Decomposition of Differential Polynomials (Extended Abstract)

Xiao-Shan Gao and Mingbo Zhang

Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS
Academia Sinica, Beijing 100080, China
xgao@mmrc.iss.ac.cn

Abstract. We present an algorithm to decompose nonlinear differential polynomials in one variable and with rational functions as coefficients. The algorithm is implemented in Maple for the *constant field* case. The program can be used to decompose differential polynomials with more than one thousand terms effectively.

Keywords. decomposition, differential polynomial, difference polynomial

1 Introduction

We propose an algorithm to decompose nonlinear univariate ordinary differential polynomials. The idea is to reduce the decomposition of nonlinear differential polynomials to the decomposition of univariate linear ordinary differential operators (LODOs). The algorithm is of exponential complexity in the worst case, but seems practically effective for a large class of problems. The reason is that the exponential complexity is mainly caused by combinatorially selections and for each such selection the algorithm uses only a small number of simple and fast operations such as polynomial factorization, solving of linear equations, and decomposition of algebraic polynomials.

We first find the right decomposition factor by reducing the problem in the general case to the decomposition of differential polynomials whose left decomposition factor is quasi linear. Then the quasi linear case is solved by decomposition of LODOs and solution of systems of linear equations. After the right decomposition factor is found, it is easy to find the left decomposition factor.

Most of the previous work on decomposition focused on decomposition of polynomials, LODOs, and linear difference operators. This seems to be the first complete algorithm to decompose nonlinear differential polynomials. We also give an algorithm to decompose nonlinear ordinary difference polynomials [5].

2 Notations and Preliminary Results

Let $\mathcal{K} = \mathbb{Q}(t)$ be the differential field of rational functions in t, x a differential indeterminate, and $\mathcal{K}\{x\}$ the ordinary differential polynomial ring over $\mathcal{K}$. We

Dagstuhl Seminar Proceedings 06271
Challenges in Symbolic Computation Software
http://drops.dagstuhl.de/opus/volltexte/2006/772

denote by x_i the i-th derivative of x. For a differential polynomial f not in $\mathcal{K}$, let x_o be the highest derivative appearing in f, which is called the *order* of f and is denoted by o_f. Let o_f be the order of f, d_f the degree of f in x_{o_f}, i_f the coefficient of $x_{o_f}^{d_f}$ in f, $s_f = \frac{\partial f}{\partial x_{o_f}}$. Then d_f, i_f, s_f are called the *degree, initial, and separant* of f respectively.

A monomial in $\mathcal{K}\{x\}$ is always arranged in the form $a\prod_{i=0}^{r} x_i^{\alpha_i}$ where $a \in \mathcal{K}$, $\alpha_i \in \mathbb{N}$. The number $\sum_{0\le i\le r}\alpha_i$ is called the *total degree* and $\sum_{0\le i\le r} i\cdot\alpha_i$ is called the *differential degree* of the monomial. The *total degree* and *differential degree* of f are denoted by $\mathrm{tdeg}(f)$ and $\mathrm{ddeg}(f)$ respectively. If $\mathrm{tdeg}(f) = k$ and f is total degree homogeneous, f is called k-total degree homogeneous. Furthermore, if $k = 1$ we say that f is *linear*.

Let $g, h \in \mathcal{K}\{x\}$, we use $g \circ h$ to denote the *composition* of two differential polynomials g and h, which is obtained by substituting x_i in g by $h_{(i)}(0 \le i \le o_g)$. 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 in the form $ax + b$ where a and b are in $\mathcal{K}$.

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

We can always write f, g, h as follows.

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

where $f_{d_f} = i_f,\ g_{d_g} = i_g$ and h_1 is of degree lower than h in x_{o_h}.

