A Triangular Decomposition Algorithm for Differential Polynomial Systems with Elementary Computation Complexity*

ZHU Wei · GAO Xiao-Shan

DOI: 10.1007/s11424-016-5040-5
Received: 11 February 2015 / Revised: 12 May 2015

Abstract In this paper, a new triangular decomposition algorithm is proposed for ordinary differential polynomial systems, which has triple exponential computational complexity. The key idea is to eliminate one algebraic variable from a set of polynomials in one step using the theory of multivariate resultant. This seems to be the first differential triangular decomposition algorithm with elementary computation complexity.

Keywords Differential polynomial system, regular triangular set, saturated triangular set, triangular decomposition.

1 Introduction

A basic problem in symbolic computation is to properly describe the solutions for a set of algebraic or differential polynomial equations and the triangular set is one of the basic ways to do that. Let $f_1, f_2, \cdots, f_s$ be polynomials in variables $x_1, x_2, \cdots, x_n$. Then it is possible to compute triangular sets $\mathcal{T}_1, \mathcal{T}_2, \cdots, \mathcal{T}_r$ such that

$$\mathrm{Zero}(f_1, f_2, \cdots, f_s) = \cup_{i=1}^r \mathrm{Zero}(\mathrm{sat}(\mathcal{T}_i)),$$

where $\mathrm{sat}(\mathcal{T}_i)$ is the saturation ideal to be defined in Section 2 of this paper. Since each $\mathcal{T}_i$ is in triangular form, many properties of its solution set can be easily deduced. Triangular decompositions also lead to many important applications such as automated theorem proving, kinematic analysis of robotics, computer vision, stability analysis of molecular systems, etc.

The concept of triangular set was introduced by Ritt[1] in the 1950s and was revised in the 1980s by Wu[2] in his work of automated geometry theorem proving. A major advantage

ZHU Wei · GAO Xiao-Shan
Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, *China.* Email: zhuwei210@mails.ucas.ac.cn; xgao@mmrc.iss.ac.cn.

*This research was supported by the National Natural Science Foundation of China under Grant No. 60821002 and the National Key Basic Research Project of China.
◇ *This paper was recommended for publication by Editor LI Hongbo.*

of the triangular decomposition method is that it can be used to give complete methods for the radical ideal membership problem of differential and difference polynomial ideals, while the well known Gröbner basis method does not suit for this purpose. By now, various kinds of triangular decomposition algorithms have been proposed for various equation systems such as polynomial systems[2–5], differential polynomial systems[6–11], difference polynomial systems[12], polynomial systems over finite fields[13–15], and semi-algebraic sets[16].

The computational complexity analysis for triangular decomposition algorithms is quite difficult and only very limited results are known. For polynomial systems, Gallo and Mishra gave a single exponential algorithm to compute the characteristic set for a finitely generated ideal[17] and Szanto gave a randomized single exponential algorithm to compute the triangular decomposition[4]. The complexity analysis of the commonly used triangular decomposition algorithms is not given yet. However, it is shown that if solutions in $\mathbb{Z}_2$ are considered, then the commonly used triangular decomposition algorithm can be made single exponential and practically very efficient[13]. For differential polynomial systems, it is generally believed that the commonly used triangular decomposition algorithms have non-elementary computational complexity[18].

In this paper, new triangular decomposition algorithms are proposed for polynomial and differential polynomial systems. The key idea is to eliminate one algebraic variable from a set of polynomials in one step using the theory of multivariate resultant. This method was introduced by Yu Grigor'ev to give a quantifier elimination algorithm with nice computational complexity[19]. In this paper, by adapting this elimination method, we give triangular decomposition algorithms for polynomial and ordinary differential polynomial systems. In the case of polynomial systems, the algorithm gives an unmixed decomposition and has double exponential complexity. In the case of ordinary differential polynomial systems, the algorithm gives an unmixed radical decomposition which has triple exponential complexity. This seems to be the first differential triangular decomposition algorithm with elementary computation complexity.

The rest of this paper is organized as follows. In Section 2, we give a new triangular decomposition algorithm for polynomial systems. In Section 3, we give a new triangular decomposition algorithm for ordinary differential polynomial systems. In Section 4, a summary is given.

2 Decomposition of Algebraic Polynomial System

In this section, we give an algorithm which for given polynomials $h_1, h_2, \cdots, h_k \in \mathbb{K}[x_1, x_2, \cdots, x_n]$, gives the decomposition $\text{Zero}(h_1, h_2, \cdots, h_k) = \cup_q \text{Zero}(\text{sat}(\mathcal{A}_q))$, where $\mathcal{A}_q$ is a regular triangular set for each q. Furthermore, the computational complexity of the algorithm is given.

2.1 Basic Definition and Property

Let $\mathbb{K}$ be a field of characteristic 0, and $x_1 < x_2 < \cdots < x_n$ ordered variables. For every $i \in \{1, 2, \cdots, n\}$, we define $\mathbb{K}_i = \mathbb{K}[x_1, x_2, \cdots, x_i]$ to be the ring of multivariate polynomials in the variables $x_1, x_2, \cdots, x_i$ with coefficients in $\mathbb{K}$. We write $\deg(f, x_i)$ for the degree of f in x_i, and $\deg_{x_{i_1}, x_{i_2}, \cdots, x_{i_t}}(f)$ for the degree of f as the multivariate polynomial in $x_{i_1}, x_{i_2}, \cdots, x_{i_t}$. We call the leading variable of f, denoted by $\text{lv}(f)$, the greatest variable $v \in \{x_1, x_2, \cdots, x_n\}$

such that $\deg(f, v) > 0$.

Assuming $\mathrm{lv}(f) = x_i$, we call i the class of f, denoted by $\mathrm{cls}(f)$. Regarding f as a univariate polynomial in $\mathbb{K}_{i-1}[x_i]$, we can write $f = cx_i^d + r$. We call $d = \deg(f, x_i)$ the leading degree of f, denoted by $\mathrm{ldeg}(f)$, and c the initial of f, denoted by $\mathrm{ini}(f)$ or I_f.

Let $\mathbb{P}$ be a polynomial set and D a polynomial in $\mathbb{K}_n$. For an algebraic closed extension field $\mathbb{E}$ of $\mathbb{K}$, let

$$\mathrm{Zero}(\mathbb{P}/D) = \{\eta \in \mathbb{E}^n \,|\, \forall P \in \mathbb{P}, P(\eta) = 0 \wedge D(\eta) \neq 0\}.$$

A subset $\mathcal{T}$ of $\mathbb{K}_n$ is called a triangular set if no element of $\mathcal{T}$ lies in $\mathbb{K}$ and for $P, Q \in \mathcal{T}$ with $P \neq Q$ we have $\mathrm{lv}(P) \neq \mathrm{lv}(Q)$.

Let $\mathcal{T} = \{T_1, T_2, \cdots, T_r\}$ be a triangular set. We always assume $\mathrm{lv}(T_1) < \mathrm{lv}(T_2) < \cdots < \mathrm{lv}(T_r)$. We can rename the variables as $u_1, u_2, \cdots, u_q, y_1, y_2, \cdots, y_r$ such that $q + r = n$ and $\mathrm{lv}(T_i) = y_i$. Then$\mathcal{T}$ has the following form:

$$\mathcal{T} = \left\{ \begin{array}{l} T_1(u_1, u_2, \cdots, u_q, y_1) \\ T_2(u_1, u_2, \cdots, u_q, y_1, y_2) \\ \qquad\vdots \\ T_r(u_1, u_2, \cdots, u_q, y_1, y_2, \cdots, y_r) \end{array} \right\}. \tag{1}$$

We call $\boldsymbol{u} = \{u_1, u_2, \cdots, u_q\}$ the parameter set of $\mathcal{T}$, and write $I_{\mathcal{T}} = I_{T_1} I_{T_2} \cdots I_{T_r}$. For a triangular set $\mathcal{T}$, the saturation ideal of $\mathcal{T}$ is defined to be

$$\mathrm{sat}(\mathcal{T}) = \{f \in \mathbb{K}_n \,|\, \exists d \in \mathbb{N}^+, \text{ s.t. } I_{\mathcal{T}}^d f \in (\mathcal{T})\},$$

where (T) is the ideal generated by $\mathcal{T}$.

A triangular set $\mathcal{T} = [T_1, T_2, \cdots, T_r]$ of form (1) is called regular, if for each $1 \leq i \leq r$, $(T_1, T_2, \cdots, T_{i-1}, \mathrm{ini}(T_i)) \bigcap \mathbb{K}[\boldsymbol{u}] \neq \{0\}$ where $(T_1, T_2, \cdots, T_{i-1}, \mathrm{ini}(T_i))$ is the ideal generated by $T_1, T_2, \cdots,$ $T_{i-1}, \mathrm{ini}(T_i)$ and $\boldsymbol{u}$ is the parameter set of $\mathcal{T}$.

Lemma 2.1 (see [20]) *For a triangular set $\mathcal{T}$, we have*

$$\sqrt{\mathrm{sat}(\mathcal{T})} = \bigcap_{i=1}^{t} \mathrm{sat}(\mathcal{T}_i),$$

where $\mathcal{T}_i$ are regular triangular sets having the same parameter set as $\mathcal{T}$, and $\mathrm{sat}(\mathcal{T}_i)$ is a prime ideal. That is, $\mathrm{sat}(\mathcal{T})$ is an unmixed ideal.

Lemma 2.2 *Let $\mathcal{T} = \{T_1, T_2, \cdots, T_r\}$ be a regular triangular set, $\boldsymbol{u}$ its parameter set, y_i the leading variable of T_i, P a polynomial in $\mathbb{K}[\boldsymbol{u}, y_1, y_2, \cdots, y_r]$. Then $(P, \mathcal{T}) \bigcap \mathbb{K}[\boldsymbol{u}] \neq \{0\}$ if P is not identically zero on all irreducible components of $\mathrm{Zero}(\mathrm{sat}(\mathcal{T}))$.*

Proof According to Lemma 2.1, $\sqrt{\mathrm{sat}(\mathcal{T})} = \bigcap_{i=1}^{t} \mathrm{sat}(\mathcal{G}_i)$. Since P is not identically zero on all irreducible component of $\mathrm{Zero}(\mathrm{sat}(\mathcal{T}))$, we have $P \notin \mathrm{sat}(\mathcal{G}_i)$ for each i. Since $\mathrm{sat}(\mathcal{G}_i)$ is prime, so $(P, \mathcal{G}_i) \bigcap \mathbb{K}(\boldsymbol{u}) \neq \{0\}$ for each i. Suppose that $\mathcal{G}_i = (G_{i,1}, G_{i,2}, \cdots, G_{i,r})$, then we have the following equalities:

$$\begin{aligned}
&S_{1,1}G_{1,1}+\cdots+S_{1,r}G_{1,r}=A_1P+h_1(\boldsymbol{u}),\\
&S_{2,1}G_{2,1}+\cdots+S_{2,r}G_{2,r}=A_2P+h_2(\boldsymbol{u}),\\
&\quad\vdots\\
&S_{t,1}G_{t,1}+\cdots+S_{t,r}G_{t,r}=A_tP+h_t(\boldsymbol{u}).
\end{aligned}$$

Multiply all the equalities. Since the left hand side of the i-th equality belongs to $\mathrm{sat}(\mathcal{G}_i)$, the product of them belongs to $\sqrt{\mathrm{sat}(\mathcal{T})}$. The product of the right hand side is of the form $AP+h$ for $h=h_1h_2\cdots h_t$. Then we have $h\in(P,\sqrt{\mathrm{sat}(\mathcal{T})})\bigcap\mathbb{K}[\boldsymbol{u}]\neq\{0\}$. Therefore, there exists an integer d_1 such that $(h)^{d_1}\in(P,\mathrm{sat}(\mathcal{T}))$. There exists an integer d_2 s.t. $(\mathrm{ini}(T_1)\mathrm{ini}(T_2)\cdots\mathrm{ini}(T_r))^{d_2}(h)^{d_1}\in(P,\mathcal{T})$. Since $\mathcal{T}$ is regular, we have $(\mathrm{ini}(T_i),\mathcal{T})\bigcap\mathbb{K}[\boldsymbol{u}]\neq\{0\}$, and then the following equality

$$(\mathrm{ini}(T_1)\mathrm{ini}(T_2)\cdots\mathrm{ini}(T_r))^{d_2}F_0=g(\boldsymbol{u})+F_1T_1+F_2T_2+\cdots+F_rT_r,$$

where $g\neq0$ and $g\in\mathbb{K}[\boldsymbol{u}]$. Hence, $(h)^{d_1}g\in(P,\mathcal{T})$ and $(P,\mathcal{T})\bigcap\mathbb{K}[\boldsymbol{u}]\neq\{0\}$. ∎

