Resolvent Systems of Difference Polynomial Ideals

Xiao-Shan Gao and Chun-Ming Yuan
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS
Academia Sinica, Beijing 100080, China
(xgao,cmyuan)@mmrc.iss.ac.cn

ABSTRACT

In this paper, a new theory of resolvent systems is developed for prime difference ideals and difference ideals defined by coherent and proper irreducible ascending chains. Algorithms to compute such resolvent systems are also given. As a consequence, we prove that any irreducible difference variety is birationally equivalent to an irreducible difference variety of codimension one. As a preparation to the resolvent theory, we also prove that the saturation ideal of a coherent and proper ascending chain is unmixed in the sense that all its prime components have the same dimension and order.

Categories and Subject Descriptors

I.1.2 [**SYMBOLIC AND ALGEBRAIC MANIPULATION**]: Algorithms—*Algebraic algorithms*

General Terms

Algorithms, Theory

Keywords

Resolvent, difference ascending chain, difference polynomial, difference variety, unmixed decomposition.

1. INTRODUCTION

A classic result in algebraic geometry states that any irreducible variety is birationally equivalent to an irreducible hypersurface. Or equivalently, any finitely generated algebraic extension field can be generated with a single element, called the primitive element of the extension field. Algorithms to construct such hypersurfaces or primitive elements were proposed based on the methods of resultant computation by Trager [17] and Loos [11], the Gröbner basis method by Gianni and Mora [9], Kobayashi et al [9], and Yokoyama et al [21], and the characteristic set method by Gao-Chou [5, 7] and Wang-Lin [18]. The idea is to introduce a linear transformation of variables and show that the new equation system can be transformed into the following special form using various elimination theories

$$R(x_0), I_1(x_0)x_1 + U_1(x_0), \ldots, I_n(x_0)x_n + U_n(x_0)$$

where R, I_i, U_i are univariate polynomials in x_0.

In [15], Ritt proved similar results for ordinary differential polynomial equation systems by introducing the concept of *resolvents* for a prime ideal. Kolchin further gave generalizations of the resolvent to the partial differential case [13]. In [1], Cluzeau and Hubert extended the concept of resolvent to regular differential ideals and proposed an algorithm to compute it. In [10], Grigoriev used the resolvent to give a differential elimination algorithm of elementary complexity.

Following the work of Ritt[16], Cohn established the *Difference Algebra* [2]. Recently, elimination theories for difference polynomial systems were studied by Mansfield and Szanto [14], van der Hoeven [19], and Gao-Luo [8]. The concept of resolvent for an irreducible difference variety was also introduced by Cohn [2, 3]. In difference case, the resolvent is not a single difference polynomial anymore. In general, it is an irreducible difference variety of codimension one, which may be called the *resolvent variety.* But, the difference resolvent theory is not as complete as in the algebraic and differential cases. First, when establishing the birational equivalence between an irreducible variety V and its resolvent variety W, the operations of inversion need to be used. More precisely, the rational map is from W to $\mathbf{E}^{-t}V$ where $\mathbf{E}$ is difference operator and t an integer. Second, no algorithms were given to compute the resolvent.

In this paper, a more complete difference resolvent theory is proposed. We prove that for an irreducible difference variety V, there exists a resolvent variety which is birational equivalent to V. The improved result is possible, because we prove that an irreducible difference variety can be represented by a coherent and strong irreducible ascending chain [8]. Based on this fact, we develop a resolvent theory with better properties. We also give algorithms to compute the resolvents. Furthermore, for a coherent and proper irreducible ascending chain (definition in Section 3), we gave an algorithm to construct a series of resolvent systems. In [8], we give an algorithm to decompose the zero sets of a set of difference polynomials into the zero sets of difference varieties represented by coherent and proper irreducible ascending chains. Combining this result and the result in this paper, it is always possible to represent the zero set of a difference polynomial system by a series of resolvent varieties.

In order to establish the resolvent theory, we also prove that the saturation ideal defined by a coherent and proper

ISSAC'06, July 9–12, 2006, Genova, Italy.

irreducible ascending chain is unmixed in the sense that all its prime components have the same dimension and order.

Comparing to the differential case, the theory and algorithm for difference resolvents are generally much more difficult. Based on the ascending chain representation of the reflexive prime ideals introduced by us, we can obtain the order of the first resolvent polynomial explicitly and hence give an effective algorithm to compute it. In the case of proper ascending chains, we introduce a method of combination to prove the existence of resolvents.

Based on the implementation of a characteristic set method for difference polynomial systems introduced in [8], we implement the algorithms proposed in this paper. Examples are given to illustrate the algorithms. The most time consuming part of the computation process is the computation of the characteristic set.

2. DIFFERENCE POLYNOMIALS

A *difference field* $\mathcal{F}$ is a field with a third unitary operation $\mathbf{E}$ satisfying: for any $a, b \in \mathcal{F}$, $\mathbf{E}(a+b) = \mathbf{E}a + \mathbf{E}b$, $\mathbf{E}(ab) = \mathbf{E}a \cdot \mathbf{E}b$, and $\mathbf{E}a = 0$ if and only if $a = 0$. Here, $\mathbf{E}$ is called the *transforming operator* or simply a *transform* of $\mathcal{F}$. If $a \in \mathcal{F}$, $\mathbf{E}a$ is called the transform of a. $\mathbf{E}^n a = \mathbf{E}(\mathbf{E}^{n-1}a)$ is known as the n'th transform. If $\mathbf{E}^{-1}a$ is defined for all $a \in \mathcal{F}$, we say that $\mathcal{F}$ is *inversive.* Every difference field has an inversive closure [2].

As an example, let $\mathcal{K}$ be the set of rational functions in variable x defined on the complex plane. Let $\mathbf{E}$ be the map: $\mathbf{E}f(x) = f(x+1), f \in \mathcal{K}$. Then $\mathcal{K}$ is a difference field with transforming operator $\mathbf{E}$. This is an inversive field. In this paper, $\mathcal{K}$ is assumed to be this difference field.

Let $\mathbb{X} = \{x_1, \ldots, x_n\}$ be indeterminants. Then $\mathcal{K}\{\mathbb{X}\} = \mathcal{K}\{x_1, \ldots, x_n\}$ is called an *n-fold difference polynomial (abbr. r-pol) ring* over $\mathcal{K}$. Any r-pol P in $\mathcal{K}\{\mathbb{X}\}$ is an ordinary polynomial in variables $\mathbf{E}^k x_j (k = 0, 1, 2, \ldots, j = 1, \ldots, n)$. For convenience, we also denote $\mathbf{E}^k x_j$ by $x_{j,k}$.

Let $P \in \mathcal{K}\{\mathbb{X}\}$. The *class* of P, denoted by $\mathrm{cls}(P)$, is the least p such that $P \in \mathcal{K}\{x_1, \ldots, x_p\}$. If $P \in \mathcal{K}$, we set $\mathrm{cls}(P) = 0$. The *order* of P w.r.t x_i, denoted by $\mathrm{ord}(P, x_i)$, is the largest j such that $x_{i,j}$ occurs in P. When $x_{i,j}$ does not occur in P, we set $\mathrm{ord}(P, x_i) = -1$. If $\mathrm{cls}(P) = p$ and $\mathrm{ord}(P, x_p) = q$, we called x_p the *leading variable* and $x_{p,q}$ 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 *n-tuple* over $\mathcal{K}$ is of the form $\mathbf{a} = (a_1, \ldots, a_n)$, where the a_i are in some difference extension field of $\mathcal{K}$. Let $P \in \mathcal{K}\{\mathbb{X}\}$. To substitute an n-tuple $\mathbf{a}$ into P means to replace $x_{i,j}$ occurring in P with $\mathbf{E}^j a_i$. Let $\mathbb{P}$ be a set of r-pols in $\mathcal{K}\{\mathbb{X}\}$. 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 in $\mathbb{P}$ is zero. We use $\mathrm{Zero}(\mathbb{P})$ to denote the set of solutions of $\mathbb{P} = 0$. For an r-pol P, we use $\mathrm{Zero}(\mathbb{P}/P)$ to denote the set of solutions of $\mathbb{P} = 0$ which are not solutions of $P = 0$. For instance, let $P = \mathbf{E}x_1 \cdot x_1 + \mathbf{E}x_1 - x_1$. Then $x_1 = \frac{1}{x+c(x)}$ is a solution of $P = 0$, where $c(x)$ is any function satisfying $c(x+1) = c(x)$.

A field $\mathcal{K}$ is called *aperiodic* if there does not exist an integer n such that for all $a \in \mathcal{K}$, $\mathbf{E}^n a = a$.

Lemma 2.1 ((p201 [2])). *Let $\mathcal{K}$ be an aperiodic field and $P \in \mathcal{K}\{\mathbb{X}\}$ a nonzero r-pol. Then we can find an n-tuple $(\alpha_1, \ldots, \alpha_n) \in \mathcal{K}^n$ such that $P(\alpha_1, \ldots, \alpha_n) \neq 0$.*

A *difference ideal* is a subset I of $\mathcal{K}\{\mathbb{X}\}$, which is an algebraic ideal in $\mathcal{K}\{\mathbb{X}\}$ and is closed under the transform. A difference ideal I is called *reflexive* if for an r-pol P, $\mathbf{E}P \in I$ implies $P \in I$. Let $\mathbb{P} \subset \mathcal{K}\{\mathbb{X}\}$. The difference ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. The (algebraic) ideal generated by $\mathbb{P}$ is denoted as $(\mathbb{P})$. A difference ideal I is called *perfect* if the presence in I of a product of powers of transforms of an r-pol P implies $P \in I$. The perfect difference ideal generated by $\mathbb{P}$ is denoted as $\{\mathbb{P}\}$. A perfect ideal is always reflexive. A difference ideal I is called a *prime ideal* if for r-pols P and Q, $PQ \in I$ implies $P \in I$ or $Q \in I$.

Let $I \subset \mathcal{K}\{\mathbb{X}\}$ be a reflexive prime ideal. Then I has a *generic zero* α which has the following property: an r-pol $P \in I$ if and only if $P(\alpha) = 0$ [2]. For a reflexive prime difference ideal $I \subset \mathcal{K}\{\mathbb{X}\}$, we define the *dimension* of I as the difference transcendental degree of a generic zero $\alpha = (\alpha_1, \ldots, \alpha_n)$ of I over $\mathcal{K}$[2].

