)(n+r-1)a_{n+1} - (n+a)(n+b)a_n = 0$, $a_0 = 1$. Denote $F(a+1, b, r; z) = \sum_0^\infty b_k z^k$. 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

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

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:

$$\begin{aligned} A_1 = {} & (b+1+n)\,(n+b)\,(n+1+a)\,(n+a)\,h_n - 2\,(n+r)\,(n+1)\,(b+1+n)\\ & \times (n+1+a)\,h_{n+1} + (n+2)\,(n+1)\,(n+r+1)\,(n+r)\,h_{n+2}. \end{aligned}$$

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 concerning Fibonacci numbers. The Fibonacci number F_n satisfies

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

We will prove the Cassini identity:

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

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 Mallinger (1996), a difference equation of order three $h_{n+3} - 2\,h_{n+2} - 2\,h_{n+1} + h_n$ is obtained with linear algebraic tools. In Chyzak and Salvy (1998), 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 it 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 a 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 strong irreducible. This last criterion gives an intrinsic criterion for a chain to be the characteristic set for a reflexive prime ideal.

References

Aubry, P., Lazard, D., Maza, M.M., 1999. On the theory of triangular sets. J. Symbolic Comput. 25, 105–124.
Boulier, F., Lazard, D., Ollivier, F., Petitiot, M., 1995. Representation for the radical of a finitely generated differential ideal. In: Proc. of ISSAC'95. ACM Press, pp. 158–166.
Bouziane, D., Kandri Rody, A., Maârouf, H., 2001. Unmixed-dimensional decomposition of a finitely generated perfect differential ideal. J. Symbolic Comput. 31, 631–649.
Chou, S.C., Gao, X.S., 1993. Automated reasoning in differential geometry and mechanics using the characteristic set method, Part I. An improved version of Ritt–Wu's decomposition algorithm. J. Automat. Reason. 10, 161–172.
Chyzak, F., Salvy, B., 1998. Non-commutative elimination in Ore algebras proves multivariate indentities. J. Symbolic Comput. 26, 187–227.
Cohn, R.M., 1948. Manifolds of difference polynomials. Trans. AMS 64, 133–172.
Cohn, R.M., 1965. Difference Algebra. Interscience Publishers.
Dahan, X., Schost, E., 2004. Sharp estimates for triangular sets. In: Proc. of ISSAC'04. ACM Press, New York, pp. 103–110.
Gallo, G., Mishra, B., 1991. Efficient Algorithms and Bounds for Wu-Ritt Characteristic Sets. In: Progress in Mathematics, vol. 94. Birkhauser, pp. 119–142.
Gao, X.S., Chou, S.C., 1993. The dimension of ascending chains. Chinese Sci. Bull. 38 (5), 396–399.
Hubert, E., 2000. Factorization-free decomposition algorithms in differential algebra. J. Symbolic Comput. 29, 641–662.
Kalkbrener, M., 1993. A generalized Euclidean algorithm for computing triangular representations of algebraic varieties. J. Symbolic Comput. 15, 143–167.
Kolchin, E., 1973. Differential Algebra and Algebraic Groups. Academic Press, New York.
Lazard, D., 1991. A new method for solving algebraic systems of positive dimension. Discrete Appl. Math. 33, 147–160.
Li, Z., Wang, D.M., 1999. Coherent, regular and simple systems in zero decomposition of partial differential systems. J. Systems Sci. Math. Sci. 12, 43–60.
Mallinger, C., 1996. Algorithmic manipulations and transformations of univariate holonomic functions and sequence. Master Thesis, RISC-Linz.
Mansfield, E.L., Szanto, A., 2002. Elimination theory for differential difference polynomials. In: Proc. ISSAC,02. ACM Press, New York, pp. 191–198.
Reid, G., 1991. Algorithms for reducing a system of PDEs to standard form. European J. Appl. Math. 2, 293–318.
Ritt, J.F., Doob, J.L., 1933. Systems of algebraic difference equations. Amer. J. Math. 55, 505–514.
Ritt, J.F., 1950. Differential algebra, Amer. Math. Soc. Colloquium.
Rosenfeld, A., 1959. Specialization in differential algebra. Trans. AMS 90, 394–407.
Seidenberg, A., 1956. An elimination theory for differential algebra. Univ. California Publication in Math. 3, 31–65.
Takayama, N., 1990. Gröbner basis, integration and transcendental functions. In: Proc. of ISSAC'90. ACM Press, New York, pp. 152–156.
van der Hoeven, J., 1996. Differential and mixed differential-difference equations from the effective viewpoint, Preprints.
Wang, D., 2000. Elimination Methods. Springer, Berlin.
Wu, W.T., 1978. On the decision problem and the mechanization of theorem in elementary geometry. Scientia Sinica 21, 159–172.
Wu, W.T., 1987. A Constructive Theorey of Differential Algebraic Geometry. In: Lect. Notes in Math., No. 1255. Springer, pp. 173–189.
Wu, W.T., 1984. Basic Principle of Mechanical Theorem Proving in Geometries. Science Press, Beijing, (in Chinese), Springer, Wien, 1994.
Yang, L., Zhang, J.Z., Hou, X.R., 1996. Non-linear Algebraic Equations and Automated Theorem Proving. ShangHai Science and Education Pub., ShangHai, (in Chinese).
Zeilberger, D., 1990. A holonomic systems approach to special function identities. J. Comput. Appl. Math. 32, 321–368.