As a consequence of Lemma 2.2, we have:

Corollary 2.1 *A triangular set $\mathcal{T}=\{T_1,T_2,\cdots,T_r\}$ is regular if for each $2\leq i\leq r$, $\mathrm{ini}(T_i)$ is not identically zero on all irreducible components of $\mathrm{sat}(T_1,T_2,\cdots,T_{i-1})$.*

Lemma 2.3 *Let $\mathcal{T}=\{T_1,T_2,\cdots,T_r\}$ be a regular triangular set with parameter set $\boldsymbol{u}$. If $M\in\mathbb{K}[\boldsymbol{u}]$, then $\overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})}=\overline{\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})}$, where $\overline{\mathbb{S}}$ is the Zariski closure of $\mathbb{S}$.*

Proof We first prove the lemma when $\mathrm{sat}(\mathcal{T})$ is prime. Introduce a new variable z and let $I=I_{\mathcal{T}}$. We have

$$\mathrm{Zero}(\mathcal{T}/MI)=\mathrm{Zero}(\mathcal{T},MIz-1)\cap\mathbb{E}^n.$$

So for any $f\in\mathbb{I}(\mathrm{Zero}(\mathcal{T}/MI))$ ($\mathbb{I}(V)$ is the ideal of polynomials which vanish on V), $f\in\sqrt{(\mathcal{T},MIz-1)}$. Let $z=\frac{1}{MI}$, then there exists an integer d such that $(MIf)^d\in(\mathcal{T})$, so we have $(Mf)^d\in\mathrm{sat}(\mathcal{T})$. Since $\mathrm{sat}(\mathcal{T})$ is prime and $M\in\mathbb{K}[\boldsymbol{u}]$ so not in $\mathrm{sat}(\mathcal{T})$, we have $f\in\mathrm{sat}(\mathcal{T})$. So we have $\overline{\mathrm{Zero}(\mathcal{T}/MI)}\supset\mathrm{Zero}(\mathrm{sat}(\mathcal{T}))=\overline{\mathrm{Zero}(\mathcal{T}/I)}$. It is obvious $\overline{\mathrm{Zero}(T_1,T_2,\cdots,T_r/MI)}\subset\overline{\mathrm{Zero}(\mathcal{T}/I)}$, so we have $\overline{\mathrm{Zero}(\mathcal{T}/MI)}=\overline{\mathrm{Zero}(\mathcal{T}/I)}$. Now assuming $\mathrm{sat}(\mathcal{T})$ is not prime. According to Theorem 1.3 in [20], we have $\mathrm{Zero}(\mathcal{T}/I)=\bigcup_{i=1}^t\mathrm{Zero}(\mathcal{G}_i/I_i)$, where $\mathcal{G}_i$ is a regular triangular set having the same parameter set with $\mathcal{T}$ and $\mathrm{sat}(\mathcal{G}_i)$ is prime for each i. Then we have

$$\overline{\mathrm{Zero}(\mathcal{T}/MI)}=\bigcup_{i=1}^t\overline{\mathrm{Zero}(\mathcal{G}_i/I_iM)}=\bigcup_{i=1}^t\overline{\mathrm{Zero}(\mathcal{G}_i/I_i)}=\overline{\mathrm{Zero}(\mathcal{T}/I)}$$

and the lemma is proved. ∎

Lemma 2.4 *Let $\mathcal{T}=\{T_1,T_2,\cdots,T_r\}$ be a regular triangular set. If M is not identically zero on all irreducible components of $\mathrm{sat}(\mathcal{T})$, then $\mathrm{Zero}(\mathrm{sat}(\mathcal{T}))=\overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})}=\overline{\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})}$, where $\overline{\mathbb{S}}$ is the Zariski closure of $\mathbb{S}$.*

Proof It is well known that $\mathrm{Zero}(\mathrm{sat}(\mathcal{T})) = \overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})}$. Then $\overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})} \supset \overline{\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})}$, since $\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}}) \supset \mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})$. Let $\boldsymbol{u}$ be the parameter set of $\mathcal{T}$, since M is not identically zero on all irreducible components of $\mathcal{T}$, according to Lemma 2.2, we have $(M, \mathcal{T}) \bigcap \mathbb{K}[\boldsymbol{u}] \neq \{0\}$. Suppose

$$AM + A_1T_1 + \cdots + A_rT_r = H(\boldsymbol{u}). \tag{2}$$

Let ξ be a zero of $\mathrm{Zero}(\mathcal{T}/HI_{\mathcal{T}})$. Substituting ξ into (2), we have $M(\xi) \neq 0$, so ξ is also a zero of $\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})$ and we have $\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}}) \supset \mathrm{Zero}(\mathcal{T}/HI_{\mathcal{T}})$. Since $H \in \mathbb{K}[\boldsymbol{u}]$, so according to Lemma 2.3, we have $\overline{\mathrm{Zero}(\mathcal{T}/HI_{\mathcal{T}})} = \overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})}$. Therefore, we have $\overline{\mathrm{Zero}(\mathcal{T}/MI_{\mathcal{T}})} \supset \overline{\mathrm{Zero}(\mathcal{T}/HI_{\mathcal{T}})} = \overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}})}$. This completes the proof. ▮

2.2 A Quasi GCD Algorithm

We need to use Lemma 1 of [19], which is modified slightly to the following form.

Lemma 2.5 (see [19]) *There is an algorithm which for given polynomials $h_i = \sum h_{i,j}Y^j \in \mathbb{K}_n[Y]$, $\deg_{x_1,x_2,\cdots,x_n,Y}(h_i) < d, i = 0, 1, \cdots, k$, yields such two families of polynomials $g_{q,t} \in \mathbb{K}_n$, $\Psi_q \in \mathbb{K}_n[Y]$ for $1 \leq q \leq N_1, 0 \leq t \leq N_2$ such that*

$$\begin{aligned}\mathrm{Zero}(h_1, h_2, \cdots, h_k/h_0) = & \bigcup_{q=1}^{N_1} \mathrm{Zero}(\Psi_q, g_{q,1}, \cdots, g_{q,N_2}/g_{q,0}) \\ & \bigcup \mathrm{Zero}(\{h_{i,j}, \quad i = 0, 1, \cdots, k, j = 0, 1, \cdots, d-1\}/h_0).\end{aligned}$$

Furthermore, we have the following properties:

1) $\deg(\Psi_q, Y) > 0, \mathrm{ini}(\Psi_q) \mid g_{q,0}$.

2) $\deg_{x_1,x_2,\cdots,x_n,Y}(\Psi_q), \deg_{x_1,\cdots,x_n}(g_{q,t}) \leq \mathcal{P}(d); N_1, N_2 \leq k\mathcal{P}(d^n)$ *where $\mathcal{P}(k)$ means a polynomial in k.*

3) *The running time of the algorithm can be bounded by a polynomial in k and d^n.*

Now, we describe the main steps of this algorithm without proof. One can refer to [19] for more details. Without loss of generality, we assume that $\deg_Y(h_i) > 0$ for $0 \leq i \leq k$.

Since $\deg_{x_1,x_2,\cdots,x_n,Y}(h_i) < d$, we have $h_i = \sum_{j=0}^{d-1} h_{i,j}Y^j$. Let $\widetilde{h}_{i,j} = \sum_{\beta=0}^{j} h_{i,\beta}Y^\beta$ and

$$U_{i,j} = \mathrm{Zero}(h_{1,d-1}, \cdots, h_{1,0}, h_{2,d-1}, \cdots, h_{2,0}, \cdots, h_{i,d-1}, \cdots, h_{i,j+1}/h_{i,j})$$

for $1 \leq i \leq k$, $0 \leq j \leq d-1$. Let $H = \{h_1, h_2, \cdots, h_k\}$,

$$\begin{aligned} H_{i,j} &= \{\widetilde{h}_{i,j}, h_{i+1}, \cdots, h_k\}, \\ H_{k+1} &= \{h_{i,j}, \quad \forall\, 1 \leq i \leq k \text{ and } j\}. \end{aligned} \tag{3}$$

Then we have $\mathrm{Zero}(H/h_0) = \mathrm{Zero}(H_{k+1}/h_0) \bigcup (\bigcup_{1 \leq i \leq k, 0 \leq j \leq d-1} \mathrm{Zero}(H_{i,j}/h_0) \cap U_{i,j})$.

Now we turn to the system $H_{i,j}$ and introduce new variables Y_0, Y_1 to make polynomials in (3) homogeneous in Y, Y_0, Y_1. Let

$$\begin{aligned}\overline{h}_i &= Y_0^j \widetilde{h}_{i,j}\Big(x_1, x_2, \cdots, x_n, \frac{Y}{Y_0}\Big),\\ \overline{h}_l &= Y_0^{\mathrm{ldeg}(h_l)} h_l\Big(x_1, x_2, \cdots, x_n, \frac{Y}{Y_0}\Big), \quad i+1 \le l \le k,\\ \overline{h}_0 &= Y_0^{\mathrm{ldeg}(h_0)+1}\Big(\frac{Y_1}{Y_0} h_0(x_1, x_2, \cdots, x_n, \frac{Y}{Y_0}) - 1\Big).\end{aligned}$$

Then $\overline{h}_0, \overline{h}_i, \cdots, \overline{h}_k$ are homogeneous polynomials in Y, Y_0, Y_1. The solutions of the following homogenous system correspond bijectively to that of (3) except $(1:0:0)$.

$$\overline{h}_i = \overline{h}_{i+1} = \cdots = \overline{h}_k = \overline{h}_0. \tag{4}$$

Here $\overline{h}_0, \overline{h}_i, \cdots, \overline{h}_k$ are considered as polynomials in Y, Y_0, Y_1.

Introduce new variables U_0, U, U_1 and let $h_{k+1} = Y_0 U_0 + YU + Y_1 U_1$. We rearrange the polynomials $\overline{h}_0, \overline{h}_i, \cdots, \overline{h}_k$ w.r.t the degree in Y, Y_0, Y_1 as $g_0, g_1, \cdots, g_{k-i+2}$ and $\gamma_0 \ge \gamma_1 \ge \cdots \ge \gamma_{k-i+2}$ where $\deg_{Y,Y_0,Y_1}(g_s) = \gamma_s$ for $0 \le s \le k-i+2$. Since $\deg_{Y,Y_0,Y_1}(h_{k+1}) = 1$, we can assume that g_{k-i+2} is h_{k+1}. Let

$$D = \Big(\sum_{1 \le l \le \min\{2, k-i+1\}} (\gamma_l - 1)\Big) + \gamma_0.$$

We construct the Macaulay matrix A as the representation of the linear map

$$\mathcal{A} : \mathcal{H}_0 \oplus \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_{k-i+2} \to \mathcal{H},$$

where $\mathcal{H}_l$ (respectively $\mathcal{H}$) is the linear space of homogenous polynomials in Y, Y_0, Y_1 of degree $D - \gamma_l$ (respectively D) for $0 \le l \le k-i+2$, and

$$\mathcal{A}(f_0, f_1, \cdots, f_{k-i+2}) = f_0 g_0 + f_1 g_1 + \cdots + f_{k-i+2} g_{k-i+2}.$$

The matrix A is of size $C_{D+2}^2 \times \sum_{l=0}^{k-i+2} C_{D-\gamma_l+2}^2$ and can be represented in a form $A = (A^{(\mathrm{num})}, A^{(\mathrm{for})})$, where the elements of the submatrix $A^{(\mathrm{num})}$ do not contain U, U_0, U_1. Actually, $A^{(\mathrm{num})}$ is the submatrix of A which corresponds to the basis of $\mathcal{H}_0, \mathcal{H}_1, \cdots, \mathcal{H}_{k-i+1}$ while $A^{(\mathrm{for})}$ corresponds to the basis of $\mathcal{H}_{k-i+2}$.

About the polynomial system (4), we have the following lemma.

