Jrl Syst Sci & Complexity (2009) 22: 627–635

A CRITERION FOR TESTING WHETHER A DIFFERENCE IDEAL IS PRIME*

Chunming YUAN · Xiao-Shan GAO

Received: 1 September 2009 / Received: 15 September 2009

Abstract This paper presents a criterion for testing the irreducibility of a polynomial over an algebraic extension field. Using this criterion and the characteristic set method, the authors give a criterion for testing whether certain difference ascending chains are strong irreducible, and as a consequence, whether the saturation ideals of these ascending chains are prime ideals.

Key words Characteristic set, difference prime ideal, irreducibility, strong irreducibility.

1 Introduction

The characteristic set method is a fundamental tool for studying systems of algebraic or algebraic differential equations[1−12]. The basic idea of the method is to privilege systems which have been put in a special "triangular form", also called an ascending chain or simply a chain. The zero-set of any systems of polynomials or differential polynomials may be decomposed into the union of the zero-sets of chains, and the properties of the solution set of a chain are much easier to study than that of the general equation system.

The notion of characteristic sets for difference polynomial systems was proposed by Ritt and Doob[13]. In the classical book[8], Ritt listed the development of difference algebra as one of the six major problems for future study. The general theory of difference algebra was established by Cohn[14]. Ritt used the characteristic set as the main tool in differential algebra[8]. Due to the intrinsic difficulty of developing difference characteristic set methods, Cohn used the difference kernel as the main tool in his theory. The characteristic set methods for difference polynomial systems were developed only very recently[15−18].

In the characteristic set method, prime ideals are described with so-called strong irreducible ascending chains[15]. But, it is still an open problem to decide whether a chain is strong irreducible. There exist no such decision methods except for the trivial case of linear ascending chains.

In this paper, we give a direct criterion for the irreducibility of a polynomial over the algebraic extension field. Using this criterion, we present a criterion for testing whether certain difference chains are strong irreducible. As a consequence, we give a criterion for testing whether a class of difference ideals are prime.

The paper is organized as follows. In Section 2, we give a direct criterion for the irreducibility of a polynomial over an extension field. In Section 3, we present the criterion for testing whether

Chunming YUAN · Xiao-Shan GAO
Key Laboratory of Mathematics Mechanization, Institute of Systems Science; Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China.*
Email: cmyuan@mmrc.iss.ac.cn, xgao@mmrc.iss.ac.cn.
*This work is partially supported by a National Key Basic Research Project of China and by NSFC.

a difference ideal $\mathrm{sat}(P)$ is prime when P is an irreducible difference polynomial. A more general result for the strong irreducibility of difference ascending chains is given in Section 4. And in Section 5, we conclude the paper.

2 Preliminary Results

In this section, we will prove several results about the irreducibility of polynomials which will be used later in this paper.

2.1 An Irreducibility Criterion for a Polynomial over an Extension Field

Let F be a field with characteristic zero and G a finite field extension of F. In this section, we give a simple criterion to decide whether an irreducible univariate polynomial in $F[x]$ is still irreducible in $G[x]$.

We suppose that G is an algebraic extension of F. Let

$$d = [G : F]$$

be the extension degree of G w.r.t. F. The following results are known.

Lemma 1[14] *Let F, G, H be fields such that $F \subseteq G \subseteq H$. Then*

(a) $[H : F] = [H : G][G : F]$.

(b) If Φ is a set of elements of H, then $[G(\Phi) : F(\Phi)] \leq [G : F]$. And equality holds if Φ is an algebraically independent set over G.

The following result is Gauss's lemma in one variable case, and these results can be generalized to the multi-variable case.

Lemma 2 *If R is a unique factorization domain (UFD) and $f(x)$ and $g(x)$ are both primitive polynomials in $R[x]$, then so is $f(x)g(x)$. Let R be a UFD and F its field of fractions. If a polynomial $f(x)$ in $R[x]$ is reducible in $F[x]$, then it is reducible in $R[x]$.*

We can give the following criterion to test whether an irreducible polynomial is still irreducible over an extension field.

Lemma 3 *Use the notations introduced above. Let $P(x)$ be an irreducible polynomial in $F[x]$. If the greatest common divisor of $n = \deg(P)$ and $d = [G : F]$ is one, that is, $\mathrm{GCD}(n, d) = 1$, then P is irreducible over G.*

Proof Let α be a root of P. Since the characteristic of F is zero and G is an algebraic extension of F, we know that there exists a β such that $G = F(\beta)$.