Lemma 1. *If $f = g \circ h$, we have $o_f = o_g + o_h, \quad s_f = (s_g \circ h) \cdot s_h$.*

Lemma 2. *If $f = g\circ h$ and $o_g = 0$, we have $o_f = o_h, d_f = d_g d_h, i_f = (i_g \circ h) i_h^{d_g}$.*

Lemma 3. *If $f = g \circ h$ and $o_g > 0$, we have $o_f = o_g + o_h, d_f = d_g, i_f = (i_g \circ h) \cdot s_h^{d_f}$.*

Lemma 4. *Use the notations in (1). If $f = g\circ h$ and $o_g > 0$, then $s_h^i (1 \le i \le d_f)$ is a factor of f_i over $\mathcal{K}$.*

Lemma 5. *Let $f = g \circ h$ and $o_g > 0$. Denote $d_f (= d_g)$ by d, $\frac{\partial^k f}{\partial^k x_{o_f}}$ by $s^{(k)}(f)$ and $\frac{\partial^k g}{\partial^k x_{o_g}}$ by $s^{(k)}(g) (1 \le k \le d)$ respectively. Then we have $s^{(i)}(f)/s_h^i = s^{(i)}(g) \circ h$ $(1 \le i \le d)$. Namely, h is a right decomposition factor of $s^i(f)/s_h^i$.*

Lemma 6. *q, u, v are differential polynomials, $q = u \circ v$. Let $d = \mathrm{tdeg}(q), d_1 = \mathrm{tdeg}(u), d_2 = \mathrm{tdeg}(v)$. Then $d = d_1 \cdot d_2$. Furthermore, if Q_d, U_{d_1}, V_{d_2} are the sums of monomials in q, u, v with total degrees d, d_1, d_2 respectively, then $Q_d = U_{d_1} \circ V_{d_2}$.*

3 Reduction to Quasi Linear Case

Two basic operations are often needed: (1) to examine whether a given differential polynomial is a right decomposition factor of another differential polynomial and (2) to find a univariate polynomial decomposition of a differential polynomial. The second problem could be considered as a univariate decomposition of multi-variate polynomials. Such an algorithm has been given in [4]. An algorithm for the first problem is simple and can be found in [1]. Therefore, we need only to find a right decomposition factor.

A differential polynomial p in $\mathcal{K}\{x\}$ is called *quasi linear* if p is of the form $p = x_{o_p} + p_1$ where p_1 is of order lower than o_p.

When $o_g > 0$, we have $s_h^i | f_i (1 \le i \le d_f)$ by Lemma 4. From this relation, we may find a finite number of candidates S for s_h. Our decomposition algorithm will start with such a possible separant S. We consider two cases.

Case 1. $\frac{f_d}{s_h^d} = \frac{i_f}{s_h^d} \notin \mathcal{K}$. By Lemma 3, h is a right decomposition factor of $\frac{f_d}{s_h^d}$. Then we can consider the decomposition of $\frac{f_d}{s_h^d}$ recursively.

Note that after an iteration, the left decomposition factor of $\frac{f_d}{s_h^d}$ could be a polynomial and the condition $o_g > 0$ is not valid anymore. We need to test whether $\frac{f_d}{s_h^d}$ has a polynomial decomposition such that the separant of the right decomposition factor is S. Such a decomposition is unique if it exists. If $\frac{f_d}{s_h^d}$ has such a polynomial decomposition, we will check whether the right decomposition factor of it is a right decomposition factor of f. If $\frac{f_d}{s_h^d}$ does not have such a polynomial decomposition or the right decomposition factor of it is not a right decomposition factor of f, we can repeat the above procedure recursively.

Case 2. $\frac{f_d}{s_h^d} = c \in \mathcal{K}$. By Lemma 2, $g_d \in \mathcal{K}$. Now let $d = d_f (= d_g)$ and $i = d - 1$ in Lemma 5, we have $s^{d-1}(f)/s_h^{d-1} = s^{d-1}(g) \circ h$. Using notations in (1), by direct computation, we have

$$s^{d-1}(f) = \frac{\partial^{d-1} f}{\partial^{d-1} x_{o_f}} = d! f_d x_{o_f} + (d-1)! f_{d-1}$$
$$s^{d-1}(g) = d! g_d x_{o_g} + (d-1)! g_{d-1}.$$

So we have

$$\big(f_d x_{o_f} + \frac{1}{d} f_{d-1}\big)/s_h^{d-1} = (g_d x_{o_g} + \frac{1}{d} g_{d-1}) \circ h \tag{2}$$

By (2) we have

$$s_h x_{o_f} + \frac{1}{cd} \cdot \frac{f_{d-1}}{s_h^{d-1}} = (\frac{g_d}{c} x_{o_g} + \frac{1}{cd} g_{d-1}) \circ h = \frac{g_d}{c}(s_h x_{o_f} + R_h) + \frac{1}{cd} g_{d-1} \circ h.$$

