MM Research Preprints, 248–263
KLMM, AMSS, Academia Sinica
Vol. 25, December 2006

Decomposition of Ordinary Difference Polynomials

Mingbo Zhang[1] and Xiao-Shan Gao
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS
Academia Sinica, Beijing 100080, China
mbzhang@ustc.edu.cn, xgao@mmrc.iss.ac.cn

Abstract.
In this paper, we present an algorithm to decompose nonlinear difference polynomials in one variable and with coefficients in a computable difference field $\mathcal{K}$. The algorithm provides an effective reduction of the decomposition of difference polynomials to the factorization of linear difference operators over the same field. The algorithm is implemented in Maple for the constant coefficient case. The program can be used to decompose difference polynomials with thousands of terms effectively.

Keywords. Difference polynomial, decomposition, difference degree.

1. Introduction

Functional decompositions for algebraic polynomials have been studied in detail and there have been many theoretical and algorithmic results [13, 1, 10]. In the 1950's, Ritt and his students established the differential algebra [9] and the difference algebra [4] to deal with the differential and difference equations from the algebraic viewpoint. Naturally, the decomposition of the differential polynomials and difference polynomials becomes a problem worth studying. In [5, 11, 12], partial results were given to decompose differential polynomials. In [6], a complete decomposition algorithm for nonlinear differential polynomials was given. In this paper, we will give an algorithm to decompose difference polynomials.

Our algorithm consists of three steps. First, the problem of decomposing a general difference polynomial is reduced to the problem of decomposing a homogeneous one, which will be introduced in Section 5. Second, the decomposition of a homogeneous difference polynomial is reduced to the construction of the linear left decomposition factors of another homogenous difference polynomial, which will be introduced in Section 4. Finally, construction of linear left decomposition factors of a homogenous difference polynomial is reduce to the factorization of difference operators, which will be introduced in Section 3. Algorithms for factoring difference operators can be found in [2, 3, 7]. The algorithm is implemented in Maple for the constant coefficient case. Extensive experiments show that the program can be used to decompose difference polynomials with thousands of terms effectively. These experimental results are given in Section 6. We will conclude the paper in Section 7.

[1] Department of Mathematics, University of Science and Technology of China.

2. Notations and Preliminary Results

Let $\mathcal{K}$ be a difference field with a difference transform operator δ, y a difference indeterminate, $\mathcal{K}\{y\}$ the ordinary difference polynomial ring over $\mathcal{K}$ [4]. An element in $\mathcal{K}\{y\}$ is called a difference polynomial. We denote by $y_i = \delta^i y$ the i-th transform of y. Let $f \in \mathcal{K}\{y\} \setminus \mathcal{K}$ be a univariate difference polynomial. The largest i such that y_i appearing in f is called the *order* of f, denoted by o_f. We can write f as the form

$$f = F_d y_{o_f}^d + F_{d-1} y_{o_f}^{d-1} + \cdots + F_0$$

where F_i is an algebraic polynomial of $y, y_1, y_2, \ldots, y_{o_f - 1}$ and $F_d \neq 0$. We call $d_f \triangleq d$ the *degree* of f, $i_f \triangleq F_d$ the *initial* of f, and $y_{o_f}^d$ the *leader* of f respectively. We can also write f as

$$f = \sum a_{i_0 i_1 \cdots i_{o_f}} y^{i_0} y_1^{i_1} \cdots y_{o_f}^{i_{o_f}}$$

where each $a_{i_0 i_1 \cdots i_{o_f}} \in \mathcal{K}$. We call $a_{i_0 i_1 \cdots i_{o_f}} y^{i_0} y_1^{i_1} \cdots y_{o_f}^{i_{o_f}}$ a *term* of f.

$$\max\{i_0 + i_1 + \cdots + i_{o_f} \mid a_{i_0 i_1 \cdots i_{o_f}} \neq 0\}$$

is called the *total degree* of f, which is denoted by $\mathrm{tdeg}(f)$.

$$\max\{i_1 + 2i_2 + \cdots + o_f i_{o_f} \mid a_{i_0 i_1 \cdots i_{o_f}} \neq 0\}$$

is called the *difference degree* of f and denoted by $\mathrm{ddeg}(f)$.

If all the total degrees of the terms in f are the same, f is called *homogeneous*; furthermore, if all the difference degrees of the terms in f are equal, we call f *difference homogeneous.* In particular, if f is homogeneous and its total degree equals one, f is called *linear.*

We usually define a rank between two terms according to the pure lexicographical order induced by the variable order $y < y_1 < y_2 < \ldots$. In a difference polynomial f, the term with the highest rank is called the *leading term* of f.

Let $g, h \in \mathcal{K}\{y\}$. We use $g \circ h$ to denote the *composition* of g and h, which is defined by substituting y_i in g with the i-th transform of $h (0 \leq i \leq o_g)$. If $f = g \circ h$, g, h are called the *left* and *right decomposition factors* of f respectively. A *decomposition* $f = g \circ h$ is called *nontrivial*, if both g and h are not of the form $ay + b$, where a and b are in $\mathcal{K}$. Two decompositions $f = g_1 \circ h_1$ and $f = g_2 \circ h_2$ are called equivalent if there exist $a, b \in \mathcal{K}$ such that $h_1 = (ay + b) \circ h_2$. A decomposition $f = p_1 \circ p_2 \cdots \circ p_n$ is called a *maximal decomposition* of f, if there is no nontrivial decomposition for each p_i. In this paper, we only consider how to compute the decomposition of length two and we are always interested in the nontrivial and nonequivalent decompositions. Let us see two examples of decompositions of difference polynomials.

Example 2.1 $y_2 + 3y_1 + 2y = (y_1 + y) \circ (y_1 + 2y)$ *is a decomposition of a linear difference polynomial over the constant field* $\mathbb{Q}$*. It's correspondent to the factorization of the difference operator* $\delta^2 + 3\delta + 2 = (\delta + 1) \cdot (\delta + 2)$.

Example 2.2 $(t + 1) y_1 y_2^3 y_3^2 + t y y_1^3 y_2^2 = ((t + 1) y_1 y_2 + t y y_1) \circ y y_1^2$ *is a decomposition over the field* $\mathbb{Q}(t)$.

Lemma 2.3 *The composition operation is associate:* $f \circ (g \circ h) = (f \circ g) \circ h$.

Proof. Let $f = \sum_J f_J y^{j_0} y_1^{j_1} \dots y_{o_f}^{j_{o_f}}, g = \sum_I g_I y^{i_0} y_1^{i_1} \dots y_{o_g}^{i_{o_g}}$ where I and J are in two index sets and f_J, g_I are in $\mathcal{K}$. For any difference polynomial q, denote the i-th transform of q by $q_{(i)}$. Then we have

$$\begin{aligned}(y_1 \circ g) \circ h &= \left(\sum_I g_{I_{(1)}} y_1^{i_0} y_2^{i_1} \cdots y_{o_g+1}^{i_{o_g}} \right) \circ h \\ &= \sum_I g_{I_{(1)}} h_{(1)}^{i_0} h_{(2)}^{i_1} \dots h_{(o_g+1)}^{i_{o_g}} \\ &= y_1 \circ \left(\sum_I g_I h^{i_0} h_{(1)}^{i_1} \dots h_{(o_g)}^{i_{o_g}} \right) = y_1 \circ (g \circ h)\end{aligned}$$