Lemma 2.6 (see [19]) *The rank of the matrix A of the polynomial system* (4) *is $r = C_{D+2}^2$. Let Δ be a nonsingular $r \times r$ submatrix of A containing* $\mathrm{rank}(A^{(\mathrm{num})})$ *columns in $A^{(\mathrm{num})}$. Then*

$$\det(\Delta) = c \prod_{i=1}^{D_1} L_i, \quad \textit{where } L_i = \xi_{i,0} U_0 + \xi_i U + \xi_{i,1} U_1 \textit{ and } c \textit{ is a constant},$$

where $(\xi_{i,0} : \xi_i : \xi_{i,1})$ is a solution of (4) *and the number of occurrences of $\xi_{i,0} U_0 + \xi_i U + \xi_{i,1} U_1$ in the product coincides with the multiplicity of the solution $(\xi_{i,0} : \xi_i : \xi_{i,1})$ of* (4).

Algorithm 1 — Quasi GCD Algorithm

Input $\{\{h_1, h_2, \cdots, h_k\}, h_0, Y\}$ where $h_0, h_1, \cdots, h_k \in \mathbb{K}_n[Y]$ and $h_i = \sum h_{i,j}Y^j$ for $i = 1, 2, \cdots, k, j = 0, 1, \cdots, d-1$.

Output $\mathbb{D} = \{\mathcal{T}_0, \mathcal{T}_1, \cdots, \mathcal{T}_{N_1}\}$, where $\mathcal{T}_0 = \{\{\}, \{h_{i,j}, 1 \le i \le k, 0 \le j < d\}, \{h_0\}\}$, $\mathcal{T}_q = \{\{\varPsi_q\}, \{g_{q,1}, g_{q,2}, \cdots, g_{q,N_2}\}, \{g_{q,0}\}\}$ $(1 \le q \le N_1)$, such that

$$\text{Zero}(h_1, h_2, \cdots, h_k/h_0) = \bigcup_{q=0}^{N_1} \text{Zero}(\varPsi_q, g_{q,1}, \cdots, g_{q,N_2}/g_{q,0}),$$

where $\varPsi_0 = 0$, $\deg(\varPsi_q, Y) > 0$, and $\deg(g_{q,i}, Y) = 0$ for $1 \le q \le N_1$, $0 \le i \le N_2$.

To find the Δ in Lemma 2.6, we use a variant of Gaussian algorithm which will compute a series of

$$\mathcal{W}_s = \{\boldsymbol{x} \in \mathbb{K}^n : P_1 = \cdots = P_{s-1} = 0, P_s \ne 0\}, \tag{5}$$

where $P_1, P_2, \cdots, P_s$ are polynomials in $\boldsymbol{x}, U, U_0, U_1$ and linearly independent. For $\boldsymbol{x} \in \mathcal{W}_s \cap U_{i,j}$, the determinant

$$\Delta_s = \sum_{i=0}^{D_2} E_s^{(i)} U_0^{D_2 - i} \tag{6}$$

is what we want. For more details about the variant Gaussian algorithm, one can refer to [19].

Now, we introduce the following quasiprojective varieties:

$$\mathcal{W}_s^{(l)} = \{\boldsymbol{x} \in \mathcal{W}_s : E_s^{(0)} = E_s^{(1)} = \cdots = E_s^{(l-1)} = 0, E_s^{(l)} \ne 0\}, \tag{7}$$

where $E_s^{(0)}, E_s^{(1)}, \cdots, E_s^{(l-1)}$ are polynomials in $\boldsymbol{x}, U, U_1$. In [19], it is proved that if we substitute $U_1 = 0, U = -1, U_0 = Y$ into $\frac{\Delta_s}{E_s^{(l)}}$, and denote the polynomial as $\varPsi_s$, then for each point $\boldsymbol{x} \in \mathcal{W}_s^{(l)} \cap U_{i,j}$, the solution of $\varPsi_s$ as a polynomial in Y is the solution of the polynomial system (3). Since the quasiprojective varieties $\mathcal{W}_s^{(l)} \cap U_{i,j}$ can be divided into a series of polynomial systems $V_t = \text{Zero}(g_{t,1}, g_{t,2}, \cdots, g_{t,N_2}/g_{t,0})$, we have

$$\text{Zero}(H_{i,j}) \cap U_{i,j} = \bigcup_t \text{Zero}(\varPsi_t, g_{t,1}, g_{t,2}, \cdots, g_{t,N_2}/g_{t,0}).$$

If $\varPsi_t = 1$, we can delete that component and finally obtain the decomposition in Lemma 2.5.

Now, we write this procedure as an algorithm to be used in the rest of the paper.

Example 2.7 We use a simple example to explain the algorithm. Let the original polynomial system be $\{Y^2 + Y/Y\}$. First, we introduce a new variable Y_1 and get an equivalence system $\{Y^2 + Y, Y_1Y - 1\}$. Second, we introduce a new variable Y_0 to make it homogeneous $\{Y^2 + YY_0, Y_1Y - Y_0^2\}$. Finally, we introduce U, U_0, U_1 and add $YU + Y_0U_0 + Y_1U_1$ to the homogeneous system. The matrix A corresponding to the homogeneous system is

$$A = \begin{bmatrix} 1&0&0&0&0&0&U&0&0&0&0&0 \\ 0&0&0&0&-1&0&0&U_0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&U_1&0&0&0 \\ 0&1&0&-1&0&0&0&U&0&U_0&0&0 \\ 0&0&0&0&0&1&0&0&U&0&U_1&0 \\ 0&0&0&0&0&0&0&0&U_0&0&0&U_1 \\ 1&1&0&0&0&0&U_0&0&0&U&0&0 \\ 0&0&1&1&0&0&U_1&0&0&0&U&0 \\ 0&0&0&0&0&-1&0&U_1&0&0&0&U_0 \\ 0&0&1&0&1&0&0&0&0&U_1&U_0&U \end{bmatrix}.$$

$A^{(\mathrm{num})}$ is the submatrix of A formed by the first 6 columns, $\mathrm{rank}(A^{(\mathrm{num})}) = 6$. According to Lemma 2.6, we must choose the first 6 columns and by calculating we find the submatrix formed by the first 9 columns and the last column is nonsingular, which is

$$\Delta = \begin{bmatrix} 1&0&0&0&0&0&U&0&0&0 \\ 0&0&0&0&-1&0&0&U_0&0&0 \\ 0&0&0&0&0&0&0&0&U_1&0 \\ 0&1&0&-1&0&0&0&U&0&0 \\ 0&0&0&0&0&1&0&0&U&0 \\ 0&0&0&0&0&0&0&0&U_0&U_1 \\ 1&1&0&0&0&0&U_0&0&0&0 \\ 0&0&1&1&0&0&U_1&0&0&0 \\ 0&0&0&0&0&-1&0&U_1&0&U_0 \\ 0&0&1&0&1&0&0&0&0&U \end{bmatrix}.$$

$\det(\Delta) = -U_1^3(U - U_0 + U_1)$. Substituting $U_1 = 0, U = -1, U_0 = Y$ to $U - U_0 + U_1$, we obtain the polynomial $-1 - Y$ and $\mathrm{Zero}(Y^2 + Y/Y) = \mathrm{Zero}(Y + 1)$.

The components of Lemma 2.5 may be empty, as shown by the following example.

Example 2.8 Let $h_1 = xy + 1, h_2 = x$, and take y as the maximal variable. According to Lemma 2.5, it can be divided into two components $\mathrm{Zero}(1, x)$ and $\mathrm{Zero}(xy + 1, x/x)$. We can delete the first component. However, we cannot delete the second component $\mathrm{Zero}(xy+1, x/x)$ which is empty. The second component will be deleted in our main algorithm later when we continue our procedure to $\mathrm{Zero}(x/x)$.

2.3 The Decomposition Algorithm

We now give the main result about polynomial systems.

Algorithm 2 — Algebraic Triangular Decomposition

```
Input $\{h_1, h_2, \cdots, h_k\}$, where $h_1, h_2, \cdots, h_k \in \mathbb{K}[x_1, x_2, \cdots, x_n]$.
Output $\mathbb{R}$, which is the set of $(\mathcal{A}_q, D_q)$ and $\mathcal{A}_q = \{\Psi_{q,1}, \Psi_{q,2}, \cdots \Psi_{q,l_q}\}$. $\Psi_{q,i}, D_q \in \mathbb{K}_n$ for
        $1 \le q \le N, 1 \le i \le l_q$ such that $\mathcal{A}_q$ are regular triangular sets, $\mathrm{ini}(\Psi_{q,i}) \ne 0$ on any
        element of $\mathrm{Zero}(\mathcal{A}_q/D_q)$, and $\mathrm{Zero}(h_1, h_2, \cdots, h_k) = \cup_q \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_q))$.
1) Let $\mathcal{T} = \{\{\}, \{h_1, h_2, \cdots, h_k\}, \{\}\}$, $\mathbb{S} = \{\mathcal{T}\}$, $\mathbb{R} = \{\}$.
2) If $\mathbb{S} = \emptyset$ output $\mathbb{R}$, else let $\mathcal{T} = \{\mathbb{F}, \mathbb{P}, \mathbb{N}\} \in \mathbb{S}$, and $\mathbb{S} = \mathbb{S} \setminus \{\mathcal{T}\}$.
3) If $|\mathbb{F}| > k$, go to Step 2.
4) If $\mathbb{P} = \emptyset$, add $(\mathbb{F}, \prod_{p\in\mathbb{N}} p)$ to $\mathbb{R}$ and go to Step 2.
5) Let $x_\gamma = \max_{h\in\mathbb{P}} \mathrm{lv}(h)$, $\widetilde{\mathbb{P}} = \{h \in \mathbb{P} \,|\, \mathrm{lv}(h) = x_\gamma\}$, $\mathbb{P} = \mathbb{P} \setminus \widetilde{\mathbb{P}}$.
6) Let $\widetilde{\mathbb{N}} = \{f \in \mathbb{N} \,|\, \mathrm{lv}(f) \le x_\gamma\}$, $H = \prod_{f\in\widetilde{\mathbb{N}}} f$.
7) Apply Algorithm 1 to $\{\widetilde{\mathbb{P}}, H, x_\gamma\}$, and let the output be $\mathbb{D}$.
8) If $\mathbb{D} = \emptyset$, go to Step 2, else let $\mathcal{T}_1 = \{\mathbb{W}, \mathbb{U}, \mathbb{V} = \{v\}\} \in \mathbb{D}$, $\mathbb{D} = \mathbb{D} \setminus \{\mathcal{T}_1\}$.
9) Let $\mathbb{U} = \mathbb{U} \cup \mathbb{P}$, $x_\eta = \max_{f\in\mathbb{U}} \mathrm{lv}(f)$.
10) If $\mathrm{lv}(v) \le x_\eta$ or $\mathbb{U} = \emptyset$, add $\{\mathbb{F} \cup \mathbb{W}, \mathbb{U}, \mathbb{N} \cup \mathbb{V}\}$ to $\mathbb{S}$.
11) If $\mathrm{lv}(v) > x_\eta$, write $v = \Sigma l_\alpha \boldsymbol{x}^\alpha$ as a multivariate polynomial in $\boldsymbol{x} = (x_\eta, \cdots, x_\gamma)$ with
coefficients in $\mathbb{K}[x_1, x_2, \cdots, x_{\eta-1}]$. Add $\{\mathbb{F} \cup \mathbb{W}, \mathbb{U}, \mathbb{N} \cup \mathbb{V} \cup \{l_\alpha\}\}$ to $\mathbb{S}$ for each $\alpha$. Go to Step 8.
```

Theorem 2.9 *For a given polynomial system $H = \{h_1, h_2, \cdots, h_k\} \in \mathbb{K}_n$, $\deg(h_i) < d$ for $1 \le i \le k$, there is an algorithm to compute regular triangular sets $\mathcal{A}_q = [\Psi_{q,1}, \Psi_{q,2}, \cdots, \Psi_{q,l_q}]$ which have the following properties:*

1) $\mathrm{Zero}(H) = \cup_{q=1}^{N} \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_q))$ *is an unmixed decomposition.*

2) *The degrees of $\Psi_{q,1}, \Psi_{q,2}, \cdots, \Psi_{q,l_q}$ are less than d^{c^n}, $N \le k^n d^{nc^{n+2}}$, where c is a constant.*

3) *The running time of the algorithm can be bounded by a polynomial in k^n and $d^{nc^{n+2}}$.*

Using the algorithm described below, we can calculate the regular triangular sets $\mathcal{A}_q$ which satisfy the properties in Theorem 2.9.