Comparing the coefficients of x_{o_f}, we have $s_h = \frac{g_d}{c} \cdot s_h$ and then $\frac{g_d}{c} = 1$. Let $w = \frac{1}{cd} \cdot \frac{f_{d-1}}{s_h^{d-1}}$, $g' = \frac{1}{cd} g_{d-1}$. Then

$$p = s_h x_{o_f} + w = (x_{o_g} + g') \circ h \tag{3}$$

So, *the left decomposition factor of* p *w.r.t.the right decomposition factor* h *is quasi linear.*

The above analysis leads to the following algorithm.

Algorithm 1 *Input: differential polynomials* f, S.

Output: There are three possibilities: (1) differential polynomials g *and* h *such that* $f = g \circ h$*; (2) a differential polynomial* p *such that if* h *is a right decomposition factor of* f *with separant* S*, then* h *is a right decomposition factor of* p *and the corresponding left decomposition factor of* p *w.r.t.* h *is quasi linear; or (3) an empty set which means that* f *has no right decomposition factors with separant* S.

S1 $q := f$.
S2 Let $d = d_q$. Write q as the form $q = q_d x_{o_q}^d + \cdots + q_1 x_{o_q} + q_0$. If $o_q < o_S$, then output the empty set and terminate the algorithm.
S3 If $c = \frac{s_q}{S} \in \mathcal{K}$, check whether there exists a nontrivial g such that $f = g \circ q$, and if it is, output g and q; otherwise output $p = \frac{q}{c}$. Terminate the algorithm.
S4 If we find a pair of r, h such that r is a polynomial and $q = r \circ h$ and $s_h = S$, then try to find a g such that $f = g \circ h$. If such a g exists, output g, h and terminate the algorithm; otherwise, go to next step. S3 and S4 consider the polynomial decomposition of q.
S5 For $i = 1, \ldots, d$, if there exists some i such that $S^i \not| q_i$, then output the empty set and terminate the algorithm.
S6 Let $c = q_d / S^d$. If $c \in \mathcal{K}$, let $w = \frac{1}{c \cdot d} \frac{q_{d-1}}{S^{d-1}}$, output $p = S x_{o_q} + w$ and terminate the algorithm.
S7 Let $q = c - c_0$, where c_0 denotes the term of c in $\mathcal{K}$. Go to S2.

4 Solving the Quasi Linear Case

We consider the following problem: if a given differential polynomial p has a decomposition $p = r \circ h$ such that r is quasi linear, how to find r and h?

We write differential polynomials p, r, h as the sum of total degree homogeneous parts:

$$p = P_d + P_{d-1} + \cdots + P_2 + P_1$$
$$r = R_{d_1} + R_{d_1-1} + \cdots + R_2 + R_1$$
$$h = H_{d_2} + H_{d_2-1} + \cdots + H_2 + H_1$$

where d, d_1, d_2 denote the total degrees of p, r, h respectively. Notice that p, r, h have no terms in $\mathcal{K}$. Since r is quasi linear, $R_1 \neq 0$ and $o_{R_i} < o_{R_1}$ for $2 \leq i \leq d_1$.

For any differential polynomial f, denote $\boxed{f}_k$ to be the sum of the monomials included in f with total degree k. We consider two cases: $P_1 \neq 0$ and $P_1 = 0$.

Case 1: $P_1 \neq 0$

We assume $d_1 < d_2$ (the case $d_1 \geq d_2$ is similar). Comparing the sum of the monomials with total degree l $(1 \leq l \leq d)$ in $p = r \circ h$, we have $(E1)$.

$$
(E1)\begin{cases}
P_1 = R_1 \circ H_1 \\
P_2 = R_1 \circ H_2 + R_2 \circ H_1 \\
\vdots \\
P_k = R_1 \circ H_k + R_k \circ H_1 + \sum\limits_{1<i<k} \boxed{R_i \circ (\sum_{1\le j\le k-1} H_j)}_k \, (k \le d_1) \\
\vdots \\
P_s = R_1 \circ H_s + \sum\limits_{1<i\le d_1} \boxed{R_i \circ (\sum_{1\le j\le s-1} H_j)}_{d_2} \; (d_1 < s \le d_2) \\
\vdots \\
P_v = \boxed{\sum\limits_{1<i\le d_1} R_i \circ (\sum_{1\le j\le v} H_j)}_v \; (v > d_1) \\
\vdots \\
P_d = R_{d_1} \circ H_{d_2}
\end{cases}
$$