By induction, we have $(y_k \circ g) \circ h = y_k \circ (g \circ h)$ for any positive integer k, so:

$$\begin{aligned}(f \circ g) \circ h &= \left(\sum_J f_J g^{j_0} (y_1 \circ g)^{j_1} \dots (y_{o_f} \circ g)^{j_{o_f}} \right) \circ h \\ &= \sum_J f_J \Big(g \circ h \Big)^{j_0} \Big((y_1 \circ g) \circ h \Big)^{j_1} \dots \Big((y_{o_f} \circ g) \circ h \Big)^{j_{o_f}} \\ &= \sum_J f_J \Big(g \circ h \Big)^{j_0} \Big(y_1 \circ (g \circ h) \Big)^{j_1} \dots \Big(y_{o_f} \circ (g \circ h) \Big)^{j_{o_f}} \\ &= \left(\sum_J f_J y^{j_0} y_1^{j_1} \dots y_{o_f}^{j_{o_f}} \right) \circ (g \circ h) = f \circ (g \circ h). \quad ▮\end{aligned}$$

By Lemma 2.3, for any $c \in \mathcal{K}$, we have $f = g \circ h = \Big(g \circ (y + c) \Big) \circ \Big((y - c) \circ h \Big)$. So we can assume that h has no term in $\mathcal{K}$. In this case, the term of f in $\mathcal{K}$ is equal to that of g. So in this paper, we always assume that f, g and h *have no term in* $\mathcal{K}$.

Lemma 2.4 *If* $f = g \circ h$ *is a decomposition of* f, *then:* $o_f = o_g + o_h$, $d_f = d_g \cdot d_h$ *and* $i_f = (i_g \circ h) \cdot (i_h)_{(o_g)}^{d_g}$.

Proof. Let

$$f = i_f y_{o_f}^{d_f} + u_f, \quad g = i_g y_{o_g}^{d_g} + u_g, \quad h = i_h y_{o_h}^{d_h} + u_h$$

where u_f, u_g and u_h are difference polynomials. Substituting g and h into $f = g \circ h$, we have

$$f = (i_g \circ h) \cdot h_{(o_g)}^{d_g} + u_g \circ h = (i_g \circ h) \cdot (i_h)_{(o_g)}^{d_g} y_{o_h+o_g}^{d_g \cdot d_h} + v$$

where v is a difference polynomial with rank lower than $y_{o_f}^{d_f}$. By comparing the order, degree and initial of both sides of the equation, we obtain the result. ▮

In this paper, we will show how to find a nontrivial decomposition $f = g \circ h$ for a given difference polynomial f. After obtaining the right decomposition factor of f, we can compute the corresponding left decomposition factor easily. One possible way is to estimate the total degree and the order of g and then find the coefficients of g by solving a linear equation system. The following algorithm gives a more direct solution to this problem.

Algorithm 2.5 *Input: difference polynomials f and h.*
Output: a difference polynomial g such that $f = g \circ h$ if such a g exists.

S1 If $f = 0$, then return $g = 0$. Let $o_g = o_f - o_h$, $d_g = d_f/d_h$. By Lemma 2.4, if $o_g < 0$ or d_g is not an integer, g does not exist and the algorithm terminates.

S2 Suppose that $g = i_g y_{o_g}^{d_g} + u_g$. We will find i_g and u_g separately.

S3 By Lemma 2.4, $i_g \circ h = i_f/(i_h)_{(o_g)}^{d_g}$. If $q = i_f/(i_h)_{(o_g)}^{d_g}$ is not a difference polynomial, g does not exist and the algorithm terminates. Otherwise, call Algorithm 2.5 with q and h as input and i_g as output. If i_g does not exist, g does not exist and the algorithm terminates.

S4 Let $f_1 = f - (i_g y_{o_g}^{d_g}) \circ h$, then $f_1 = u_g \circ h$. Call Algorithm 2.5 with f_1 and h as input and u_g as output. If u_g exists, output $i_g y_{o_g}^{d_g} + u_g$; otherwise g does not exist.

In the rest of this paper, we will concentrate on computing the right decomposition factor of the given difference polynomial.

3. Linear Left Decomposition Factor

In this section, we will solve the following problem: *for a homogeneous difference polynomial f, compute a decomposition $f = g \circ h$ such that g is linear.* Therefore, in the rest of this section, we will assume that f and h are homogeneous and g is linear.

Proposition 3.1 *If* $\mathrm{ddeg}(f) < \mathrm{tdeg}(f)$*, then f has no nontrivial decomposition $f = g \circ h$ such that g is linear.*

Proof: If such a decomposition exists, then by $\mathrm{ddeg}(f) < \mathrm{tdeg}(f)$, y must appear in each term of f: otherwise, if $a_I y_1^{i_1} \cdots y_m^{i_m}$ is a term of f, then $\mathrm{ddeg}(f) \geq i_1 + \cdots + m \cdot i_m \geq i_1 + \cdots + i_m = \mathrm{tdeg}(f)$. But for a non-trivial decomposition $f = g \circ h$, we have $o_g > 0$ and $g \circ h$ must contain a term which does not involve y, a contradiction. ▮

Let $a = \mathrm{ddeg}(f), \alpha = \mathrm{tdeg}(f)$ and write f as the sum of difference homogeneous parts:

$$f = F_a + F_{a-1} + \cdots + F_0$$

where F_j is the sum of terms included in f with difference degree j $(0 \leq j \leq a)$. Let $k = a \ mod \ \alpha$ and $a = t \cdot \alpha + k$. By Proposition 3.1 we have $t \geq 1$. Let

$$L_i = F_{a-i} z_t + F_{a-\alpha-i} z_{t-1} + \cdots + F_{a-t\alpha-i} z \ (0 \leq i \leq k) \tag{1}$$

Then L_i is a linear difference polynomial over the difference ring $\mathcal{K}\{y\}$.

Lemma 3.2 *A linear difference polynomial g is a left decomposition factor of f if and only if g is a left decomposition factor of each $L_i (0 \leq i \leq k)$ with coefficients in $\mathcal{K}$.*

Proof: ($\Longrightarrow$). Let $g = c_n z_n + \cdots + c_0 z$ be a linear left decomposition factor of f and $h = H_b + H_{b-1} + \cdots + H_1$ be the corresponding right decomposition factor, where $b = \mathrm{ddeg}(h)$ and H_l is the sum of the terms in the with difference degree $l (1 \le l \le b)$. Then

$$F_a + F_{a-1} + \cdots + F_1 = (c_n y_n + c_{n-1} y_{n-1} + \cdots + c_0 y) \circ (H_b + H_{b-1} + \cdots + H_1) \qquad (2)$$

By comparing the difference degrees of both sides of (2) we have $a = b + n\alpha$. For a fixed $0 \le i \le k$, by comparing the parts with difference degree $a - j\alpha - i = b - i + (n-j)\alpha$ $(0 \le j \le t)$ of both sides of (2), we have

$$F_{a-j\alpha-i} = c_n z_n \circ H_{b-i-j\alpha} + c_{n-1} z_{n-1} \circ H_{b-i-(j-1)\alpha} + \cdots + c_{n-j} z_{n-j} \circ H_{b-i}$$

While the coefficient of z_{t-j} in

$$(c_n z_n + \cdots + c_0 z) \circ (H_{b-i} z_{t-n} + H_{b-i-\alpha} z_{t-n-1} + \cdots + H_{b-i-(t-n)\alpha} z)$$

is equal to $c_n z_n \circ H_{b-i-j\alpha} + c_{n-1} z_{n-1} \circ H_{b-i-(j-1)\alpha} + \cdots + c_{n-j} z_{n-j} \circ H_{b-i} = F_{a-j\alpha-i}$. From (1), we have

$$L_i = (c_n z_n + \cdots + c_0 z) \circ (H_{b-i} z_{t-n} + H_{b-i-\alpha} z_{t-n-1} + \cdots + H_{b-i-(t-n)\alpha} z)$$

Namely, g is a left decomposition factor of L_i.