By Lemma 1(a), we have

$$[G(\alpha) : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] = n[F(\alpha, \beta) : F(\alpha)]$$

and

$$[G(\alpha) : F] = [F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = d[F(\alpha, \beta) : F(\beta)].$$

Therefore,

$$n[F(\alpha, \beta) : F(\alpha)] = d[F(\alpha, \beta) : F(\beta)].$$

Since $\mathrm{GCD}(n, d) = 1$, we have $n | [F(\alpha, \beta) : F(\beta)]$. By Lemma 1(b), $1 \leq [F(\alpha, \beta) : F(\beta)] \leq [F(\alpha) : F] = n$, which implies $n = [F(\alpha, \beta) : F(\beta)] = [G(\alpha) : G]$. Hence, P is irreducible over G. ∎

According to the proof of Lemma 3 and Gauss's lemma, we can extend Lemma 3 to the following form.

Lemma 4 *Let F be a field with characteristic zero, G a finite extension of F, $(\alpha_1, \alpha_2, \cdots, \alpha_m)$ a transcendental basis of G w.r.t. F, and $d = [G : F(\alpha_1, \alpha_2, \cdots, \alpha_m)]$. For an irreducible polynomial $P(x)$ in $F[x]$, if $\mathrm{GCD}(d, \deg(P, x)) = 1$, then $P(x)$ is still irreducible in $G[x]$.*

2.2 Irreducible Triangular Set

We will introduce some notations about algebraic triangular sets. Details about these notations can be found in [3, 19].

A finite sequence of nonzero polynomials $\mathcal{A} = A_1, A_2, \cdots, A_p$ is called a triangular set, if either $p = 1$ and $A_1 \neq 0$ or $0 < \mathrm{cls}(A_1) < \mathrm{cls}(A_2) < \cdots < \mathrm{cls}(A_p)$. $\mathcal{A}$ is called trivial if $\mathrm{cls}(A_1) = 0$. If $\mathcal{A}$ is nontrivial, we call

$$\deg(\mathcal{A}) = \prod_{i=1}^{p} \deg(A_i, \mathrm{lvar}(A_i))$$

the degree of $\mathcal{A}$.

Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a nontrivial triangular set in $F[x_1, x_2, \cdots, x_n]$. Let y_i be the leading variable of A_i, $Y = \{y_1, y_2, \cdots, y_p\}$ and $U = \{x_1, x_2, \cdots, x_n\} \setminus Y = \{u_1, u_2, \cdots, u_q\}$. U is called the parameter set of $\mathcal{A}$. We denote $F[x_1, x_2, \cdots, x_n]$ as $F[U, Y]$.

A polynomial f is said to be invertible w.r.t. $\mathcal{A}$ if either $f \in F[U]$ or $(f, A_1, A_2, \cdots, A_s) \cap F[U] \neq \{0\}$, where $\mathrm{lvar}(f) = \mathrm{lvar}(A_s)$.

$\mathcal{A}$ is called regular if the initials of A_i are invertible w.r.t. $\mathcal{A}$. We denote by $I_{\mathcal{A}}$ the initial product of $\mathcal{A}$. We denote by $\mathrm{asat}(\mathcal{A})$ the algebraic saturation ideal:

$$\mathrm{asat}(\mathcal{A}) = (\mathcal{A}) : I_{\mathcal{A}}^{\infty} = \{P | \exists s \in \mathbb{N}, \text{ s.t. } I_{\mathcal{A}}^{s} P \in (\mathcal{A})\}.$$

$\mathcal{A}$ is called irreducible if $\mathcal{A}$ is a regular triangular set and A_i is an irreducible polynomial in y_i modulo $\mathrm{asat}(A_1, A_2, \cdots, A_{i-1})$. It is known that if $\mathcal{A}$ is irreducible, then $\mathrm{asat}(\mathcal{A})$ is a prime ideal.

Lemma 5 *Use above notations. Let $\mathcal{A}$ be an irreducible algebraic triangular set with $A_i \in F[U, Y]$. Let $K_0 = F(u_0, u_1, \cdots, u_q)$, then*

$$[K_0[y_1, y_2, \cdots, y_p]/\mathrm{asat}(\mathcal{A}) : K_0] = \deg(\mathcal{A}). \tag{1}$$

Proof Since $\mathcal{A}$ is an irreducible algebraic triangular set, $\mathrm{asat}(\mathcal{A})$ is a zero dimensional prime ideal over K_0. We know that $K_0[y_1, y_2, \cdots, y_p]/\mathrm{asat}(\mathcal{A})$ is an algebraic extension field of K_0. Let $(\beta_1, \beta_2, \cdots, \beta_p)$ be a generic zero of $\mathrm{asat}(\mathcal{A})$. By the definition of irreducible triangular set, A_i is the definition polynomial of β_i over $K_0(\beta_1, \beta_2, \cdots, \beta_{i-1})$, $i = 1, 2, \cdots, p$. Then, we have $[K_0[y_1, y_2, \cdots, y_p]/\mathrm{asat}(\mathcal{A}) : K_0] = [K_0(\beta_1, \beta_2, \cdots, \beta_p) : K_0] = [K_0(\beta_1, \beta_2, \cdots, \beta_p) : K_0(\beta_1, \beta_2, \cdots, \beta_{p-1})] * \cdots * [K_0(\beta_1) : K_0] = \prod_{i=1}^{p} \deg(A_i) = \deg(\mathcal{A})$. ∎

