A Characteristic Set Method For
Ordinary Difference Polynomial Systems

Xiao-Shan Gao, Yong Luo, and Gui-Lin Zhang
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS, Academia Sinica, Beijing, 100080, China
xgao@mmrc.iss.ac.cn, guilin80@163.com

Abstract. We prove several basic properties for difference ascending chains including a unique representation theorem for a coherent ascending chain, 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.

Keywords: difference polynomial, ascending chain, characteristic set, invertibility, coherence, irreducibility, Ritt-Wu’s zero decomposition theorem.

1. Introduction

This is an improved version of the paper [11] by Gao and Luo. Major changes have been made for Sections 4 and 5. Section 6 is new.

We give a new definition for the concept of proper irreducible chain. Comparing to the old definition, the new definition is more natural. We show that if a chain is proper irreducible in the old sense, then it is also proper irreducible according to the new definition. As a consequence, results proved in the above mentioned paper are still correct. In particular, proper irreducible chains under the old definition is much easier to check than the old one. Another advantage of using the new definition is that the following result is now valid: the characteristic set of a reflexive prime ideal is coherent and strong irreducible. If using the old definition, we can only prove that: there exists a variable order such that the characteristic set of a reflexive prime ideal is coherent and strong irreducible under this variable order.

With the new definition of the proper irreducible chain, the zero decomposition algorithm in Section 5 is also updated. The new algorithm appears much simpler than the old one.

In [6], Cohn gave an algorithm to solve the nullstellensatz test of perfect difference ideals. The idea is to transform the problem to a difference ideal with order less than or equal to one and then use zero decomposition algorithms in algebraic case to construct a difference kernel. This certainly simplifies the problem. On the other hand, reduce the order of r-pols to one by introducing new auxiliary variables destroy the structure of the ideal itself. In Section 6, by combining the idea of Cohn and the concept of algebraic irreducible chains, we give another algorithm of zero decomposition for difference polynomial systems.
To make the paper self contained, we keep Sections 2 and 3, which are basically the same as the old version, although minor revisions are made to these two sections.

2. Preliminaries

We will introduce the notions and preliminary properties needed in this paper. Details on these concepts can be found in [6, 22].

2.1. Difference fields, difference polynomials and difference ideals

A difference field \( \mathcal{F} \) is a field with a third unitary operation \( \sigma \) satisfying: for any \( a, b \in \mathcal{F} \), \( \sigma(a + b) = \sigma a + \sigma b \), \( \sigma(ab) = \sigma a \cdot \sigma b \), and \( \sigma a = 0 \) if and only if \( a = 0 \). Here, \( \sigma \) is called the transforming operator of \( \mathcal{F} \). If \( a \in \mathcal{F} \), \( \sigma a \) is called the transform of \( a \). \( \sigma^n a = \sigma(\sigma^{n-1} a) \) is known as the \( n \)'th transform. If \( \sigma^{-1} a \) is defined for all \( a \in \mathcal{F} \), we say that \( \mathcal{F} \) is inversive. Every difference field has an inversive closure [6]. In this paper, all difference fields are assumed to be inversive.

As an example, let \( \mathcal{K} \) be the set of rational functions in variable \( x \) defined on the complex plane. Let \( \sigma \) be the mapping: \( \sigma f(x) = f(x + 1) \), \( f \in \mathcal{K} \). Then \( \mathcal{K} \) is a difference field with transforming operator \( \sigma \). This is an inversive field.

Let \( x_1, x_2, \ldots, x_n \) be difference indeterminants. Then \( \mathcal{R} = \mathcal{K}\{x_1, \ldots, x_n\} \) is called an \( n \)-fold difference polynomial ring over \( \mathcal{K} \). Any difference polynomial \( f \) (abbr. \( r \)-pol) in the ring \( \mathcal{K}\{x_1, \ldots, x_n\} \) is an ordinary polynomial in variables \( \sigma^k x_j (k = 0, 1, 2, \ldots, j = 1, \ldots, n) \).

For convenience, we also denote \( \sigma^k x_j \) by \( x_{j,k} \).

Let \( f \in \mathcal{K}\{x_1, \ldots, x_n\} \). The class of \( f \), denoted by \( \text{class}(f) \), is the least \( p \) such that \( f \in \mathcal{K}\{x_1, \ldots, x_p\} \). If \( f \in \mathcal{K} \), we set \( \text{class}(f) = 0 \). The order of \( f \) w.r.t. \( x_i \), denoted by \( \text{ord}(f, x_i) \), is the largest \( j \) such that \( x_{i,j} \) appears in \( f \). When \( x_i \) does not occur in \( f \), we set \( \text{ord}(f, x_i) = 0 \). If \( \text{class}(f) = p \) and \( \text{ord}(f, x_p) = q \), we call \( x_p \) the leading variable and \( x_{p,q} \) the lead of \( f \), denoted as \( \text{ivar}(f) \) and \( \text{lead}(f) \), respectively. The leading coefficient of \( f \) as a univariate polynomial in \( \text{lead}(f) \) is called the initial of \( f \), and is denoted as \( \text{init}(f) \).

An \( r \)-pol \( f_1 \) has higher rank than an \( r \)-pol \( f_2 \), denoted as \( f_1 \prec f_2 \), if

i). \( \text{class}(f_1) > \text{class}(f_2) \), or

ii). \( c = \text{class}(f_1) = \text{class}(f_2) \) and \( \text{ord}(f_1, x_c) > \text{ord}(f_2, x_c) \)

iii). \( c = \text{class}(f_1) = \text{class}(f_2), o = \text{ord}(f_1, x_c) = \text{ord}(f_2, x_c) \) and \( \text{deg}(f_1, x_{c,o}) > \text{deg}(f_2, x_{c,o}) \).

If no one has higher rank than the other for two \( r \)-pols, they are said to have the same rank, denoted as \( f_1 \equiv f_2 \). We use \( f_1 \preceq f_2 \) to denote the relation of either \( f_1 \prec f_2 \) or \( f_1 \equiv f_2 \).

It is easy to see that \( \preceq \) is a total order on the \( r \)-pol ring.

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 \( f \in \mathcal{K}\{x_1, \ldots, x_n\} \). To substitute an \( n \)-tuple \( \mathbf{a} \) into \( f \) means to replace each of the \( x_{i,j} \) occurring in \( f \) with \( \sigma^i a_i \). Let \( \mathbb{P} \) be a set of \( r \)-pols in \( \mathcal{K}\{x_1, \ldots, x_n\} \). 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. We use \( \text{Zero}(\mathbb{P}) \) to denote the set of solutions of \( \mathbb{P} = 0 \). Let \( f \in \mathcal{K}\{x_1, \ldots, x_n\} \). It is easy to check that \( \text{Zero}(f) = \text{Zero}(\sigma f) \).

We use \( \text{Zero}(\mathbb{P}/\mathbb{D}) \) to denote the set of solutions of \( \mathbb{P} = 0 \) which do not annihilate any \( r \)-pol of \( \mathbb{D} \).

A difference ideal is a subset \( \mathcal{I} \) of \( \mathcal{R} = \mathcal{K}\{x_1, \ldots, x_n\} \), which is an algebraic ideal in \( \mathcal{R} \) and is closed under transforming. A difference ideal \( \mathcal{I} \) is called reflexive if for an \( r \)-pol \( f \),
σf ∈ ℐ implies f ∈ ℐ. Let ℙ be a set of elements of ℓ. The difference ideal generated by ℙ is denoted by [ℙ]. Obviously, [ℙ] is the set of all linear combinations of the r-pols in ℙ and their transforms. The (ordinary or algebraic) ideal generated by ℙ is denoted as (ℙ). A difference ideal ℐ is called perfect if the presence in ℐ of a product of powers of transforms of an r-pol f implies f ∈ ℐ. The perfect difference ideal generated by ℙ is denoted as {ℙ}. A perfect ideal is always reflexive. A difference ideal ℐ is called a prime ideal if for r-pols f and g, fg ∈ ℐ implies f ∈ ℐ or g ∈ ℐ.

2.2. Difference ascending chains

Let f₁,f₂ be two r-pols and lead(f₁) = xₚ,q. f₂ is said to be reduced w.r.t. f₁ if deg(f₂,xₚ,q+i) < deg(f₁,xₚ,q) for any nonnegative integer i.

A finite sequence of nonzero r-pols A = A₁,...,Aₚ is called an ascending chain, or simply a chain, if one of the two following conditions holds:

i). p = 1 and A₁ ≠ 0, or

ii). 0 < class(Aₙ), Aᵢ < Aⱼ and Aⱼ is reduced w.r.t. Aᵢ for 1 ≤ i < j ≤ p.

A is called trivial if class(A₁) = 0.