($\Longleftarrow$). If $g = c_n z_n + \cdots + c_0 z$ is a left decomposition factor of each L_i with coefficients over $\mathcal{K}$, let

$$F_{a-i} z_t + F_{a-\alpha-i} z_{t-1} + \cdots + F_{a-t\alpha-i} z = (c_n z_n + \cdots + c_0 z) \circ (K_{t,i} z_t + K_{t-1,i} z_{t-1} + \cdots + K_{0,i} z)$$

Substituting $z = 1$, we have

$$F_{a-i} + F_{a-\alpha-i} + \cdots + F_{a-t\alpha-i} = (c_n y_n + \cdots + c_0 y) \circ (K_{t,i} + K_{t-1,i} + \cdots + K_{0,i}) \qquad (3)$$

where z_i in $c_n z_n + \cdots + c_0 z$ can be replaced by y_i because z is only a variable name of the left decomposition factor. Summing the equation (3) for i from 0 to k, we have

$$F_a + F_{a-1} + \cdots + F_1 = (c_n y_n + c_{n-1} y_{n-1} + \cdots + c_0 y) \circ (\sum_{0 \le i \le k, 0 \le j \le t} K_{j,i})$$

So g is a linear left decomposition factor of f. ∎

By Lemma 3.2, to compute the linear left decomposition factor of f, we need only to compute the common left decomposition factor of the linear difference polynomials $L_i (0 \le i \le k)$. Note that L_i also involves the difference variable y. Substituting y with γ_i in

$$L_i(z) = (c_n z_n + \cdots + c_0 z) \circ (H_{b-i} z_{t-n} + H_{b-i-\alpha} z_{t-n-1} + \cdots + H_{b-i-(t-n)\alpha} z)$$

we have

$$\begin{aligned} L_i(\gamma_i) &= F_{a-i}(\gamma_i) z_t + F_{a-\alpha-i}(\gamma_i) z_{t-1} + \cdots + F_{a-t\alpha-i}(\gamma_i) z \\ &= (c_n z_n + \cdots + c_0 z) \circ (H_{b-i}(\gamma_i) z_{t-n} + \cdots + H_{b-(t-n)\alpha-i}(\gamma_i) z) \end{aligned}$$

So, if $f = g \circ h$ and g is linear, g must be the linear left decomposition factor of

$$L_i(\gamma_i) = F_{a-i}(\gamma_i)z_t + F_{a-\alpha-i}(\gamma_i)z_{t-1} + \cdots + F_{a-t\alpha-i}(\gamma_i)z$$

for i from 0 to k and any $\gamma_i \in \mathcal{K}$. From [4], we can always choose a $\gamma_i \in \mathcal{K}$ such that $L_i(\gamma_i) \neq 0$ for each i.

For any linear difference polynomial $q = a_m y_m + a_{m-1}y_{m-1} + \cdots + a_1 y_1 + a_0 y$, let $\tilde{q} = a_m\delta^m + a_{m-1}\delta^{m-1} + \cdots + a_1\delta + a_0$ be the corresponding difference operator over $\mathcal{K}$, then the decomposition $q = u \circ v$ of q is one-one correspondent to the factorization $\tilde{q} = \tilde{u} \cdot \tilde{v}$ of $\tilde{q}$. So the problem of finding g becomes the problem of factorization of difference operators over $\mathcal{K}$. If the difference operator δ is an automorphism over $\mathcal{K}$, we can compute the greatest common left divisor $\tilde{L}$ of $\tilde{L}_i(\gamma_i)(0 \le i \le k)$ by the left Euclidean remainder sequence [2] and then compute the left factors of $\tilde{L}$; otherwise, we can first compute all the factors of $\tilde{L}_0(\gamma_0)$ and then exclude those who are not the left factors of $\tilde{L}_i(\gamma_i)(1 \le i \le k)$.

Based on the above analysis, we give the following algorithm to solve the problem proposed in the beginning of this section.

Algorithm 3.3 *Input: a homogeneous difference polynomial f and a positive integer n.*
Output: a set S of all possible (g, h) such that $f = g \circ h$ is a nontrivial decomposition of f, $o_g = n$ and g is linear.

S1 $S := \{\}$. If y appears in every term of f, then return S.

S2 Let $\alpha = \mathrm{tdeg}(f), a = \mathrm{ddeg}(f), t = \lfloor \frac{a}{\alpha} \rfloor$. If $a < \alpha \cdot n$, g, h do not exist and the algorithm terminates. Otherwise, write f as the sum of the difference degree homogeneous parts: $f = F_a + F_{a-1} + \cdots + F_0$ and let $L_i = F_{a-i}z_t + F_{a-\alpha-i}z_{t-1} + \cdots + F_{a-t\alpha-i}z(0 \le i \le k)$.

S3 For each L_i, choose a $\gamma_i \in \mathcal{K}$ such that $L_i(\gamma_i) \neq 0(0 \le i \le k)$. Compute all the common left decomposition factors of $L_i(\gamma_i)$ with degree n. This is just a problem of factorization of difference operators and there have been some algorithms to deal with it [2, 3, 7].

S4 For each g obtained in S3 (which may contain parameters), check whether g is a left decomposition factor of f with Algorithm 3.4. If it is, compute the correspondent right decomposition factor h and add (g, h) to S. Return S.

Algorithm 3.4 *Input: a difference polynomial f and a linear difference polynomial g.*
Output: a difference polynomial h such that $f = g \circ h$ if such an h exists.

S1 Let $h := 0$.

S2 Since g is linear, by Lemma 2.4 we have $o_h = o_f - o_g$, $d_h = d_f$, $i_h = y_{-o_g} \circ (i_f/i_g)$. If i_h is not a difference polynomial, then h does not exist and the algorithm terminates.

S3 Let $h := h + i_h y_{o_h}^{d_h}$, $f := f - g \circ (i_h y_{o_h}^{d_h})$. If $f = 0$, output h; otherwise, go to S2.

In step S2, we use $y_{-o_g} \circ p$ to represent the following procedure. Let m be the minimal integer such that y_m appears in p and $p = \sum a_{i_m \cdots i_{o_f}} y_m^{i_m} \cdots y_{o_f}^{i_{o_f}}$. If $o_g > m$, $y_{-o_g} \circ p$ does not exist; otherwise $y_{-o_g} \circ p = \sum (\delta^{-o_g} a_{i_m \cdots i_{o_f}}) y_{m-o_g}^{i_m} \cdots y_{o_f - o_g}^{i_{o_f}}$.

Algorithm 3.4 is correct because g is linear and hence $g \circ (i_h y_{o_h}^{d_h} + u_h) = g \circ (i_h y_{o_h}^{d_h}) + g \circ u_h$.