3 Strong Irreducibility of a Single Difference Polynomial

In this section, we will give a criterion to decide whether a difference polynomial is strong irreducible and as a consequence whether its saturation ideal is prime.

A difference field $\mathbb{F}$ is a field with a homomorphism δ satisfying: for any $a, b \in \mathbb{F}$, $\delta(a+b) = \delta a + \delta b$, $\delta(ab) = \delta a \cdot \delta b$, and $\delta a = 0$ if and only if $a = 0$. Here, δ is called the transforming operator of $\mathbb{F}$. If $a \in \mathbb{F}$, δa is called the transform of a. $\delta^n a = \delta(\delta^{n-1} a)$ is known as the nth transform. If $\delta^{-1} a$ is defined for all $a \in \mathbb{F}$, we say that $\mathbb{F}$ is inversive. Every difference field has an inversive closure[14].

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

In this paper, all difference fields are assumed to be inversive and with characteristic zero. $\mathbb{K}$ could be the field of rational numbers or the field of rational functions $Q(x)$.

Let y be an indeterminate, and $\mathbb{K}\{y\}$ the difference polynomial ring. We denote $z_0 = y, z_i = \delta^i y$. Then, $\mathbb{K}\{y\} = \mathbb{K}[z_0, z_1, \cdots]$.

A difference ideal is a subset $\mathbb{I}$ of $\mathbb{K}\{y\}$, which is an algebraic ideal in $\mathbb{K}\{y\}$ and is closed under transforming. A difference ideal $\mathbb{I}$ is called reflexive if for any difference polynomial P, $\delta P \in \mathbb{I}$ implies $P \in \mathbb{I}$. Let $\mathbb{P}$ be a set of elements of $\mathbb{K}\{y\}$. The difference ideal generated by $\mathbb{P}$ is denoted by $[\mathbb{P}]$. Obviously, $[\mathbb{P}]$ is the set of all linear combinations of the difference polynomials in $\mathbb{P}$ and their transforms. The (ordinary or algebraic) ideal generated by $\mathbb{P}$ is denoted as $(\mathbb{P})$. A difference ideal $\mathbb{I}$ is called perfect if the presence in $\mathbb{I}$ of a product of powers of transforms of a difference polynomial P implies $P \in \mathbb{I}$. The perfect difference ideal generated by $\mathbb{P}$ is denoted as $\{\mathbb{P}\}$. A perfect ideal is always reflexive. A difference ideal $\mathbb{I}$ is called a prime ideal if for difference polynomials P and Q, $PQ \in \mathbb{I}$ implies $P \in \mathbb{I}$ or $Q \in \mathbb{I}$.

A difference polynomial $P \in \mathbb{K}\{y\} \setminus \mathbb{K}$ can be written as the following form:

$$P = a_d(z_0, z_1, \cdots, z_{m-1}) z_m^d + \cdots + a_0(z_0, z_1, \cdots, z_{m-1}) \in \mathbb{K}\{y\},$$

where $d = \deg(P, z_m) > 0$. The order of P is m. We denote by $\boldsymbol{I}_P$ the set of products of powers a_d and its transformations. For convenience, let $P_0 = P, P_i = \delta P_{i-1}$, $i = 1, 2, \cdots$. Then $(P_0, P_1, \cdots, P_k)$ is a triangular set when the z_i are considered as algebraic indeterminates.

Use the notation above. We denote by $\mathrm{sat}(P)$ the saturation ideal of P.

$$\mathrm{sat}(P) = [P] : \boldsymbol{I}_P.$$

We say that P is strong irreducible if $\deg(P, z_0) \neq 0$ and for any integer l, $(P, P_1, 2, \cdots, P_l)$ is an irreducible triangular set.

The following result proved in [15] gives the relation between prime ideals and strong irreducible polynomials.

Theorem 1 *If P is strong irreducible, then* $\mathrm{sat}(P)$ *is a reflexive prime ideal.*

The following example shows that for an irreducible polynomial P, P is not necessarily strong irreducible.