Let I be a difference ideal. Rename $\mathbb{X} = \{x_1, \ldots, x_n\}$ as two subsets: $\mathbb{U} = \{u_1, \ldots, u_q\}$ and $\mathbb{Y} = \{y_1, \ldots, y_p\}$ $(p+q = n)$. $\mathbb{U}$ is called a *parametric set* of I if $I \cap \mathcal{K}\{\mathbb{U}\} = \{0\}$ and $\forall y_i \in \mathbb{Y}, I \cap \mathcal{K}\{\mathbb{U}, y_i\} \neq \{0\}$. The dimension of a reflexive prime ideal is the number of its parameters.

Let $\mathbb{U}$ be a parametric set of a reflexive prime ideal I. The *order of I w.r.t* $\mathbb{U}$, denoted as $\mathrm{ord}_{\mathbb{U}} I$, is $\max\limits_{I \cap \mathcal{K}\{\mathbb{U}\}[Y_s] = \{0\}} |Y_s|$ where Y_s is a finite set of $y_{i,j}$. Let $(\beta_1, \ldots, \beta_q, \gamma_1, \ldots, \gamma_p)$ be a generic zero of I corresponding to $\mathbb{U}$ and $\mathbb{Y}$. Then, the order of I w.r.t $\mathbb{U}$ is the algebraic transcendental degree of $(\gamma_1, \ldots, \gamma_p)$ over the extension field $\mathcal{K}\langle\beta_1, \ldots, \beta_q\rangle$ of $\mathcal{K}$[2].

The effective order of I w.r.t $\mathbb{U}$ is the maximum number of y_{ij} which is algebraic independent over $\mathcal{K}\{\mathbb{U}\}^*$, where $\mathcal{K}\{\mathbb{U}\}^*$ is the inversive closure of $\mathcal{K}\{\mathbb{U}\}$ [2], and we denote it as $\mathrm{Eord}_{\mathbb{U}} I$. It is clear that $\mathrm{Eord}_{\mathbb{U}} I \leq \mathrm{ord}_{\mathbb{U}} I$.

Let $\mathbb{U}$ be a parametric set of a reflexive prime ideal I, and $(\beta_1, \ldots, \beta_q, \gamma_1, \ldots, \gamma_p)$ a generic zero of I where $\beta_1, \ldots, \beta_q$ are corresponding to $\mathbb{U}$. Then the *limit degree* of I w.r.t $\mathbb{U}$ is defined as $\mathrm{ld}_{\mathbb{U}}(I) = \liminf\limits_{k} [\mathcal{K}_0(\phi_k) : \mathcal{K}_0(\phi_{k-1})]$, where $\mathcal{K}_0 = \mathcal{K}\langle\beta_1, \ldots, \beta_q\rangle$ and $\phi_s = \{\gamma_{ij}, 1 \leq i \leq p, 0 \leq j \leq s\}$.

Let $\mathcal{D}$ be a difference field. A *difference kernel* R over $\mathcal{D}$ is an extension field, $\mathcal{D}(a, a_1, \ldots, a_r), r \geq 1$, of $\mathcal{D}$, each a_i denoting a vector $(a_i^{(1)}, \ldots, a_i^{(n)})$, and an extension τ of $\mathbf{E}$ to an isomorphism of $\mathcal{D}(a, a_1, \ldots, a_{r-1})$ onto $\mathcal{D}(a_1, \ldots, a_r)$, such that $\tau a_i = a_{i+1}, i = 0, 1, \ldots, r-1$. $(a_0 = a.)$ r is called the *length* of the kernel. Let $\phi_r \subset a_r$ be an algebraic transcendental basis of the elements in a_r over $\mathcal{D}(a, \ldots, a_{r-1})$. Then the *limit degree of R w.r.t ϕ* is defined as $\mathcal{D}(a, \ldots, a_r) : \mathcal{D}(a, \ldots, a_{r-1}, \phi_r)$.

3. DIMENSION, ORDER, AND DEGREE OF A PROPER IRREDUCIBLE CHAIN

Let P_1,P_2 be two r-pols and $\mathrm{lead}(P_1) = y_{p,q}$. P_2 is said to be *reduced* w.r.t P_1 if $\deg(P_2, y_{p,q+i}) < \deg(P_1, y_{p,q})$ for any nonnegative integer i.

An r-pol P_1 has *higher rank* than an r-pol P_2, denoted as $P_1 >_{rank} P_2$, if 1). $\mathrm{cls}(P_1) > \mathrm{cls}(P_2)$, 2). $c = \mathrm{cls}(P_1) = \mathrm{cls}(P_2)$ and $\mathrm{ord}(P_1, x_c) > \mathrm{ord}(P_2, x_c)$, or 3). $c = \mathrm{cls}(P_1) = \mathrm{cls}(P_2)$, $o = \mathrm{ord}(P_1, x_c) = \mathrm{ord}(P_2, x_c)$ and $\deg(P_1, x_{c,o}) > \deg(P_2, x_{c,o})$. If $P_1 >_{rank} P_2$ and $P_2 >_{rank} P_1$ are not valid, P_1 and P_2 are said to have the same rank, denoted as $P_1 =_{rank} P_2$.

A finite sequence of nonzero r-pols $\mathcal{A} = A_1, \ldots, A_p$ is called an *ascending chain* or simply a *chain*, if $p = 1$ and

$A_1 \neq 0$ or $\mathrm{cls}(A_1) > 0$, $A_i <_{rank} A_j$ and A_j is reduced w.r.t A_i for $1 \leq i < j \leq p$.

A chain $\mathcal{A}$ is called trivial if $\mathrm{cls}(A_1) = 0$. For a chain (algebraic or difference), we denote by $\mathbf{I}_{\mathcal{A}}$ the product of the initials of $\mathcal{A}$, by $\mathbb{I}_{\mathcal{A}}$ the set of products of initials of $\mathcal{A}$ and their transforms.

Example 3.1. *Let us consider $P_1 = \mathbf{E}y^2 - y^2 + 1$, $P_2 = \mathbf{E}^2 y + \mathbf{E}y \in \mathcal{K}\{y\}$. Since $P_1 <_{rank} P_2$, deg($P_2, \mathbf{E}y$)) $<$ deg($P_1, \mathbf{E}y$)) and deg($P_2, \mathbf{E}^2 y$) $<$ deg($P_1, \mathbf{E}y$), P_2 is reduced w.r.t P_1. Hence, P_1, P_2 is a chain.*

The saturation ideal of a chain $\mathcal{A}$ is defined as follows

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

If $\mathcal{B}$ is an algebraic chain, we define

$$\textbf{a-sat}(\mathcal{B}) = \{P \,|\, \exists k,\ s.t.\ \mathbf{I}_{\mathcal{B}}^k P \in (\mathcal{B})\}.$$

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 $\mathcal{A} >_{rank} \mathcal{B}$, if one of the following conditions holds: (1) $\exists\ 0 < j \leq \min\{p, s\}$, such that $\forall\ i < j$, $A_i =_{rank} B_i$ and $A_j >_{rank} B_j$, or (2) $s > p$ and $A_i =_{rank} B_i$ for $i \leq p$.

We use $\mathcal{A}_1 \leq_{rank} \mathcal{A}_2$ to denote the relation of either $\mathcal{A}_1 <_{rank} \mathcal{A}_2$ or $\mathcal{A}_1 =_{rank} \mathcal{A}_2$. It is known that this is a Notherian total order, that is, any strictly decreasing sequence of chains must be finite.

A *characteristic set* of any r-pol set $\mathbb{P}$ is a chain contained in $\mathbb{P}$ and has the lowest rank. An r-pol is said to be *reduced w.r.t a chain* if it is reduced to every r-pol in the chain. It is known that [16].

Lemma 3.2. *$\mathcal{A} \subset \mathbb{P}$ is a characteristic set of $\mathbb{P}$ if and only if there is no nonzero r-pol in $\mathbb{P}$ which is reduced w.r.t $\mathcal{A}$.*

We can define the pseudo-remainder of an r-pol P w.r.t a chain $\mathcal{A}$: $\mathrm{rprem}(P, \mathcal{A})$ and prove [8]:

Lemma 3.3. *Let P be an r-pol, $\mathcal{A}$ a chain, and R = rprem($P, \mathcal{A}$). Then there is a $J \in \mathbb{I}_{\mathcal{A}}$ with lead(J) $<_{rank}$ lead(P) s.t. $JP \equiv R \mod [\mathcal{A}]$ and R is reduced w.r.t $\mathcal{A}$.*

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 $p + q = n$. The orders of $A_{i,j}$ in y_i are increasing and the degrees of $A_{i,j}$ in $\mathrm{lead}(A_{i,j})$ are decreasing. Let $o_{(i,j)} = \mathrm{ord}(A_{i,j}, y_i)$. $\mathbb{U}$ is called the *parametric set* of $\mathcal{A}$. We define the *dimension* of $\mathcal{A}$ as $\dim(\mathcal{A}) = |\mathbb{U}|$, the *degree* of $\mathcal{A}$ as $\deg(\mathcal{A}) = \prod_{i=1}^{p} \deg(A_{i,k_i}, y_{i,o_{(i,k_i)}})$, the *order* of $\mathcal{A}$ as $\mathrm{ord}(\mathcal{A}) = \sum_{i=1}^{p} o_{(i,1)}$, and the *effective order* of $\mathcal{A}$ as $\mathrm{Eord}(\mathcal{A}) = \sum_{i=1}^{p} (o_{(i,1)} - m_i)$ where m_i is the minimal integer such that y_{i,m_i} occurs in $A_{i,1}$.