Example 3.5 *$\mathcal{K}$ is the rational function field $\mathbb{Q}(t)$. The difference operator over $\mathcal{K}$ is defined by $\delta\ \theta(t) = \theta(t+1)$. Let $f = y_2y_3 + y_3^2 + y_2y_4 + yy_1 + y_1^2 + yy_2$ be a homogeneous difference polynomial over $\mathcal{K}$. We use algorithm 3.3 to compute its linear left decomposition factors of order 2.*

In S2, we have $\alpha = \mathrm{tdeg}(f) = 2$, $a = \mathrm{ddeg}(f) = 6$ and $f = F_6 + F_5 + \cdots + F_1 = (y_3^2 + y_2y_4) + (y_2y_3) + (yy_2 + y_1^2) + (yy_1)$. By lemma 3.2, if $g(y)$ is a linear left decomposition factor of f, $g(z)$ must be a linear left decomposition factor of $L_0 = (y_3^2 + y_2y_4)z_3 + (yy_2 + y_1^2)z_1$. In S3, if we choose $y = 1$, we have that $g(z)$ is a linear left decomposition factor of $L_0(1) = z_3 + z_1$. It is clear that $g(z) = z_2 + z_1$. If we choose $y = t$, then $L_0(t) = (2t^2 + 12t + 17)z_3 + (2t^2 + 4t + 1)z_1$. The only non-equivalent linear left decomposition factor of $L_0(t)$ with order 2 is $g(z) = z_2 + z_1$ ($L = (z_2 + z) \circ ((2t^2 + 4t + 1)z_1)$). In S4, we can check that that $g(y) = y_2 + y$ is really a linear left decomposition factor of f: $f = (y_2 + y) \circ (yy_2 + y_1^2 + yy_1)$.

Remark 3.6 *Some parameters may appear in the decomposition factors of linear difference polynomials, which take values in the constant field [2]. The number of the parameters are finite and satisfy some algebraic constraints. We can deal with these parameters as in the case of differential polynomials decomposition[6].*

Remark 3.7 *If $\mathcal{K}$ is a constant field, then computing the common left divisor of $L_i(\gamma_i)(0 \leq i \leq k)$ is equivalent to computing the GCD of $k+1$ algebraic polynomials over $\mathcal{K}$, which is completely similar to the differential case [5].*

4. Decomposition of homogeneous difference polynomials

In the previous section, we proposed an algorithm to compute a special decomposition of a given homogeneous difference polynomial, in which the left decomposition factor is linear. In this section, we will give an algorithm to give out all the decompositions(maybe expressed by parameters) of a homogeneous difference polynomial. This is also a special case for the general decomposition problem, but we will see its relation to the general case in section 5.

If $f = g \circ h$, we write f, g, h as

$$\begin{aligned} f &= f_{d_f} y_{o_f}^{d_f} + f_{d_f - 1} y_{o_f}^{d_f - 1} + \ldots + f_1 y_{o_f} + f_0 \\ g &= g_{d_g} y_{o_g}^{d_g} + g_{d_g - 1} y_{o_g}^{d_g - 1} + \ldots + g_1 y_{o_g} + g_0 \\ h &= h_{d_h} y_{o_h}^{d_h} + h_{d_h - 1} y_{o_h}^{d_h - 1} + \ldots + h_1 y_{o_h} + h_0 \end{aligned}$$

where d_f, d_g, d_h is the degree, o_f, o_g, o_h is the order of f, g, h respectively.

$$\begin{aligned} g \circ h = (g_{d_g} \circ h) \cdot [(y_{o_g} \circ h_{d_h}) y_{o_g + o_h}^{d_h} + \cdots + y_{o_g} \circ h_0]^{d_g} + (g_{d_g - 1} \circ h) \cdot \\ [(y_{o_g} \circ h_{d_h}) y_{o_g + o_h}^{d_h} + \cdots + y_{o_g} \circ h_0]^{d_g - 1} + \cdots + g_0 \circ h \end{aligned}$$

Comparing the coefficients of $y_{o_f}^i (d_f \geq i \geq d_f - d_h - 1)$ of both sides of $f = g \circ h$ we have:

$$(E1)\begin{cases} f_{d_f} = (g_{d_g} \circ h) \cdot y_{o_g} \circ h_{d_h}^{d_g} \\ f_{d_f-1} = (g_{d_g} \circ h) \cdot y_{o_g} \circ [d_g h_{d_h}^{d_g-1} h_{d_h-1}] \\ \vdots \\ f_{d_f-i} = (g_{d_g} \circ h) \cdot y_{o_g} \circ [d_g h_{d_h}^{d_g-1} h_{d_h-i} + T_i] \\ \vdots \\ f_{d_f-d_h} = (g_{d_g} \circ h) \cdot y_{o_g} \circ [d_g h_{d_h}^{d_g-1} h_0 + T_{d_h}] + (g_{d_g-1} \circ h) \cdot (y_{o_g} \circ h_{d_h}^{d_g-1}) \end{cases}$$

where

$$T_i = \boxed{(h_{d_h} y_{o_h}^{d_h} + h_{d_h-1} y_{o_h}^{d_h-1} + \cdots + h_{d_h-i+1} y_{o_h}^{d_h-i+1})^{d_g}}_{\,d_f-i} \tag{4}$$

denotes the coefficient of $y_{o_h}^{d_f-i}$ in $(h_{d_h} y_{o_h}^{d_h} + h_{d_h-1} y_{o_h}^{d_h-1} + \cdots + h_{d_h-i+1} y_{o_h}^{d_h-i+1})^{d_g}$ $(1 \leq i \leq d_h)$.

Note that T_i is divided by $h_{d_h}^{d_g-i}$, so we have the lemma following below:

Lemma 4.1 *If $f = g \circ h$, then f_{d_f-i} is divided by $y_{o_g} \circ h_{d_h}^{d_g-i} (0 \leq i \leq d_g)$, where f_j is the coefficient of $y_{o_f}^j$ in f.*

If (d_h, o_h, h_{d_h}) is known (by Lemma 2.4 and 4.1, they satisfy $d_h \mid d_f$, $o_h \leq o_f$, $y_{o_g} \circ h_{d_h}^{d_g-i}$ divides $f_{d_f-i}(0 \leq i \leq d_g)$), then $d_g = \frac{d_f}{d_h}$, $o_g = o_f - o_h$. By the first equality of E1 we have

$$g_{d_g} \circ h = \frac{f_{d_f}}{y_{o_g} \circ h_{d_h}^{d_g}} \triangleq f^{(1)}$$

Now $f^{(1)}$ can be computed and h is a right decomposition factor of $f^{(1)}$. If $f^{(1)} \notin \mathcal{K}$, then $g_{d_g} \notin \mathcal{K}$. By the same analysis we have $g^{(2)} \circ h = f^{(2)}$, where $g^{(2)}$ is the initial of g_{d_g} and $f^{(2)}$ can be computed by $f^{(1)}$ and other known elements. Go on the reduction until we have $g^{(k)} \circ h = f^{(k)}$, where $f^{(k)}$ is known and the initial of $g^{(k)}$ belongs to the coefficients field $\mathcal{K}$. We have that if h is a right decomposition factor f, then h is also a right decomposition factor of $f^{(k)}$; but it's not necessarily correct for the contrary. Our basic idea is to compute the possible right decomposition factor h from the equality $g^{(k)} \circ h = f^{(k)}$ and then check that if h is really a right decomposition factor of f. So we now must consider such a problem firstly: if we know f has a decomposition $f = g \circ h$, in which (d_h, o_h, h_{d_h}) is what we have known and **the initial of g is in $\mathcal{K}$**, how to compute g, h?