The idea of our algorithm is as follows: find R_1, H_1 from the first equation of $(E1)$ and substitute R_1, H_1 into $P_k = 0 (k > 1)$ to obtain H_k and R_k by solving a linear equation system in the coefficients of H_k and R_k. To make this into an algorithm, we need to answer the following questions.

Q1. How to determine d_1 and d_2?
Q2. How to determine R_1, H_1 from the first equation of $(E1)$, that is, how to decompose LODOs over $\mathcal{K}$?
Q3. Can $R_k, H_k (1 \le k \le \min\{d_1, d_2\})$ be determined uniquely by R_1 and H_1? If the answer is no, then some new parameters over $\mathcal{K}$ will appear and we may face the difficult problem of solving algebraic differential equations about the coefficients in the next step.
Q4. If $d_1 < d_2$, we will obtain $R_i, H_i (1 \le i \le d_1)$ firstly and then compute $H_j (d_1 < j \le d_2)$. We need to know whether $H_j (d_1 < j \le d_2)$ can be determined uniquely. Similarly, how about the case of $d_1 \ge d_2$?

For problem Q1, by Lemma 6 we have $d = d_1 d_2$. It is obvious that $d_2 = \mathrm{tdeg}(h) \ge \mathrm{tdeg}(S) + 1$, where S is the possible separant of h. So we will search all possible pairs (d_1, d_2) satisfying these two conditions.

For problem Q2, we may use the algorithm in [3] to find a complete enumeration of all decompositions of P_1.

Theorem 2 below answers the first part of problem Q3 affirmatively.

Theorem 2. *Let R_1, H_1 be two linear differential polynomials and P_k' a k-total degree homogeneous differential polynomial($k > 1$) over $\mathcal{K}$. If there exist k-total degree homogeneous differential polynomials R_k, H_k over $\mathcal{K}$ such that $o_{R_k} < o_{R_1}$ and $P_k' = R_1 \circ H_k + R_k \circ H_1$, then they are unique.*

As shown by the following example, parameters will be introduced in the decomposition of LODOs:

Example 1. $\mathcal{K} = \mathbb{C}(t)$, $x_2 \in \mathcal{K}\{x\}$ has the following two decompositions

$$x_2 = x_1 \circ x_1 = (x_1 + \frac{1}{t+c}x) \circ (x_1 - \frac{1}{t+c}x)$$

where $c \in \mathbb{C}$ is a constant parameter.

Theorem 2 asserts that no new parameters will be introduced in both of R_k and $H_k (1 < k \leq d_1)$. If R_1, H_1 contain parameters, H_k, R_k may contain these parameters, too. Furthermore, the identical equation $R_1 \circ H_k + R_k \circ H_1 = P'_k$ may add new constraints on the parameters in R_1 and H_1. These newly added constraints can be handled by the method in [2].

When R_1, H_1, P_k are given and R_i, H_i $(2 \leq i \leq k-1)$ have been obtained, we hope to find R_k, H_k from

$$R_1 \circ H_k + R_k \circ H_1 = P'_k = P_k - \sum_{1<i<k} \boxed{R_i \circ (\textstyle\sum_{1\leq j\leq k-1} H_j)}_{\,k}$$

Denote $\tilde{R}_k, \tilde{H}_k$ to be the sums of the terms in R_k, H_k with maximal differential degree respectively. Comparing the sum of the terms with maximal differential degree of both sides, we have:

$$a_m \sum_J b_J (x_m \circ x^{j_0} x_1^{j_1} \cdots x_{o_2}^{j_{o_2}}) + b_n^k \sum_I (a_I x^{i_0} x_1^{i_1} \cdots x_{o_1}^{i_{o_1}}) \circ x_n - \tilde{P}'_k = 0 \quad (4)$$

Notice that in the identity (4), all the coefficients a_I, b_J are algebraic linear. So **we need only to solve an algebraic linear system** to obtain $\tilde{R}_k, \tilde{H}_k$.