Example 2.1 Let us consider f₁ = x₁²,₁,₁ − x₁₀,₀ + 1, f₂ = x₁,₂ + x₁,₁ ∈ Ω{x₁} which is 1-fold polynomial difference ring over Ω. Since f₁ ∼ f₂, deg(f₂,x₁,₁) < deg(f₁,x₁,₁) and deg(f₂,x₁,₂) < deg(f₁,x₁,₁), by the definition, f₂ is reduced w.r.t. f₁. Hence, {f₁,f₂} is a difference chain.

Let A be a chain and ℐ₄ the set of all products of powers of the initials and their transforms of the r-pols in A. The saturation ideal of A is defined as follows

\[ \text{sat}(A) = \{ f ∈ Ω{x₁,...,xₙ} | ∃ g ∈ ℐ₄, fg ∈ [A] \}. \]

Let B be an algebraic chain and ℐ₅ the set of products of powers of initials of the polynomials in B. Then we define

\[ \text{a-sat}(B) = \{ f ∈ Ω[x₁,...,xₙ] | ∃ g ∈ ℐ₅, fg ∈ (B) \}. \]

Note that ℐ₄ is closed under transforming and multiplication. Then [A] : ℐ₄ is a difference ideal.

A chain A = A₁,...,Aᵢ is said to be of higher rank than another chain B = B₁,...,Bᵢ, denoted as A ∼ B, if one of the following conditions holds:

i). ∃ 0 < j ≤ min{t,s}, such that ∀ i < j, Aᵢ ≡ Bᵢ and Aⱼ > Bⱼ, or

ii). s > t and Aᵢ ≡ Bᵢ for i ≤ t.

If no one has higher rank than the other for two chains, they have the same rank, and is denoted as A ∼ B. We use A₁ ≤ A₂ to denote the relation of either A₁ < A₂ or A₁ ≡ A₂. It is easy to see that ≤ is a total order on the difference chain set.

Lemma 2.2 [22] Let Aᵢ be a sequence of chains satisfying

\[ A₁ ≥ A₂ ≥ ... ≥ Aₖ ≥ ... \]  

Then there is an index i₀ such that for any i > i₀, Aᵢ ≡ Aᵢ₀.

Let ℙ be a set of r-pols. It is possible to form chains with r-pols in ℙ. Among all those chains, by the above lemma, there are some which have a lowest rank. Any of those
chairs contained in \( \mathcal{P} \) with the lowest rank is called a characteristic set of \( \mathcal{P} \), and denoted by \( \mathcal{B} = C.S(\mathcal{P}) \).

An r-pol is said to be reduced w.r.t. a chain if it is reduced to every r-pol in the chain.

**Lemma 2.3** [22] If \( \mathcal{A} \) is a characteristic set of \( \mathcal{P} \) and \( \mathcal{A}' \) a characteristic set of \( \mathcal{P} \cup \{f\} \) for an r-pol \( f \), then we have \( \mathcal{A} \succeq \mathcal{A}' \). Moreover, if \( f \) is reduced with respect to \( \mathcal{A} \), we have \( \mathcal{A} \succ \mathcal{A}' \).

As a consequence, we have

**Lemma 2.4** \( \mathcal{A} \) is a characteristic set of \( \mathcal{P} \) if and only if there is no nonzero r-pol in \( \mathcal{P} \) which is reduced w.r.t. \( \mathcal{A} \).

### 2.3. Difference Pseudo-remainders

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

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

where \( \text{lvar}(A_{i,j}) = y_i \) and \( U = \{u_1, \ldots, u_q\} \) such that \( p + q = n \). Let \( o_{i,j} = \text{ord}(A_{i,j}, y_i) \) and \( h_1, \ldots, h_m (m \leq p) \) nonnegative integers. We use \( \mathcal{A}_{(h_1, \ldots, h_m)} \) to denote the following sequence of r-pol

\[
A_{1,1}, \sigma A_{1,1}, \ldots, \sigma^{o_{1,2}-o_{1,1}}A_{1,1}, A_{1,2}, \ldots, A_{1,k_1}, \sigma A_{1,k_1}, \ldots, \sigma^{h_1-o_{1,1}}A_{1,k_1}, \\
\ldots, \\
A_{m,1}, \sigma A_{m,1}, \ldots, \sigma^{o_{m,2}-o_{m,1}}A_{m,1}, \ldots, \sigma A_{m,k_m}, \ldots, \sigma^{h_m-o_{m,k_m}}A_{m,k_m} \tag{2}
\]

where \( \bar{h}_i \) is defined as follows: \( \bar{h}_m = \max\{h_m, o_{m,k_m}\} \), and for \( i = m - 1, \ldots, 1 \), \( o_i = \max\{\text{order of } y_i \text{ appears in } A_{i+1,1}, \sigma A_{i+1,1}, \ldots, \sigma^{\bar{h}_m-o_{m,k_m}}A_{m,k_m}\} \),

\( \bar{h}_i = \max\{h_i, o_i, o_{i,k}\} + 1 \). Note that the definition for \( \bar{h}_i \) is used in the proof of Theorem 4.4. For a chain \( \mathcal{A} \) and an r-pol \( f \), let

\[
\mathcal{A}^* = \mathcal{A}_{(0,\ldots,0)} \\
\mathcal{A}_f = \mathcal{A}_{(\text{ord}(f,y_1),\ldots,\text{ord}(f,y_p))} \tag{3}
\]

We also let \( \mathcal{A}_c = \{f \in \mathcal{A}^*|\text{class}(f) \leq c\} \), \( \mathcal{A}_{c,j} \) is the \( j \)th r-pol of \( \mathcal{A}_c \backslash \mathcal{A}_{c-1} \), clearly \( \mathcal{A}_{c,1} \in \mathcal{A} \).

**Lemma 2.5** Use the notations in (2). Let \( e_j = \max_{A \in \mathcal{A}_{(h_1, \ldots, h_m)}} \{|\text{ord}(A, u_j)| \} \), \( V = \{\sigma^i u_j | 1 \leq j \leq q, 0 \leq i \leq e_j\} \), \( Y = \{\sigma^i y_j | 1 \leq j \leq m, 0 \leq i \leq \bar{h}_j\} \). Then \( \mathcal{A}_{(h_1, \ldots, h_m)} \) is an algebraic triangular set in \( \mathcal{K}[V, Y] \) when the elements in \( V \) and \( Y \) are treated as independent variables. Furthermore, the parameters of \( \mathcal{A}_{(h_1, \ldots, h_m)} \) as a triangular set are \( V \) and \( y_{i,0}, y_{i,1}, \ldots, y_{i,o_{i,1}}, i = 1, \ldots, m \).

The difference pseudo-division is defined as follows.

**Algorithm 2.6** \texttt{prem}(g, f)

- **Input**: \( g, f \in \mathcal{K}\{x_1, \ldots, x_n\} \).
- **Output**: an r-pol \( r \) which is the pseudo remainder of \( g \) w.r.t. \( f \).
Begin
\[c := \text{class}(f); \quad s := \text{ord}(g, x_c); \quad t := \text{ord}(f, x_c);\]
If \(c = 0\) then Return 0;
If \(s < t\) then Return \(g\);
else
\[r := g;\]
for \(i\) from \(s - t\) to 0 by -1 do
\[r := \text{a-prem}(r, \sigma^i f, x_{c,t+i}); \tag{(*)}\]
If \(r = 0\) then Return 0;
Return \(r\);
End;

In (*) \(\text{a-prem}(f, g, x)\) is the algebraic pseudo-remainder of \(f\) w.r.t. \(g\) about variable \(x\), where the variables \(x_i\) and their transforms are treated as independent algebraic variables. \(\text{a-prem}(f, g)\) is \(\text{a-prem}(f, g, x)\) where \(x\) is the leading variables of \(g\).

From the above algorithm, it is easy to check that

**Lemma 2.7** Let \(r = \text{prem}(g, f)\) be the difference pseudo-remainder of \(g\) w.r.t. \(f\), and \(\text{lead}(f) = x_{c,s}(c > 0), t = \text{ord}(g, x_c)\) and \(k = t - s \geq 0\). Then \(r\) is reduced w.r.t. \(f\) and we have the remainder formula

\[J g = g_1 \sigma^k f + g_2 \sigma^{k-1} f + \cdots + g_{k+1} f + r,\]

where \(r, g_i(i = 1, \ldots, k + 1)\) are \(r\)-pols and \(J = \prod_{i=0}^{k} (\sigma^i \text{init}(f))^{s_i}\) for non-negative integers \(s_i\). Note that \(\text{lead}(J) \prec x_{c,t} = \text{lead}(g)\).