Let $h_1, \ldots, h_m\, (m \leq p)$ be nonnegative integers. We use $\mathcal{A}_{(h_1,\ldots,h_m)}$ to denote the following sequence of r-pols

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

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{order of $y_i(x)$ appears in $A_{i+1,1}, \mathbf{E}A_{i+1,1}$, …, $\mathbf{E}^{\hat{h}_m - o_{(m,k_m)}} A_{m,k_m}$}, $\hat{h}_i = \max\{h_i, o_i, o_{(i,k_i)}\}$ $+1$. It is obvious that $\mathcal{A}_{(h_1,\ldots,h_m)}$ is an algebraic triangular set with parameters:

$$\mathcal{P}(\mathcal{A}) = \{y_{i,j} | 1 \leq i \leq p, 0 \leq j \leq \mathrm{ord}(A_{i,1}, y_i) - 1\}. \tag{3}$$

For a chain $\mathcal{A}$ and an r-pol P, let

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

Let $\mathcal{A} = A_1, \ldots, A_p$ be an algebraic nontrivial triangular set in $\mathcal{K}[x_1, \ldots, x_n]$ over a field $\mathcal{K}$. Let y_i be the leading variable of A_i, $Y = \{y_1, \ldots, y_p\}$ and U the parametric set of $\mathcal{A}$. A polynomial f is said to be *invertible* w.r.t $\mathcal{A}$ if either $f \in \mathcal{K}[U]$ or $(f, A_1, \ldots, A_s) \cap \mathcal{K}[U] \neq \{0\}$ where y_s is the leading variable of f. 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.

An r-pol P is called *effective* in variable y_i if $y_{i,0} = y_i(x)$ occurs in P. P is called *effective* if P is effective in $\mathrm{lvar}(P)$.

Let $\mathcal{A} = A_1, \ldots, A_m$ be a difference chain in $\mathcal{K}\{\mathbb{X}\}$ and $k_i = \mathrm{ord}(A_i, \mathrm{lvar}(A_i))$, $i = 1, \ldots, m$. For any $1 \leq i < j \leq m$, if $\mathrm{cls}(A_i) = \mathrm{cls}(A_j) = t$, let $\Delta_{ij} = \mathrm{prem}(\mathbf{E}^{k_j - k_i} A_i, A_j, y_{t,k_j})$ be the algebraic pseudo-remainder of $\mathbf{E}^{k_j - k_i} A_i$ w.r.t A_j in variable y_{t,k_j}; 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 difference chain.*

Definition 3.4. *A chain $\mathcal{A}$ of the form (1) is said to be* proper irreducible *if*

- *$\mathcal{A}^*$ 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 = 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 $A_{c,1}$.*

Proper irreducible chains have the following properties[8].

Lemma 3.5. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1). If P is invertible w.r.t $\mathcal{A}$, then $\mathbf{E}P$ is invertible w.r.t $\mathcal{A}$.*

Lemma 3.6. *Let $\mathcal{A}$ be a coherent and proper irreducible chain. Then $\mathcal{A}$ is a characteristic set of* $\mathbf{sat}(\mathcal{A})$*.*

Lemma 3.7. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1), and $f \in \mathcal{K}\{\mathbb{U}, Y\}$, $g \in \mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})] \backslash \{0\}$. If $gf \in$* $\mathbf{sat}(\mathcal{A})$*, then $f \in$* $\mathbf{sat}(\mathcal{A})$*.*

Definition 3.8. *A proper irreducible chain $\mathcal{A}$ of the form (1) is said to be* strong irreducible *if for any nonnegative integers h_i, $\mathcal{A}_{(h_1,\ldots,h_p)}$ is an irreducible triangular set in algebraic case.*

Lemma 3.9. *[8] If $\mathcal{A}$ is a coherent and strong irreducible chain, then* $\mathbf{sat}(\mathcal{A})$ *is a reflexive prime ideal.*

Theorem 3.10. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1). We have:*

(1) *$\mathbb{U}$ is a parametric set of ideal* $\mathbf{sat}(\mathcal{A})$*. That is,* $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}\} = \{0\}$ *and* $\forall i, \mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}, y_i\} \neq \{0\}$.

(2) *If* $\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} P_i$ *is an irredundant intersection of a set of prime difference ideals, then* $\forall i$, $\mathbb{U}$ *is a parametric set for* P_i *and thus* $dim(P_i) = dim(\mathcal{A})$.

(3) $Eord_{\mathbb{U}} P_i = ord_{\mathbb{U}} P_i = ord(\mathcal{A})$ *and* P_i *is reflexive. Let* $P_i = \mathbf{sat}(\mathcal{A}_i)$ *and* $\mathcal{A}_i$ *a chain under the same variable order as* $\mathcal{A}$. *Then* $\mathcal{A}_i$ *is strong irreducible.*

(4) $deg(\mathcal{A}) = \sum_{i=1}^{r} ld_{\mathbb{U}}(P_i)$.

Proof: By Lemma 3.6, $\mathcal{A}$ is a characteristic set of $\mathbf{sat}(\mathcal{A})$. As a consequence, we have $\mathbf{sat}(\mathcal{A}) \cap \mathcal{K}\{\mathbb{U}\} = \emptyset$, 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 $h = |\mathcal{P}(\mathcal{A})|$ and $\mathcal{C} = \mathcal{A}_{(0,\ldots,0,h,0,\ldots,0)}$, where h is at the i-th place. Let $Y^{'}$ and U' be the set of all $y_{i,j}$ and $u_{k,l}$ occurring in $\mathcal{C}$. By Lemma 3.5, all the initials of $\mathcal{C}$ are invertible w.r.t $\mathcal{C}$. Then Zero($\mathbf{a\text{-}sat}(\mathcal{C})$) is an unmixed algebraic ideal of dimension $\dim(A) = h$ in $\mathcal{K}(U')[Y']$ [6]. On the other hand, $\mathbf{a\text{-}sat}(\mathcal{C}) \cap \mathcal{K}(U')[y_{i,0}, \ldots, y_{i,h}] \subset \mathbf{sat}(\mathcal{A}) \cap \mathcal{K}(U')[y_{i,0}, \ldots, y_{i,h}] = \{0\}$. From this, we have $\dim(\mathbf{a\text{-}sat}(\mathcal{C})) \geq h + 1$, a contradiction. This proves (1).

Let $\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} P_i$ be an irredundant intersection of prime difference ideals. Since $\forall i, \{\mathbf{sat}(\mathcal{A})\} \subseteq P_i$, for each i we have $P_i \cap \mathcal{K}\{\mathbb{U}, y_i\} \neq \{0\}$. Then we need only to prove $P_i \cap \mathcal{K}\{\mathbb{U}\} \neq \{0\}$ for all i. Suppose $P_1 \cap \mathcal{K}\{\mathbb{U}\} \neq \{0\}$. Then $\exists g \in \mathcal{K}\{\mathbb{U}\} \cap P_i$ and $g \neq 0$. Since $\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} P_i$ is an irredundant representation, there exists an $f \in \mathcal{K}\{\mathbb{U}, Y\}$, such that $f \in \bigcap_{i=2}^{r} P_i, f \notin \{\mathbf{sat}(\mathcal{A})\}$. We have $gf \in \{\mathbf{sat}(\mathcal{A})\}$. So there exist non negative integers $s_0, s_1, \ldots, s_r$, such that

$$\Pi_{i=0}^{r}(\mathbf{E}^{i}(gf))^{s_i} = \Pi_{i=0}^{r}(\mathbf{E}^{i}(g))^{s_i} * \Pi_{i=0}^{r}(\mathbf{E}^{i}(f))^{s_i} \in \mathbf{sat}(\mathcal{A}).$$

By Lemma 3.7, we have $\Pi_{i=0}^{r}(\mathbf{E}^{i}(f))^{s_i} \in \mathbf{sat}(\mathcal{A})$. Therefore, $f \in \{\mathbf{sat}(\mathcal{A})\}$, which contradicts to the choice of f. So $\mathbb{U}$ is a transform independent set of P_i. Hence $\dim(P_i) = |\mathbb{U}|$. This proves (2).

Let $o_i = \mathrm{ord}(A_{i,1}, y_i)$. It is clear that $|\mathcal{P}(\mathcal{A})| = \sum_{i=1}^{p} o_i$. Since $\mathcal{A}$ is proper irreducible, for any $y_{ij}, j \geq o_i$, there is a nonzero $P \in \mathbf{sat}(\mathcal{A})$ such that $P \in \mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A}), y_{i,j}]$. Since $\mathbf{sat}(\mathcal{A}) \subseteq P_i$, $\mathrm{ord}_{\mathbb{U}} P_i \leq \sum_{i=1}^{p} o_i$. If there exists an i, say $i = 1$, such that $P_i \cap \mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})] \neq \{0\}$, then there exists a $g \neq 0, g \in P_1 \cap \mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})]$. Also, there exists an $f \in \mathcal{K}\{\mathbb{U}, Y\}$, such that $f \in \bigcap_{i=2}^{r} P_i, f \notin \{\mathbf{sat}(\mathcal{A})\}$ and $gf \in \{\mathbf{sat}(\mathcal{A})\}$. There exist non negative integers $s_0, \ldots, s_l$ such that

$$\Pi_{i=0}^{l}(\mathbf{E}^{i}(gf))^{s_i} \in \mathbf{sat}(\mathcal{A}).$$

Since g is invertible w.r.t $\mathcal{A}$, by Lemma 3.5, $\mathbf{E}^{i}g$ is also invertible w.r.t $\mathcal{A}$. So, there exists $g^{'} \in \mathcal{K}\{\mathbb{U}, Y\}$, such that $g^{'} * \Pi_{i=0}^{l}(\mathbf{E}^{i}g)^{s_i} = M \neq 0, M \in K\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})]$. Then $M * \Pi_{i=0}^{l}(\mathbf{E}^{i}f)^{s_i} \in \mathbf{sat}(\mathcal{A})$. By Lemma 3.7, $\Pi_{i=0}^{l}(\mathbf{E}^{i}f)^{s_i} \in \mathbf{sat}(\mathcal{A})$, so $f \in \{\mathbf{sat}(\mathcal{A})\}$, a contradiction. Therefore, $\mathbb{U} \cup \mathcal{P}(\mathcal{A})$ is algebraic independent in P_i and hence $\mathrm{ord}_{\mathbb{U}} P_i \geq |\mathcal{P}(\mathcal{A})|$. Then $\mathrm{ord}_{\mathbb{U}} P_i = \mathrm{ord}(\mathcal{A})$. Let $\mathcal{P}(\mathcal{A})^{(T)} = \{E^{T_i} y_{ij} | y_{ij} \in \mathcal{P}(\mathcal{A})\}$, where $T = (T_1, \ldots, T_p)$ is a set of non negative integers. Notice that $\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} P_i$ is an irredundant representation and $\mathcal{A}$ is effective. In each P_i, using the properties of the transcendental degree, we have $P_i \bigcap \mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})^{(T)}] = \{0\}$. So $\mathrm{Eord}_{\mathbb{U}} P_i \geq |\mathcal{P}(\mathcal{A})|$. Since $\mathrm{Eord}_{\mathbb{U}} P_i \leq \mathrm{ord}_{\mathbb{U}} P_i = |\mathcal{P}(\mathcal{A})|$, we have $\mathrm{Eord}_{\mathbb{U}} P_i = \mathrm{ord}_{\mathbb{U}} P_i$. Then P_i is reflexive.