Now there are two cases:

(1) $d_g = 1$. For g is homogeneous, g is linear, we can compute g, h by Algorithm 3.3.

(2) $d_g > 1$. We can obtain $h_i (d_h - 1 \geq i \geq 1)$ step by step by the first $d_h - i + 1$ equalities in E1 and then by the last one we have

$$d_g g_{d_g} \cdot y_{o_g} \circ h_0 + g_{d_g-1} \circ h = \left(f_{d_f-d_h} - g_{d_g} \cdot y_{o_g} \circ T_{d_h} \right) \Big/ y_{o_g} \circ h_{d_h}^{d_g-1} \triangleq F_1$$

By $h_0 = h - \sum\limits_{1 \leq i \leq d_h} h_i y_{o_h}^i$,

$$(d_g g_{d_g} y_{o_g} + g_{d_g-1}) \circ h = f^{(1)} + d_g g_{d_g} y_{o_g} \circ (\sum_{1 \leq i \leq d_h} h_i y_{o_h}^i) \triangleq F_2$$

Note that g_{d_g-1} is linear and F_2 can be computed, so we can obtain all possible h by executing Algorithm 3.3 with input $(F_2,\ o_g)$.

Based on the analysis above, we propose the algorithm to compute all the decompositions of a given homogeneous difference polynomial.

Algorithm 4.2 *Input: a homogeneous difference polynomial f.*

Output: a set $T = \{(g,h) : f = g \circ h$ is a non-trivial decomposition of $f\}/\sim$, where $\sim$ is the equivalent relation defined by $(g_1,h_1) \sim (g_2,h_2) \Leftrightarrow h_1,h_2$ is the equivalent right decomposition factor of f.

S1 $T := \{\}$, $\bar{f} := f$. Let $S = \{(d_h, o_h, h_{d_h}) : d_h | d_f,\ o_h \le o_f,\ y_{o_f-o_h} \circ h_{d_h}^{d_g-i}$ divides $f_{d_f-i}(0 \le i \le d_g-1)\}$, where f_i is the coefficient of $y_{o_f}^i$ in f.

S2 If S is empty, then return T; otherwise, let $\bar{f}_i$ be the coefficient of $y_{o_{\bar{f}}}^i$ in $\bar{f}$. Choose a (d_h, o_h, h_{d_h}) in S and let $S := S - \{(d_h, o_h, h_{d_h})\}$, go to S3.

S3 If $\frac{d_{\bar{f}}}{d_h}$ is not an integer, or $o_{\bar{f}} < o_h$, or there exists an i $(0 \le i \le d_g)$ such that $y_{o_g} \circ h_{d_h}^{d_g-i}$ does not divide $\bar{f}_{d_{\bar{f}}-i}$, go to S2; else, go to S4.

S4 Let $d_g := \frac{d_{\bar{f}}}{d_h}$, $o_g := o_{\bar{f}} - o_h$. Let $\hat{f} := \frac{\bar{f}_{d_{\bar{f}}}}{y_{o_g} \circ h_{d_h}^{d_g}}$. If $\hat{f} \notin \mathcal{K}$, then $\bar{f} := \hat{f}$, go to S3; else, go to S5.

S5 If $d_g = 1$, then execute Algorithm 3.3 with input $\bar{f}, o_g$. Let the output be the set G. Goto S7.

S6 If $d_g > 1$, let $g_{d_g} = \frac{f_{d_f}}{y_{o_g} \circ h_{d_h}^{d_g}}$, $h_{d_h-i} = (y_{-o_g} \circ \frac{f_{d_f-i}}{g_{d_g}} - T_i)/(d_g h_{d_h}^{d_g-1})(i = 1, \ldots, d_h - 1)$ and $F_2 = \left(f_{d_f-d_h} - g_{d_g} \cdot y_{o_g} \circ T_{d_h}\right) \Big/ y_{o_g} \circ h_{d_h}^{d_g-1} + d_g g_{d_g} y_{o_g} \circ (\sum\limits_{1 \le i \le d_h} h_i y_{o_h}^i)$, where T_i is defined in (4). In the above computation, if one of the results is not a difference polynomial, then go to S2. Execute Algorithm 3.3 with input F_2, o_g. Let the output be the set G.

S7 For each (g,h) in G, check that if h is a right decomposition factor of f. If it is and the corresponding left decomposition factor is g', then add (g',h) to T. Go to S2.

Example 4.3 *Let $\mathcal{K} = \mathbb{Q}(t)$, $f = (t+1)y_1y_2^3y_3^2 + tyy_1^3y_2^2 \in \mathcal{K}\{y\}$. We compute all the decompositions of f.*

In step S1, we have $S = \{(1,1,1), (1,2,1), (1,3,1), (1,1,y), (1,2,y_1), (1,3,y_2), (2,3,1), (2,3,y_2), (2,3,y_2^2), (2,3,y_2^3), (2,3,y_1), (2,3,y_1y_2), (2,3,y_1y_2^2), (2,3,y_1y_2^3), (2,2,1), (2,2,y_1), (2,2,y_1^2), (2,2,y_1^3), (2,2,y), (2,2,yy_1), (2,2,yy_1^2), (2,2,yy_1^3), (2,1,1), (2,1,y), (2,1,y^2), (2,1,y^3)\}$.

In step S2, we choose $(2,1,y) \in S$ to start the computation. Steps S3 and S4 run three times continually and output $\bar{f} = (t+1)y_2y_3^2$ $(d_g = 1)$. In step S5, execute Algorithm 3.3 to compute the second order linear left decomposition factor of $\bar{f} = (t+1)y_2y_3^2$, the output is $(y_2, (t-1)yy_1^2)$. In step S7, we can check that $f = (\frac{y_1y_2}{t} + \frac{yy_1}{t-1}) \circ ((t-1)yy_1^2)$.

If we choose other elements in S to start in step S2, only $(2,2,yy_1^3)$ leads to the decomposition $f = (y_1 + y) \circ (tyy_1^3y_2^2)$. Here we omit the details.

From the above example, we can see that there could exist many choices for (d_h, o_h, h_{d_h}), but most of them do not lead to a decomposition. This may reduce the efficiency badly. How to improve the algorithm on this problem is one of our future research topics.

5. Decomposition in the General Case

We now consider the decomposition algorithm in the general case, which is based on the following result.

Theorem 5.1 *Let $f = g \circ h$ be a nontrivial decomposition of f. t, a, b are the total degrees of f, g, h and*

$$\begin{aligned} f &= F_t + F_{t-1} + \cdots + F_1 \\ g &= G_a + G_{a-1} + \cdots + G_1 \\ h &= H_b + H_{b-1} + \cdots + H_1 \end{aligned}$$

are the representations of f, g, h as sums of the homogeneous parts respectively. Then $F_t = G_a \circ H_b$ and $H_i (1 \le i \le b-1)$ can be determined uniquely by H_b and f.

Therefore, for a given difference polynomial f, we write f as the sum of the homogeneous parts $f = F_t + F_{t-1} + \cdots + F_1$. If we can obtain a decomposition $F_t = p \circ q$, then we can use q as a candidate for H_b to compute h and g. Certainly, not all the candidates of H_b will lead to a decomposition of f. So we must try all possible decompositions of F_t. This will not cause any essential difficulties and it can be reduced to the problem of factorization of difference operators, as we have shown in section 4.

Before proving theorem 5.1, we need to give a crucial sub-algorithm.