The above analysis leads to the following algorithm.

Algorithm 3 *Input: differential polynomials $R_1, H_1, P'_k \in \mathcal{K}\{x\}$ and a positive integer o_p. R_1, H_1 are linear, $i_{R_1} = 1$ and P'_k is k-total degree homogeneous.*

Output: differential polynomials $R_k, H_k \in \mathcal{K}\{x\}$ such that $o_{R_k} < o_{R_1}$, $o_{H_k} \leq o_p - o_{R_1}$ and $R_1 \circ H_k + R_k \circ H_1 = P'_k$ if they exist.

S1 Let $m = o_{R_1}$, $n = o_{H_1}, b_n = i_{H_1}$, $o_2 = o_p - m$, $R_k = H_k = 0$.

S2 If $P'_k = 0$, return R_k, H_k; If $\mathrm{ddeg}(P'_k) < \max\{m, n \cdot k\}$, then R_k, H_k do not exist, return. Let $\tilde{P}'_k$ be the sum of the terms included in P'_k with maximal differential degree.

S3 Let

$$T_1 = \{(i_0, i_1, \cdots, i_{m-1}) : \sum_{0\leq s\leq m-1} i_s = k, \sum_{0\leq s\leq m-1} s \cdot i_s = \mathrm{ddeg}(P'_k) - m\}$$

$$T_2 = \{(j_0, j_1, \cdots, j_{o_2}) : \sum_{0\leq l\leq o_2} j_l = k, \sum_{0\leq l\leq o_2} l \cdot j_l = \mathrm{ddeg}(P'_k) - n \cdot k\}$$

$$\tilde{R}_k = \sum_{I\in T_1} a_I x^{i_0} x_1^{i_1} \cdots x_{m-1}^{i_{m-1}}, \quad \tilde{H}_k = \sum_{J\in T_2} b_J x^{j_0} x_1^{j_1} \cdots x_{o_2}^{j_{o_2}}$$

Then we have

$$\sum_{J\in T_2} b_J(x_m \circ x^{j_0}x_1^{j_1}\cdots x_{o_2}^{j_{o_2}}) - b_n^k \sum_{I\in T_1}(a_I x^{i_0}x_1^{i_1}\cdots x_{m-1}^{i_{m-1}})\circ x_n - \tilde{P}_k' = 0 \quad (5)$$

If T_1 (T_2) is empty, then $R_k := 0$ ($H_k := 0$) and the corresponding sum is defined to be zero. Simplify the left part of (5) and let the coefficients of each monomial be zero. We obtain **linear equations** about a_I and b_J. If this equation system does not have a solution, then R_k, H_k do not exist, return; else, $R_k := R_k + \tilde{R}_k$, $H_k := H_k + \tilde{H}_k$.

S4 $P_k' := P_k' - R_1 \circ \tilde{H}_k - \tilde{R}_k \circ H_1$, go to S2.

Problem Q4 is easier to explain: when $d_1 \geq d_2$, we obtain all $H's$ firstly, then we have obtained the right decomposition factor of p and the corresponding left decomposition factor is certainly uniquely determined by the coefficients of h.

Case 2: $P_1 = 0$

Let $k = \min\{i: \ P_i \neq 0\}$. Then $k = \min\{i: \ H_i \neq 0\}$. Comparing the sum of the monomials with total degree l ($k \leq l \leq d$) in $p = r \circ h$, we have

$$(E2)\begin{cases} P_k = R_1 \circ H_k \\ P_{k+1} = R_1 \circ H_{k+1} \\ \vdots \\ P_{2k-1} = R_1 \circ H_{2k-1} \\ P_{2k} = R_1 \circ H_{2k} + R_2 \circ H_k \\ P_{2k+1} = R_1 \circ H_{2k+1} + \boxed{R_2 \circ (H_k + H_{k+1})}_{\,2k+1} \\ \vdots \\ P_d = R_{d_1} \circ H_{d_2} \end{cases}$$

Generally, for $m, n \leq \min\{k \cdot d_1, d_2\}$, we have :

$$P_m = R_1 \circ H_m + \sum_{2\leq l\leq [\frac{m}{k}]} \boxed{R_l \circ (\textstyle\sum_{k\leq j\leq [\frac{m}{l}]} H_j)}_{\,m} (k \nmid m) \quad (6)$$

$$P_n = R_1 \circ H_n + R_{\frac{n}{k}} \circ H_k + \sum_{2\leq l < \frac{n}{k}} \boxed{R_l \circ (\textstyle\sum_{k\leq j\leq [\frac{n}{l}]} H_j)}_{\,n} (k \mid n) \quad (7)$$

where $[\frac{m}{l}]$ denotes the maximal integer not larger than $\frac{m}{l}$.