In order to prove $\mathcal{A}_i$ is strong irreducible, we need only to prove that $\mathcal{A}_i$ is effective. Let $A_{i,j}$ be the first r-pol in $\mathcal{A}_i$ with $\mathrm{lvar}(A_{i,j}) = y_j$. We need only to prove that $A_{i,j}$ is effective in y_j. We already proved that $\mathrm{ord}(A_{i,j}, y_j) = o_j$. Let $\mathcal{P}_{j-1} = \{y_{i,k} | 1 \leq i \leq j-1, 0 \leq k \leq o_i - 1\}$. If $A_{i,j}$ is not effective, we may obtain an r-pol $Q \in \mathcal{K}\{\mathbb{U}\}[\mathcal{P}_{j-1}, y_{j,1}, \ldots, y_{j,o_j}] \cap P_i$. This is impossible, because from $P_i \cap \mathcal{K}\{\mathbb{U}\}[\mathcal{P}_{j-1}, y_{j,0}, \ldots, y_{j,o_j-1}] = \{0\}$ and $\mathrm{Eord}_{\mathbb{U}} P_i = \mathrm{ord}_{\mathbb{U}} P_i$, we have $P_i \cap \mathcal{K}[\mathbb{U}, \mathcal{P}_{j-1}, y_{j,1}, \ldots, y_{j,o_j}] = \{0\}$. We proved (3).

We denote a generic zero of $\mathcal{A}^{*}$ as $\eta = (\alpha_{ij}, \beta_{ij})$, where α_{ij}, β_{ij} correspond to u_{ij}, y_{ij} respectively. By the proof of Theorem 4.2 in [8], we know that there exists a difference kernel R of length one: $\mathbf{E} : \mathcal{K}(a_0) \rightarrow \mathcal{K}(a_1)$, and $\alpha = \{\alpha_{ij} | 1 \leq i \leq q, j \geq 0\} \cap a_1$ is a parametric set of R, $\mathrm{deg}_{\mathbb{U}} R = \mathcal{K}(a_1) : \mathcal{K}(a_0, \alpha) = \mathrm{deg}(\mathcal{A})$. By Lemma 5 in chapter 6 of [2], we know that R has a finite number of principal realizations, denoted as $V_i, 1 \leq i \leq m$, and the generic zero of V_i is denoted as η_i. We define $\mathrm{Spec}(V_i) = \{f \in \mathcal{K}\{\mathbb{U}, \mathbb{Y}\} | f(\eta_i) = 0\}$, so $\mathbf{sat}(\mathcal{A}) \subset \mathrm{Spec}(V_i)$ and $\mathrm{Spec}(V_i)$ is a prime difference ideal. Since $\mathbf{sat}(\mathcal{A}) = \bigcap_{i=1}^{r} P_i \subset \mathrm{Spec}(V_i)$, there exists a j such that $\mathrm{Spec}(V_i) \subset P_j$. Since P_j and $\mathrm{Spec}(V_i)$ have the same dimension and order, $\mathrm{Spec}(V_i) = P_j$. So for each i, there is an l_i such that $\mathrm{Spec}(V_i) = P_{l_i}$, and the generic zero for each P_j is a principal realization of R, so it must be some η_i. Hence, there is a one to one corresponding between V_i and P_j. By Lemma 5 in chapter 6 of [2], we have $\mathrm{deg}(\mathcal{A}) = \mathrm{deg}_{\mathbb{U}} R = \sum_{i=1}^{m} \mathrm{ld}_{\mathbb{U}} V_i = \sum_{i=1}^{r} \mathrm{ld}_{\mathbb{U}}(P_i)$. This proves (4). ▌

If two ideals I_1 and I_2 have the same parametric set $\mathbb{U}$ and $\mathrm{ord}_{\mathbb{U}} I_1 = \mathrm{ord}_{\mathbb{U}} I_2$ and $\mathrm{Eord}_{\mathbb{U}} I_1 = \mathrm{Eord}_{\mathbb{U}} I_2$, then we say that I_1 and I_2 are of the same type. As a consequence of Theorem 3.10, we have the following corollaries (proofs omitted).

Corollary 3.11. *If* $\mathcal{A}$ *is coherent and proper irreducible, all the irredundant prime divisors of* $\mathbf{sat}(\mathcal{A})$ *are of the the same type with* $\mathbf{sat}(\mathcal{A})$. *In other words,* $\mathbf{sat}(\mathcal{A})$ *is unmixed in the sense that all its essential prime ideals have the same parametric set, the same dimension, and the same order.*

As a consequence, we can define $\dim(\mathbf{sat}(\mathcal{A})) = \dim(\mathcal{A})$ and $\mathrm{ord}_{\mathbb{U}}(\mathbf{sat}(\mathcal{A})) = \mathrm{ord}(\mathcal{A})$.

It is proved in [8] that if $\mathcal{A}$ is coherent and strong irreducible, then $\mathbf{sat}(\mathcal{A})$ is a reflexive prime ideal with $\mathbb{U}$ as a set of parameters. Furthermore, we have

Corollary 3.12. *If* $\mathcal{A}$ *is a coherent and strong irreducible chain, then* $\mathbf{sat}(\mathcal{A})$ *is a reflexive prime ideal satisfying* $\dim(\mathbf{sat}(\mathcal{A})) = \dim(\mathcal{A})$, $\mathrm{ord}_{\mathbb{U}}(\mathbf{sat}(\mathcal{A})) = \mathrm{Eord}_{\mathbb{U}}(\mathbf{sat}(\mathcal{A})) = \mathrm{ord}(\mathcal{A})$, and $\mathrm{ld}_{\mathbb{U}}(\mathbf{sat}(\mathcal{A})) = \mathrm{deg}(\mathcal{A})$.

Corollary 3.13. *Let* $\mathcal{A}$ *be a coherent and proper irreducible chain, and*

$$\{\mathbf{sat}(\mathcal{A})\} = \bigcap_{i=1}^{r} \mathbf{sat}(\mathcal{A}_i)$$

a decomposition of $\{\mathbf{sat}(\mathcal{A})\}$ *as irredundant prime difference ideals, where* $\mathcal{A}_i$ *are strong irreducible chains under the same variable order as that of* $\mathcal{A}$. *Then the first r-pol of* $\mathcal{A}_i$ *is the same as the first r-pol of* $\mathcal{A}$.

Corollary 3.14. *Let* $\mathcal{A}$ *be a coherent and proper irreducible chain of the form (1). If* $\{\mathbf{sat}(\mathcal{A})\}$ *has only one prime component, then* $\mathcal{A}$ *is strong irreducible and* $\mathbf{sat}(\mathcal{A})$ *is a prime ideal.*

4. RESOLVENT SYSTEM FOR A REFLEXIVE PRIME IDEAL

It is proved in [8] that for a reflexive prime difference ideal I, we can choose a proper order of variables such that under this variable order $I = \mathbf{sat}(\mathcal{A})$ and $\mathcal{A}$ is coherent and strong irreducible. So, we will start our discussion from a coherent and strong irreducible chain.

4.1 Resolvent systems

Theorem 4.1. *Let $\mathcal{A}$ be a coherent and strong irreducible chain of the form (1), $\mathcal{K}$ an aperiodic difference field or $|\mathbb{U}| \neq 0$, and $\lambda_1, \ldots, \lambda_p$ variables. There exists $Q \in \mathcal{K}\{\lambda_1, \ldots, \lambda_p, \mathbb{U}\}$ such that if $\sigma_1, \ldots, \sigma_p$ satisfy $Q(\sigma_1, \ldots, \sigma_p, \mathbb{U}) \neq 0$, then the characteristic set of $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)$ under the variable order $\mathbb{U} < w < y_i$ is of the following form*

$$R, R_1, \ldots, R_s, I_1 y_{1,0} - V_1, \ldots, I_p y_{p,0} - V_p \tag{5}$$

where $R, R_i, I_i, V_i \in K\{\mathbb{U}, w\}$. Furthermore, R is effective in w, ord$(R, w) =$ ord$(\mathcal{A})$, ord$(I_i, w) <$ ord$(\mathcal{A})$, and ord$(V_p, w) \leq$ ord$(\mathcal{A})$.