Proposition 5.2 *Let u, v, h, p be difference polynomials. We denote the leading term of u by l_u. We use rank(u)>rank(v) to denote that the rank of u is higher than the rank of v. It is easy to check the following properties about the leading term:*

1. $l_{u \cdot v} = l_u \cdot l_v$

2. $l_{u \circ v} = l_u \circ l_v$

3. *If y_j appear in l_u, then* $l_{\frac{\partial u}{\partial y_j}} = \frac{\partial l_u}{\partial y_j}$

4. *For a nonnegative integer j, if y_j appears in l_u, the leading term of $\frac{\partial u}{\partial y_j} \circ h \cdot y_j \circ p$ is*

$$\frac{\partial l_u}{\partial y_j} \circ l_h \cdot y_j \circ l_p = \beta_j l_u \circ l_h \cdot y_j \circ \frac{l_p}{l_h}$$

where $\beta_j = \deg_{y_j} l_u$ is the degree of l_u in y_j.

Proof. The first three properties can be easily proved and the fourth can be deduced from the first three. ∎

Lemma 5.3 *Let f, g, and h be homogeneous difference polynomials. If a difference polynomial p satisfies*

$$f = \sum_{0\le j\le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ p$$

and $\mathrm{tdeg}(p) < \mathrm{tdeg}(h)$*, then it is unique and can be computed from f, g and h.*

Proof : Assume that there is a p satisfying the conditions in the lemma and q is an arbitrary term included in g. Let

$$l_g = \alpha y_k^{a_k} y_{k+1}^{a_{k+1}} \cdots y_{o_g}^{a_{o_g}},\ q = \beta y_n^{b_n} y_{n+1}^{b_{n+1}} \cdots y_m^{b_m}$$

where k is the least integer such that y_k appears in l_g and n, m are the minimal and maximal integers such that y_n, y_m appears in q respectively. We divide the problem into two cases.

1) rank(p)>rank(h). By Proposition 5.2, the leading term of $\sum\limits_{0\le j\le o_g} \frac{\partial q}{\partial y_j} \circ h \cdot y_j \circ p$ is

$$\frac{\partial q}{\partial y_m} \circ l_h \cdot y_m \circ l_p = b_m q \circ l_h \cdot y_m \circ \frac{l_p}{l_h}.$$

Since rank(l_g)>rank(q), $o_g \ge m$ and rank(p)>rank(h), the rank of $a_{o_g} l_g \circ l_h \cdot y_{o_g} \circ \frac{l_p}{l_h}$ is higher than $b_m q \circ l_h \cdot y_m \circ \frac{l_p}{l_h}$. Then the leading term of $\sum\limits_{0\le j\le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ p$ is

$$\frac{\partial l_g}{\partial y_{o_g}} \circ l_h \cdot y_{o_g} \circ l_p = a_{o_g} l_g \circ l_h \cdot y_{o_g} \circ \frac{l_p}{l_h}.$$

So we have $l_f = \frac{\partial l_g}{\partial y_{o_g}} \circ l_h \cdot y_{o_g} \circ l_p$ and hence

$$l_p = y_{-o_g} \circ \left(l_f \Big/ \left(\frac{\partial l_g}{\partial y_{o_g}} \circ l_h\right) \right) \tag{5}$$

2) rank(p)<rank(h). By Proposition 5.2, the leading term of $\sum\limits_{0\le j\le o_g} \frac{\partial q}{\partial y_j} \circ h \cdot y_j \circ p$ is

$$\frac{\partial q}{\partial y_n} \circ l_h \cdot y_n \circ l_p = b_n q \circ l_h \cdot y_n \circ \frac{l_p}{l_h}.$$

If $n \ge k$, by rank(l_p)<rank(l_h), we have rank($y_k \circ \frac{l_p}{l_h}$)>rank($y_n \circ \frac{l_p}{l_h}$) and the rank of $a_k l_g \circ l_h \cdot y_k \circ \frac{l_p}{l_h}$ is higher than that of $b_i q \circ l_h \cdot y_n \circ \frac{l_p}{l_h}$. Then the leading term of $\sum\limits_{0\le j\le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ p$ is

$$\frac{\partial l_g}{\partial y_k} \circ l_h \cdot y_k \circ l_p = a_k l_g \circ l_h \cdot y_k \circ \frac{l_p}{l_h}.$$

So we have $l_f = \frac{\partial l_g}{\partial y_k} \circ l_h \cdot y_k \circ l_p$ and hence

$$l_p = y_{-k} \circ \left(l_f \Big/ \left(\frac{\partial l_g}{\partial y_k} \circ l_h\right) \right) \tag{6}$$

If $n < k$, it is easy to check that rank($\frac{\partial l_g}{\partial y_k}$)>rank($\frac{\partial q}{\partial y_n}$) and rank($y_k \circ l_p$)>rank($y_n \circ l_p$). So the rank of $\frac{\partial l_g}{\partial y_k} \circ l_h \cdot y_k \circ l_p$ is higher than that of $\frac{\partial q}{\partial y_n} \circ l_h \cdot y_n \circ l_p$ and the equality (6) still holds.

Since tdeg(p) $<$ tdeg(h) and p, h are both homogeneous, the case of rank(p)=rank(h) will not happen. Hence l_p can be computed from (5) and (6). Let $p = l_p + \bar{p}$. Since $y_j \circ p = y_j \circ l_p + y_j \circ \bar{p}$, p can be computed using (5) and (6) repeatedly.

If there exist two distinct difference polynomials p_1, p_2 such that

$$\begin{cases} f = \sum\limits_{0 \le j \le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ p_1 \\ f = \sum\limits_{0 \le j \le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ p_2 \end{cases}$$

then we have

$$\sum_{0 \le j \le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ (p_1 - p_2) = 0.$$

Either (5) or (6) must hold. We have $l_{p_1 - p_2} = 0$, which means $l_{p_1} = l_{p_2}$. Repeating the procedure recursively, we can deduce that $p_1 = p_2$, a contradiction. ∎

Following the proof of Lemma 5.3, we give the following algorithm.

Algorithm 5.4 *Input: homogeneous difference polynomials f, g, h.*

Output: a difference polynomial p such that $f = \sum\limits_{0 \le i \le o_g} \frac{\partial g}{\partial y_i} \circ h \cdot y_i \circ p$ and tdeg(p) $<$ tdeg(h), *if it exists.*

S1 Let l_f, l_g, l_h be the leading terms of f, g, h respectively, $k = \min\{i : y_i \text{ appears in } l_g\}$ and $p := 0$. By the proof of Lemma 5.3, the leading term l_p of p must satisfy one and only one of the following two equalities

$$\begin{cases} \frac{\partial l_g}{\partial y_k} \circ l_h \cdot y_k \circ l_p = l_f & \text{if rank}(p)\text{>rank}(h) \\ \frac{\partial l_g}{\partial y_{o_g}} \circ l_h \cdot y_{o_g} \circ l_p = l_f & \text{if rank}(p)\text{<rank}(h) \end{cases}$$

S2 If $f = 0$, then return p. Use (6) to compute l_p. If l_p is not a difference polynomial, then go to S3; else go to S4. This step computes l_p in the case of rank(p)>rank(h).

S3 Use (5) to compute l_p. If l_p is not a difference polynomial, then terminate the algorithm and return "p does not exist"; else go to step S4. This step computes l_p in the case of rank(p)<rank(h).