Example 1 Let $\mathbb{K} = \mathbb{Q}$, $P = z_1^2 + z_0^2 + 1$. Then P is irreducible in $\mathbb{K}\{y\}$. Moreover, as an algebraic polynomial in $\mathbb{Q}[z_0, z_1]$, it is irreducible over the complex field (absolutely irreducible). But, $\mathrm{sat}(P)$ is not prime, since $P_1 - P = (z_2 - z_0)(z_2 + z_0)$.

An open problem in difference algebra is how to decide whether a difference polynomial is strong irreducible.

A natural way to solve the above problem is to ask: whether we can find an l such that if $(P_0, P_1, 2, \cdots, P_l)$ is an irreducible triangular set, then P is strong irreducible. The following example shows that it is impossible to find such an l which only depends on the order and degree of P.

Example 2 Let $F = \mathbb{Q}(x)$ be the field of rational functions and $\delta x = x + 1$. Let $P = z^4 - 4xz^2 - 2kz^2 + k^2$ be a polynomial with order 0 and degree 4. We will show that for any $i < k$, $P_0 = P, P_1, 2, \cdots, P_i$ is an irreducible triangular set and $P_0, P_1, 2, \cdots, P_k$ is reducible.

From [14], $\sqrt{x}, \sqrt{x+1}, \sqrt{x+2}, \cdots$ is successive quadratic extension of F. In other words, if we denote by $K_i = F(\sqrt{x}, \sqrt{x+1}, \cdots, \sqrt{x+i})$, then $[K_i : K_{i-1}] = 2$ for $i = 1, 2, \cdots$. By computing the resolvent[17], we can show that $\sqrt{x} + \sqrt{x+k}$ is the primitive element of $\sqrt{x}$

and $\sqrt{x+k}$ for each $k = 1, 2, \cdots$. Then a generic zero of P is $\sqrt{x}+\sqrt{x+k}$. And a generic zero of $P_1 = \delta(P)$ is $\sqrt{x+1}+\sqrt{x+k+1}$, and so on. Let $\theta_i = \sqrt{x+i}+\sqrt{x+k+i}, i = 0, 1, 2, \cdots$.

By theorem 3 of page 4 in [14], we have

$$\begin{aligned}[F(\theta_i) : F] &\geq [F(\theta_i, \sqrt{x}, \sqrt{x+1}, \cdots, \sqrt{x+i-1}) : K_{i-1}] \\ &= [K_i : K_{i-1}][F(\sqrt{x+i}, \sqrt{x+k+i}, \sqrt{x}, \sqrt{x+1}, \cdots, \sqrt{x+i-1}) : K_i] \\ &\geq 2[K_{i+k} : K_{i+k-1}] = 4,\end{aligned}$$

hence $[F(\theta_i) : F] = 4$. Similarly, we can show that $[F(\theta_0, \theta_1, \cdots, \theta_i) : F] = 4^{i+1}$ for $i < k$, hence $F(\theta_0, \theta_1, \cdots, \theta_i)$ is a quartic extension of $F(\theta_0, \theta_1, \cdots, \theta_{i-1})$ for $i < k$. As a consequence, $P_0, P_1, \cdots, P_i$ form an irreducible triangular set for $i < k$. Since $[F(\theta_0, \theta_1, \cdots, \theta_k) : F(\theta_0, \theta_1, \cdots, \theta_{k-1})] = [K_{i+k} : K_{x+2k-1}] = 2$, we know that P_k can be factored modulo the algebraic prime ideal $\mathrm{asat}(P_0, P_1, \cdots, P_{k-1})$, which is

$$P_k = -\frac{z_0^2 - 4x - 2k}{k^2}((z_0 z_k^2 + k z_k + z_0^2 z_k - k z_0) * (z_0 z_k^2 - z_0^2 z_k - k z_k - k z_0) - z_k^2 P).$$

The following theorem gives a simple criterion to decide whether P is strong irreducible.

Theorem 2 *Let $P = P(z_0, z_1, \cdots, z_m), m \geq 1$ be an irreducible difference polynomial in $\mathbb{K}\{y\}$, $\deg(P, z_m) = d, \deg(P, z_0) = s \neq 0$ and $\mathrm{GCD}(s, d) = 1$. Then $\mathrm{sat}(P)$ is a reflexive prime ideal.*

Proof By Theorem 1, we know that if P is strong irreducible, then $\mathrm{sat}(P)$ is a reflexive prime ideal. Thus, all we need to show is that $(P_0, P_1, \cdots, P_n)$ is an irreducible triangular set for any $n \in \mathbb{N}$.

We will prove a stronger conclusion that $(P_0, P_1, \cdots, P_n)$ is an irreducible triangular set under the variable ordering $z_0 < z_1 < \cdots < z_{m+n}$ and $(P_n, P_{n-1}, \cdots, P_0)$ is an irreducible triangular set under the variable ordering $z_{m+n} < z_{m+n-1} < \cdots < z_0$. When we use the notation $(P_n, P_{n-1}, \cdots, P_0)$, we always assume that the ordering of the variables is $z_{m+n} < z_{m+n-1} < \cdots < z_0$.