Proof: Denote $\mathcal{B} = \mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i$. Then $\mathcal{B}$ is also coherent and strong irreducible and $\mathbf{sat}(\mathcal{B})$ is a reflexive prime ideal. Since $\mathbb{U}$ is a parametric set of $\mathbf{sat}(\mathcal{B})$, we could treat $\mathcal{K}_0 = \mathcal{K}\langle\mathbb{U}, \lambda\rangle$ as the ground field where $\lambda = \{\lambda_1, \ldots, \lambda_p\}$. We denote by $\mathrm{ord}_X(Z)$ the number of an algebraic transcendental basis of Z and their transformations over $\mathcal{K}_0\langle X\rangle$. Let $(\alpha_1, \ldots, \alpha_p, \omega)$ be a generic zero of $\mathbf{sat}(\mathcal{B})$, and $\alpha = \{\alpha_1, \ldots, \alpha_p\}$. Then

$$\begin{aligned}\mathrm{Eord}(\mathbf{sat}(\mathcal{A})) &= \mathrm{Eord}(\mathbf{sat}(\mathcal{B})) = \mathrm{Eord}(\omega) + \mathrm{Eord}_\omega(\alpha)\\ &\leq \mathrm{ord}(\omega) + \mathrm{ord}_\omega(\alpha) = \mathrm{ord}(\omega, \alpha) \qquad (6)\\ &= \mathrm{ord}(\mathbf{sat}(\mathcal{A})) = \mathrm{Eord}(\mathbf{sat}(\mathcal{A})).\end{aligned}$$

The last equation is due to Corollary 3.12. As a consequence, Eord$(\omega) =$ ord(ω). Let $T(w) \in \mathbf{sat}(\mathcal{B})$ be an r-pol in $\mathbb{U}$ and w with the lowest rank. Since $\mathbf{sat}(\mathcal{B})$ is a prime ideal, $T(w)$ can be chosen as an irreducible r-pol. Also, $T(w)$ must be the first element of the characteristic set of $\mathbf{sat}(\mathcal{B})$ under the variable order $\mathbb{U} < \lambda_i < w < y_i$. Since Eord$(\omega) =$ ord(ω), by Corollary 3.12, we have Eord$(T, w) =$ ord$(T, w) \leq o_{\mathcal{A}}$. In other words, T is effective in w. Differentiating T w.r.t λ_{i0} and substituting α_i for y_i, we have

$$\frac{\partial T}{\partial \lambda_{i0}} + y_{i,0}\frac{\partial T}{\partial w_0}|_{(y_1,\ldots,y_p,w)=(\alpha_1,\ldots,\alpha_p,\sum_{i=1}^{p}\lambda_i\alpha_i)} = 0$$

Since (α, ω) is a generic zero of $\mathbf{sat}(\mathcal{B})$ and $S_i(\alpha, \omega) = 0$, $S_i = \frac{\partial T}{\partial \lambda_{i0}} + y_{i0}\frac{\partial T}{\partial w_0} \in \mathbf{sat}(\mathcal{B}), 1 \leq i \leq p$. Let H be the resultant of $\frac{\partial T}{\partial w_0}$ and T w.r.t w_o. We have ord$(H, w) < o$. Then there exist r-pols A, B such that $AT + B\frac{\partial T}{\partial w_0} = H$. Let $Q_i = BS_i + ATy_{i,0} = Hy_{i,0} + B\frac{\partial T}{\partial \lambda_{i0}} \in \mathbf{sat}(\mathcal{B})$. Let $P_i = \mathrm{rprem}(Q_i, T, w_o) = I_{i0}y_{i0} + V_{i0}$. Then $I_{i0} \neq 0$ and $P_i \in \mathbf{sat}(\mathcal{B})$, where $I_0, V_{i0} \in \mathcal{K}\{\mathbb{U}, \lambda, w\}$, ord$(I_{i0}, w) <$ ord$(\mathcal{A})$, and ord$(V_{i0}, w) \leq$ ord$(\mathcal{A})$. Since T is irreducible and has the lowest order in w, we have $I_{i0} \notin \mathbf{sat}(\mathcal{B})$. From $P_i \in \mathbf{sat}(\mathcal{B})$, we have $\mathrm{Eord}_w(y_i) = \mathrm{ord}_w(y_i) = 0$. By (6), we have

$$\mathrm{Eord}(T, w) = \mathrm{ord}(T, w) = \mathrm{ord}(\mathcal{A}).$$

Since $T, P_i \in \mathbf{sat}(\mathcal{B})$, the characteristic set of $\mathbf{sat}(\mathcal{B})$ under the variable order $\mathbb{U} < \lambda_i < w < y_i$ must be of the form:

$$T, T_1, \ldots, T_s, P_1, \ldots, P_p$$

where $T_i \in \mathcal{K}\{\mathbb{U}, \lambda, w\}$. Let $Q \in \mathcal{K}\{\mathbb{U}, \lambda\}$ be the product of all the coefficients of rprem$(I_{i0}, \mathcal{B})$ as a polynomial in $y_{i,j}$. Since $\mathcal{K}\langle\mathbb{U}\rangle$ is aperiodic, there exist $\sigma_1, \ldots, \sigma_p \in \mathcal{K}\{\mathbb{U}\}$ such that $Q(\sigma_1, \ldots, \sigma_p) \neq 0$. Let $\overline{\mathcal{B}}$ be the chain $\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i$. We have $\overline{I}_0 y_{i0} + \overline{V}_{i0} \in \mathbf{sat}(\overline{\mathcal{B}})$, where $\overline{I}_0, \overline{V}_{i0}$ are obtained by replacing each λ_i with σ_i in Q, V_{i0} respectively. Since $Q(\sigma_1, \ldots, \sigma_p) \neq 0$, we have $\overline{I}_0 \notin \mathbf{sat}(\overline{\mathcal{B}})$. We denote $I_i = \overline{I}_0, V_i = \overline{V}_{i0}$. Then $\overline{P}_i = I_i y_{i,0} + V_i \in \mathbf{sat}(\overline{\mathcal{B}})$. From ord$(I_0, w) <$ ord$(\mathcal{A})$ and ord$(V_{i0}, w) \leq$ ord$(\mathcal{A})$, we have ord$(I_i, w) <$ ord$(\mathcal{A})$ and ord$(V_i, w) \leq$ ord$(\mathcal{A})$. As a consequence, a characteristic set of $\mathbf{sat}(\overline{\mathcal{B}})$ must be of the form (5). Repeat the process for proving equation (6), we can show that Eord$(R, w) =$ ord$(R, w) =$ ord$(\mathcal{A})$. Hence R is effective in w. This proves the theorem. ▌

Now, we may extend the following well-known result in algebraic geometry to difference case.

Corollary 4.2. *Any irreducible difference variety V is birationally equivalent to an irreducible difference variety of codimension one if the ground field $\mathcal{K}$ is aperiodic or V is of positive dimension.*

Proof: Let I be the set of r-pols which vanish on V. Then I is a reflexive prime ideal. Construct a resolvent (5) for I as done in Theorem 4.1. Let $W = \mathrm{Zero}(\mathbf{sat}(R, R_1, \ldots, R_s))$. The rational maps are defined as follows:

$$\begin{aligned} M_1 &: V \Rightarrow W; (\mathbb{U}, y_1, \ldots, y_p) \Rightarrow (\mathbb{U}, \sum_{i=1}^{p} \sigma_i y_i)\\ M_2 &: W \Rightarrow V; (\mathbb{U}, w) \Rightarrow (\mathbb{U}, \frac{V_1(\mathbb{U}, w)}{I_1(\mathbb{U}, w)}, \ldots, \frac{V_p(\mathbb{U}, w)}{I_p(\mathbb{U}, w)}).\end{aligned}$$

M_2 can be defined on $W - \mathrm{Zero}(\prod_i I_i)$. From the construction of σ_i, it is easy to show that M_1 and M_2 are inverse to each other. Hence V and W are birationally equivalent. ▌

We hence call $\mathbf{sat}(R, R_1, \ldots, R_s)$ the *resolvent ideal* and $R, R_1, \ldots, R_s$ the *resolvent system* of V or $I = \mathbf{sat}(\mathcal{A})$.

Note that from the results about resolvents in [2], we cannot obtain Corollary 4.2. The reason is that in [2], it is only proved that $I_i y_{i,m_i} - V_i \in I$ for some non-negative integer m_i. So the construction of M_2 is not valid. In our case, due to the introduction of characteristic set, we can show that $I_i y_i - V_i \in I$, which leads to the result proved in this section.

4.2 Algorithm to compute resolvent system

We first give an algorithm to compute the first element of the resolvent system for $\mathbf{sat}(\mathcal{A})$.

Algorithm 4.3. *Input: a coherent and strong irreducible chain $\mathcal{A}$ of the form (1) and a variable set $\Lambda = \{\lambda_1, \ldots, \lambda_p\}$. Output: a $T \in \mathcal{K}\{\mathbb{U}, \Lambda, w\}$ which is an r-pol in $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$ with the lowest rank w.r.t the variable order $\mathbb{U} < \lambda_i < w < y_i$.*

Step 1 Let $o =$ ord$(\mathcal{A})$, $\mathcal{A}_o = \mathcal{A}_{(o,\ldots,o)}$, and $\mathbb{U}^*, \mathbb{Y}^*$ the sets of u_{ij} and y_{ij} occurring in $\mathcal{A}_o$ respectively. Then $\mathcal{A}_o$ is an irreducible algebraic triangular set in $\mathcal{K}[\mathbb{U}^*, \mathbb{Y}^*]$[8].

Step 2 Let $\mathcal{A}_o' = \mathcal{A}_o, w_0 - \sum_{i=1}^{p} \lambda_{i,0} y_{i,0}, \ldots, w_o - \sum_{i=1}^{p} \lambda_{i,o} y_{i,o}$ and $\Lambda_o = \{\lambda_{i,j}, i = 1, \ldots, p; j = 0, \ldots, o\}$. Then it is clear that $\mathcal{A}_o'$ is an irreducible algebraic triangular set in $\mathcal{K}[\Lambda_o, \mathbb{U}^*, \mathbb{Y}^*]$.

Step 3 Compute a characteristic set $\mathcal{C}$ of $\mathbf{a\text{-}sat}(\mathcal{A}_o')$ in the polynomial ring $\mathcal{K}[\Lambda_o, \mathbb{U}^*, \mathbb{Y}^*]$ under the variable order $\mathbb{U} < \lambda_{i,j} < w_0 < w_1 < \ldots < w_o < y_{i,j}$ with methods proposed in [4, 20] and output the first element in $\mathcal{C}$.

Proof of the correctness of Algorithm 4.3. Let $\mathcal{B}$ be a characteristic set of $\mathbf{a\text{-}sat}(\mathcal{A}'_o)$ under the given variable order. It is clear that $\mathbb{U}^*$ and Λ_o are in the parametric set of $\mathbf{a\text{-}sat}(\mathcal{A}'_o)$. By the definition of the order for a chain, $\mathcal{A}'_o$ has $o = \mathrm{ord}(\mathcal{A})$ parameters of the form $y_{i,j}$. In other words, $\mathbf{a\text{-}sat}(\mathcal{A}'_o)$ is of dimension o over the base field $\mathcal{K}(\mathbb{U}^*, \Lambda_o)$. Since $w_i, i = 0, \ldots, o$ are $o+1$ linear combinations of $y_{i,j}$, they must satisfy an algebraic relation. Let T be such a relation and with the lowest rank. Then $T \in \mathbf{a\text{-}sat}(\mathcal{A}'_o) \subset \mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$. From Theorem 4.1, we know that the r-pol in $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$ with the lowest rank under the variable order $\mathbb{U} < \Lambda < w < y_i$ is of order o in w. Hence T must involve w_o and is an r-pol in $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$ with the lowest rank w.r.t the variable order $\mathbb{U} < \lambda_i < w < y_i$. ▌

ALGORITHM 4.4. *Input: a coherent and strong irreducible chain $\mathcal{A}$ of form (1). Output: $\sigma_i \in \mathcal{K}\{\mathbb{U}\}$ and a characteristic set of $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)$ which is of form (5).*

Step 1 Let $\lambda_i, i = 1, \ldots, p$ be p variables. With Algorithm 4.3, we may compute a $T \in \mathcal{K}\{\mathbb{U}, \lambda_1, \ldots, \lambda_p, w\}$ which is an r-pol in $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$ with the lowest rank w.r.t the variable order $\mathbb{U} < \lambda_i < w < y_i$.