S4 Let $p := p + l_p$, $f := f - \sum\limits_{0 \le j \le o_g} \frac{\partial g}{\partial y_j} \circ h \cdot y_j \circ l_p$. Go to step S2.

Now we give the proof of Theorem 5.1.

If f has a decomposition $f = g \circ h$, we have

$$F_t + F_{t-1} + \cdots + F_1 = (G_a + G_{a-1} + \cdots + G_1) \circ (H_b + H_{b-1} + \cdots + H_1).$$

Comparing the homogeneous parts on both sides of $f = g \circ h$ we have

$$(E2)\begin{cases} F_t = G_a \circ H_b \\ F_{t-1} = \sum\limits_{0\le i\le o_{G_a}} \frac{\partial G_a}{\partial y_i} \circ H_b \cdot y_i \circ H_{b-1} \\ \vdots \\ F_{t-k} = \boxed{G_a \circ (H_b + H_{b-1} + \cdots + H_{b-k+1})}_{\,t-k} + \sum\limits_{0\le i\le o_{G_a}} \frac{\partial G_a}{\partial y_i} \circ H_b \cdot y_i \circ H_{b-k} \\ \vdots \\ F_{t-b+1} = \boxed{G_a \circ (H_b + H_{b-1} + \cdots + H_2)}_{\,t-b+1} + \sum\limits_{0\le i\le o_{G_a}} \frac{\partial G_a}{\partial y_i} \circ H_b \cdot y_i \circ H_1 \end{cases}$$

where $\boxed{u}_{\,i}$ is the sum of terms in u with total degree i. By lemma 5.3, we can determine $H_{b-1}, \cdots, H_1$ uniquely one by one starting from the second equality. So we have $h = H_b + H_{b-1} + \cdots + H_1$. Such an h is not necessarily a right decomposition factor of f, because we have only compared the terms with total degree from $t - b + 1$ to t. We need to check whether h is a right decomposition factor of f, which can be done by Algorithm 2.5. ∎

Based on the analysis in this section, we have the following decomposition algorithm for the general case.

Algorithm 5.5 *Input: a difference polynomial f.*
Output: a nontrivial decompositions of f: $f = g \circ h$.

S1 Write f as the sum of homogeneous parts $f = F_t + F_{t-1} + \cdots + F_1$.

S2 Execute algorithm 4.2 with input F_t. Assume that the output is T.

S3 If T is empty, then return "f has no nontrivial decompositions"; otherwise, choose a $(g, h) \in T$ and $T := T - \{(g, h)\}$.

S4 Let $a = \mathrm{tdeg}(g), b = \mathrm{tdeg}(h)$ and $G_a = g, H_b = h$. For $k = 1, \cdots, b-1$, execute Algorithm 5.4 to compute $H_{b-k}, \cdots, H_1$ with input

$$F_{t-k} - \boxed{G_a \circ (H_b + H_{b-1} + \cdots + H_{b-k+1})}_{\,t-k}, G_a, H_b$$

respectively.

S5 Let $h = H_b + H_{b-1} + \cdots + H_1$ and compute a left decomposition factor g such that $f = g \circ h$ by Algorithm 2.5. If g exists, return (g, h); otherwise, go to S3.

The worst case complexity of the algorithm is exponential. The reason is due to the combinatorial selection in several places. For instance, in step S4 of Algorithm 3.3, we need to consider all the decomposition factors of a linear difference polynomial, which could be exponential. It is worth noting that the complexity of factoring difference operators, which is equivalent to the decomposition of linear difference polynomials, is also exponential.

Example 5.6 *Let $\mathcal{K} = \mathbb{Q}(t)$, $f = (t+1)y_1y_2^3y_3^2 + tyy_1^3y_2^2 + (t+1)(t+2)y_1y_2^2y_3 + (t+1)^2y_2^2y_3^2 + t(t+1)yy_1^2y_2 + t^2y_1^2y_2^2 + y_1y_2^2 + tyy_1^2 + (t+1)^2(t+2)y_2y_3 + t^2(t+2)y_1y_2 + (t+1)y_2 + t^2y_1$.*

In step S1, write f as the homogeneous parts $f = F_6 + F_4 + F_3 + F_2 + F_1$, where $F_6 = (t+1)y_1y_2^3y_3^2 + tyy_1^3y_2^2$, $F_4 = (t+1)(t+2)y_1y_2^2y_3 + (t+1)^2y_2^2y_3^2 + t(t+1)yy_1^2y_2 + t^2y_1^2y_2^2$, $F_3 = y_1y_2^2 + tyy_1^2$, $F_2 = (t+1)^2(t+2)y_2y_3 + t^2(t+2)y_1y_2$, $F_1 = (t+1)y_2 + t^2y_1$.

In step S2, using Algorithm 4.2, we obtain the decomposition of F_6: $T = \{((t+1)y_1y_2 + tyy_1, yy_1^2), (y_1+y, tyy_1^3y_2^2)\}$ (In example 4.3, $(\frac{y_1y_2}{t}+\frac{yy_1}{t-1})\circ((t-1)yy_1^2) = ((t+1)y_1y_2+tyy_1)\circ yy_1^2$ are two equivalent decompositions).

In step S3, choose $((t+1)y_1y_2 + tyy_1, yy_1^2)$ and in step S4, we obtain $H_3 = yy_1^2, H_2 = 0, H_1 = ty_1$. In step S5, we can check that $h = H_3 + H_2 + H_1 = yy_1^2 + ty_1$ is a right decomposition factor of f: $f = ((t+1)y_1y_2 + tyy_1 + y_1 + ty) \circ (yy_1^2 + ty_1)$.

6. Experimental Results

We implemented Algorithm 5.5 in Maple for the constant field case $\mathcal{K} = \mathbb{Q}$. To implement Algorithm 5.5 for $\mathcal{K} = \mathbb{Q}(t)$, we need an implementation which could give all the possible factorizations of a difference operator, which is a quite difficult task and is not available in Maple. For $\mathcal{K} = \mathbb{Q}$, we can easily find all the factorizations of a difference operator similar to the differential case [6]. Besides this point, our implementation suits the case of $\mathcal{K} = \mathbb{Q}(t)$.

Two sets of experiments are done. In Table 1, we generate a difference polynomial randomly and decompose it. All the randomly generated difference polynomials in Table 1 are indecomposable. In Table 2, we generate two difference polynomials g and h randomly and decompose $f = g \circ h$. The difference polynomials g and h are given in Table 3. The running times are collected on a PC with a 1.6GHz CPU and 256M memory and are given in seconds. In Tables 1 and 2, o_f, t_f, l_f means the order, the total degree and the number of terms in f respectively.