We will prove that by induction on n. For $n = 0$, the conclusion is true since P is irreducible. Assume that the conclusion is true for $n = k > 0$. Then, we need to prove the following results:

1) P_{k+1} is irreducible modulo the irreducible triangular set $(P_0, P_1, \cdots, P_k)$, or equivalently, the algebraic prime ideal $\mathrm{asat}(P_0, P_1, \cdots, P_k)$.

2) P_0 is irreducible modulo the irreducible triangular set $(P_{k+1}, P_k \cdots, P_1)$, or equivalently, the algebraic prime ideal $\mathrm{asat}(P_{k+1}, P_k \cdots, P_1)$.

Let $\alpha = (\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m+k})$ be a generic zero of $\mathrm{asat}(P_0, P_1, \cdots, P_k)$. By [15], for any polynomial $R(z_{k+1}, \cdots, z_{m+k})$, R is invertible w.r.t. $(P_0, P_1, \cdots, P_k)$. Then $\alpha_{k+1}, \cdots, \alpha_{m+k}$ form a transcendental basis of the generic zero α. Now, we can treat $(z_{k+1}, \cdots, z_{m+k})$ as the parameters of the triangular set. By the assumption, we know that $\widetilde{P} = (P_k, P_{k-1}, \cdots, P_0)$ is also an irreducible triangular set. Then, $\deg(P_{k+1}, z_{m+k+1}) = d$ and by Lemma 5, $\mathbb{K}(\alpha)$ can be treated as an extension of $\mathbb{K}(\alpha_{k+1}, \cdots, \alpha_{m+k})$ with extension degree s^{k+1}. Since $\mathrm{GCD}(d, s) = 1$, $\mathrm{GCD}(d, s^{k+1}) = 1$, by Lemma 3, P_{k+1} is irreducible modulo $\widetilde{P}$, or equivalently, $\mathrm{asat}(\widetilde{P})$.

Now, in order to prove (1), we need to show $\mathrm{asat}(\widetilde{P}) = \mathrm{asat}(P_0, P_1, \cdots, P_k)$. Since $(P_0, P_1, \cdots, P_k)$ and $\widetilde{P}$ are both irreducible triangular sets, by Lemma 4.1 of [15], the initial product of $\widetilde{P}$ is invertible w.r.t. the irreducible set $(P_0, P_1, \cdots, P_k)$, we know that $\mathrm{asat}(\widetilde{P}) \subseteq \mathrm{asat}(P_0, P_1, \cdots, P_k)$. Since both of the ideals are prime with the same dimension, $\mathrm{asat}(P_0, P_1,$

$\cdots, P_k) = \text{asat}(\widetilde{P})$. Now, we have proved conclusion (1) that P_{k+1} is irreducible modulo $\text{asat}(P_0, P_1, \cdots, P_k)$.

Since $(P_k, P_{k-1} \cdots, P_0)$ is an irreducible triangular set by the assumption, and δ is an isomorphism, we know that $(P_{k+1}, P_k \ \cdots, P_1)$ is also an irreducible triangular set under the ordering $z_{m+k+1} < z_{m+k} < \cdots < z_1$.

Similarly, for conclusion (2), since $\text{asat}(P_{k+1}, P_k \cdots, P_1) = \text{asat}(P_1, 2, \cdots, P_{k+1})$. Let $\beta = (\beta_1, \beta_2, \cdots, \beta_{m+k+1})$ be a generic zero of $\text{asat}(P_1, P_2, \cdots, P_{k+1})$. We can treat $\beta_1, \beta_2, \cdots, \beta_m$ as the transcendental basis of β. The field extension degree is $[\mathbb{K}(\beta) : \mathbb{K}(\beta_1, \beta_2, \cdots, \beta_m)] = d^{k+1}$. Since $\deg(P_0, z_0) = s$, $\text{GCD}(d^{k+1}, s) = 1$, by Lemma 3, P_0 is irreducible modulo the irreducible triangular set $(P_{k+1}, P_k \cdots, P_1)$. ∎

Using this criterion, we can easily decide whether the saturation ideal of certain difference polynomial P is prime.

Example 3 Let $\mathbb{K} = \mathbb{Q}\{u\}$, $P = u^3 z_1^3 + u_1^3 z_0^4$. It is easy to decide that P is irreducible over $\mathbb{Q}\{u\}$, since $\deg(P, z_1) = 3$ and $\deg(P, z_0) = 4$. By Theorem 2, we know that $\text{sat}(P)$ is a reflexive prime difference ideal.