Step 2 Let S be the resultant of $\frac{\partial T}{\partial w_0}$ and T w.r.t w_o. Find r-pols A, B such that $AT + B\frac{\partial T}{\partial w_0} = S$.

Step 3 For $i = 1, \ldots, p$, let $Q_i = B(\frac{\partial T}{\partial \lambda_{i,0}} + y_{i,0}\frac{\partial T}{\partial w_0}) + ATy_{i,0} = Sy_{i,0} + B\frac{\partial T}{\partial \lambda_{i0}} \in \mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i)$, $R_i = \mathrm{rprem}(Q_i, T)$.

Step 4 Let $\mathcal{B} = \mathcal{A}, w - \sum_{i=1}^{p} \lambda_i y_i$ and $Q \in \mathcal{K}\{\mathbb{U}, \lambda\}$ be the product of the coefficients of $\mathrm{rprem}(\mathrm{init}(R_i), \mathcal{B})$ as a polynomial in $y_{i,j}$. By Lemma 2.1, we may select $\sigma_i \in \mathcal{K}\{\mathbb{U}\}$ s.t. $Q(\sigma_1, \ldots, \sigma_p) \neq 0$.

Step 5 Let $P_i = (R_i)|_{(\lambda_1,\ldots,\lambda_p)=(\sigma_1,\ldots,\sigma_p)}$. From the proof of Theorem 4.1, we know that $P_i = I_i y_{i0} - V_i \in \mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)$, $I_i \notin \mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)$, and $\mathrm{ord}(I_i, w) < \mathrm{ord}(\mathcal{A})$.

Step 6 Using the zero decomposition theorem proposed in [8], we may find the following decomposition under the variable order $\mathbb{U} < w < y_1 < \ldots < y_p$

$$\begin{aligned} & \mathrm{Zero}(\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i, P_1, \ldots, P_p)/\mathbf{I}_{\mathcal{A}}) \\ = \quad & \mathrm{Zero}(\mathcal{A} \cup \{w - \sum_{i=1}^{p} \sigma_i y_i, P_1, \ldots, P_p\}/\mathbf{I}_{\mathcal{A}}) \\ = \quad & \cup_i \mathrm{Zero}(\mathbf{sat}(\mathcal{B}_i)/\mathbf{I}_{\mathcal{A}}) \end{aligned}$$

where $\mathcal{B}_i$ are coherent and proper irreducible after a proper renaming of the variables.

Step 7 By Theorem 4.1, a characteristic set of $\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i, P_1, \ldots, P_p)$ is of the form (5). By Corollary 3.11, one of $\mathcal{B}_i$, say $\mathcal{B}_1$, must have $\mathbb{U}$ as its parametric set and $\mathrm{ord}(\mathcal{B}_1) = \mathrm{ord}(\mathcal{A})$. Then $\mathbf{sat}(\mathcal{A} \cup \{w - \sum_{i=1}^{p} \sigma_i y_i\})$ must be the only prime component of $\{\mathbf{sat}(\mathcal{B}_1)\}$. By Corollary 3.14, $\mathcal{B}_1$ is strong irreducible and $\mathbf{sat}(\mathcal{A} \cup \{w - \sum_{i=1}^{p} \sigma_i y_i\}) = \mathbf{sat}(\mathcal{B}_1)$. Output $\mathcal{B}_1$.

In the above algorithm, we need to introduce p new parameters, which will increase the computational costs. In the following, we will give a probabilistic algorithm.

THEOREM 4.5. *Let $\mathcal{A}$ be a coherent and strong irreducible chain of the form (1) and $\sigma_i, i = 1, \ldots, p$ elements in $\mathcal{K}\{\mathbb{U}\}$. Using the zero decomposition theorem proposed in [8], we may find the following decomposition under the variable order $\mathbb{U} < w < y_1 < \ldots < y_p$*

$$\begin{aligned} & Zero(\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)/\mathbf{I}_{\mathcal{A}}) \qquad (7) \\ = \quad & Zero(\mathcal{A} \cup \{w - \sum_{i=1}^{p} \sigma_i y_i\}/\mathbf{I}_{\mathcal{A}}) = \cup_i Zero(\mathbf{sat}(\mathcal{B}_i)/\mathbf{I}_{\mathcal{A}}) \end{aligned}$$

where $\mathcal{B}_i$ are coherent and proper irreducible chains after a proper renaming of the variables. If one of $\mathcal{B}_i$, say $\mathcal{B}_1$, is of the form (5), then $\mathcal{B}_1$ is strong irreducible and is a resolvent system for $\mathbf{sat}(\mathcal{A})$.

The proof of Theorem 4.5 is omitted. Based on this theorem, we may just select p elements σ_i from $\mathcal{K}\{\mathbb{U}\}$ randomly and compute the zero decomposition (7). The probability of success is nearly one since by Theorem 4.1, the "bad" σ_i are solutions of an r-pol equation $Q = 0$.

EXAMPLE 4.6. *Consider the coherent and strong irreducible chain $\mathcal{A} = \{y_1^2 + x, y_{2,1}^2 + y_2^2 + 1, y_{2,2} - y_2\}$. Let $w = y_1 + y_2$. Using the zero decomposition theorem proposed in [8], we find the following decomposition under the variable order $w < y_1 < y_2$:*

$$\begin{aligned} & Zero(\mathbf{sat}(\mathcal{A}, w - y_1 - y_2)) \\ = \quad & Zero(\mathcal{A} \cup \{w - y_1 - y_2\}) = Zero(\mathbf{sat}(\mathcal{B}_1)) \end{aligned}$$

where $\mathcal{B}_1$ is:

$R = w_1^8 + (8 + 4w^2)w_1^6 + (16w^2 + 6w^4 + 8x^2 + 16)w_1^4 + (4w^6 + 8w^4 + 32x^2 - 48w^2x^2 - 64w^2x)w_1^2 + w^8 + 8w^4x^2 + 16x^4$,

$R_1 = (2w_1^2w + 2w^3 - 4wx)w_2^2 + (-2w_1^2w^2 + w_1^4 - 3w^4 + 4w_1^2 + 4x^2)w_2 + 4w^3 + w^5 - 8wx - ww_1^4 + 4xw^3 - 4wx^2$,

$P_1 = (-4w^3 - 4w_1^2w + 8wx)y_1 + 4w_1^2 + 2w_1^2w^2 + w^4 + w_1^4 - 8w^2x + 4x^2$,

$P_2 = (-8wx + 4w_1^2w + 4w^3)y_2 - 3w^4 - 2w_1^2w^2 + 4w_1^2 + w_1^4 + 4x^2$.

By Theorem 4.5, $\{R, R_1\}$ is a resolvent system for $\mathbf{sat}(\mathcal{A})$.

5. RESOLVENT SYSTEM OF A PROPER IRREDUCIBLE CHAIN

Generally, we do not know how to decide wether a chain is strong irreducible or not. On the other hand, we can decide whether a chain is proper irreducible. In this section, we will give an algorithm for the resolvent system of a proper irreducible chain.

THEOREM 5.1. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1) and $\lambda_1, \ldots, \lambda_p$ difference variables. We assume that $\mathcal{K}$ is an aperiodic difference field or $|\mathbb{U}| \neq 0$. Then there exists $Q \in \mathcal{K}\{\lambda_1, \ldots, \lambda_p, \mathbb{U}\}$ such that if $\sigma_1, \ldots, \sigma_p$ satisfy $Q(\sigma_1, \ldots, \sigma_p, \mathbb{U}) \neq 0$, the characteristic set of the perfect ideal $\{\mathbf{sat}(\mathcal{A}, w - \sum_{i=1}^{p} \sigma_i y_i)\}$ under the variable order $\mathbb{U} < w < y_i$ is of the following form*

$$R, R_1, \ldots, R_s, I_1 y_{1,0} - V_1, \ldots, I_p y_{p,0} - V_p \qquad (8)$$

where $R, R_i, I_i, V_i \in K\{\mathbb{U}, w\}$. Furthermore, R is effective in w and $ord(R, w) = ord(\mathcal{A})$.

Proof: Let $o = \mathrm{ord}(\mathcal{A})$, $Y_h = (y_{1,0}, y_{1,1}, \ldots, y_{1,h}, \ldots, y_{p,0}, \ldots, y_{p,h})$, $W_h = (w_0, \ldots, w_h)$, and $\Lambda = \{\lambda_1, \ldots, \lambda_p\}$. For any r-pol set $\mathbb{P}$, we denote $\mathbb{P}' = \{\mathbb{P}, w - \sum_{i=1}^{p} \lambda_i y_i\}$. Let $\{\mathbf{sat}(\mathcal{A})\} =$

$\bigcap\limits_{s=1}^{r} P_s$ be an irredundant decomposition of $\{\mathbf{sat}(\mathcal{A})\}$ as the intersection of prime difference ideals. Then $\{\mathbf{sat}(\mathcal{A}), w - \sum_{i=1}^{p}\lambda_i y_i\} = \bigcap\limits_{i=1}^{r} P_i^{'}$, where $P_s' = \{P_s, w - \sum \lambda_i y_i\}$. By Theorem 4.1, for each s, the characteristic set for P_s' under the variable order $\mathbb{U} < \lambda_i < w < y_i$ is of the following form:

$$T_s, T_{s,1}, \ldots, T_{s,l_s}, I_{s,1}y_{s,0} - V_{s,1}, \ldots, I_{s,p}y_{s,0} - V_{s,p}$$

where $T_i, T_{i,j}, I_{i,j}, V_{i,j} \in \mathcal{K}\{\mathbb{U}, w\}$ and $\mathrm{ord}(T_s, w) = o$, $\mathrm{ord}(I_{i,j}) < o$, and $\mathrm{ord}(V_{i,j}) \leq o$.