We define the pseudo-remainder of an \(r\)-pol \(g\) w.r.t. a chain \(A = A_1, \ldots, A_p\) recursively as \(\text{rprem}(g, A) = \text{rprem}(\text{rprem}(g, A_p), A_1, \ldots, A_{p-1})\), and \(\text{rprem}(g, \emptyset) = g\). With these notations, it is clear that

\[\text{prem}(f, A) = \text{a-prem}(f, A_f)\]

where the variables and their transforms in \(\text{a-prem}(P, A_f)\) are treated as independent algebraic variables. As a direct consequence of Lemma 2.7, we have

**Lemma 2.8** Let \(g, A\) be as above. Then there is a \(J \in \mathbb{I}_A\) with \(\text{lead}(J) \prec \text{lead}(g)\) such that \(J g \equiv r \mod [A]\) and \(r\) is reduced w.r.t. \(A\).

3. Coherent and regular difference chains

In this section, properties of coherent and regular chains are introduced.

3.1. Coherent difference chains

Note that in Example 2.1, we have \(\sigma f_1 - (y_2 + y_1) f_2 = 1\), i.e. \(1 \in [f_1, f_2]\). This fact leads to the following concept.

Let \(A = A_1, \ldots, A_m\) be a difference chain in \(\mathcal{K}\{y_1, \ldots, y_n\}\) and \(k_i = \text{ord}(A_i, \text{lvar}(A_i)), \quad i = 1, \ldots, m\). For any \(1 \leq i < j \leq m\), if \(\text{class}(A_i) = \text{class}(A_j) = t\), let \(\Delta_{ij} = \text{a-prem}(\sigma^{k_j - k_i} A_i, A_j, y_{i,j})\) be the algebraic pseudo-remainder of \(\sigma^{k_j - k_i} A_i\) w.r.t. \(A_j\) about variable \(y_{i,j}\); otherwise, let \(\Delta_{ij} = 0\). If \(\text{prem}(\Delta_{ij}, A) = \text{a-prem}(\Delta_{ij}, A^*) = 0\), we call \(A\) a coherent difference chain.
Let $\mathcal{A} = A_1, \ldots, A_n$ be a chain. A linear combination $g = \sum_{i,j} f_{ij}\sigma^j A_i$ is called canonical if $\sigma^j A_i$ in the expression are distinct elements in $\mathcal{A}_h$ for some nonnegative integers $h_1, \ldots, h_p$. In other words, $g \in (\mathcal{A}_{(h_1,\ldots,h_p)})$.

**Lemma 3.1** Let $\mathcal{A} = A_1, \ldots, A_m$ be a coherent difference chain, $\text{class}(A_i) = \text{class}(A_j) = t, i < j$, and $k_i = \text{ord}(A_i, lvar(A_i)), i = 1, \ldots, m$. Then there exists a $J \in I_{\mathcal{A}}^*$ such that $\text{lead}(J) < \text{lead}(A_j)$ and

$$J \cdot \sigma^{k_j-k_i} A_i \equiv 0 \mod (\mathcal{A}^*).$$

**Proof.** Let $\Delta_{ij} = \text{a-prem}(\sigma^{k_j-k_i} A_i, A_j, y_{t,k_j})$, $I_j = \text{init}(A_j)$. Then there is a nonnegative integer $v$ such that $I_j^v \cdot \sigma^{k_j-k_i} A_i = g A_j + \Delta_{ij}$. By the definition of r-prem, we have $\mathcal{A}_\Delta = \mathcal{A}^*$. Then there exists a $J \in I_{\mathcal{A}}^*$ such that $\text{lead}(J) < \text{lead}(\Delta_{ij}) < \text{lead}(A_j)$ such that

$$\bar{J} \cdot \Delta_{ij} \equiv 0 \mod (\mathcal{A}^*)$$

Let $J = I_j^v \bar{J}$. Then $J \cdot \sigma^{k_j-k_i} A_i \equiv J \Delta_{ij} \equiv 0 \mod (\mathcal{A}^*)$. It is clear that $\text{lead}(J) < \text{lead}(A_j)$.

**Lemma 3.2** Let $\mathcal{A}$ be a coherent chain of form (1), $f \in (\mathcal{A}_{(l_1,\ldots,l_p)})$ for $l_i \geq \text{ord}(A_{i,k_i}, y_i)$. Then $\exists J \in I_{\mathcal{A}}^*$ s.t. $\text{lead}(J) < \text{lead}(\sigma f)$ and $J \sigma f \in (\mathcal{A}_{(l_1+1,\ldots,l_p+1)})$.

**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 $lvar(B_{i,j}) = y_i$. Then we have $f = \sum_{i,j} p_{i,j} B_{i,j}$ and $\sigma f = \sum_{i,j} \sigma p_{i,j} B_{i,j}$. Since $B_{i,c_i} \in \mathcal{A}_{(l_1,\ldots,l_p)}$ and $l_i \geq \text{ord}(A_{i,k_i}, y_i)$, $\sigma B_{i,c_i}$ must be in $\mathcal{A}_{(l_1+1,\ldots,l_p+1)}$. For $j < c_i$, $\sigma B_{i,j}$ is either in $\mathcal{A}_{(l_1,\ldots,l_p)}$ or fall in the situation considered in Lemma 3.1. This proves the Lemma.

**Lemma 3.3** 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 $\text{lead}(J) < \text{lead}(\sigma^m A)$ and $J \cdot \sigma^m A$ has a canonical representation.

**Proof.** Let $l_i = \text{ord}(\sigma^m A, y_i), c = \text{class}(A)$. We divide the proof into three cases. First, if $\sigma^m A \in \mathcal{A}_{(l_1,\ldots,l_p)}$, the result is obvious. Second, if there exists a $B \in \mathcal{A}$ such that $\text{ord}(B, y_c) = \text{ord}(\sigma^m A, y_c)$, then this is Lemma 3.1. Third, if there exists a $B \in \mathcal{A}$ with a higher lead than that of $A$ and an integer $h > 0$ such that $\text{ord}(\sigma^h B, y_c) = \text{ord}(\sigma^m A, y_c)$. It is clear that $h < m$. 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 3.1, there is a $J_1 \in I_{\mathcal{A}}$ such that $\text{lead}(J_1) < \text{lead}(\sigma^{m-h} A)$ and

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

Without loss of generality, we may assume that $h_i \geq \text{ord}(A_{i,k_i}, y_i)$ in order to use Lemma 3.2. Perform $h$ transformations, we have

$$\sigma^h J_1 \cdot \sigma^m A \equiv 0 \mod (\sigma^h \mathcal{A}_{(h_1,\ldots,h_c)}).$$

Each element of $\sigma^h \mathcal{A}_{(h_1,\ldots,h_c)}$ which appear in the right of the above formula satisfy the induction hypothesis. Then by the induction hypothesis and Lemma 3.2 there is a $J_2 \in I_{\mathcal{A}}$ such that $\text{lead}(J_2) < \text{lead}(\sigma^m A)$ and

$$\sigma^h J_1 \cdot J_2 \cdot \sigma^m A \equiv 0 \mod (\mathcal{A}_{(h_1+h,\ldots,h_c+h)}).$$
the condition $\text{lead}(\sigma^h J_1 \cdot J_2) \prec \text{lead}(\sigma^m A)$ is clearly valid.  

The following is the key property of a coherent chain.

**Theorem 3.4** If $\mathcal{A} = A_1, \ldots, A_s$ is a coherent difference chain, for any $f = \sum g_{ij} \sigma^j A_i$, there is a $J \in \mathbb{I}_\mathcal{A}$ such that $J \cdot f$ has a canonical representation, and $\text{lead}(J) \prec \max\{\text{lead}(\sigma^j A_i)\}$. 

**Proof.** This is a direct consequence of Lemma 3.3.

### 3.2. Invertibility of algebraic polynomials

We will introduce some notations and known results about invertibility of algebraic polynomials w.r.t. a chain. In this section, all notions mean to be algebraic case.

Let $\mathcal{A} = A_1, \ldots, A_m$ be a nontrivial triangular set in $K[x_1, \ldots, x_n]$ over a field $K$ of characteristic zero. Let $y_i$ be the leading variable of $A_i$, $y = \{y_1, \ldots, y_p\}$ and $u = \{x_1, \ldots, x_n\} \setminus y$. $u$ is called the parameter set of $\mathcal{A}$. We can denote $K[x_1, \ldots, x_n]$ as $K[u, y]$. A polynomial $f$ is said to be invertible w.r.t. $\mathcal{A}$ if $(f, A_1, \ldots, A_s) \cap K[u] \neq \{0\}$ where $\text{lvar}(f) = \text{lvar}(A_s)$. $\mathcal{A}$ is called regular if the initials of $A_i$ are invertible w.r.t. $\mathcal{A}$.

**Theorem 3.5** [1, 3] Let $\mathcal{A}$ be a triangular set. Then $\mathcal{A}$ is a characteristic set of $(\mathcal{A}) : I_A$ iff $\mathcal{A}$ is regular.

**Lemma 3.6** [3] A finite product of polynomials which are invertible w.r.t. $\mathcal{A}$ is also invertible w.r.t. $\mathcal{A}$.