4 Strong Irreducibility of Difference Triangular Set

Now, we are ready to give a more general result about the strong irreducibility of a difference ascending chain.

Let $y_1, y_2, \cdots, y_n$ be indeterminates. Then $\mathbb{R} = \mathbb{K}\{y_1, y_2, \cdots, y_n\}$ is called an n-fold polynomial difference ring over $\mathbb{K}$. Any difference polynomial P in the ring $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$ is an ordinary polynomial in variables $\delta^k y_j (k = 0, 1, 2, \cdots, \ j = 1, 2, \cdots, n)$. For convenience, we also denote $\delta^k y_j$ by $y_{j,k}$.

Let $P \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$. The class of P, denoted by $\text{cls}(P)$, is the least p such that $P \in \mathbb{K}\{y_1, y_2, \cdots, y_p\}$. If $P \in \mathbb{K}$, we set $\text{cls}(P) = 0$. The order of P w.r.t. y_i, denoted by $\text{ord}(P, y_i)$, is the largest j such that $y_{i,j}$ appears in P. When y_i does not occur in P, we set $\text{ord}(P, y_i) = 0$. If $\text{cls}(P) = p$ and $\text{ord}(P, y_p) = q$, we called y_p the leading variable and $y_{p,q}$ the lead of P, denoted as $\text{lvar}(P)$ and $\text{ld}(P)$, respectively. The leading coefficient of P as a univariate polynomial in $\text{ld}(P)$ is called the initial of P, and is denoted as $\text{I}(P)$ or I_P.

A difference polynomial P_1 has higher rank than a difference polynomial P_2, denoted as $P_1 >_{\text{rank}} P_2$, if

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

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

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

Let P_1 and P_2 be two polynomials and $\text{ld}(f_1) = x_{c,o}$. P_2 is said to be reduced w.r.t. P_1 if $\deg(P_2, x_{c,o+i}) < \deg(P_1, x_{c,o)})$ for any nonnegative integer i.

A finite sequence of nonzero r-pols $\mathcal{A} = A_1, A_2, \cdots, A_p$ is called an ascending chain, or simply a chain, if one of the two following conditions holds:

i) $p = 1$ and $A_1 \neq 0$, or

ii) $\text{cls}(A_1) > 0$, $A_i \prec A_j$, and A_j is reduced w.r.t. A_i for $1 \leq i < j \leq p$.

$\mathcal{A}$ is called trivial if $\text{cls}(A_1) = 0$.

Let $\mathcal{A}$ be a chain and $\mathbb{I}_{\mathcal{A}}$ the set of all products of powers of the initials and their transforms of the polynomials in $\mathcal{A}$. The saturation ideal of $\mathcal{A}$ is defined as follows

$$\text{sat}(\mathcal{A}) = \{f \in \mathbb{K}\{x_1, x_2, \cdots, x_n\} \mid \exists g \in \mathbb{I}_{\mathcal{A}}, \text{ s.t. } gf \in [\mathcal{A}]\}.$$

The concept of coherent and strong irreducible chain is introduced in [15], which has the following property.

Theorem 3 *Let $\mathcal{A}$ be a coherent and strong irreducible chain. Then* $\mathrm{sat}(A)$ *is a reflexive prime ideal.*

Let $\mathcal{A} = P^{(1)}, P^{(2)}, \cdots, P^{(n)}$ be an irreducible triangular set, and $P^{(i)} \in \mathbb{K}\{y_i\}, 1 \leq i \leq n$. The order of $P^{(1)}, P^{(2)}, \cdots, P^{(n)}$ are $p_i > 0, 1 \leq i \leq n$, respectively. Let $d_i = \deg(P^{(i)}, \delta^{p_i} y_i), 1 \leq i \leq n$, $s_i = \deg(P^{(i)}, y_i)$, $1 \leq i \leq n$. For convenience, let $P_j^{(i)} = \delta^j P^{(i)}, 1 \leq i \leq n$.

Using the above notations, we have the following theorem.

Theorem 4 *If $s_i \neq 0, 1 \leq i \leq n$, and there exist $m_i \in \{d_i, s_i\}, 1 \leq i \leq n$, such that $m_0 = 1, m_1, m_2, \cdots, m_{k-1}, d_k, s_k$ are pairwise coprime for $k = 1, 2, \cdots, n$, then* $\mathrm{sat}(\mathcal{A})$ *is a reflexive prime ideal.*

Proof We prove that by induction on n. When $n = 1$, the conclusion is true by Theorem 2. Moreover, by Lemma 4, when we consider the irreducibility of polynomials over an extension field, we can ignore the transcendental extension. By the proof of Theorem 2 we can treat the related field extension as a successive extension of degree m_1. Assume that the conclusion is true for $n = k > 1$, then we need to show that it is true when $n = k + 1$.