Example 2.10 A simple example is used to explain the algorithm. Let $f = xyz + 1, g = x^2 + x$, $x < y < z$. In Step 5), $x_\gamma = z$ and $\widetilde{\mathbb{P}} = \{f\}$. In Step 7), applying Algorithm 1 to $\widetilde{\mathbb{P}}$, the output is $\mathbb{D}_1 = \{\mathcal{T}_1\}$ where $\mathcal{T}_1 = \{\{xyz + 1\}, \{\}, \{xy\}\}$. In Step 9), we have $\mathbb{U} = \{x^2 + x\}$, $x_\eta = x$. Since $lv(xy) = y > x$, we execute Step 11) and add $\{\{xyz + 1\}, \{x^2 + x\}, \{xy, x\}\}$ to $\mathbb{S}$ and go to Step 2). Now we have $\mathcal{T} = \{\mathbb{F}, \mathbb{P}, \mathbb{N}\}$, where $\mathbb{F} = \{xyz + 1\}$, $\mathbb{P} = \{x^2 + x\}$, $\mathbb{N} = \{xy, x\}$. In Step 5), we have $x_\gamma = x$, $\widetilde{\mathbb{P}} = \{x^2 + x\}$. In Step 6), we have $\widetilde{\mathbb{N}} = \{x\}$, $H = x$. Applying Algorithm 1 to $\{\widetilde{\mathbb{P}}, H, x\}$, the output is $\{\{x + 1\}, \{\}, \{\}\}$. In Step 10), we add $\{\{xyz + 1, x + 1\}, \{\}, \{xy\}\}$ to $\mathbb{S}$. In Step 4), since $\mathbb{P} = \emptyset$, we add $\{\{xyz + 1, x + 1\}, \{xy\}\}$ to $\mathbb{R}$ and output $\mathbb{R}$. Finally, we have

$$\mathrm{Zero}(xyz + 1, x^2 + x) = \mathrm{Zero}(xyz + 1, x + 1/xy) = \mathrm{Zero}(\mathrm{sat}(xyz + 1, x + 1)).$$

The purpose of Step 11) is to add x to $\mathbb{N}$. Otherwise, we will apply Algorithm 1 to $\{\{x^2 + x\}, xy, x\}$, which does not satisfy the input condition of Algorithm 1 since $x < y$.

Before proving Theorem 2.9, we first prove several lemmas.

Lemma 2.11 *Algorithm* 2 *terminates and each* $\mathcal{A}_q$ *is a triangular set.*

Proof By Lemma 2.5, after Step 7), for any $\{\mathbb{W},\mathbb{U},\mathbb{V}\}\in\mathbb{D}$, we have $\mathrm{lv}(p)<x_\gamma$ for any $p\in\mathbb{U}$. In other words, for any new $\{\mathbb{F},\mathbb{P},\mathbb{N}\}$ added to $\mathbb{S}$ in Steps 10) and 11), the class of the polynomials in $\mathbb{P}$ will be decreased at least by one. Therefore, the algorithm terminates. Also, $\mathbb{W}$ is either empty or $\mathbb{W}=\{p\}$ and $\mathrm{lv}(p)=x_\gamma$, which means $\mathcal{A}_q$ is a triangular set for each q. ▌

Lemma 2.12 *Omitting Step* 3), $\mathrm{Zero}(h_1,h_2,\cdots,h_k)=\cup_{q=1}^{N}\mathrm{Zero}(\mathcal{A}_q/D_q)$, *and* $\mathrm{ini}(\mathit{\Psi}_{q,i})\neq 0$ *on any element of* $\mathrm{Zero}(\mathcal{A}_q/D_q)$.

Proof To show $\mathrm{Zero}(h_1,h_2,\cdots,h_k)=\bigcup_q\mathrm{Zero}(\mathcal{A}_q/D_q)$, it suffices to show that the equality

$$\mathrm{Zero}(h_1,h_2,\cdots,h_k)=\cup_{\{\mathbb{F},\mathbb{P},\mathbb{N}\}\in\mathbb{S}}\mathrm{Zero}\Bigg(\mathbb{F}\cup\mathbb{P}/\prod_{p\in\mathbb{N}}p\Bigg) \tag{8}$$

always holds in the algorithm, and when $\mathbb{P}=\emptyset$ the algorithm returns the required equation. $\mathbb{S}$ is modified in Steps 7), 10) and 11). In Step 7), by Lemma 2.5, $\mathrm{Zero}(\widetilde{\mathbb{P}}/H)=\cup_{\{\mathbb{W},\mathbb{U},\{v\}\}\in\mathbb{D}}\mathrm{Zero}(\{\mathbb{W}\cup\mathbb{U}/v)$. Clearly, after applying Algorithm 1, (8) remains valid when $\widetilde{\mathbb{P}}$ and $\widetilde{\mathbb{N}}$ are properly replaced as in Steps 10) and 11). In Step 1), a special substitution is performed. Let $v=\mathit{\Sigma}l_\alpha\boldsymbol{x}^\alpha$. Then $\mathrm{Zero}(/v)$ is replaced by $\cup_\alpha\mathrm{Zero}(/l_\alpha v)$. Since $\mathrm{Zero}(/v)=\cup_\alpha\mathrm{Zero}(/l_\alpha v)$, (8) is still valid after Step 11).

Now suppose $(\mathit{\Psi}_1,\mathit{\Psi}_2,\cdots,\mathit{\Psi}_t/M)$ is one component of the output. From the procedure of the algorithm, we know that this component is obtained in the following manner:

$$\begin{aligned}\mathrm{Zero}(f_{0,1},f_{0,2},\cdots,f_{0,k^{(0)}}/M_0)&\rightarrow\mathrm{Zero}(\mathit{\Psi}_1,f_{1,1},\cdots,f_{1,k^{(1)}}/M_1)\\&\rightarrow\mathrm{Zero}(\mathit{\Psi}_1,\mathit{\Psi}_2,f_{2,1},\cdots,f_{2,k^{(2)}}/M_1M_2)\\&\rightarrow\cdots\\&\rightarrow\mathrm{Zero}(\mathit{\Psi}_1,\mathit{\Psi}_2,\cdots,\mathit{\Psi}_t/M_1\cdots M_t)\end{aligned}$$

and $M=M_1M_2\cdots M_t$. Note that after applying Algorithm 1, $\mathrm{Zero}(\mathit{\Psi}_1,f_{1,1},f_{1,2},\cdots,f_{1,k^{(1)}}/T_1)$ is a component of $\mathrm{Zero}(f_{0,1},f_{0,2},\cdots,f_{0,k^{(0)}})/M_0)$. If $\mathrm{lv}(v)\le x_\eta$ in Step 10, $M_1=T_1$. Otherwise, M_1 is the multiplication of T_1 and a coefficient l_α of T_1 as shown in step 11. The component $\mathrm{Zero}(\mathit{\Psi}_2,f_{2,1},f_{2,2},\cdots,f_{2,k^{(2)}}/M_2)$ is obtained similarly from $\mathrm{Zero}(f_{2,1},f_{2,2},\cdots,f_{2,k^{(2)}}/S_2)$, where S_2 is the maximal factor of M_1 satisfying $\mathrm{lv}(S_2)\le\mathrm{lv}(f_{2,j})$ for all j. Continuing this procedure, we will obtain (9). It is obvious that

$$\begin{aligned}\mathrm{Zero}(f_{0,1},f_{0,2},\cdots,f_{0,k^{(0)}}/M_0)&\supset\mathrm{Zero}(\mathit{\Psi}_1,f_{1,1},f_{1,2},\cdots,f_{1,k^{(1)}}/M_1)\\&\supset\mathrm{Zero}(\mathit{\Psi}_1,\mathit{\Psi}_2,f_{2,1},\cdots,f_{2,k^{(2)}}/M_1M_2)\\&\supset\cdots\\&\supset\mathrm{Zero}(\mathit{\Psi}_1,\mathit{\Psi}_2,\cdots,\mathit{\Psi}_t/M_1\cdots M_t).\end{aligned} \tag{9}$$

According to (1) of Lemma 2.5, we have $\mathrm{ini}(\mathit{\Psi}_i)|M_i$, so $\mathrm{ini}(\mathit{\Psi}_i)\neq 0$ on any element of $\mathrm{Zero}(\mathit{\Psi}_1,\mathit{\Psi}_2,\cdots,\mathit{\Psi}_t/M)$. ▌

Lemma 2.13 *The triangular sets* $\mathcal{A}_q = \{\mathit{\Psi}_{q,1}, \mathit{\Psi}_{q,2}, \cdots \mathit{\Psi}_{q,l_q}\}$ *are regular and* $\overline{\mathrm{Zero}(\mathcal{A}_q/D_q)} = \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_q))$.

Proof Let $\mathrm{Zero}(\mathit{\Psi}_1, \mathit{\Psi}_2, \cdots, \mathit{\Psi}_t/M)$ be a component of the output. According to the proof of Lemma 2.12, this component comes from Procedure (9). Now we assume that $\mathrm{lv}(\mathit{\Psi}_1) = x_{k_1}, M_1 \in \mathbb{K}_{k_1-1}$, $\mathrm{lv}(\mathit{\Psi}_2) = x_{k_2}, M_2 \in \mathbb{K}_{k_2-1}$, $\cdots$, $\mathrm{lv}(\mathit{\Psi}_t) = x_{k_t}, M_t \in \mathbb{K}_{k_t-1}$.

According to Lemma 2.1, to show that $\mathcal{A}_q$ is regular, it suffices to prove that $\mathrm{ini}(\mathit{\Psi}_i)$ is not always zero on any irreducible component of $\mathrm{sat}(\mathit{\Psi}_{i+1}, \mathit{\Psi}_{i+2}, \cdots, \mathit{\Psi}_t)$ for $1 \le i \le t-1$. We prove this by induction. First, supposing $\mathrm{ini}(\mathit{\Psi}_{t-1})$ is zero on an irreducible component of $\mathrm{sat}(\mathit{\Psi}_t)$. $\mathrm{Zero}(\mathit{\Psi}_t/M_t)$ is a component of $\mathrm{Zero}(f_{t-1,1}, f_{t-1,2}, \cdots, f_{t-1,k^{(t-1)}}/S_{t-1})$ after applying Algorithm 1, where S_{t-1} is a factor of M_{t-1}. Obviously, $\mathrm{Zero}(\mathit{\Psi}_t/M_t)$ is not empty and $\overline{\mathrm{Zero}(\mathit{\Psi}_t/M_t)} = \overline{\mathrm{Zero}(\mathit{\Psi}_t/\mathrm{ini}(\mathit{\Psi}_t))} = \mathrm{Zero}(\mathrm{sat}(\mathit{\Psi}_t))$ since $\mathrm{lv}(M_t) < \mathrm{lv}(\mathit{\Psi}_t)$. Since $\mathrm{ini}(\mathit{\Psi}_{t-1})$ is always zero on an irreducible component of $\mathrm{sat}(\mathit{\Psi}_t)$, there exists an $\eta_{k_t} = (\xi_1, \xi_2, \cdots, \xi_{k_t})$ in $\mathrm{Zero}(\mathit{\Psi}_t/M_t)$ such that $\mathrm{ini}(\mathit{\Psi}_{t-1})(\eta_{k_t}) = 0$. Since $\mathrm{Zero}(f_{t-1,1}, f_{t-1,2}, \cdots, f_{t-1,k^{(t-1)}}/S_{t-1}) \supset \mathrm{Zero}(\mathit{\Psi}_t/M_t)$, $\eta_{k_t} \in \mathrm{Zero}(f_{t-1,1}, f_{t-1,2}, \cdots, f_{t-1,k^{(t-1)}}/S_{t-1})$. If $\mathrm{Zero}(\mathit{\Psi}_t/M_t)$ is obtained from Step 10), then $\eta = \eta_{k_t}$ is also in $\mathrm{Zero}(f_{t-1,1}, f_{t-1,2}, \cdots, f_{t-1,k^{(t-1)}}/M_{t-1})$. Otherwise, $\mathrm{Zero}(\mathit{\Psi}_t/M_t)$ is obtained from Step 11), η_{k_t} can be extended to a zero $\eta = \eta_{k_{t-1}-1}$ of $\mathrm{Zero}(f_{t-1,1}, f_{t-1,2}, \cdots, f_{t-1,k^{(t-1)}}/M_{t-1})$, since S_{t-1} is a coefficient of M_{t-1}. So in each case $M_{(t-1)}(\eta) \neq 0$, but we have $\mathrm{ini}(\mathit{\Psi}_{t-1}) | M_{t-1}$, a contradiction. We have proved $\{\mathit{\Psi}_{t-1}, \mathit{\Psi}_t\}$ is regular. We can prove in the same way that M_{t-1} is not always zero on any irreducible component of $\mathrm{sat}(\mathit{\Psi}_t)$. According to Lemma 2.4, we have $\overline{\mathrm{Zero}(\mathit{\Psi}_{t-1}, \mathit{\Psi}_t/\mathrm{ini}(\mathit{\Psi}_t)\mathrm{ini}(\mathit{\Psi}_{t-1}))} = \overline{\mathrm{Zero}(\mathit{\Psi}_t, \mathit{\Psi}_{t-1}/M_{t-1}M_t)}$. The induction step can be proved similarly. ▌

Lemma 2.14 *In Algorithm* 2, *the degree of the polynomials* $\mathit{\Psi}_{q,1}, \mathit{\Psi}_{q,2}, \cdots, \mathit{\Psi}_{q,l_q}$ *are less than* d^{c^n} *and* $N \le k^n d^{nc^{n+2}}$, *where c is a constant. The running time of the algorithm can be bounded by a polynomial in* k^n *and* $d^{nc^{n+2}}$.