Let $P_s^* = P_s' \bigcap \mathcal{K}\{\mathbb{U}, \Lambda\}[W_o, Y_0]$. Then $\mathbb{P}^* = \{\mathbf{sat}(\mathcal{A}), w - \sum_{i=1}^{p}\lambda_i y_i\} \bigcap \mathcal{K}\{\mathbb{U}, \lambda\}[W_o, Y_0] = \bigcap_{s=1}^{r} P_s^*$. Also, $T_s, I_{s,j}y_{s,0} - V_{s,j} \in P_s^*$. It is easy to see that $P_s^* = \textbf{a-sat}(T_s, I_{s,1}y_{s,0} - V_{s,1}, \ldots, I_{s,p}y_{s,0} - V_{s,p})$ is an algebraic prime ideal. From the proof of Theorem 4.1, we know that $I_{s,i}y_{s,i} - V_{s,i}$ are constructed from T_s. Thus if $T_s = T_t$, $P_s^* = P_t^*$. Let $P_{i_0}^* = P_{i_1}^* = \ldots = P_{i_t}^*(i_0 = 1)$ be the distinct P_i^*. We have $T_{i_k} \neq T_{i_j}$ for $k \neq j$. So $\mathbb{P}^* = \bigcap_{j=0}^{t} P_{i_j}^*$ is an irredundant representation and $S_k = \prod_{l=0}^{k} T_{i_l} \in \bigcap_{j=0}^{k} P_{i_j}^*$. We will show that there exist $I_i, V_i \in \mathcal{K}\{\mathbb{U}, \Lambda, w\}$, such that $I_i y_{i0} - V_i \in \mathbb{P}^*$ and $\mathrm{ord}(I_i, w) < o$. We will construct such r-pols by doing induction on k. Suppose that there exists $J_{i,k}y_{i,0} + W_{i,k} \in \cap_{j=0}^{k} P_{i_j}^*$ and $\mathrm{ord}(J_{i,k}, w) < o$. Since $S_k \in \cap_{j=0}^{k} P_{i_j}^*$ and $Q_k = T_{i_{k+1}} \in P_{i_{k+1}}^*$ are distinct r-pols of the same order w.r.t w and Q_k is irreducible, the resultant H of S_k and Q_k w.r.t w_o is not zero. From the property of the resultant, there exist $A(w), B(w) \in \mathcal{K}\{\mathbb{U}\}[W_o]$ such that $H = AS_k + BQ_k$. Let

$$\begin{aligned} J_{i,k+1} &= BQ_k J_{i,k} + AS_k I_{i,k+1}, \\ W_{i,k+1} &= BQ_k W_{i,k} + AS_k V_{i,k+1}. \end{aligned}$$

Then, we have

$$\begin{aligned} & J_{i,k+1}y_{i,0} - W_{i,k+1} = AS_k I_{i,k+1} y_{i,0} - AS_k V_{i,k+1} \\ = \;& H(I_{i,k+1}y_{i,0} - V_{i,k+1}) = 0 \bmod P_{i_{k+1}}^* \\ & J_{i,k+1}y_{i,0} - W_{i,k+1} = BQ_k J_{i,k} y_{i,0} - BQ_k W_{i,k} \\ = \;& H(J_{i,k}y_{i,0} - W_{i,k}) = 0 \bmod \cap_{j=0}^{k} P_{i_j}^* \end{aligned}$$

Therefore, $J_{i,k+1}y_{i,0} - W_{i,k+1} \in \cap_{j=0}^{k+1} P_{i_j}^*$. Since $J_{i,k+1} = HI_{i,k+1} \neq 0 \bmod P_{i_{k+1}}^*$ and $J_{i,k+1} = HJ_{i,k} \neq 0 \bmod \cap_{j=0}^{k} P_{i_j}^*$, the resultant H' of $J_{i,k+1}$ and S_{k+1} w.r.t w_o is not zero. We have r-pols A', B' such that $H' = A'J_{i,k+1} + B'S_{k+1}$. Let $P_i = A'(J_{i,k+1}y_{i,0} - W_{i,k+1}) + B'S_{k+1}y_{i,0} = H'y_{i,0} - A'W_{i,k+1} \in \cap_{j=0}^{k+1} P_{i_j}^*$. Then there exists $P_i = I_i y_{i,0} - V_i \in \mathbb{P}^* \subset \{\mathbf{sat}(\mathcal{A}), w - \sum \lambda_i y_i\}$. Similar to the proof of Theorem 4.5, we may select an r-pol Q and $\sigma_i \in \mathcal{K}\{\mathbb{U}\}$, such that when replacing λ_i by σ_i we have $\overline{I_i} \neq 0$ and $\overline{I_i}y_{i0} + \overline{V}_i \in \{\mathbf{sat}(\mathcal{A}), w - \sum \sigma_i y_i\} \subset \{P_i, w - \sum \sigma_i y_i\}$. From the Theorem 4.1, the characteristic set of $\{P_i, w - \sum \sigma_i y_i\}$ under variable order $\mathbb{U} < w < y_i$ is of the following form

$$S_i, S_{i,1}, \ldots, S_{i,l_i}, I_{i,1}y_{i,0} - V_{i,1}, \ldots, I_{s,p}y_{s,0} - V_{s,p}$$

where $S_i, S_{i,j}, I_{i,j}, V_{i,j} \in \mathcal{K}\{\mathbb{U}, w\}$ and $\mathrm{ord}(T_s, w) = o$. Let R be the product of the distinct S_i. Then $R \in \cap_i\{P_i, w - \sum \sigma_i y_i\} = \{\mathbf{sat}(\mathcal{A}), w - \sum \sigma_i y_i\}$ and must be such an r-pol with lowest rank. This proves the theorem. ▌

For a proper irreducible chain, we can find a resolvent system for $\mathbf{sat}(\mathcal{A})$.

THEOREM 5.2. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1), $\mathcal{K}$ an aperiodic difference field or $|\mathbb{U}| \neq 0$. Then we can find $\sigma_1, \ldots, \sigma_p \in \mathcal{K}\{\mathbb{U}\}$ such that*

$$\begin{aligned} \mathit{Zero}(\mathbf{sat}(\mathcal{A}, w - \textstyle\sum \sigma_i y_i)) &= \cup_{i=1}^{t} \mathit{Zero}(\mathbf{sat}(\mathcal{R}_i)) \quad \mathit{or} \\ \{\mathbf{sat}(\mathcal{A}, w - \textstyle\sum \sigma_i y_i)\} &= \cap_{i=1}^{t} \{\mathbf{sat}(\mathcal{R}_i)\} \end{aligned}$$

where $\mathcal{R}_i$ is coherent and proper irreducible under the variable order $\mathbb{U} < w < y_i$ and of the following form:

$$R_i, R_{i,1}, \ldots, R_{i,s_i}, I_{i,1}y_{1,0} - V_{i,1}, \ldots, I_{i,p}y_{p,0} - V_{i,p} \qquad (9)$$

$R_i, R_{i,j}, I_{i,j}, V_{i,j} \in K\{\mathbb{U}, w\}$. Furthermore, R_i is effective in w and ord$(R_i, w) =$ ord$(\mathcal{A})$.

We call $\{R_i, R_{i,1}, \ldots, R_{i,s_i}\}, i = 1, \ldots, t$, *resolvent systems* for $\mathbf{sat}(\mathcal{A})$. We will prove the theorem by giving an algorithm to compute the resolvent systems.

ALGORITHM 5.3. *Input: a coherent and proper irreducible chain $\mathcal{A}$ of the form (1). Output: the resolvent systems for* $\mathbf{sat}(\mathcal{A})$.

Step 1 Let $\mathcal{B} = \mathcal{A}, w - \sum_{i=1}^{p}\lambda_i y_i$. Then $\mathcal{B}$ is also a coherent and proper irreducible chain. By Lemma 3.3, we have $\mathrm{Zero}(\mathbf{sat}(\mathcal{B})/\mathbf{I}_{\mathcal{B}}) = \mathrm{Zero}(\mathcal{B}/\mathbf{I}_{\mathcal{B}})$.

Step 2 Using the difference zero decomposition theorem proposed in [8], under the variable order $\mathbb{U} < \lambda_i < w < y_1 < \ldots < y_p$, we may find a decomposition

$$\mathrm{Zero}(\mathcal{B}/\mathbf{I}_{\mathcal{B}}) = \cup_{i=1}^{s}\mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i)/\mathbf{I}_{\mathcal{B}}) \qquad (10)$$

where $\mathcal{A}_i$ are coherent and proper irreducible after a proper renaming of the variables.

Step 3 Let T_i, and $P_{i,j}$ be the r-pols with lowest rank in $\mathcal{A}_i$ such that $\mathrm{lvar}(T_i) = w, \mathrm{lvar}(P_{i,j}) = y_j$. By Theorem 4.1, the characteristic sets for all the prime components of $\mathbf{sat}(\mathcal{B})$ are of the form (5). By Corollary 3.11, $\{\mathbf{sat}(\mathcal{A}_i)\}$ is an unmixed ideal, and hence only for those $\mathcal{A}_i$ with $\mathbb{U}$ as the parametric set and satisfying $\mathrm{ord}(T_i, w) = \mathrm{ord}(\mathcal{A})$ and $\mathrm{ord}(P_{i,j}, y_j) = 0$, $\mathrm{Zero}(\mathbf{sat}(\mathcal{A}_i)/J)$ is not redundant. We may simply assume that all the $\mathcal{A}_i$ in (10) satisfy this condition.