**Lemma 3.7** [3] A polynomial $f$ is not invertible w.r.t. a regular triangular set $\mathcal{A}$ iff there is a nonzero $g$ in $K[u, y]$ such that $fg \in (\mathcal{A})$ and $g$ is reduced w.r.t. $\mathcal{A}$.

**Lemma 3.8** Let $f, g$ be polynomials in $K[x_1, \ldots, x_n]$ with $\text{class}(f) = \text{class}(g) = n$. $f$ is irreducible and $\text{resultant}(f, g, x_n) = 0$ then $f \mid g$.

**Proof.** It is a corollary of the Lemma 7.2.3 in Mishra’s book [19].

**Lemma 3.9** [30, 19] Let $\mathcal{A}$ be an irreducible algebraic triangular set with a generic point $\eta$. Then for any polynomial $f$, the following facts are equivalent.

- $g$ is invertible w.r.t. $\mathcal{A}$.
- $\text{prem}(g, \mathcal{A}) \neq 0$, or equivalently $g \notin (\mathcal{A}) : I_A$.
- $\bar{g} \neq 0$, where $\bar{g}$ is obtained by substituting $\eta$ into $g$.
- $\text{resl}(g, \mathcal{A}) \neq 0$. Let $\mathcal{A} = A_1, \ldots, A_m$, $\text{resl}(g, \mathcal{A})$ is defined as follows: $\text{resl}(g, \mathcal{A}) = \text{resl}(\text{resl}(g, A_m, \text{lvar}(A_m)), A_1, \ldots, A_{m-1})$, and $\text{resl}(g, \emptyset) = g$.

### 3.3. Difference regular chains

Let $\mathcal{A}$ be a difference chain of form (1), $f$ an r-pol. $f$ is said to be invertible w.r.t. $\mathcal{A}$ if it is invertible w.r.t. $\mathcal{A}_f$ when $f$ and $\mathcal{A}_f$ are treated as algebraic polynomials.

Let $\mathcal{A} = A_1, \ldots, A_m$ be a difference chain and $I_i = \text{init}(A_i)$. $\mathcal{A}$ is said to be (difference) regular if $\sigma^i I_j$ is invertible w.r.t. $\mathcal{A}$ for any non-negative integer $i$ and $1 \leq j \leq m$. 
Lemma 3.10 Let $\mathcal{A}$ be a characteristic set of an ideal $I$. If an r-pol $f$ is invertible w.r.t $\mathcal{A}$, then $f \not\in I$.

Proof. Let $\forall$ be the algebraic parameter set of $\mathcal{A}$. Since $f$ is invertible w.r.t $\mathcal{A}$, there exists an r-pol $g$ and a nonzero $r \in K[\forall]$ such that $gf = r \mod [\mathcal{A}]$. If $f \in I$, we have $r \in I$. Since $r$ is reduced w.r.t $\mathcal{A}$, by Lemma 2.4, we have $r = 0$, a contradiction. \qed

Lemma 3.11 If a difference chain $\mathcal{A}$ of form (1) is the characteristic set of sat($\mathcal{A}$), then for any nonnegative integers $h_1, \ldots, h_p$, $\mathcal{A}_{(h_1, \ldots, h_p)}$ is a regular algebraic triangular set.

Proof. By Theorem 3.5, we need only to prove that $\mathcal{B} = \mathcal{A}_{(h_1, \ldots, h_p)}$ is the characteristic set of sat($\mathcal{B}$). Let $\forall$ be the set of all the $\sigma^k u_j$ and $\sigma^j y_k$ such that $\sigma^j y_k$ is of equal or lower rank than an $\sigma^u y_k$, which occurs in $\mathcal{B}$. Then $\mathcal{B} \subset K[\forall]$. If $\mathcal{B}$ is not the characteristic set of sat($\mathcal{B}$), then there is a $f \in$ sat($\mathcal{B}$) $\cap K[\forall]$ which is reduced w.r.t $\mathcal{B}$ and is not zero. By Lemma 2.5, $f$ does not contain $\sigma^j y_k$ which is of higher rank than those in $\forall$. As a consequence, $f$ is also reduced w.r.t. $\mathcal{A}$. Since $f \in$ sat($\mathcal{B}$) $\subset$ sat($\mathcal{A}$) and $\mathcal{A}$ is the characteristic set of sat($\mathcal{A}$), $f$ must be zero, a contradiction. \qed

Lemma 3.12 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 $r = 0$. As a consequence, $\mathcal{A}$ is the characteristic set of sat($\mathcal{A}$).

Proof. Let $\mathcal{A} = A_1, A_2, \ldots, A_m$. Since $r \in$ sat($\mathcal{A}$), there is a $J_1 \in I_{\mathcal{A}}$ such that $J_1 \cdot r \equiv 0 \mod [\mathcal{A}]$. By Lemma 3.6, $J_1$ is invertible w.r.t $\mathcal{A}$, i.e. there is an r-pol $J_1$ and a nonzero $N \in K[\forall]$ such that

$$J_1 \cdot J_1 \equiv N \mod [\mathcal{A}]$$

where $\forall$ is the set of parameters of $A^*$ as an algebraic triangular set (see Lemma 2.5). Hence, $N \cdot r \equiv J_1 \cdot J_1 \cdot r \equiv 0 \mod [\mathcal{A}]$. Or equivalently,

$$N \cdot r = \sum g_{i,j} \sigma^j A_j. \quad (5)$$

Since $\mathcal{A}$ is a coherent chain, by Theorem 3.4, there is a $J_2 \in I_{\mathcal{A}}$ such that $J_2 N \cdot r$ has a canonical representation in $[\mathcal{A}]$, where lead($J_2$) $\prec$ max{lead($\sigma^j A_j$)} in (5). That is

$$J_2 \cdot N \cdot r = \sum g_{i,j} \sigma^j A_i, \quad (6)$$

where, each $\sigma^j A_i$ has a different lead. If the max{lead($\sigma^j A_i$)} in (6) is of lower rank than that of max{lead($\sigma^j A_i$)} in (5), we already reduce the rank of max {lead ($\sigma^j A_i$)} in (5). Otherwise, assume $y_{k,q} = \max \{\text{lead($\sigma^j A_i$)}\}$ and lead($\sigma^a A_b$) = $y_{k,q}$. Let us assume $A_b = I_b y_{k,s}^d + R_b$. Then $\sigma^a A_b = \sigma^a I_b y_{k,s}^d + \sigma^a R_b$. Substituting $y_{k,q}^d$ by $\frac{-\sigma^a R_b}{\sigma^a I_b}$ in (6), the left side keeps unchanged since lead($J_2$) $\prec$ $y_{k,q}$, $N$ is free of $y_{k,q}$ and $r$ is reduced with respect to $\mathcal{A}$. In the right side, the $\sigma^a A_b$ becomes zero, i.e. the max{lead($\sigma^j A_i$)} decreases. Clearing denominators of the substituted formula of (6), we obtain a new equation:

$$(\sigma^a I_b)^l \cdot J_2 \cdot N \cdot r = \sum f_{i,j} \sigma^j A_i. \quad (7)$$

In the right side of (7), the lead of $\sigma^j A_i$ with highest rank is less than $y_{k,q}$ and $(\sigma^a I_b)^l \cdot J_2$ is invertible w.r.t $\mathcal{A}$ and can be represented as a linear combination of a nonzero polynomial in $K[\forall]$ and $\sigma^j A_i$ with leads of rank lower than $y_{k,q}$. Repeating the above process, we obtain
Let us consider difference chain \( \mathcal{A} \) is coherent and regular, w.r.t. \( A \). We will give a constructive criterion for \( \mathcal{A} \) to be difference regular. 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.

Theorem 3.14 A difference chain \( \mathcal{A} \) is the characteristic set of \( \text{sat}(\mathcal{A}) \) iff \( \mathcal{A} \) is coherent and difference regular.

Proof. If \( \mathcal{A} \) is coherent and difference regular, then by Lemma 3.12, \( \mathcal{A} \) is a characteristic set of \( \text{sat}(\mathcal{A}) \). Conversely, let \( \mathcal{A} = A_1, A_2, \ldots, A_m \) be a characteristic set of the saturation ideal \( \text{sat}(\mathcal{A}) \) and \( I_i = \text{init}(A_i) \). For any \( 1 \leq i < j \leq p \), let \( r = \text{prem}(\Delta_{ij}, \mathcal{A}) \) as in the definition of regular chains. Then \( r \) is in \( \text{sat}(\mathcal{A}) \) and is reduced w.r.t. \( \mathcal{A} \). Since \( \mathcal{A} \) is the characteristic set of \( \text{sat}(\mathcal{A}) \), \( f = 0 \). Then \( \mathcal{A} \) is coherent. To prove that \( \mathcal{A} \) is regular, for any \( i \geq 0, 1 \leq j \leq m \), we need to prove that \( f = \sigma^i I_j \) is invertible w.r.t. \( \mathcal{A} \). Assume this is not valid. By definition, \( f \) is not invertible w.r.t. \( \mathcal{A}_f \) when they are treated as algebraic equations. By Lemma 3.11, \( \mathcal{A}_f \) is a regular algebraic chain. By Lemma 3.7, there is a \( 0 \neq g \) which is reduced w.r.t. \( \mathcal{A}_f \) (and hence \( \mathcal{A} \)) such that \( fg = \sigma^i I_j g \in [A_f] \subset [\mathcal{A}] \). Then \( g \in \text{sat}(\mathcal{A}) \) and \( g \) is reduced w.r.t. \( \mathcal{A} \). Since \( \mathcal{A} \) is the characteristic set of \( \text{sat}(\mathcal{A}) \), this is impossible. Hence, \( f = \sigma^i I_j \) is invertible w.r.t. \( \mathcal{A} \) and \( \mathcal{A} \) is difference regular.