Proof According to Lemma 2.5, for given polynomials $h_1, h_2, \cdots, h_k \in \mathbb{K}_n$ with $\deg(h_i) < d$, after applying Algorithm 1, we obtain no more than kd^{cn} components, each component has no more than kd^{cn} polynomials, the degrees of polynomials in these components are less than d^c, and the running time of the algorithm can be bounded by a polynomial in k, d^n. After applying Algorithm 1, the most complicated situation is that the maximal leading variable of the polynomials $g_{q,t}$ is x_{n-1}. Applying Algorithm 1 to these components, each component will be split to at most $kd^{cn}d^{c^2(n-1)} \le kd^{c^3n}$ components, each component has at most $kd^{cn}d^{c^2(n-1)} \le kd^{c^3n}$ polynomials, and the degree of each polynomial is less than d^{c^2}. This procedure will terminate in at most n steps. In Step n, each component will be split to at most $kd^{c^{n+1}n}$ components, each component has at most $kd^{c^{n+1}n}$ polynomials, and each polynomial has degree less than d^{c^n}. Then in total, there are at most $k^n d^{c^{n+2}n}$ components, and the degree of the polynomials can be bounded by d^{c^n}. The running time of Algorithm 2 can be bounded by a polynomial in $k^n, d^{c^{n+2}n}$. ▌

Proof of Theorem 2.9 Omitting Step 3), the correctness of the theorem follows from Lemmas 2.11, 2.12, 2.13, and 2.14. It suffices to show that with Step 3), the theorem is also correct. Suppose $\widetilde{\mathcal{A}}_k, k = 1, 2, \cdots, N_0$ are the extra regular triangular sets obtained by omitting Step 3) and $\mathcal{A}_l, l = 1, 2, \cdots, N$ are those obtained with Step 3). Then

$$\mathrm{Zero}(h_1, \cdots, h_k) = \cup_{l=1}^{N}\mathrm{Zero}(\mathrm{sat}(\mathcal{A}_l)) \bigcup \cup_{k=1}^{N_0}\mathrm{Zero}(\mathrm{sat}(\widetilde{\mathcal{A}}_k)).$$

From the condition $|\mathbb{F}| > k$ in Step 3), we have $|\widetilde{\mathcal{A}}_k| > k$. By the dimension theorem proved in [20], $\dim(\mathrm{Zero}(\mathrm{sat}(\widetilde{\mathcal{A}}_k))) < n - k$. While by the affine dimension theorem[21], any component of $\mathrm{Zero}(h_1, \cdots, h_k)$ is of dimension no less than $n - k$. Thus, $\mathrm{Zero}(\mathrm{sat}(\widetilde{\mathcal{A}}_k))$ are redundant in the decomposition and can be deleted. ▌

3 Decomposition of Ordinary Differential Polynomial Systems

In this section, a decomposition algorithm for ordinary differential polynomial systems will be given, which has an elementary worst case complexity bound.

3.1 Basic Definition and Property

Let $\mathbb{K}$ be a field of characteristic zero in which an operation of differentiation is performable such that for any $a, b \in \mathbb{K}$,

$$(a + b)' = a' + b', \quad (ab)' = ab' + ba'.$$

Then we call $\mathbb{K}$ a differential field. Let $y_1, y_2, \cdots, y_n$ be differential indeterminates. We write the j-th derivative of y_i as $y_i^{(j)}$. Let $\mathbb{K}\{y_1, y_2, \cdots, y_n\} = \mathbb{K}[y_i^{(j)}, i = 1, 2, \cdots, n; j \in \mathbb{N}]$ be the ring of differential polynomials in $y_1, y_2, \cdots, y_n$.

Let f be a differential polynomial in $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$. The class of f denoted by $\mathrm{cls}(f)$, is the greatest p such that some $y_p^{(j)}$ is present in f. If $f \in \mathbb{K}$, then $\mathrm{cls}(f) = 0$. The order of f w.r.t y_i, denoted by $\mathrm{ord}(f, y_i)$, is the greatest j such that $y_i^{(j)}$ appears effectively in f. We write $\mathrm{ord}(f) = \max_{1 \le i \le n} \mathrm{ord}(f, y_i)$. If $\mathrm{cls}(f) = i$ and $\mathrm{ord}(f, y_i) = j$ then we call $y_i^{(j)}$ the leader of f, and we write it as $\mathrm{ld}(f) = y_i^{(j)}$. We define $y_i^{(j)} = \mathrm{ld}(f) > \mathrm{ld}(g) = y_\alpha^{(\beta)}$ if $i > \alpha$ or $i = \alpha, j > \beta$. We can write f as a univariant polynomial in its leader such that $f = a_d(y_i^{(j)})^d + \cdots + a_0$, and we call a_d the initial of f, which is denoted by I_f. We call $\frac{\partial f}{\partial y_i^{(j)}}$ the separant of f, which is denoted by S_f. For $f, g \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, we say f is of higher rank than g, if one of the following conditions is satisfied:

1) $\mathrm{cls}(f) > \mathrm{cls}(g)$.

2) $\mathrm{cls}(f) = \mathrm{cls}(g) = p$ and $\mathrm{ord}(f, y_p) > \mathrm{ord}(g, y_p)$.

3) $\mathrm{cls}(f) = \mathrm{cls}(g) = p, \mathrm{ord}(f, y_p) = \mathrm{ord}(g, y_p) = j$, and $\deg(f, y_p^{(j)}) > \deg(g, y_p^{(j)})$.

Let $\mathrm{cls}(g) = p > 0$. We say f is reduced w.r.t g, if $\mathrm{ord}(f, y_p) < \mathrm{ord}(g, y_p)$ or $\mathrm{ord}(f, y_p) = \mathrm{ord}(g, y_p) = j$, and $\deg(f, y_p^{(j)}) < \deg(g, y_p^{(j)})$.

For $f_1, f_2, \cdots, f_k \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, we use $[f_1, f_2, \cdots, f_k]$ to denote the differential ideal generated by $f_1, f_2, \cdots, f_k$, which is the linear combination of $f_1, f_2, \cdots, f_k$ and their derivatives.

A set $\mathcal{T} := \{T_1, T_2, \cdots, T_r\}$ of differential polynomials in $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$ is called a triangular set, if $\mathrm{cls}(T_i) \neq \mathrm{cls}(T_j)$ for $i \neq j$. Assuming that $\mathrm{cls}(T_1) < \mathrm{cls}(T_2) < \cdots < \mathrm{cls}(T_r)$, we rename the variables as $u_1, u_2, \cdots, u_t, y_1, y_2, \cdots, y_r$ such that $r + t = n$ and $\mathrm{ld}(T_i) = y_i^{(\gamma_i)}$.

A differential polynomial $f \in \mathbb{K}\{u_1, u_2, \cdots, u_t, y_1, y_2, \cdots, y_r\}$ is said to be invertible w.r.t $\mathcal{T}$ if $[f, T_1, T_2, \cdots, T_r] \cap \mathbb{K}\{u_1, u_2, \cdots, u_t\} \neq \{0\}$. $\mathcal{T}$ is called regular if I_{T_i} are invertible w.r.t to $\mathcal{T}_{i-1}$ for $0 \leq i \leq r$. $\mathcal{T}$ is called saturated if $\mathcal{T}$ is regular and S_{T_i} are invertible w.r.t to T_i for $1 \leq i \leq r$.

Let $\mathcal{T} := \{T_1, T_2, \cdots, T_r\}$ be a triangular set. Denote $I_{\mathcal{T}} = I_{T_1} I_{T_2} \cdots I_{T_r}$ and $S_{\mathcal{T}} = S_{T_1} S_{T_2} \cdots S_{T_r}$. Then the saturation ideal of $\mathcal{T}$ is

$$\mathrm{dsat}(T) = \{f \in \mathbb{K}\{y_1, y_2, \cdots, y_n\} \,|\, \exists d \in N, \text{s.t.}\, (I_{\mathcal{T}} S_{\mathcal{T}})^d f \in [T_1, T_2, \cdots, T_r]\}.$$

It is known that if $\mathcal{T}$ is saturated, then $\mathrm{dsat}(\mathcal{T})$ is an unmixed radical differential ideal[6, 7].

Lemma 3.1 *Let $\mathcal{T} := \{T_1, T_2, \cdots, T_r\}$ be a triangular set in $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$. Then $\mathcal{T}$ is saturated if I_{T_i} and S_{T_i} are not identically zero on all irreducible components of* $\mathrm{dsat}(\mathcal{T}_{i-1})$ *and* $\mathrm{dsat}(\mathcal{T}_i)$*, for $1 \leq i \leq r$, respectively.*

Proof This lemma can be proved similar to Lemma 2.1. ∎

Lemma 3.2 *Let $\mathcal{T} := \{T_1, T_2, \cdots, T_r\}$ be a saturated triangular set in $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$. If $M \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$ is not identically zero on all irreducible components of* $\mathrm{dsat}(\mathcal{T})$*, then we have* $\overline{\mathrm{Zero}(\mathcal{T}/I_{\mathcal{T}} S_{\mathcal{T}})} = \overline{\mathrm{Zero}(\mathcal{T}/M I_{\mathcal{T}} S_{\mathcal{T}})} = \mathrm{Zero}(\mathrm{dsat}(\mathcal{T}))$.

Proof This lemma can be proved similar to Lemma 2.3. ∎

3.2 A Squarefree Quasi GCD Algorithm

In order to decompose differential polynomial systems, we need to modify Lemma 2.5. In Lemma 2.5, for given polynomials $h_0, h_1, h_2, \cdots, h_k \in \mathbb{K}[x_1, x_2, \cdots, x_n, Y]$, $\deg(h_i) < d$, we can write $h_i (i > 0)$ as $h_i = \sum_{j=0}^{d-1} h_{i,j} Y^j$, and divide the whole space as $\mathbb{K}^n = \bigcup_{i,j} U_{i,j} \bigcup \{\boldsymbol{x} \in \mathbb{K}^n \,|\, h_{i,j}(\boldsymbol{x}) = 0, \forall\, 1 \leq i \leq k \text{ and } 0 \leq j \leq d-1\}$, where

$$U_{i,j} = \mathrm{Zero}(h_{1,d-1}, \cdots, h_{1,0}, h_{2,d-1}, \cdots, h_{2,0}, \cdots, h_{i,d-1}, \cdots, h_{i,j+1}/h_{i,j})$$

for $1 \leq i \leq k$, $0 \leq j \leq d-1$. We write $\widetilde{h}_{i,j} = \sum_{0 \leq \beta \leq j} h_{i,\beta} Y^\beta$. Then on $U_{i,j}$, the original polynomial system becomes

$$\widetilde{h}_{i,j} = h_{i+1} = \cdots = h_k = 0; \quad h_0 \neq 0. \tag{10}$$

We add a step here to divide (10) into the following polynomial systems:

$$\begin{aligned}
&\widetilde{h}_{i,j} = h_{i+1} = \cdots = h_k = 0, \quad h_0, \frac{\partial \widetilde{h}_{i,j}}{\partial Y} \neq 0, \\
&\widetilde{h}_{i,j} = h_{i+1} = \cdots = h_k = \frac{\partial \widetilde{h}_{i,j}}{\partial Y} = 0, \quad h_0 \frac{\partial^2 \widetilde{h}_{i,j}}{\partial Y^2} \neq 0, \\
&\cdots \\
&\widetilde{h}_{i,j} = h_{i+1} = \cdots = h_k = \frac{\partial \widetilde{h}_{i,j}}{\partial Y} = \cdots = \frac{\partial^{j-1} \widetilde{h}_{i,j}}{\partial Y^{j-1}} = 0, \quad h_0 \neq 0.
\end{aligned} \tag{11}$$

Since $\frac{\partial^j \widetilde{h}_{i,j}}{\partial Y^j} = h_{i,j}$, and $h_{i,j} \neq 0$ on $U_{i,j}$, we actually have $\frac{\partial^j \widetilde{h}_{i,j}}{\partial Y^j} \neq 0$. Then the zero set of (10) equals to the union of the zero sets of (11). Now we continues to introduce new variables as in

Lemma 2.5 to make the polynomial systems homogenous. After this modification, Lemma 2.5 becomes the following form.