Since there exist $m_i \in \{d_i, s_i\}, 1 \leq i \leq k$, such that they are coprime for each other. Then, we consider the following extension of the triangular set:

$$\begin{aligned} P_0^{(1)} &= P^{(1)}, P_1^{(1)}, \cdots, P_{r_1}^{(1)}, \\ P_0^{(2)} &= P^{(2)}, P_1^{(2)}, \cdots, P_{r_2}^{(2)}, \\ &\vdots \\ P_0^{(k)} &= P^{(k)}, P_1^{(k)}, \cdots, P_{r_k}^{(k)}, \\ P_0^{(k+1)} &= P^{(k+1)}, P_1^{(k+1)}, \cdots, P_{r_{k+1}}^{(k+1)}. \end{aligned} \tag{2}$$

We denote by $\mathcal{A}_t$ the extended triangular set of the first t rows in (2). Then, we select a suitable variable ordering according to the selection of $m_i \in \{d_i, s_i\}$, more precisely, the ordering of $\mathcal{A}_k$ can be explained as follows, if $m_i = d_i$, we do not change the natural ordering of $\mathcal{A}_k$, if $m_i = s_i$, we change the part of variable ordering of y_i as $\delta^{l+1} y_i < \delta^l y_i$ for $l \geq 0$. Similar to the proof of Theorem 2, $\mathcal{A}_k$ can still form an irreducible triangular set. By Lemma 5, we can treat the extension field of the above irreducible triangular set $\mathcal{A}_k$ as an algebraic extension with the degree $q_k = \prod_{i=1}^{k} m_i^{r_i+1}$. Then, according to the definition of strong irreducible chain, we need to show that $(P_0^{(k+1)} = P^{(k+1)}, P_1^{(k+1)}, \cdots, P_{r_{k+1}}^{(k+1)})$ is irreducible modulo the irreducible triangular set $\mathcal{A}_k$. We can prove that by induction on r_{k+1}.

When $r_{k+1} = 0$, by Lemma 4, the conclusion is true since $\mathrm{GCD}(q_k, d_{k+1}) = \mathrm{GCD}(q_k, s_{k+1}) = 1$. Assume the conclusion is also true for $r_{k+1} = t$. Similar to the proof of Theorem 2, we can treat $(\mathcal{A}_k, P^{(k+1)}, P_1^{(k+1)}, \cdots, P_t^{(k+1)})$ as an irreducible triangular set under the natural ordering and $(\mathcal{A}_k, P_t^{(k+1)}, \cdots, P_1^{(k+1)}, P^{(k+1)})$ as an irreducible triangular set under the variable ordering $y_1 < y_{1,1} < \cdots < y_2 < \cdots < y_k < \cdots < y_{k+1,s+t} < \cdots < y_{k+1,0}$, where $s = \mathrm{ord}(P^{(k+1)}, y_{k+1})$. Then, by treating the transcendental variables as parameters, the field extension of the irreducible triangular sets are algebraic extension with degree $q_k * d_{k+1}^{t+1}$ and $q_k * s_{k+1}^{t+1}$, respectively. Since $\mathrm{GCD}(d_{k+1}, q_k * s_{k+1}^{t+1}) = 1$ and $\mathrm{GCD}(s_{k+1}, q_k * d_{k+1}^{t+1}) = 1$, by Lemma 4, we know that $(\mathcal{A}_k, P^{(k+1)}, P_1^{(k+1)}, \cdots, P_{t+1}^{(k+1)})$ and $(\mathcal{A}_k, P_{t+1}^{(k+1)}, \cdots, P_1^{(k+1)}, P^{(k+1)})$ are irreducible triangular sets. Then, we know that $\mathcal{A}_{k+1}$ is an algebraic triangular set. Moreover, we can treat the extension of $\mathcal{A}_{k+1}$ as an algebraic extension of degree $q_k * d_{k+1}^{r_{k+1}+1}$ or $q_k * s_{k+1}^{r_{k+1}+1}$.

Hence, we have proved that $(P^{(1)}, P^{(2)}, \cdots, P^{(n)})$ is a strong irreducible triangular set. Then, $\mathrm{sat}(P^{(1)}, P^{(2)}, \cdots, P^{(n)})$ is a reflexive prime ideal by Theorem 3. ∎

The following corollary is obviously true by the above proof.