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

Theorem 3.15 If \( \mathcal{A} \) is a coherent and regular chain of form (1), then

\[
\text{sat}(\mathcal{A}) = \bigcup_{h_1 \geq 0, \ldots, h_p \geq 0} (a\text{-sat}(\mathcal{A}_{(h_1, \ldots, h_p)}))
\]

Proof. It is easy to see that \( \text{sat}(\mathcal{A}) \supset \bigcup_{h_1 \geq 0, \ldots, h_m \geq 0} (a\text{-sat}(\mathcal{A}_{(h_1, \ldots, h_p)})) \). Let \( f \in \text{sat}(\mathcal{A}) \). Since \( \mathcal{A} \) is coherent and regular, \( \mathcal{A} \) is the characteristic set of \( \text{sat}(\mathcal{A}) \), and hence \( \text{prem}(f, \mathcal{A}) = a\text{-prem}(f, \mathcal{A}_f) = 0 \). That is \( f \in a\text{-sat}(\mathcal{A}_f) \). Hence \( \text{sat}(\mathcal{A}) \subset \bigcup_{h_1 \geq 0, \ldots, h_m \geq 0} a\text{-sat}(\mathcal{A}_{(h_1, \ldots, h_p)}) \).

4. Proper and strong irreducible chains

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

- \( \mathcal{A}^* \) as defined in (3) is an algebraic irreducible triangular set; and
- If \( f = \sigma g \in a\text{-}sat(\mathcal{A}^*) \) then \( g \in a\text{-}sat(\mathcal{A}^*) \).

**Lemma 4.1** Let \( \mathcal{A} \) be a coherent and proper irreducible chain of the form (1) and \( V \) be the algebraic parameter set of \( \mathcal{A}^* \). If \( g \in \mathcal{K}[V] \), then \( \sigma g \) is invertible w.r.t. \( \mathcal{A}^* \).

**Proof.** Since \( \mathcal{A}^* \) is an algebraic irreducible chain, by Lemma 3.9, if \( \sigma g \) is not invertible w.r.t. \( \mathcal{A}^* \) then \( \sigma g \in a\text{-}sat(\mathcal{A}^*) \). Since \( \mathcal{A} \) is proper irreducible, we have \( g \in a\text{-}sat(\mathcal{A}^*) \). But \( g \in \mathcal{K}[V] \) and hence is invertible w.r.t. \( \mathcal{A}^* \). Which is a contradiction.

The following is a key property of a proper irreducible chain.

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

**Proof.** Let \( V \) be the parameter set of the algebraic chain \( \mathcal{A}_f \) and \( Y \) other variables occurring in \( \mathcal{A}_f \). By Lemma 2.5, \( V \) is also the parameter set of \( \mathcal{A}^* \). Since \( f \) is invertible w.r.t. \( \mathcal{A} \), there are \( \bar{f} \in \mathcal{K}[V, Y] \) and a nonzero \( g \in \mathcal{K}[V] \) such that \( \bar{f} \cdot f \equiv g \mod (\mathcal{A}_f) \), that is

\[
\bar{f} \cdot f = g + \sum_{A \in \mathcal{A}_f} B_A A. \tag{8}
\]

Performing the transforming operator on the formula, we have

\[
\sigma \bar{f} \cdot \sigma f \equiv \sigma g \mod (\sigma \mathcal{A}_f). \tag{9}
\]

If \( \text{ord}(f, y_i) \geq \text{ord}(A_{i,k_i}, y_i) \) for all \( i \), by Lemma 3.2, we can find a \( J \in I_{\mathcal{A}^*} \) such that

\[
J \sigma \bar{f} \cdot \sigma f \equiv J \sigma g \mod (A_{\sigma f}). \tag{10}
\]

If \( \text{ord}(f, y_i) < \text{ord}(A_{i,k_i}, y_i) \) for some \( i \), we may assume that for \( A \) in (8), \( \text{ord}(A, y_i) < \text{ord}(A_{i,k_i}, y_i) \). Similar to Lemma 3.2, we can also find \( J \in I_{\mathcal{A}^*} \) such that (10) is true. Since \( J \) is a product of powers of initials of \( \mathcal{A}^* \), it is invertible w.r.t. \( \mathcal{A}^* \). \( \sigma g \) is invertible w.r.t. \( \mathcal{A}^* \) by Lemma 4.1. As a consequence, there is an \( h \) and a nonzero \( r \in \mathcal{K}[V] \) such that

\[
h \cdot J \sigma g \equiv r \mod (\mathcal{A}^*).
\]

Hence,

\[
h \cdot J \sigma \bar{f} \cdot \sigma f \equiv h \cdot J \cdot \sigma g \equiv r \mod (\mathcal{A}_{\sigma f}).
\]

That is, \( \sigma f \) is invertible w.r.t. \( \mathcal{A} \).

The following theorem is one of the main properties of proper irreducible chains. It is significant because it gives a constructive criterion for a chain to be regular.

**Theorem 4.3** A coherent and proper irreducible chain is difference regular.

**Proof.** Let \( \mathcal{A} = A_1, \ldots, A_m \) and \( I_j = \text{init}(A_j) \). Since \( \mathcal{A}^* \) is an irreducible algebraic chain, by Lemma 3.9, \( I_i \) are invertible w.r.t. \( \mathcal{A}^* \) and hence invertible w.r.t. \( \mathcal{A} \). By Lemma 4.2, all \( \sigma^j I_i \) are invertible w.r.t. \( \mathcal{A} \).
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, $\text{Zero}(\text{sat}(\mathcal{A}))$ is not empty. The proof of Theorem 4.4 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 certain chains.

Let $a_i = (a_{i,1}, \ldots, a_{i,n})$, $i = 0, \ldots, r$ be $n$-tuples, where $a_{i,j}$ are elements from an extension field of $K$. A difference kernel of length $r$, $\mathcal{R} = K(a_0, a_1, \ldots, a_r)$, over the difference field $\mathcal{K}$ is an algebraic field extension of $K$ such that the difference operator $\sigma$ of $\mathcal{K}$ can be extended to a field isomorphism from $\mathcal{K}(a_0, \ldots, a_{r-1})$ to $\mathcal{K}(a_1, \ldots, a_r)$ and $\sigma a_i = a_{i+1}, i = 0, \ldots, r-1$.

**Theorem 4.4** Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then $\text{Zero}(\text{sat}(\mathcal{A})) \neq \emptyset$.

**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 $\text{ivar}(B_{i,j}) = y_i$. Let $\alpha_i = \text{ord}(B_{i,c_1, y_i}), i = 1, \ldots, p$, $e = \max\{\alpha_i \leq e\}$, $U_0 = \{\sigma^j u_j | 1 \leq j \leq q, 0 \leq i \leq e\}$, $U_1 = \{\sigma^j u_j | 1 \leq j \leq q, 1 \leq i \leq e + 1\}$, $Y_0 = \{\sigma^j y_j | 1 \leq j \leq p, 0 \leq i \leq o_j - 1\}$, and $Y_1 = \{\sigma^j y_j | 1 \leq j \leq p, 1 \leq i \leq o_j\}$. 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 $\sigma^j u_j$ and $\sigma^j y_j$ are treated as independent variables. Hence, $\text{sat}(\mathcal{A}^*)$ is a prime ideal in $\mathcal{K}[\hat{V}]$, where $\hat{V} = U_0 \cup Y_0 \cup \{\sigma^{p_0} y_1, \ldots, \sigma^{p_q} y_p\}$. Let $\eta = (\alpha_j^{(i)}, \beta_j^{(i)})$ be a generic zero of this prime ideal. Then $\sigma^j u_i = \alpha_i^{(j)}, \sigma^j y_i = \beta_i^{(j)}$ annul every polynomial in $\mathcal{A}^*$ but not their initials.