Lemma 3.3 *Given polynomials* $h_0, h_1, h_2, \cdots, h_k \in \mathbb{K}_n[Y]$, $\deg(h_i) < d$, *and* $h_i = \sum_{j=0}^{d-1} h_{i,j} Y^j$ *for* $0 \le i \le k$, *we may compute* $g_{q,t} \in \mathbb{K}_n$, $\Psi_q \in \mathbb{K}_n[Y] \setminus \mathbb{K}_n$ *for* $1 \le q \le N_1, 0 \le t \le N_2$ *such that:*

$$\begin{aligned}&\mathrm{Zero}(h_1, h_2, \cdots, h_k/h_0)\\ &= \bigcup_{q=1}^{N_1} \mathrm{Zero}(\Psi_q, g_{q,1}, \cdots, g_{q,N_2}/g_{q,0}) \cup \mathrm{Zero}(\{h_{i,j}, 1 \le i \le k, 0 \le j < d\}/h_0),\end{aligned}$$

which has the following properties:

1) *We have* $\mathrm{ini}(\Psi_q) \mid g_{q,0}$, *and* $S_{\Psi_q} \ne 0$ *on any element of* $\mathrm{Zero}(\Psi_q, g_{q,1}, g_{q,2}, \cdots, g_{q,N_2}/g_{q,0})$.

2) $\deg_{X_1, x_2, \cdots, X_n, Y}(\Psi_q)$, $\deg_{X_1, X_2, \cdots, X_n}(g_{q,t}) \le \mathcal{P}(d); N_1, N_2 \le k\mathcal{P}(d^n)$.

3) *The running time of the algorithm can be bounded by a polynomial in* k, d^n.

Proof For Property 1, we need only to prove that $S_{\Psi_q} \ne 0$ on any element of $\mathrm{Zero}(\Psi_q, g_{q,1}, g_{q,2}, \cdots, g_{q,N_2})$. Since we divide (10) into the union of (11), each component of the output, for example $(\Psi_1, g_1, g_2, \cdots, g_{N_2}/g_0)$, comes from one of (11). Without loss of generality, suppose it is the first one in (11). Then we have

$$\mathrm{Zero}\left(\widetilde{h}_{i,j}, h_{i+1}, \cdots, h_k/h_0 \frac{\partial \widetilde{h}_{i,j}}{\partial Y}\right) \supset \mathrm{Zero}(\Psi_1, g_1, g_2, \cdots, g_{N_2}/g_0).$$

If S_{Ψ_1} vanishes on $(\xi_1, \xi_2, \cdots, \xi_n, \eta) \in \mathrm{Zero}(\Psi_1, g_1, g_2, \cdots, g_{N_2}/g_0)$, then η must be a multiple root of Ψ_1 when substituting $(x_1, x_2, \cdots, x_n)$ by $(\xi_1, \xi_2, \cdots, \xi_n)$. According to Lemma 2.6, η is also a multiple root of the homogeneous equation system of (11) after introduce new variables Y_1, Y_0, which means $\frac{\partial \widetilde{h}_{i,j}}{\partial Y}(\xi_1, \xi_2, \cdots, \xi_n, \eta) = 0$, a contradiction. Property 1 has been proved.

Property 2 comes from Lemma 2.5. We now prove Property 3. According to the procedure of this algorithm, the origin system has been divided into no more than kd subsystems $H_{i,j}$ in (3). For each $H_{i,j}$, we divide it into no more than d subsystems in (11), and each system has no more than $k + d$ polynomials, and the degree of these polynomials are bounded by $2d$. The related matrix A has C_{D+2}^2 rows, where

$$D = \left(\sum_{1 \le l \le \min\{2, k-i+1\}} (\gamma_l - 1) \right) + \gamma_0 \le 6d.$$

The degree of the elements in A are bounded by $2d$, so the degree of P_s in (5) and Δ_s in (6) are bounded by $2dC_{D+2}^2 \le d(6d+1)(6d+2)$. Since P_s are linearly independent, we have $s \le (d(6d+1)(6d+2))^n)$. For each $\mathcal{W}_s$ in (5), we divided it into $\mathcal{W}_s^{(l)}$ in (7) and l is no more than the degree of Δ. So in total, we have $kd^2(d(6d+1)(6d+2))^{(n+1)})$ components and $N_1 \le k\mathcal{P}(d^n)$. According to the above proof, it is obvious that the degree of each polynomial in these components is no more than the degree of P_s and Δ, so is bounded by $\mathcal{P}(d)$. The polynomials $g_{q,t}$ come from three parts. The first part is the polynomials in $U_{i,j}$ and whose number is bounded by kd; the second part is the coefficient of P_s when taken as polynomials in U, U_0, U_1 and so the number is bounded by $(d(6d+1)(6d+2))^{2n}$); the third part is the coefficients of $E_s^{(i)}$ and so the number is bounded by $(d(6d+1)(6d+2))^{n+1}$). Therefore, $N_2 \leq k\mathcal{P}(d^n)$. ▌

Now we write this theorem as an algorithm. We only give the input and output of this algorithm, since the procedure of this algorithm has been described above.

Algorithm 3 — Squarefree Quasi GCD

Input $\{\{h_1, h_2, \cdots, h_k\}, \{h_0\}, \{x_1, x_2, \cdots, x_n\}, Y\}$ where $h_0, h_1, h_2, \cdots, h_k \in \mathbb{K}[x_1, x_2, \cdots, x_n, Y]$, $\deg(h_i) < d$.

Output $\mathbb{D} = \{\mathcal{T}_0, \mathcal{T}_1, \cdots, \mathcal{T}_{N_1}\}$, where $\mathcal{T}_0 = \{\{\}, \{h_{i,j}, 1 \leq i \leq k, 0 \leq j \leq d-1\}, \{h_0\}\}$, $\mathcal{T}_q = \{\{\Psi_q\}, \{g_{q,1}, g_{q,2}, \cdots, g_{q,N_2}\}, \{g_{q,0}\}\} (1 \leq q \leq N_1)$, which satisfy the conditions in Lemma 3.3.

3.3 The Algorithm

We now give the main result for differential polynomial systems.

Theorem 3.4 *Let* $h_1, h_2, \cdots, h_k \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, *where* $\deg(h_i) < d$ *and* $\operatorname{ord}(h_i) < R$ *for* $1 \leq i \leq k$. *There is an algorithm to compute saturated triangular sets* $\mathcal{A}_q := \Psi_{q,1}, \Psi_{q,2}, \cdots, \Psi_{q,l_q}$ *which have the following properties:*

1) $\mathrm{Zero}(h_1, h_2, \cdots, h_k) = \cup_{q=1}^{N} \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_q))$.

2) *We have* $\deg(\Psi_{q,i}) \leq d^{c^{2^n R}}$, $\operatorname{ord}(\Psi_{q,i}) \leq 2^n R$, *and* $N < k^{2^n R} d^{c^{2^n R} Rn}$.

3) *The running time of this algorithm can be bounded by a polynomial in* $k^{2^n R} d^{c^{2^n R} Rn}$.

We will give an algorithm to produce those saturated triangular sets in the theorem. Before giving the main algorithm, two sub-algorithms will be given. The first one is the partial remainder[6, 19].

Algorithm 4 — DPM Algorithm

Input $\{\{g_0\}, \{f_1, f_2, \cdots, f_k\}, \{f_0\}\}$, where $g_0, f_0, f_1, \cdots, f_k \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, $\operatorname{ord}(f_i, y_\alpha) \leq r$ for $0 \leq i \leq k$, and $\mathrm{ld}(g_0) = y_\alpha^{(r-t)}, t \geq 1$.

Output $\{\{g_0, \widetilde{f}_1, \widetilde{f}_2, \cdots, \widetilde{f}_k\}, \{\widetilde{f}_0 S_{g_0}\}\}$ where $\operatorname{ord}(\widetilde{f}_i, y_\alpha) \leq r - t$ for $0 \leq i \leq k$ such that $\mathrm{Zero}(g_0, f_1, f_2, \cdots, f_k / f_0 S_{g_0}) = \mathrm{Zero}(g_0, \widetilde{f}_1, \cdots, \widetilde{f}_k / \widetilde{f}_0 S_{g_0})$.

```
1) For $i = 0, 1, \cdots, k$,
    1.1) $\widetilde{f}_i = f_i$.
    1.2) If $\operatorname{ord}(\widetilde{f}_i, y_\alpha) \leq r - t$, goto Step 1).
    1.3) Let $\operatorname{ord}(\widetilde{f}_i, y_\alpha) = r_i$ and $g_0^{(r_i - r + t)} = S_{g_0} y_\alpha^{(r_i)} - H_{r_i}$.
    1.4) Replace $y_\alpha^{(r_i)}$ in $\widetilde{f}_i$ by $\frac{H_{r_i}}{S_{g_0}}$ and multiply by $(S_{g_0})^{\deg(\widetilde{f}_i, y_\alpha^{(r_i)})}$, and let $\widetilde{f}_i$ be the new
differential polynomial. Goto Step 1.2).
2) Output $\{\{g_0, \widetilde{f}_1, \widetilde{f}_2, \cdots, \widetilde{f}_k\}, \{\widetilde{f}_0 S_{g_0}\}\}$.
```

Lemma 3.5 (see [19]) *Use the notations in Algorithm* 4 *and assume* $\deg(f_j) < d, \deg(g_0) < d$, $\operatorname{ord}(f_i, y_\gamma) < R$ *for* $0 \leq i \leq k, 1 \leq \gamma \leq n$. *Then, we have the following bounds:* $\operatorname{ord}(\widetilde{f}_j, y_\gamma) \leq R + t, \deg(\widetilde{f}_j) \leq \mathcal{P}(d, t)$ *for any* $0 \leq j \leq k, 1 \leq \gamma \leq n$.

Next, we describe a splitting subroutine from [19]. Let $g \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$. For $\alpha \in \{1, 2, \cdots, n\}$, let $\operatorname{ord}(g, y_\alpha) = r$, $g = \sum_a g_a(y_\alpha y_\alpha^{(1)} \cdots y_\alpha^{(r)})^a, a = (a_0, a_1, \cdots, a_r), (y_\alpha y_\alpha^{(1)} \cdots y_\alpha^{(r)})^a = y_\alpha^{a_0} \cdots (y_\alpha^{(r)})^{a_r}$. Denote $\operatorname{coeff}(g, y_\alpha)$ to be set of $g_{i,\alpha}$. For $G \subset \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, denote

$$\operatorname{coeff}(G, y_\alpha) = \cup_{g\in G} \operatorname{coeff}(g, y_\alpha).$$

We have the following split algorithm.

Algorithm 5 — SPLIT Algorithm

Input $\{G, y_\alpha\}$, where $G = \{g_1, g_2, \cdots, g_l\} \subset \mathbb{K}\{y_1, y_2, \cdots, y_n\}$.