We will obtain R_1 from the first k equalities $R_1 \circ H_j = P_j (k \leq j \leq 2k-1)$ by decomposing linear differential polynomials with coefficients in $\mathcal{K}$ and get other R_i, H_j by solving linear systems as before. The choice of (d_1, d_2) and the uniqueness of $R(H)$ are almost the same with that in the case $P_1 \neq 0$. When R_1 is given, the uniqueness for H_j ($k \nmid j$) is obvious by (6) and the uniqueness for $R_{\frac{j}{k}}$ and $H_j(k \mid j)$ in (7) is guaranteed by Theorem 4.

Theorem 4. *Let R_1 be a linear differential polynomial and P_{ik} an $i \cdot k$-total degree homogeneous differential polynomial. If there exists an $i-$total degree homogeneous differential polynomial R_i and an $i \cdot k$-total degree homogeneous differential polynomial H_{ik} such that $o_{R_i} < o_{R_1}$ and $P_{ik} = R_1 \circ H_{ik} + R_i \circ H_k$, then they are unique.*

Now we show how to get R_1 from $P_j = R_1 \circ H_j (k \le j \le 2k-1)$. We consider the general problem: *given a total degree homogeneous differential polynomial q ($\mathrm{tdeg}(q) > 1$), how to obtain all enumerations of linear differential polynomial s such that $q = s \circ r$ for some differential polynomial r?* We first prove a lemma.

Lemma 7. *If $l \circ q = u \circ x_m$, where l, q, u are total degree homogeneous, l is linear, $\mathrm{tdeg}(q) > 1$ and m is a positive integer, then there exists a differential polynomial q' such that $q = q' \circ x_m$.*

Assume that q can be decomposed as $q = s \circ r$, where s is linear and r is total degree homogeneous. Let $v = \min\{i : x_i \text{ appears in } q\}$. By Lemma 7, there exists a differential polynomial r' such that $r = r' \circ x_v$, thus $q' = s \circ r'$. So we need only to consider the case of $v = 0$. Let $a = \deg_x q,\ e = \deg_x r, n = o_s$, we can write $q,\ s,\ r$ as follows:

$$q = q_a x^a + \cdots + q_1 x + q_0$$
$$s = s_n x_n + \cdots + s_1 x_1 + s_0 x$$
$$r = r_e x^e + \cdots + r_1 x + r_0$$

where $o_{r_e} \ge 1$ or $r_e = 1 \left(\text{if } r_e \in \mathcal{K}, \text{ then } s \circ r = (s \circ r_e x) \circ (\frac{r}{r_e}) \right)$. We have

$$s \circ r = \begin{cases} (s \circ r_e) x^e + u_2 & o_{r_e} \ge 1 \\ s_0 x^e + \left(s \circ (r_{e-1} + ex) - e s_0 x \right) x^{e-1} + u_3 & r_e = 1 \textit{ and } s_0 \ne 0 \\ \left(s \circ (r_{e-1} + ex) \right) x^{e-1} + u_4 & r_e = 1 \textit{ and } s_0 = 0 \end{cases}$$

where u_1, u_3, u_4 are of degree lower than $e - 1$ in x and u_2 is of degree lower than e in x.

From $q = s \circ r$, we have

1. If $q_a \notin \mathcal{K}$, then s satisfies $s \circ r_e = q_a$ or $s \circ (r_{e-1} + ex) = q_a$. In these cases, s is a linear left decomposition factor of q_a. So, we will find the linear left decomposition factors of q_a.