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

Let

$$
\mathcal{B}_0 = \mathcal{A}^* - \{B_{1,1}, \ldots, B_{p,c_p}\}
$$

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, $a_0$ is a generic zero of the algebraic prime ideal $\text{a-sat}(\mathcal{A}^*) \cap \mathcal{K}[V_0] = \text{a-sat}(\mathcal{B}_0)$ with $\mathcal{B}_0$ as a characteristic set. To prove the isomorphism, we need only to show that $a_1$ is a generic zero of the algebraic prime ideal $\text{a-sat}(\mathcal{A}^*) \cap \mathcal{K}[V_1] = \text{a-sat}(\mathcal{B}_1)$ with $\mathcal{B}_1$ as a characteristic set. First, if $g \in \mathcal{K}[V_0]$ and $g(a_0) = 0, f = \sigma g$, we will show that $f(a_1) = 0$. From $\text{a-prem}(g, \mathcal{B}_0) = 0$, we have $I_g = \Sigma B_i C_i$ where $B_i \in \mathcal{B}_0$ and $I \in I_{\hat{B}_0}$. Perform the transforming operator on the formula, we have $\sigma I_\sigma g = \Sigma \sigma B_i \sigma C_i$. Since $\mathcal{A}$ is coherent and $\text{ord}(\sigma B_i, y_i) \leq \text{ord}(B_{i,c_1, y_i})$, by Lemma 3.3 we have $I_\sigma I_\sigma g = I_\sigma I_\sigma f = \Sigma B'_i \sigma C_i$ where $B'_i \in \mathcal{A}^*$ and $I_1 \in I_{\hat{A}}$. Since $\mathcal{A}^*$ is proper irreducible, we have $\text{a-prem}(f, \mathcal{A}^*) = 0$ and hence $f(\eta) = f(a_1) = 0$. Second, if $f \in \mathcal{K}[V_1]$ and $f(a_1) = 0, f = \sigma g$, we will show that $g(a_0) = 0$. Otherwise $g(a_0) \neq 0$. By Lemma 3.9, $g$ is invertible with respect to $\mathcal{A}^*$. By Lemma 4.2, $\sigma g$ is also invertible wrt $\mathcal{A}^*$. By Lemma 3.9 again, $f(\eta) = f(a_1) \neq 0$, a contradiction. So $\sigma$ introduces an isomorphism between $\mathcal{K}(a_0)$ and $\mathcal{K}(a_1)$. 
Now, we proved that $\mathcal{K}(a_0, a_1)$ is a difference kernel over $\mathcal{K}$. By Lemma V on page 156 of [6], this kernel has a principal realization $\psi$ corresponding to a series of kernels $\mathcal{K}(a_0, a_1)$, $\mathcal{K}(a_0, a_1, a_2), \ldots$. We will show that $\psi$ is a zero of $\text{sat}(A)$. From the construction of the kernel, for any $A \in \mathcal{A}^*$, we have $A(\psi) = A(\eta) = 0$. Hence $\psi$ is a zero of the polynomials in $\mathcal{A}^*$ but does not annul any initials of $\mathcal{A}^*$. Then for any $A \in \mathcal{A}$, $\psi$ is a zero of $\sigma^k A$ for any $k$, since $\sigma$ is an isomorphism. Also, $\psi$ does not annul any $J \in \mathbb{I}_A$. As a consequence, $\psi \in \text{Zero}(\text{sat}(A))$.

The following example shows that a coherent and regular chain could have no solutions.

**Example 4.5** $f_1 = y_1^2 - 1, f_2 = y_{1,1} + y_1 \in \mathcal{K}\{y_1\}$. $A = \{f_1, f_2\}$. $A$ is coherent and regular difference. But $A$ is not proper irreducible, since $f_1$ is not irreducible. We have $\text{Zero}(\text{sat}(A)) = \text{Zero}(A) = \text{Zero}(y_1 - 1, y_{1,1} + y_1) \cup \mathbb{Z}(y_1 + 1, y_{1,1} + y_1) = \emptyset$.

### 4.3. Characteristic sets of reflexive prime ideals

In the algebraic case, prime ideals can be described by irreducible chains. In this section, we will extend this result to the difference case. In order to do that, we need to introduce the concept of strong irreducible chains.

A proper irreducible chain $A$ is called strong irreducible if for any nonnegative integers $h_i$, $A_{(h_1, \ldots, h_p)}$ is an irreducible algebraic triangular set.

**Theorem 4.6** Let $A$ be a coherent and strong irreducible difference chain. Then $\text{sat}(A)$ is a reflexive prime difference ideal.

**Proof.** Let $f, g$ be two r-pols such that $fg \in \text{sat}(A)$. By Lemma 3.15, there exist nonnegative integers $h_1, \ldots, h_p$ such that $fg \in D = \text{a-sat}(A_{(h_1, \ldots, h_p)})$. Since $A$ is strong irreducible, $A_{(h_1, \ldots, h_p)}$ is an irreducible algebraic triangular set and hence $D$ is a prime ideal. We thus have $f \in D$ or $g \in D$. In other words, $f \in \text{sat}(A)$ or $g \in \text{sat}(A)$. Hence, $\text{sat}(A)$ is a prime ideal. We still need to show that $\text{sat}(A)$ is reflexive, that is, if $\sigma f \in \text{sat}(A)$ then $f \in \text{sat}(A)$. Suppose $f \notin \text{sat}(A)$. By Lemma 3.15, $f \notin \text{a-sat}(A_f)$. Since $A_f$ is an irreducible algebraic triangular set, $f$ must be invertible w.r.t. $A_f$. As a consequence, $f$ is invertible w.r.t. $A$. By Lemmas 4.2 and 3.10, $\sigma f$ is invertible w.r.t. $A$ and hence $f \notin \text{sat}(A)$, which contradicts the fact $\sigma f \in \text{sat}(A)$. \[\square\]

**Example 4.7** Consider $A = \{A_1 = x_{1,0}^2 + t, A_2 = x_{2,0}^2 + t + k\}$ from $[7]$ in $\mathcal{K}\{x_1, x_2\}$ where $\mathcal{K}$ is $Q(t)$ with the difference operator $\sigma t = t + 1$ and $k$ is a positive integer. $A^* = \{A_1, \sigma A_1, A_2, \sigma A_2\}$. If $k > 1$, $A$ is proper irreducible. But $\text{sat}(A)$ is not prime, because $A_2 - \sigma^k A_1 = (x_{2,0} - x_{1,1})(x_{2,0} + x_{1,1})$.

Conversely, we have

**Theorem 4.8** Let $I$ be a reflexive prime difference ideal, $A$ the characteristic sets of $I$. Then $A$ is coherent, strong irreducible, and $I = \text{sat}(A)$.

**Proof.** By Lemma 4.9, for any characteristic set $A$ of $I$, we have $I = \text{sat}(A)$. By Theorem 3.14, $A$ is coherent. By Lemma 4.10, we have for any nonnegative integers $t_i$, $A_{(t_1, \ldots, t_p)}$ is algebraic irreducible. Also, if $\sigma g \in \text{a-sat}(A^*)$, then $\sigma g \in I$. Since $I$ is reflexive, $g \in I$. Then $g \in \text{a-sat}(A^*)$. \[\square\]

**Lemma 4.9** Let $I$ be a prime difference ideal, $A$ its characteristic set. Then $I = \text{sat}(A)$. \[\square\]
Let $I \subseteq \text{sat}(\mathcal{A})$. Let $f \in \text{sat}(\mathcal{A})$. Then there is a $J \in \mathbb{I}_\mathcal{A}$ such that $Jf \in [A] \subseteq I$. By Theorem 3.14, $J$ is invertible w.r.t. $\mathcal{A}$ and hence not in $I$ by Lemma 3.10. Since $I$ is a prime ideal, $f \in I$.

Lemma 4.10 Let $I$ be a reflexive prime difference ideal, $\mathcal{A}$ its characteristic set. Then for any nonnegative integers $t_i, A_{(t_1, \ldots, t_p)}$ is algebraic irreducible.

Proof. Otherwise, we have nonnegative integers $t_1, \ldots, t_p$ such that $A_{(t_1, \ldots, t_p)}$ is a reducible algebraic triangular set. By definition, there exist r-pols $f$ and $g$ which are reduced w.r.t. $A_{(t_1, \ldots, t_p)}$ and with order not higher than those r-pols in $A_{(t_1, \ldots, t_p)}$ such that $fg \in A_{(t_1, \ldots, t_p)} \subseteq \text{sat}(\mathcal{A}) = I$. From this we have $f \in I$ or $g \in I$, which is impossible since $f$ and $g$ are reduced w.r.t. $\mathcal{A}$.

5. Algorithms of Zero Decomposition

In this section, we will present two algorithms which can be used to decompose the zero set of a general r-pol set into the zero set of proper irreducible chains. Such algorithms are called zero decomposition theorems.