Output $\mathbb{D} = \{\mathcal{T}_0, \mathcal{T}_1, \cdots, \mathcal{T}_N\}$ where $\mathcal{T}_0 = (\operatorname{coeff}(G, y_\alpha), \emptyset)$, $\mathcal{T}_i = (\{h_{i,1}, h_{i,2}, \cdots, h_{i,l_i}\}, \{\frac{\partial h_{i,1}}{\partial y_\alpha^{(\gamma_i)}}\})$ such that $\operatorname{ord}(h_{i,1}, y_\alpha) = \gamma_i \geq 0$ and

$$\operatorname{Zero}(g_1, g_2, \cdots, g_l) = \cup_{i=1}^N \operatorname{Zero}\left(h_{i,1}, h_{i,2}, \cdots, h_{i,l_i} / \frac{\partial h_{i,1}}{\partial y_\alpha^{(\gamma_i)}}\right) \cup \operatorname{Zero}(\operatorname{coeff}(G, y_\alpha)). \quad (12)$$

1) Let $\mathbb{S} = \{\{g_1, g_2, \cdots, g_l\}\}$, $\mathbb{D} = \emptyset$.
2) If $\mathbb{S} = \emptyset$, return $\mathbb{D}$; else let $\mathbb{F} \in \mathbb{S}$ and $\mathbb{S} = \mathbb{S} \setminus \{\mathbb{F}\}$.
3) If $\forall f \in \mathbb{F}$, $\operatorname{ord}(f, y_\alpha) = 0$, then add $(\mathbb{F}, \emptyset)$ to $\mathbb{D}$. Go to Step 2).
4) Let $f \in \mathbb{F}$ such that $\operatorname{ord}(f, y_\alpha) = t \geq 0$, $\deg(f, y_\alpha^{(t)}) = d$. Set $\mathbb{F} = \mathbb{F} \setminus \{f\}$.
5) Let $f = \sum_{j=0}^d l_d(y_\alpha^{(t)})^d$ and $f_i = \frac{\partial^i f}{\partial (y_\alpha^{(t)})^i}, i = 1, 2, \cdots, d$.
6) Let $\mathbb{D} = \mathbb{D} \bigcup \{(\{f\} \cup \mathbb{F}, \{f_1\}), (\{f_1, f\} \cup \mathbb{F}, \{f_2\}), \cdots, (\{f_{d-1}, \cdots, f\} \cup \mathbb{F}, \{f_d\})\}$, and $\mathbb{S} = \mathbb{S} \bigcup \{\mathbb{F} \cup \{l_0, l_1, \cdots, l_d\}\}$. Go to Step 2).

Note that the order and degree of the difference polynomials in the output are smaller than or equal to that of g_i in the input. We now give the decomposition algorithm.

We use two examples to illustrate Algorithm 6.

Example 3.6 Note that Algorithm 6 can also be used to algebraic polynomial systems and return a radical decomposition. Let $f = xy^2$ with $x < y$. Using Algorithm 2 to f, we obtain two components $\{x\}$ and $\{y^2\}$, where the second one is not radical. In Step 6 of Algorithm 6, when applying Algorithm 3 to $\{\{f\}, \{\}, y\}$, the system $\{f = 0\}$ is first split into $\{xy^2 = 0, 2xy \neq 0)$, $\{xy^2 = 2xy = 0, x \neq 0)$, and $\{x = 0\}$ and then returns $\emptyset$, $\{\{y\}, \{\}, \{x\}\}$, and $\{\{\}, \{x\}, \{\}\}$. Finally, we obtain the decomposition $\operatorname{Zero}(f) = \operatorname{Zero}(x) \cup \operatorname{Zero}(y)$.

Algorithm 6 — Differential Triangular Decomposition

Input $\{h_1, h_2, \cdots, h_k\} \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$.

Output $\{\mathcal{A}_q, D_q\}, 1 = 1, 2, \cdots, N$, where $\mathcal{A}_q = \{\Psi_{q,1}, \cdots \Psi_{q,l_q}\}$ satisfies the conditions in Theorem 3.4.

1) Let $\mathcal{T} = \{\{\}, \{h_1, h_2, \cdots h_k\}, \{\}\}$, $\mathbb{S} = \{\mathcal{T}\}$, $\mathbb{R} = \{\}$.
2) If $\mathbb{S} = \emptyset$, output $\mathbb{R}$, else let $\mathcal{T} = \{\mathbb{F}, \mathbb{P}, \mathbb{N}\} \in \mathbb{S}$ and $\mathbb{S} = \mathbb{S} \setminus \{\mathcal{T}\}$.
3) If $\mathbb{P} = \emptyset$, add $(\mathbb{F}, \prod_{p\in\mathbb{N}} p)$ to $\mathbb{R}$ and go to Step 2).
4) Let $y_\alpha^{(\gamma)} = \max_{h\in\mathbb{P}} \operatorname{ld}(h)$, $\widetilde{\mathbb{P}} = \{h \in \mathbb{P} \,|\, \operatorname{ld}(h) = y_\alpha^{(\gamma)}\}$, $\mathbb{P} = \mathbb{P} \setminus \widetilde{\mathbb{P}}$.

Algorithm 6— Differential Triangular Decomposition (Continued)

```
5) Let $\widetilde{\mathbb{N}} = \{f \in \mathbb{N} \,|\, \mathrm{ld}(f) \le y_\alpha^{(\gamma)}\}$, $H = \prod_{f \in \widetilde{\mathbb{N}}} f$.
6) Apply Algorithm 3 to $\{\widetilde{\mathbb{P}}, H, \mathrm{vars}(\widetilde{\mathbb{P}} \cup \{H\}) \setminus \{y_\alpha^{(\gamma)}\}, y_\alpha^{(\gamma)}\}$, the output is $\mathbb{D}$.
7) If $\mathbb{D} = \emptyset$, go to Step 2), else for $\mathcal{T}_1 = \{\mathbb{W} = \{\varPsi\}, \mathbb{U}, \mathbb{V} = \{v\}\} \in \mathbb{D}$, $\mathbb{D} = \mathbb{D} \setminus \{\mathcal{T}_1\}$, $\mathbb{U} = \mathbb{U} \cup \mathbb{P}$.
8) If $\mathbb{U} = \emptyset$, add $\{\mathbb{F} \cup \mathbb{W}, \mathbb{U}, \mathbb{N} \cup \mathbb{V}\}$ to $\mathbb{R}$ and go to Step 7).
9) Apply Algorithm 5 to $\{\mathbb{U}, y_\alpha\}$, the output is $\mathbb{D}_1$.
10) If $\mathbb{D}_1 = \emptyset$, go to Step 7), else let $C = (\varGamma, \varTheta) \in \mathbb{D}_1$ and $\mathbb{D}_1 = \mathbb{D}_1 \setminus \{C\}$.
11) If $\varTheta \ne \emptyset$, assume $\varTheta = \{\frac{\partial g}{\partial y_\alpha^{(l)}}\}$. Applying Algorithm 4 to $\{\{g\}, \mathbb{W} \cup (\varGamma \setminus \{g\}), \mathbb{V}\}$, the output is $\{\widetilde{\mathbb{W}}, \widetilde{\mathbb{V}}\}$. Add $\{\mathbb{F}, \widetilde{\mathbb{W}}, \mathbb{N} \cup \widetilde{\mathbb{V}}\}$ to $\mathbb{S}$. Go to Step 10).
12) If $\varTheta = \emptyset$, let $y_\varepsilon^{(r)} = \max_{h \in \varGamma}\ \mathrm{ld}(h)$, $y_\beta^{(t)} = \mathrm{ld}(v)$.
13) If $y_\varepsilon^{(r)} \le y_\beta^{(t)}$ add $\{\mathbb{F} \cup \mathbb{W}, \varGamma, \mathbb{V} \cup \mathbb{N}\}$ to $\mathbb{S}$. Goto Step 10).
14) Let $\boldsymbol{x} = \{y_\gamma^{(e)} \,|\, \deg(v, y_\gamma^{(e)}) > 0$ and $y_\gamma^{(e)} > y_\varepsilon^{(r)}\}$ and write $v$ as a multivariate polynomial in $\boldsymbol{x}$: $v = \varSigma l_\varTheta \boldsymbol{x}^\varTheta$. Add $\{\mathbb{F} \cup \mathbb{W}, \varGamma, \mathbb{N} \cup \mathbb{V} \cup \{l_\varTheta\}\}$ to $\mathbb{S}$ for each $\varTheta$. Go to Step 10).
```

Example 3.7 Let $f = y'^2 - xy^2$, $x < y$. In Step 4), we have $y_\alpha^{(\gamma)} = y'$, $\widetilde{\mathbb{P}} = \{f\}$. In Step 5), $\mathbb{N} = \emptyset$ and $H = 1$. In Step 6), Algorithm 3 is applied to $\{\widetilde{\mathbb{P}}, H, y'\}$. $\widetilde{\mathbb{P}}$ is first split into two components $\{y'^2 - xy^2 = 0, 2y' \ne 0\}$ and $\{y'^2 - xy^2 = 2y' = 0\}$. The output of the first component is $\{\{y'^2 - xy^2\}, \{\}, \{xy^2\}\}$ and the output of the second one is $\{\{y'\}, \{xy^2\}, \{\}\}$.

In Step 8), $C_0 = \{\{y'^2 - xy^2\}, \{\}, \{xy^2\}\}$ will be put into $\mathbb{S}$ and eventually be added to $\mathbb{R}$.

In Step 9), we will handle $\{\{y'\}, \{xy^2\}, \{\}\}$. Applying Algorithm 5 to $\mathbb{U} = \{xy^2\}$ and $y_\alpha = y$, the output $\mathbb{D}_1$ consists of $C_1 = (\{xy^2\}, \{2xy\})$, $C_2 = (\{xy^2, 2xy\}, \{2x\})$, and $C_3 = (\{2x\}, \{\})$.

C_1 is handled in Step 11). Algorithm 4 is applied to $\{\{xy^2\}, \{y'\}, \{2xy\}\}$ and returns $\{\{xy^2, x'y^2\}, \{2xy\}\}$. Finally, $C_4 = \{\{\}, \{xy^2, x'y^2\}, \{2xy\}\}$ is added to $\mathbb{S}$.

C_2 is handled in Step 11). Algorithm 4 is applied to $\{\{2xy\}, \{y', xy^2\}, \{2x\}\}$ and returns $\{\{2xy, 2x'y, xy^2\}, \{2x\}\}$. Finally, $C_5 = \{\{\}, \{2xy, xy^2, 2x'y\}, \{2x\}\}$ is added to $\mathbb{S}$.

C_3 is handled in Steps 12) and 13). $C_6 = \{\{y'\}, \{2x\}, \{\}\}$ is added to $\mathbb{S}$.

For C_4, in Step 6), Algorithm 3 is applied to $\{\{xy^2, x'y^2\}, 1, \{2xy\}\}$ and returns the empty set. We omit the computing procedures for C_5 and C_6. The algorithm give the decomposition $\mathrm{Zero}(f) = \mathrm{Zero}(\mathrm{dsat}(f)) \cup \mathrm{Zero}(y', x) \cup \mathrm{Zero}(y)$.

Now we prove Theorem 3.4 with the following lemmas.

Lemma 3.8 *Algorithm* 6 *terminates,* $\mathrm{Zero}(h_1, h_2, \cdots, h_k) = \cup_q \mathrm{Zero}(\mathcal{A}_q/D_q)$*, and* $I_{\varPsi_{q,i}}$, $S_{\varPsi_{q,i}} \ne 0$ *on any element of* $\mathrm{Zero}(\mathcal{A}_q/D_q)$.

Proof The algorithm has three loops, starting at Steps 2), 7), and 10), respectively. We need only to show that the loop starting at Step 2) will terminate. Let $\{\mathbb{F}_1, \mathbb{P}_1, \mathbb{N}_1\}$ be a component added to $\mathbb{S}$ in this loop and $y_c^\delta = \max_{p \in \mathbb{P}_1} \mathrm{ld}(p)$. Then, we have either $y_c^\delta < y_\alpha^\gamma$ which means that the algorithm terminates.

$\mathrm{Zero}(h_1, h_2, \cdots, h_k) = \bigcup_q \mathrm{Zero}(\varPsi_{q,1}, \cdots \varPsi_{q,l_q}/D_q)$ can be proved similar to Lemma 2.12. In the proof, we also need the equalities in Lemmas 3.3 and 3.5, and (12).