Step 4 For each $\mathcal{A}_i$, let $S_{i,j} = \frac{\partial T_i}{\partial \lambda_{j0}} + y_j \frac{\partial T_i}{\partial w_0}$. By Corollary 3.13, the first r-pol in the characteristic set for each prime component of $\{\mathbf{sat}(\mathcal{A}_i)\}$ is also T_i. $S_{i,j}$ is in each prime component of $\{\mathbf{sat}(\mathcal{A}_i)\}$ and hence $S_{i,j} \in \{\mathbf{sat}(\mathcal{A}_i)\}$. Let R_i be the resultant of $\frac{\partial T_i}{\partial w_0}$ and T_i w.r.t w_o and A, B r-pols such that $R_i = A\frac{\partial T_i}{\partial w_0} + BT_i$. Let $Q_{i,j} = AS_{i,j} + BT_i y_{j,0} = R_i y_{i,0} + A\frac{\partial T_i}{\partial \lambda_{j0}}$ and $P_{i,j} = \mathrm{rprem}(Q_{i,j}, T_i)$. We have $P_{i,j} \in \{\mathbf{sat}(\mathcal{A}_i)\}$.

Step 5 Let $P_{i,j} = I_{i,j}y_{j,0} - V_{i,j}$ where $I_{i,j}, V_{i,j} \in \mathcal{K}\{\mathbb{U}, \lambda, w\}$. Since $\mathrm{ord}(I_{i,j}, w) < \mathrm{ord}(\mathcal{A})$ and $\mathrm{ord}(T_i, w) = \mathrm{ord}(\mathcal{A})$, $I_{i,j}$ is not in each of $\mathbf{sat}(\mathcal{A}_i)$. Hence $I_{i,j}$ is invertible w.r.t $\mathcal{B}$. Let Q_0 be obtained by taking the successive resultant of $I_{i,j}$ and the r-pols in $\mathcal{B}_{I_{i,j}}$. Then Q_0 is not zero and in $\mathcal{K}\{\mathbb{U}\}[\mathcal{P}(\mathcal{A})]$, where $\mathcal{P}(\mathcal{A})$ is defined in (3). Let $Q \in \mathcal{K}\{\mathbb{U}, \lambda\}$ be the product of the coefficients of Q_0 as a polynomial in $y_{i,j}$. Select $\sigma_i \in \mathcal{K}\{\mathbb{U}\}$ such that $Q(\sigma_1, \ldots, \sigma_p) \neq 0$.

Step 6 For an r-pol P and a chain $\mathcal{C}$, let $\overline{P}$ and $\overline{\mathcal{C}}$ be obtained by replacing λ_i with σ_i. It is clear that $\overline{P}_{i,j} \in \{\mathbf{sat}(\overline{\mathcal{A}}_i)\}$. Since $Q(\sigma_1, \ldots, \sigma_p) \neq 0$, $\overline{Q}_0 \neq 0$. Then $\overline{I}_{i,j}$ is invertible w.r.t $\overline{\mathcal{B}}$ and hence not in $\mathbf{sat}(\overline{\mathcal{B}})$. Due to (10), $\overline{I}_{i,j} \notin \{\mathbf{sat}(\overline{\mathcal{A}}_i)\}$.

Step 7 Using the difference zero decomposition theorem proposed in [8], we may find the following decomposition under the variable order $\mathbb{U} < w < y_1 < \ldots < y_p$

$$\begin{aligned} & \mathrm{Zero}(\mathbf{sat}(\overline{\mathcal{A}}_i) \cup \{\overline{P}_{i,1}, \ldots, \overline{P}_{i,p})/\mathbf{I}_{\overline{\mathcal{A}}_i}) \\ = \quad & \mathrm{Zero}(\overline{\mathcal{A}}_i \cup \{\overline{P}_{i,1}, \ldots, \overline{P}_{i,p}\}/\mathbf{I}_{\overline{\mathcal{A}}_i}) \\ = \quad & \cup_j \mathrm{Zero}(\mathbf{sat}(\mathcal{B}_{i,j})/\mathbf{I}_{\overline{\mathcal{A}}_i}) \end{aligned}$$

where $\mathcal{B}_{i,j}$ are coherent and proper irreducible chains.

Step 8 Using the similar argument in Step 3, we only select those $\mathcal{B}_{i,j}$ which are of the form (8). This is possible since $\overline{P}_{i,j}$ are linear in $y_{i,0}$. Output $\mathcal{B}_{i,j}$. We have proved the Theorem 5.2.

In the following, we will give a probabilistic algorithm.

THEOREM 5.4. *Let $\mathcal{A}$ be a coherent and proper irreducible chain of the form (1) and $\sigma_i, i = 1, \ldots, p$, elements in $\mathcal{K}\{\mathbb{U}\}$. Suppose that we find the following decomposition under the variable order $\mathbb{U} < w < y_1 < \ldots < y_p$*

$$Zero(\mathbf{sat}(\mathcal{A}, w - \sum \sigma_i y_i)) \quad = \quad \cup_{i=1}^{t} Zero(\mathbf{sat}(\mathcal{R}_i))$$

where $\mathcal{R}_i$ is proper irreducible and of the following form

$$R_i, R_{i,1}, \ldots, R_{i,s_i}, I_{i,1}y_{1,0} - V_{i,1}, \ldots, I_{i,p}y_{p,0} - V_{i,p} \qquad (11)$$

$R_i, R_{i,j}, I_{i,j}, V_{i,j} \in K\{\mathbb{U}, w\}$ and $ord(R_i, w) = ord(\mathcal{A})$. Then $\{R_i, R_{i,1}, \ldots, R_{i,s_i}\}$ are the resolvent systems for $\mathbf{sat}(\mathcal{A})$.

The Proof is omitted.

EXAMPLE 5.5. *Consider the chain $\mathcal{A} = \{y_1^2 + x, y_{2,1}^2 + y_2^2 + 1\}$. Let $w = y_1 + y_2$. Using the zero decomposition theorem proposed in [8], we find the following decomposition under the variable order $w < y_1 < y_2$:*

$$\begin{aligned} & Zero(\mathbf{sat}(\mathcal{A}, w - y_1 - y_2)) = Zero(\mathcal{A} \cup \{w - y_1 - y_2\}) \\ = \quad & Zero(\mathbf{sat}(\mathcal{B}_1)) \cup Zero(\mathbf{sat}(\mathcal{B}_2)) \end{aligned}$$

where $\mathcal{B}_2 = \{R, R_1', P_1, P_2\}$, $\mathcal{B}_1, R, P_1, P_2$ are given in Example 4.6 and $R_1' = (-2w_1^2 w - 2w^3 + 4wx)w_2^2 + (-2w_1^2 w^2 + w_1^4 - 3w^4 + 4w_1^2 + 4x^2)w_2$. By Theorem 5.4, $\{R, R_1\}$ and $\{R, R_1'\}$ are the resolvent systems for $\mathbf{sat}(\mathcal{A})$.

6. CONCLUSION

Intuitively speaking, resolvents can be used to establish a birational correspondence between the solutions of a set of equations and the solutions of equations in one variable. For difference equations, the theory of resolvent is not complete in several aspects. In this paper, we give a more complete theory of resolvents. For an irreducible difference variety V, we can construct a coherent and strong irreducible chain $\mathcal{R}$ in one variable such that V and Zero($\mathbf{sat}(\mathcal{R})$) are birationally equivalent. For a coherent and proper irreducible chain $\mathcal{A}$, we can construct coherent and proper irreducible chains $\mathcal{R}_i$ in one variable such that Zero($\mathbf{sat}(\mathcal{A})$) and $\cup_i$Zero($\mathbf{sat}(\mathcal{R}_i)$) are birationally equivalent.

An interesting problem is to see whether $\cup_i$Zero($\mathbf{sat}(\mathcal{R}_i)$) in the proper irreducible case can be combined into one chain. That is, can we find a chain $\mathcal{B}$ such that Zero($\mathbf{sat}(\mathcal{B})$) = $\cup_i$Zero($\mathbf{sat}(\mathcal{R}_i)$)? To develop more efficient algorithms for difference resolvent systems is a very interesting and challenging problem.

7. REFERENCES

[1] T. Cluzeau and E. Hubert, Resolvent Representation for Regular Differential Ideals, *AAECC*, **29**, 395-425, 2003.

[2] R.M. Cohn, *Difference Algebra*, Interscience Pbulishers, 1965.

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

[4] S.C. Chou, *Mechanical Geometry Theorem Proving,* D.Reidel Publishing Company, 1988.

[5] X.S. Gao and S.C. Chou, On the Parameterization of Algebraic Curves, *AAECC*, **3**, 27-38, 1992.

[6] X.S. Gao and S.C. Chou, On the Dimension for Arbitrary Ascending Chains, *Chinese Bull. of Scis.*, vol. 38, 396-399, 1993.

[7] X.S. Gao and S.C. Chou, On the Theory of Resolvents and its Applications, *Sys. Sci. and Math. Sci.*, **12**, 17-30, 1999,

[8] X.S. Gao and Y. Luo, A Characteristic Set Method for Difference Polynomial Systems, *Inter Conf on Poly Sys. Sol.*, Nov. 24-26, Paris, 2004. Submitted to JSC.

[9] P. Gianni and T. Mora, Algebraic Solution of Systems of Polynomial Equations Using Gröbnert bases, 247-257, *LNCS*, vol. 356, Springer-Verlag, 1987.

[10] D. Grigoriev, Complexity of Quantifier Elimination in the Theory of Ordinary Differential Equations, *LNCS*, vol. 378, 11-25, 1989.

[11] R. Loos, Computing in Algebraic Extensions, in *Computer Algebra* (Ed. by B. Buchberger, et al), 173–187, Springer-Verlag, New York, 1982.

[12] H. Kobayashi, S. Moritsugu and R.W. Hogan, Solving Systems of Algebraic Equations, *Proc. of ISSAC-88*, pp.139–149, LNCS No. 358, Springer-Verlag, 1988.

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

[14] E.L. Mansfield and A. Szanto, Elimination Theory for Differential Difference Polynomials, *Proc. ISSAC 2002*, 191-198, ACM Press.

[15] J.F. Ritt, *Differential Algebra*, Amer. Math. Soc. Colloquium, 1950.

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

[17] B.M. Trager, Algebraic Factoring and Rational Integration, *Proc. of ACM Sym. on Symbolic and Algebraic Computation*, 1976.

[18] D. Wang and D. Lin, A Method for Multivariate Polynomial Factorization over Successive Algebraic Extension Fields, *Mathematics and Mathematics Mechanization*, 138-172, 2001.

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

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

[21] K. Yokoyama, M. Noro and T. Takeshima, Computing Primitive Elements of Extension Fields, *Journal of Symbolic Computation*, **8**, 553–580, 1989.