Corollary 1 *Let $\mathcal{A}$ be a difference triangular set of the following form:*

$$\mathcal{A} = \begin{cases} A_{1,1}, A_{1,2}, \cdots, A_{1,p_1}, \\ A_{2,1}, A_{2,2}, \cdots, A_{2,p_2}, \\ \qquad\qquad \vdots \\ A_{m,1}, A_{m,2}, \cdots, A_{m,p_m}. \end{cases} \tag{3}$$

The leading variables of the polynomial in each row are $y_i, 1 \leq i \leq m$.

Let $D = \deg(\mathcal{A})$. Let P be an irreducible polynomial in a new indeterminate z with order o. Let $d = \deg(P, z_o), s = \deg(P, z) \neq 0$. If $\mathcal{A}$ is a coherent and strong irreducible triangular set and D, d, s are pair wise coprime, then $\mathcal{A} \cup \{P\}$ is also a coherent and strong irreducible triangular set.

5 Conclusion

Deciding whether a difference ideal is prime is an open problem in difference algebra. Using the notations and results presented in [15, 18], this problem can be reduced to deciding whether a difference ascending chain is strong irreducible. In this paper, we give criteria to decide whether certain difference ascending chains are strong irreducible, and hence give criteria to test whether certain difference ideals are prime. It is still an interesting and open problem to decide whether a general difference chain is strong irreducible.

Acknowledgment

We want to thank Ziming Li, Huaifu Wang, and Shaoshi Chen for their kindly help for the writing of Section 2.

References

[1] P. Aubry, D. Lazard, and M. M. Maza, On the theory of triangular sets, *Journal of Symbolic Computation*, 1999, **28**: 105–124.

[2] F. Boulier, D. Lazard, F. Ollivier, and M. Petitiot, *Representation for the Radical of a Finitely Generated Differential Ideal*, Proc. of ISSAC'95, 158–166, ACM Press, New York, 1995.

[3] D. Bouziane, A. Kandri Rody, and H. Maârouf, Unmixed-dimensional decomposition of a finitely generated perfect differential ideal, *Journal of Symbolic Computation*, 2001, **31**: 631–649.

[4] F. Chai, X. S. Gao, and C. M. Yuan, A characteristic set method for solving boolean equations and applications in cryptanalysis of stream ciphers, *Journal of Systems Science & Complexity*, 2008, **21**(2): 191–208.

[5] O. Golubitsky, M. Kondratieva, and A. Ovchinnikov, Algebraic transformation of differential characteristic decompositions from one ranking to another, *Journal of Symbolic Computation*, 2009, **44**(4): 333–357.

[6] É. Hubert, Factorization-free decomposition algorithms in differential algebra, *Journal of Symbolic Computation*, 2000, **29**: 641–662.

[7] M. V. Kondratieva, A. B. Levin, A. V. Mikhalev, and E. V. Pankratiev, *Differential and Difference Dimension Polynomials*, Kluwer Academic Publishers, Dordrecht, 1999.

[8] J. F. Ritt, *Differential Algebra*, American Mathematical Society, Now York, 1950.

[9] D. Wang, *Elimination Methods*, Springer, Berlin, 2000.

[10] W. T. Wu, Basic principle of mechanical theorem proving in elementray geometries, *Journal of Automated Reasoning*, 1986, **2**: 221–252.

[11] W. T. Wu, On the foundation of algebraic differential polynomial geometry, *Sys. Sci. & Math. Sci.*, 1989, **2**(4): 289–312.
[12] L. Yang, J. Z. Zhang, and X. R. Hou, *Non-linear Algebraic Equations and Automated Theorem Proving* (in Chinese), ShangHai Science and Education Pub., Shanghai, 1996.
[13] J. F. Ritt and J. L. Doob, Systems of algebraic difference equations, *American Journal of Mathematics*, 1933, **55**: 505–514.
[14] R. M. Cohn, *Difference Algebra*, Interscience Publishers, New Brunswick, 1965.
[15] X. S. Gao, Y. Luo, and C. M. Yuan, A characteristic set method for difference polynomial systems, *Journal of Symbolic Computation*, 2009, **44**(3): 242–260.
[16] X. S. Gao, J. Van der Hoeven, C. M. Yuan, and G. Zhang, Characteristic set method for differential–difference polynomial systems, *Journal of Symbolic Computation*, 2009, **44**(9): 1137–1163.
[17] X. S. Gao and C. M. Yuan, *Resolvent Systems of Difference Polynomial Ideals*, in *Proc. ISSAC*, 2006, 101–108, ACM Press, New York.
[18] X. S. Gao, C. M. Yuan, and G. Zhang, Ritt-Wu's characteristic set method for ordinary difference polynomial systems with arbitrary ordering, *Acta Mathematica Scientia*, 2009, **29**(3/4): 1063–1080.
[19] W. T. Wu, *Mathematics Machenization*, Science Press/Kluwer, Beijing, 2001.