We now show that $\mathcal{A}_q$ is a triangular set. It suffices to show that for any $\{\mathbb{F}, \mathbb{P}, \mathbb{N}\} \in \mathbb{S}$, $\max_{p\in\mathbb{P}} \mathrm{cls}(p) < \max_{q\in\mathbb{F}} \mathrm{cls}(q)$. New polynomials are added to $\mathbb{F}$ in Steps 8), 13), and 14). In Step 8), since $\mathbb{U} = \emptyset$, this is indeed the case. In Steps 13) and 14), we have $\Theta = \emptyset$ which means that y_α and its derivatives do not appear in Γ. Hence, $\max_{p\in\Gamma} \mathrm{cls}(p) < \alpha$ and $\mathcal{A}_q$ is a triangular set for any q.

Finally, if $(\mathit{\Psi}_1, \mathit{\Psi}_2, \cdots, \mathit{\Psi}_t/M)$ is one component of the output, then according to the algorithm it comes from a procedure like (9) and (10). In the algebraic case, from one step to the next step in (9), Algorithm 1 is used one time. In the differential case, from one step to the next step in (9), Algorithm 3 is used many times. For instance, the procedure to obtain $\mathit{\Psi}_1$ is as follows:

$$\begin{aligned}
&\mathrm{Zero}(f_{0,1}, f_{0,2}, \cdots, f_{0,k^{(0)}}/M_0)\\
\to\ &\mathrm{Zero}(\mathit{\Psi}_1, h_{1,1}, \cdots, h_{1,t^{(1)}}/M_1)\\
\to\ &\mathrm{Zero}(g_{1,0}, g_{1,1}, \cdots, g_{1,l^{(1)}}/S_1M_1)\\
\to\ &\mathrm{Zero}(\mathit{\Psi}_2, h_{2,1}, h_{2,2}, \cdots, h_{2,t^{(2)}}/M_2S_1M_1)\\
\to\ &\cdots\\
\to\ &\mathrm{Zero}(g_{s,0}, g_{s,1}, \cdots, g_{s,l^{(s)}}/M_{s+1}\cdots S_1M_1)\\
\to\ &\mathrm{Zero}(\mathit{\Psi}_{s+1}, h_{s+1,1}, h_{s+1,2}, \cdots, h_{s+1,t^{(s+1)}}/S_{s+1}M_{s+1}\cdots S_1M_1),
\end{aligned}\tag{13}$$

where $\mathit{\Psi}_1 = \mathit{\Psi}_{s+1}$ and $\{h_{s+1,1}, h_{s+1,2}, \cdots, h_{s+1,t^{(s+1)}}\} = \{f_{1,1}, f_{1,2}, \cdots, f_{1,k^{(1)}}\}$ in (9). $(\mathit{\Psi}_1, h_{1,1}, h_{1,2}, \cdots, h_{1,t^{(1)}}/M_1)$ is a component of $(f_{0,1}, f_{0,2}, \cdots, f_{0,k^{(0)}}/M_0)$ after using Algorithm 3, so $I_{\mathit{\Psi}_1}|M_1$ and $S_{\mathit{\Psi}_1} \neq 0$ on any element of $\mathrm{Zero}(\mathit{\Psi}_1, h_{1,1}, h_{1,2}, \cdots, h_{1,k^{(1)}}/M_1)$ by Lemma 3.3. $(g_{1,0}, g_{1,1}, \cdots, g_{1,l^{(1)}}/S_1M_1)$ is a component obtained from $(\mathit{\Psi}_1, h_{1,1}, h_{1,2}, \cdots, h_{1,k^{(1)}}/M_1)$ by Algorithms 5 and 6 in Steps 9) and 11). So we have $\mathrm{Zero}(g_{1,0}, g_{1,1}, \cdots, g_{1,l^{(1)}}/S_1M_1) \subset \mathrm{Zero}(\mathit{\Psi}_1, h_{1,1}, h_{1,2}, \cdots, h_{1,k^{(1)}}/M_1)$. The procedure is repeated until $\mathrm{cls}(\mathit{\Psi}_{s+1}) > \mathrm{cls}(g_{s+1,j})$ for all j and $\mathit{\Psi}_1$ is obtained. Then, we have

$$\begin{aligned}
&\mathrm{Zero}(f_{0,1}, f_{0,2}, \cdots, f_{0,k^{(0)}}/M_0)\\
\supseteq\ &\mathrm{Zero}(\mathit{\Psi}_1, h_{1,1}, h_{1,2}, \cdots, h_{1,t^{(1)}}/M_1)\\
\supseteq\ &\mathrm{Zero}(g_{1,0}, g_{1,1}, \cdots, g_{1,l^{(1)}}/S_1M_1)\\
\supseteq\ &\cdots\\
\supseteq\ &\mathrm{Zero}(g_{s,0}, g_{s,1}, \cdots, g_{s,l^{(s)}}/S_s\cdots S_1M_1)\\
\supseteq\ &\mathrm{Zero}(\mathit{\Psi}_{s+1}, h_{s+1,1}, h_{s+1,2}, \cdots, h_{s+1,t^{(s+1)}}/M_{s+1}\cdots S_1M_1).
\end{aligned}\tag{14}$$

By Lemma 3.3, $I_{\mathit{\Psi}_1}|M_{s+1}$ and $S_{\mathit{\Psi}_1} \neq 0$ on any element of $\mathrm{Zero}(\mathit{\Psi}_{s+1}, h_{s+1,1}, h_{s+1,2}, \cdots, h_{s+1,t^{(s+1)}}$ $/M_{s+1}\cdots S_1M_1)$. The lemma is proved. ▮

Lemma 3.9 *In Algorithm* 6, $\mathcal{A}_q := \mathit{\Psi}_{q,1}, \mathit{\Psi}_{q,2}, \cdots \mathit{\Psi}_{q,l_q}$ *are saturated triangular sets and* $\mathrm{Zero}(\mathrm{dsat}(\mathcal{A}_q)) = \overline{\mathrm{Zero}(\mathit{\Psi}_{q,1}, \mathit{\Psi}_{q,2}, \cdots \mathit{\Psi}_{q,l_q}/D_q)}$.

Proof Using Lemmas 3.1 and 3.2 instead of Lemmas 2.1 and 2.3, the proof of this lemma is the same with that of Lemma 2.13. ▮

The following lemma gives the complexity part of Theorem 3.4.

Lemma 3.10 *In Algorithm* 6*, the degree of $\Psi_{q,i}$ is less than $d^{c^{2^nR}}$, the order of $\Psi_{q,i}$ is less than 2^nR, $N < k^{2^nR}d^{c^{2^nR}Rn}$. The running time of this algorithm can be bounded by a polynomial in $k^{2^nR}d^{c^{2^nR}Rn}$.*

Proof For given differential polynomials $h_1, h_2, \cdots, h_k \in \mathbb{K}\{y_1, y_2, \cdots, y_n\}$, since $\mathrm{ord}(h_i, y_j) < R$ for $1 \le i \le k, 1 \le j \le n$, there are at most Rn variables when applying Algorithm 3. Consider the most complicated case where $y_n^{(R-1)}$ is the maximal leader. After applying Lemma 3.3 to $h_1, h_2, \cdots, h_k$, there are at most kd^{cRn} components, each component has at most kd^{cRn} differential polynomials, and the degree of each polynomial is no more than d^c. After applying Algorithm 5, each component will be split into at most d^{cR} components, and each component has at most kd^{cRn+cR} polynomials. After applying Lemma 3.5, the number of the components and the number of polynomials in each component do not change, and the degrees of the polynomials are less than d^{2c}. The most complicated case occurs when the order of y_n decreases by one and the maximal leader becomes $y_n^{(R-2)}$. Continuing this procedure until the main variable becomes y_{n-1}. There are no more than $k^Rd^{c^RRn}$ components in total, each component has no more than kd^{c^RRn} polynomials, the degree of these polynomials are less than d^{c^R}, and the order of these polynomials are less than $2R$. Repeating this procedure to $y_1, y_2, \cdots, y_{n-1}$, finally we obtain no more than $k^{2^nR}d^{c^{2^nR}Rn}$ components, the degree of the polynomials are bounded by $d^{c^{2^nR}}$, and the order of these polynomials are less than 2^nR. ∎

4 Summary

Two triangular decomposition algorithms are given in this paper. For a set of polynomials $F = \{f_1, f_2, \cdots, f_s\}$ in $\mathbb{K}[x_1, x_2, \cdots, x_n]$, we can compute regular triangular sets $\mathcal{T}_1, \mathcal{T}_2, \cdots, \mathcal{T}_r$ such that $\mathrm{Zero}(F) = \cup_i \mathrm{Zero}(\mathrm{sat}(\mathcal{T}_i))$ which gives an unmixed decomposition for the solution set of $F = 0$. We also show that the complexity of the algorithm is double exponential in n. For a set of ordinary differential polynomials $F = \{f_1, f_2, \cdots, f_s\}$ in $\mathbb{K}\{y_1, y_2, \cdots, y_n\}$, we can give a similar decomposition $\mathrm{Zero}(F) = \cup_i \mathrm{Zero}(\mathrm{dsat}(\mathcal{T}_i))$, where $\mathrm{dsat}(\mathcal{T}_i)$ are radical differential ideals and the complexity is triple exponential. This seems to be the first triangular decomposition algorithm for differential polynomial systems with elementary computation complexity.

References

[1] Ritt J F, *Differential Algebra*, American Mathematical Society, Colloquium Publications, Vol. 33, 1950.

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

[3] Aubry P, Lazard D, and Maza M M, On the theories of triangular sets, *J. Symb. Comput.*, 1999, **28**: 105–124.

[4] Szanto A, *Computation with Polynomial Systems*, Doctoral Dissertation, Cornell University, 1999.

[5] Wang D, An elimination method for polynomial systems, *J. Symb. Comput.*, 1993, **16**: 83–114.

[6] Boulier F, Lazard D, Ollivier F, et al., Representation for the radical of a finitely generated differential ideal, *Proc. of ISSAC'95*, ACM Press, 1995, 158–166.

[7] Bouziane D, Kandri Rody A, and Maârouf H, Unmixed-dimensional decomposition of a finitely generated perfect differential ideal, *J. Symb. Comput.*, 2001, **31**: 631–649.

[8] Chou S C and Gao X S, Automated reasoning in differential geometry and mechanics using the characteristic set method, Part I. An improved version of Ritt-Wu's decomposition algorithm, *Journal of Automated Reasoning*, 1993, **10**: 161–172.

[9] Hubert E, Factorization-free decomposition algorithms in differetntial algebra, *J. Symb. Comput.*, 2000, **29**(4–5): 641–662.

[10] Wu W T, A constructive theorey of differential algebraic geometry, *Lect. Notes in Math.*, Springer, 1987, **1255**: 173–189.

[11] Cheng J S and Gao X S, Multiplicity-preserving triangular set decomposition of two polynomials, *Journal of Systems Science and Complexity*, 2014, **27**(6): 1320–1344.

[12] Gao X S, Luo Y, and Yuan C, A characteristic set method for difference polynomial systems, *J. Symb. Comput.*, 2009, **44**(3): 242–260.

[13] Gao X S and Huang Z, Characteristic set algorithms for equation solving in finite fields, *J. Symb. Comput.*, 2012, **47**: 655–679.

[14] Huang Z, Parametric equation solving and qiantifier elimination in finite fields with characteristic set method, *Journal of Systems Science and Complexity*, 2012, **25**(4): 778–791.

[15] Li X, Mou C, and Wang D, Decomposing polynomial sets into somple sets over finite fields: The zero-dimensional case, *Computer and Mathematics with Applications*, 2010, **60**: 2983–2997.

[16] Chen C, Davenport J H, May J P, et al., Triangular decomposition of semi-algebraic systems, *Proc. ISSAC* 2010, ACM Press, New York, 2010, 187–194.

[17] Gallo G and Mishra B, Efficient algorithms and bounds for Wu-Ritt characteristic sets, *Progress in Mathematics*, 1991, **94**: 119–142.

[18] Golubitsky O, Kondratieva M, Ovchinnikov A, et al., A bound for orders in differential nullstellensatz, *Journal of Algebra*, 2009, **322**(11): 3852–3877.

[19] Grigor'ev D Y, Complexity of quantifier elimination in the theory of ordinary differential equations, *Lecture Notes in Computer Science*, 1984, **176**: 17–31.

[20] Gao X S and Chou C, On the dimension of an arbitrary ascending chain, *Chinese Sci. Bull.*, 1993, **38**: 799–804.

[21] Hartshorne R, *Algebraic Geometry*, Springer-Verlag, Berlin, 1977.