(o_f, t_f, l_f)	time(s)	(o_f, t_f, l_f)	time(s)
(2,20,164)	0.110	(2, 30, 261)	0.203
(2,40,735)	0.204	(3, 10, 242)	0.047
(3,20,992)	0.672	(3, 30, 3424)	4.328
(4,10,693)	0.781	(4, 20, 4253)	6.890
(5,10,1198)	3.969	(5, 10, 1929)	2.532
(6,8,2698)	5.391	(6,10,3708)	6.859
(7,8,2101)	7.468	(8,6,2682)	8.188
(9,6,4870)	18.969	(10,6,4747)	27.641

Table 1. Decomposing Randomly Generated Differential Polynomials

From these experimental results, we may conclude that our algorithm is efficient in handling large difference polynomials with thousands of terms. The computational efficiency is due to the fact that all computations in the algorithm are based on explicit formulas. Our program is especially fast for randomly generated difference polynomials. The reason can be explained below. From Lemmas 4.1 and 5.3, we can see that a difference polynomial with a nontrivial decomposition has certain structures and a randomly generated difference polynomial does not have these structures. As a consequence, the program will stop early before going through all the cases.

g, h	(o_g, t_g)	(o_h, t_h)	(o_f, t_f, l_f)	time(s)
g_1, h_1	(0,8)	(1,8)	(1,64,761)	11.406
g_2, h_2	(1,6)	(1,8)	(2,48,2302)	4.844
g_3, h_3	(1,6)	(2,4)	(3,24,1538)	3.250
g_4, h_4	(1,4)	(3,4)	(4,16,2329)	1.047
g_5, h_5	(2,4)	(1,6)	(3,24,1558)	0.891
g_6, h_6	(2,4)	(2,6)	(4,24,363)	10.172
g_7, h_7	(2,4)	(3,4)	(5,16,716)	1.500
g_8, h_8	(3,4)	(2,6)	(5,24,4475)	4.921
g_9, h_9	(3,4)	(3,4)	(6,16,10079)	26.063
g_{10}, h_{10}	(4,3)	(3,4)	(7,12,807)	1.797

Table 2. Decompose $f = g \circ h$

g_1	$-37y^8 - 20y^7 - 29y^6 + 48y^5 + 20y^4 - 3y^3$
h_1	$48y - 18yy_1 - 48y^4 + 42y^3y_1^2 + 2y^6 + 41y^4y_1^3 + 19y^4y_1^4$
g_2	$-10y^2y_1 - 11y_1^3 - 31y^5y_1$
h_2	$32y + 19y_1 - 39y^3 - 19y^2y_1 - 24y^2y_1^2 - y^5y_1^2 - 9y^3y_1^5 + 29yy_1^7$
g_3	$13y^2 - 49y^2y_1^2 - 21y^3y_1^2 + 17y_1^5 + 21y^4y_1^2$
h_3	$38y_1y_2^2 - 13y^3y_1 - 37yy_1^3 + 19y_1^3y_2 - 40y_1y_2^3$
g_4	$36y - 50y_1 - 17y^2y_1 + 10y_1^2y - 21y_1^3 - 22y_1^2y^2 - 3y_1^3y$
h_4	$48y_1^2 - 32y^2y_1 - 40y_2^2y_3 + 23yy_2^2y_3 + yy_3^3 + 8y_1^2y_2y_3 + 5y_1^2y_3^2 + 32y_2^4$
g_5	$-5y + 44y_1^3 + 16y_1^2y_2 + 14y^2y_2^2 - 13yy_1y_2^2 + 31y_1^2y_2^2$
h_5	$-18yy_1 + 15y^3 - 20y_1^4 - 3yy_1^4 + 28y^6 - 19y^4y_1^2$
g_6	$17y^2 + 20y_1y_2 - 18y^2y_1 + 47y^2y_2 + 43y^2y_2^2 - 46yy_1^2y_2$
h_6	$43y^3 - 34y_1^4 + 25y^4y_1 - 47y^2y_1^3y_2$
g_7	$35y_2 - 30y^3 - 19y_1^3 - 18y^3y_1 + 2yy_1^2y_2 + 19y_1y_2^3$
h_7	$3y^2y_1 + 46y^2y_2^2 + 13yy_1^3 - 5y_1y_2^2y_3 + 26y_1y_3^3$
g_8	$-5y - 9y_3y^2 + 28y_2^2y - 45y_1y_2^2 + 32y_1y^3 - 24y_2y^3 - 16y_2^2y^2 + 28y_2^2y_3y - 16y_1^2y_3^2 + 7y_2y_3^3$
h_8	$45yy_2 - 41y_1^3 - 6y_1^5 - 44y_1^3y_2^2 + 16y_1^2y_2^3 + 6y_1y_2^4 + 32y_1y_2^2y^3$
g_9	$-41y^2 - 10y_1y_2^2 + 25y^2y_1^2 - 29yy_1y_3^2 + 5yy_2y_3^2 - 48y_2^2y_3^2$
h_9	$18y^2 + 36y_2^2 - 37y^3y_2 - 3y^2y_1y_3 + 20y^2y_2^2 + 33y^2y_2y_3 + 46yy_1^3 + 31yy_1^2y_3 + 37y_1^3y_2 - 5y_1^2y_2y_3$
g_{10}	$21y_2 - 13y_3 + 6yy_1 - 23y_3y_4 + 12yy_1y_3 - 38yy_1y_4 - 6yy_2^2 - 16yy_4^2 - 24y_1^2y_3 + 18y_2^3$
h_{10}	$-26yy_1 + 14y_2y_3 + 32y^2y_2 + 29y^2y_3 - 27y_1^2y_3 - 46y_2^2y_3^2$

Table 3. Randomly generated g and h

Based on these experimental results, we may conclude that our algorithm provides an efficient reduction of the decomposition of nonlinear difference polynomials to the linear case.

7. Conclusions

In this paper, we give a complete and practical algorithm to decompose a given nonlinear difference polynomial in one variable and over a computable difference field. The algorithm provides an efficient reduction of the problem to the decomposition of difference operators.

Besides the algorithmic study for the decomposition, the uniqueness problem is also an important property to be explored. Ritt gave a perfect result for the uniqueness of decompositions for an algebraic polynomial [10]. Similar results were proved for Ore polynomials and hence for linear difference polynomials [8]. It is interesting to see whether these properties can be extended to the case of difference polynomials.

References

[1] F. Binder, *Polynomial Decomposition Theoretical Results and Algorithms*, Thesis, Johannes Kepler University, 1995.

[2] M. Bronstein and M. Petkovšek, An introduction to pseudo-linear algebra, *Theoretical Computer Science*, **157**, 3-33, 1996.

[3] M. Bronstein and M. Petkovšek. On Ore Rings, Linear Operators and Factorization, *Programmirovanie*, **20**, 27-45, 1994.

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

[5] X.S. Gao and M. Zhang, Decomposition of Differential Polynomials with Constant Coefficients, *Proc. ISSAC 2004*, 175-182, ACM Press, New York, 2004.

[6] X.S. Gao and M. Zhang, Decomposition of Differential Polynomials with Rational Function Coefficients, In *MM-Preprints*, **23**, 92-112, December, 2004.

[7] M. Giesbrecht and Y. Zhang, Factoring and Decomposing Ore Polynomials Over $F_q(t)$, *Proc. ISSAC 2003*, 127-134, ACM Press, New York, 2003.

[8] O. Ore, Theory of noncommutative polynomials. *Annals of Mathematics*, **34**(3), 480-508, 1933.

[9] J.F. Ritt, *Differential Algebra*, AMS, New York, 1950.

[10] J.F. Ritt, Prime and composite polynomials, *Trans. Amer. Math. Soc.*, **23**, 51-66, 1922.

[11] M.V. Sosnin, An Algorithm for Nonparametric Decomposition of Differential Polynomials, *Programming and Computing Software*, **27**(1), 43 - 49, 2001.

[12] S.P. Tsarev, On Factorization of Non-linear Ordinary Differential Equations, *Proc. ISSAC 1999*, 159-164, ACM Press, New York, 1999.

[13] J. von zur Gathen, Functional Decomposition of Polynomials: the Tame Case, *J. Symb. Comput.*, **9**, 281-299, 1990.