2. If $q_a \in \mathcal{K}$, then $s_0 = q_a,\ e = a$ and $q_{a-1} = s \circ (r_{e-1} + ex) - e s_0 x$. So $q_{a-1} + a q_a x = s \circ (r_{e-1} + ex)$ and we will consider the decomposition of $q_{a-1} + a q_a x$, which is linear.

The above analysis leads to the following algorithm.

Algorithm 5 *Input: a total degree homogeneous differential polynomial q with $\mathrm{tdeg}(q) > 1$. Output: a set Δ contains all possible enumerations of linear left decomposition factors s of q with $o_s > 0,\ i_s = 1$.*

S1 Let $v = \min\{i : x_i \text{ appears in } q\}$, find q' such that $q = q' \circ x_v$, that is, replace x_i with x_{i-v} in q. Let $a = \deg_x q'$, q_a and q_{a-1} be the coefficient of x^a and x^{a-1} in q' respectively.

S2 If $q_a \in \mathcal{K}$, $\Delta := \{s : s/i_s$ is the left decomposition factor of $q_{a-1} + a q_a x\}$, return.

S3 $q := q_a$. If $\mathrm{tdeg}(q) = 1$, $\Delta := \{s : s$ is the left decomposition factor of q and $i_s = 1$ $\}$, return; else, go to S1.

5 Experimental Results

We implemented the algorithm in Maple for the *constant field case* $\mathcal{K} = \mathbb{Q}$. In Table 1, we generate a differential polynomial randomly and decompose it. All the randomly generated differential polynomials in Table 1 are indecomposable. In Table 2, we generate two differential polynomials g and h randomly and decompose $f = g \circ h$. The running times are collected on a PC with a 1.6G CPU and 128M memory and are given in seconds. In Tables 1 and 2, o_f, t_f, l_f represent the order, the total degree and the number of terms of f respectively. From these results, we may conclude that our algorithm is efficient in handling differential polynomials with hundreds of terms.

(o_f, t_f, l_f)	time(s)	(o_f, t_f, l_f)	time(s)	(o_f, t_f, l_f)	time(s)	(o_f, t_f, l_f)	time(s)
(2,10,32)	0.237	(2, 20, 116)	1.174	(2,30,254)	4.200	(2, 40, 414)	12.938
(2,50,624)	35.021	(3, 10, 102)	2.365	(3, 12,322)	14.078	(3, 15, 368)	11.167
(4, 8,415)	19.786	(4, 10, 555)	32.171	(5, 8,1084)	55.986	(6, 6,596)	68.843
(7, 6,1308)	164.44.	(8, 5, 325)	14.266	(9, 4,415)	19.786	(10, 4, 677)	72.534

Table 1. Decomposing Randomly Generated Differential Polynomials

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)	(1,64,639)	10.079
g_2, h_2	(1,6)	(1,8)	(2,48,1174)	85.640
g_3, h_3	(1,4)	(2,4)	(3,16,458)	38.672
g_4, h_4	(1,4)	(3,2)	(4,8,994)	95.063
g_5, h_5	(1,4)	(3,4)	(4,16,970)	144,467
g_6, h_6	(2,4)	(1,4)	(3,16,1229)	189.109
g_7, h_7	(2,3)	(2,4)	(4,12,1360)	120.093
g_8, h_8	(2,3)	(3,2)	(5,6,709)	90.405
g_9, h_9	(3,2)	(1,4)	(4,8,231)	15.562
g_{10}, h_{10}	(3,2)	(2,4)	(5,8,535)	32.891

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

References

1. X.S. Gao and M.B. Zhang, Decomposition of Differential Polynomials with Rational Function Coefficients, *MM-Preprints*, KLMM, Vol, 23, 92-112, 2004.
2. W.T. Wu, *Basic Principles of Mechanical Theorem Proving in Geometries*, Springer, Berlin, 1995.

3. S.P. Tsarev, An Algorithm for Complete Enumeration of all Factorizations of a Linear Ordinary Differential Operator, *ISSAC'96*, 226-231, ACM Press, 1996.
4. J. von zue Gathen, Functional Decomposition of Polynomials: the Tame Case. *Journal of Symbolic Computation*, 9, 281-299, 1990.
5. M. Zhang, *Theories and Algorithms for Ordinary Differential and Difference Polynomials Decomposition*, thesis, KLMM, CAS, 2006.