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

Lemma 5.1 Let $P$ 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

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

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

$$\{P\} = \{\text{sat}(\mathcal{A})\} \cap \bigcap_{i=1}^m \{\mathbb{P} \cup \mathcal{A} \cup \{I_i\}\}.$$ 

Proof. Since for any $f \in \mathbb{P}$, $\text{prem}(f, \mathcal{A}) = 0$, Zero($\mathbb{P}$) $\supset$ Zero($\text{sat}(\mathcal{A})$). Moreover, Zero($\mathbb{P}$) $\supset$ Zero($\mathbb{P}, I_i$) for $i = 1, \ldots, m$. Therefore Zero($\mathbb{P}$) $\supset$ Zero($\text{sat}(\mathcal{A})$) $\cup$ $\bigcup_{i=1}^m$ Zero($\mathbb{P} \cup \{I_i\}$). Conversely, since $\mathcal{A} \subseteq [\mathbb{P}]$, Zero($\mathbb{P}$) $\subseteq$ Zero($\mathcal{A}$). Let $\eta$ be a solution of $\mathbb{P}$ in some extension field of $\mathbb{K}$. If $\eta$ annihilates some $I_i$, it is a solution of $\mathbb{P} \cup \{I_i\}$. If $\eta$ annihilates no $I_i$, then by Lemma 2.8, $\eta$ is a solution of $\text{sat}(\mathcal{A})$. Hence, Zero($\mathbb{P}$) $\subseteq$ Zero($\text{sat}(\mathcal{A})$) $\cup$ $\bigcup_{i=1}^m$ Zero($\mathbb{P} \cup \{I_i\}$). Thus, Zero($\mathbb{P}$) $=$ Zero($\text{sat}(\mathcal{A})$) $\cup$ $\bigcup_{i=1}^m$ Zero($\mathbb{P} \cup \{I_i\}$). Since $\mathcal{A}$ is the Wu characteristic set of $\mathbb{P}$, we have Zero($\mathbb{P} \cup \mathcal{A}$) $=$ Zero($\mathbb{P}$). The second equation is proved. The first equation can be proved similarly. By the difference Hilbert zero theorem [6], $\{\mathbb{P}\} = \{\text{sat}(\mathcal{A})\} \cap \bigcap_{i=1}^m \{\mathbb{P} \cup \{I_i\}\}$. 

Lemma 5.2 Let $\mathcal{A}$ be a Wu characteristic set of a finite set $\mathbb{P}$. If $\mathcal{A}$ is not a proper irreducible chain, then we can find $f_1, f_2, \ldots, f_k$ which are reduced w.r.t. $\mathcal{A}$ and some initials $I_i$ of $\mathcal{A}$ such that

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^k \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{f_i\}) \bigcup \bigcup_{i=1}^k \text{Zero}(\mathbb{P} \cup \mathcal{A} \cup \{I_i\}).$$

Proof. Denote $\mathcal{B} = \mathcal{A}^* = B_1, \ldots, B_p$. First, if $\mathcal{A}^*$ is not algebraic irreducible, by Lemma 3 in Section 4.5 of [30], there are $f_1, \ldots, f_k$ which are reduced w.r.t. $\mathcal{A}^*$ such that

$$f = \prod_{i=1}^p I_i^{v_i} f_1^{l_1} \ldots f_k^{l_{k+1}} = \sum_{i=1} g_i B_i$$
where $I_i$ is the initial of $B_i$. Since $A$ is a Wu characteristic set of $\mathbb{P}$, $f \in [\mathbb{P}]$. Then $\text{Zero}(\mathbb{P}) = \text{Zero}(\mathbb{P} \cup \{f\}) = \bigcup_{i=1}^{p} \text{Zero}(\mathbb{P}, f_i) \cup \bigcup_{i} \text{Zero}(\mathbb{P}, I_i)$. If $I_i$ is the initial of $\sigma^d A$ for some $A \in \mathcal{A}$, then $\text{Zero}(\mathbb{P}, I_i) = \text{Zero}(\mathbb{P}, \text{init}(A))$. In other words, we need only to include the initials of the r-pols in $A$.

If $A^*$ is algebraic irreducible, let $c$ be the least one such that there exists an $f \in a\text{-sat}(A_{c-1}, A_{c,1})$, class($f$) = $c$, $a\text{-prem}(f, A_{c-1}) \neq 0$. Without loss of generality, we may assume that $f$ contains those $y_{i,j}$ occurring in $A_{c-1}, A_{c,1}$. Let $f_1 = a\text{-prem}(g, A_{c-1})$, we have $f_1 \neq 0$, $f_1$ is reduced wrt $A$,

$$f_1 = \prod_{i=1}^{p} I_i^v_i - \sum_{i=1}^{k+1} g_i B_i$$

then $\text{Zero}(\mathbb{P}) = \text{Zero}(\mathbb{P} \cup \{f\}) = \text{Zero}(\mathbb{P} \cup \{g\}) = \text{Zero}(\mathbb{P} \cup \{f_1\})$.

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

**Theorem 5.3** Let $\mathbb{P}$ be a finite set of r-pols in $\mathcal{K}\{y_1, \ldots, y_n\}$, then there exist a sequence of coherent and proper irreducible difference chains $A_i$, $i = 1, \ldots, k$ such that

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \text{Zero}(A_i/J_i)$$

$$\text{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \text{Zero}(\text{sat}(A_i))$$

$$\{\mathbb{P}\} = \bigcap_{i=1}^{k} \{\text{sat}(A_i)\}$$

(11)

Zero($\mathbb{P}$) = $\emptyset$ iff $k = 1$ and $A_1$ is trivial.

**Algorithm 5.4 RittWuZDT($\mathbb{P}$)**

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

Begin

$B = C.S(\mathbb{P})$, $B = B_1, \ldots, B_p$;

If $B = 1$ then

$W = \{1\}$

Else

$R = \{\text{prem}(f, B) \neq 0 | f \in (\mathbb{P} \setminus B) \cup \Delta(B)\}$

If $R = \emptyset$ then (test, $\mathbb{P}$) := ProIrr($B$)

If test then $W = \{B\} \cup \text{RittWuZDT}(\mathbb{P} \cup B \cup \{I_1\})$

Else $W := \bigcup_{i=1}^{k} \text{RittWuZDT}(\mathbb{P}, B, f_i) \cup \text{RittWuZDT} (\mathbb{P}, B, I_i)$
where $I_i$ are the initials of the r-pols in $B$

and $\bar{P} = \{ f_i \mid i = 1, \ldots, k \}$

Else $W := \text{Ritt WuZDT}(\bar{P} \cup \mathbb{R})$

End.

This is a quite straightforward extension of the procedure proposed in [30], except the procedure \textbf{ProIrr} to find a proper irreducible chain. The correctness of the algorithm is guaranteed by Lemma 5.1 and Lemma 5.2. The termination of it is guaranteed by Lemma 2.2.

In the above algorithm, we need to check whether a coherent difference chain is proper irreducible. The procedure \textbf{ProIrr}, when it applied to a coherent difference chain $B$, returns two argument: test, $\bar{P}$. If $B^*$ is proper irreducible, then test is true and $\bar{P} = \emptyset$; else test is false, $\bar{P}$ consists of some difference polynomials $f_1, \ldots f_k$ mentioned in Lemma 5.2.

\textbf{Algorithm 5.5 ProIrr($A$)}

- **Input:** a difference coherent chain $A$ of the form (1).

- **Output:**
  (true, $\emptyset$) if $A$ is proper irreducible
  (false, $\bar{P}$) otherwise. $\bar{P}$ consists of the difference polynomials in Lemma 5.2.

Begin

\text{test}:=\text{true}

If $A^*$ is algebraic irreducible then

$G := \text{GBasis(a-sat}(A^*))*/$

$G_1 := G \cap K[U_1, Y_1]$ where $U_1, Y_1$ are the variables in $G$ minus those $u_{j,0}, y_{k,0}$ with order zero.

$G_1 := \sigma^{-1}G$

If $G_1 \subset G$

\text{test}:=\text{true}; Return.

Else $\bar{P} := \{ g \in G_1 \mid g \notin G \}$, test:= false; Return.

Else

\text{test}:=false, $\bar{P}$ consists of the difference polynomials which we get in the first case of Lemma 5.2.

End.

/* $G := \text{GBasis(a-sat}(A^*))$ compute the Groebner basis w.r.t. the eliminating ordering $y_{c,0} > y_{c-1,0} > \ldots > y_{1,0} > u_{d,0} > \ldots > u_{1,0} > \ldots$ In [10], it is proved that for any chain $A \subset K[x_1, \ldots, x_n]$, we have a-sat($A$) = ($A, zI_A^{-1}) \cap K[x_1, \ldots, x_n]$, where $z$ is a new variable. Based on this result, we can compute a finite basis for a-sat($A^*$) and its Groebner basis.

\textbf{Example 5.6} Consider $B = \{ f_1 = x_3^2, x_1, + 1, f_2 = x_3 + x_2 + 1 \} \subset K\{x_1, x_2, x_3\}$, it is not coherent. Since $x_3^2 + x_1, + 1 = (x_3, x_2 + 1)(x_3, x_2 - 1) + (x_2, + 1)^2 + x_1, + 1$. When we apply the above algorithm to $B$, we get $A = \{ x_2^2, 2x_2, + x_1, + 2, x_3^2, + x_1, + 1, x_3, + x_2, + 1 \}$, and $A$ is coherent and proper irreducible difference chain. Zero($B$) = Zero($\text{sat}(A)$).
As an application of Ritt-Wu’s zero decomposition algorithm, we can solve the membership problem of perfect difference ideals.

**Theorem 5.7** Let \( \mathbb{P} \) be a finite set of r-pols and \( f \) r-pols in \( K[x_1, \ldots, x_n] \), then \( f \in \{ \mathbb{P} \} \) iff \( \text{Zero}(\mathbb{P} \cup \{ fx_{n+1} + 1 \}) \) has no component in decomposition (11).

**Proof.** This is a consequence of Theorem 4.4 and the difference version of Hilbert’s Nullstellensatz [6].

### 6. A Modified Cohn’s Algorithm

In [6], Cohn gave an algorithm to solve the nullstellensatz test of perfect difference ideals. The idea is to transform the problem to a difference ideal with order less than or equal to one and then use zero decomposition algorithms in algebraic case to construct a difference kernel. This certainly simplifies the problem. On the other hand, reduce the order of r-pols to one by introducing new auxiliary variables destroy the structure of the ideal itself. In this section, by combining the idea of Cohn and the concept of algebraic irreducible chains, we will give another algorithm of zero decomposition for difference polynomial systems.

An algebraic ideal \( I \) in \( K[x_{i,e}] \) where \( 1 \leq i \leq n, d_i = e_i \leq o_i \), satisfies left (right) consistent condition w.r.t. \( \{ d_i : o_i \} \), if \( \forall f \in I \cap K[x_{i,e}], d_i + 1 \leq e_i \leq o_i (d_i \leq e_i \leq o_i - 1), \sigma^{-1}f \in I \ (\sigma f \in I) \). In the above definition, if \( o_i = d_i \), we assume that \( K[x_{i,e}] = \emptyset \), \( d_i + 1 \leq e_i \leq o_i \ (d_i \leq e_i \leq o_i - 1) \). If \( I \) satisfies left and right consistent condition w.r.t. \( \{ d_i : o_i \} \), we say that \( I \) satisfies consistent condition w.r.t. \( \{ d_i : o_i \} \).

**Lemma 6.1** Let \( \mathbb{P} \subset K\{x_1, \ldots, x_n\} \), and \( d_i, o_i \) the minimal and maximal orders of \( x_i \) appearing in \( \mathbb{P} \) respectively. Suppose that \( \mathbb{P} \) generates a prime algebraic ideal \( I \) in \( K[x_{i,e}] \), where \( 1 \leq i \leq n, d_i = e_i \leq o_i \), and \( \eta \) be the generic zero of \( I \). Then \( \eta \) can be extended to a difference zero of \( \mathbb{P} \) iff \( I \) satisfies the consistent condition w.r.t. \( \{ d_i : o_i \} \).

**Proof.** Suppose that \( I \) satisfies the consistent condition w.r.t. \( \{ d_i : o_i \} \). We will extend \( \eta \) to be a difference kernel of length one. Let \( A = A_1, \ldots, A_p \) be a characteristic set of \( I \). Then \( I = \text{a-sat}(A) \). Let \( I_1 \) be \( \sigma I \). Since \( \sigma \) is an isomorphism, \( I_1 \) is an algebraic prime ideal in \( K[x_{i,e}] \), \( d_i + 1 \leq e_i \leq o_i + 1 \). \( I_1 = \text{a-sat}(\sigma A) \). If \( u_{i,j} \) are the parameters of \( I \), then \( u_{i,j+1} \) are the parameters of \( I_1 \). Let \( \eta = (\eta_{i,j}) \). If \( \eta_{i,e} \) are algebraic transcendental over \( K \), \( \eta_{i,e+1} \) \( d_i \leq e_i \leq o_i - 1 \) are transcendental over \( K \) due to the consistent condition. If \( \sigma A_i \in K[x_{i,e}] \), \( d_i + 1 \leq e_i \leq o_i \), \( \sigma A_i \) becomes zero when we substitute \( x_{i,j} \) by \( \eta_{i,j} \). Let \( \eta_d = \{ \eta_{i,d_i} \} \), \( \eta_o = \{ \eta_{i,e} \} \) where \( d_i + 1 \leq e_i \leq o_i \). \( I_2 = \{ f(\eta_o)(x_{i,o_i+1}) \mid f \in I_1 \} \). These show that \( I_2 \) generated a prime algebraic ideal denoted also by \( I_2 \) in \( K(\eta_o)[x_{i,o_i+1}] \) and every generic zero of \( I_2 \) is the generic zero of \( \sigma I \). Let \( I_2 \) generated an ideal denoted as \( I_3 \) in \( K(\eta_d)(\eta_o)[x_{i,o_i}] \). If \( P \) is an essential prime divisor of \( I_3 \), \( P \cap K(\eta_o)[x_{i,o_i+1}] = I_2 \) by the Corollary in the page 32 of [6]. Let the generic zero of \( P \) be \( \{ \eta_{i,o_i+1} \} \). Then \( \eta_d, \eta_o \) and \( \eta_o, \eta_{i,o_i+1} \) is the generic zero of \( I \) and \( \sigma I \) respectively. \( \eta_i, \eta_{i,o_i+1} \) is a difference kernel of length one.

If \( o_i = d_i > 0, \forall i \), then the generic zero of \( I \) is difference kernel of length one. This is the same as Cohn’s theory.

**Algorithm 6.2 Cohn(\( \mathbb{P} \))**

- **Input:** a finite set \( \mathbb{P} \) of r-pols.
• Output:
  \((\Sigma = \emptyset)\) if Zero\((\mathcal{P}) = \emptyset\)
  \((\Sigma = \{\mathcal{B}_i\})\) otherwise, Zero\((\mathcal{P}) = \cup\text{Zero}(\mathcal{B}_i)\) and Zero\((\mathcal{B}_i) \neq \emptyset\)

Begin
  \(\Sigma = \emptyset\)
  \(\sqrt{\mathcal{P}} = \cap \text{a-sat}(\mathcal{A}_i) \) \(// \mathcal{A}_i\) is algebraic irreducible
  If \(\sqrt{\mathcal{P}} = \{1\}\), Return
  Else For all \(\mathcal{A}_i\)
    \(I = \text{a-sat}(\mathcal{A}_i)\)
    \((\text{test}, \bar{I}) = \text{Consistent}(I)\)
    If test \(\Sigma = \Sigma \cup \{\mathcal{A}_i\}\)
    Else Cohn\((I \cup \bar{I})\)
End.

Algorithm 6.3 Consistent\((\text{a-sat}(\mathcal{A}))\)

• Input: an algebraic irreducible chain \(\mathcal{A}\), and \(d_i, o_i\) the minimal and maximal order of \(x_i\) appearing in \(\mathcal{A}\).

• Output:
  \((\text{true}, \emptyset)\) if \(\text{a-sat}(\mathcal{A})\) is consistent w.r.t. \(\{d_i ; o_i\}\).
  \((\text{false}, \bar{I})\) Otherwise.

Begin
  test:=true
  \(GL := \text{LGBasis}(\text{a-sat}(\mathcal{A}^*))//\)
  \(GR := \text{RGBasis}(\text{a-sat}(\mathcal{A}^*))//\)
  \(G_1 = GL \cap K[x_{i,e_i}], d_i + 1 \leq e_i \leq o_i\).
  \(G_2 = GR \cap K[x_{i,e_i}], d_i \leq e_i \leq o_i - 1\).
  If \(\sigma^{-1}G_1 \subset I\) and \(\sigma G_2 \subset I\)
    then test:=true; Return.
  Else
    test:=false, \(\bar{I} = \{\sigma^{-1}f, \sigma g \mid f \in G_1, \sigma^{-1}f \notin I, g \in G_2, \sigma g \notin I\}\).
End.

/*LGBasis(RGBasis) (a-sat(A)) compute the Groebner bases of a-sat(A) w.r.t. the eliminating ordering \(x_{1,d_1} > x_{2,d_2} > \ldots x_{n,d_n} > \ldots (x_{1,o_1} > x_{2,o_2} > \ldots x_{n,o_n} > \ldots)\).*/

References


Characteristic Set Method for Difference Polynomial Systems


[31] J. van der Hoeven, Differential and Mixed Differential-difference Equations from the Effective
Viewpoint, Preprints, 1996.
