J Syst Sci Complex (2019) 32: 62–77

Ritt-Wu Characteristic Set Method for Laurent Partial Differential Polynomial Systems*

HU Youren · GAO Xiao-Shan

DOI: 10.1007/s11424-019-8343-5
Received: 19 August 2018 / Revised: 8 November 2018

Abstract In this paper, a Ritt-Wu characteristic set method for Laurent partial differential polynomial systems is presented. The concept of Laurent regular differential chain is defined and its basic properties are proved. The authors give a partial method to decide whether a Laurent differential chain $\mathcal{A}$ is Laurent regular. The decision for whether $\mathcal{A}$ is Laurent regular is reduced to the decision of whether a univariate differential chain $\mathcal{A}_1$ is Laurent regular. For a univariate differential chain $\mathcal{A}_1$, the authors first give a criterion for whether $\mathcal{A}_1$ is Laurent regular in terms of its generic zeros and then give partial results on deciding whether $\mathcal{A}_1$ is Laurent regular.

Keywords Newton polygon, Laurent partial differential polynomial system, Laurent regular triangular set, Ritt-Wu characteristic set.

1 Introduction

The Ritt-Wu characteristic set method can be used to decompose the zero set of an arbitrary polynomial system into the union of zero sets of polynomial systems in triangular form or to decompose the radical ideal generated by a set of polynomials into the intersection of un-mixed radical ideals represented by polynomial systems in triangular form. The characteristic set method was proposed by Ritt[1] for theoretical purposes and was extensively studied in the past thirty years after Wu's seminal work on automated geometry theorem proving and polynomial system solving[2–4]. By far, the Ritt-Wu characteristic set method had been developed for polynomial systems[4–12], semi-algebraic sets[13], polynomial systems over finite fields[14–16], differential polynomial systems[17–22], and difference polynomial systems[23]. The Ritt-Wu characteristic set method had been applied to automated reasoning, robotics, computer vision, computer-aided design, and analysis of cryptosystems, etc.[24].

HU Youren · GAO Xiao-Shan
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, *China; School of Mathematics, University of Chinese Academy of Sciences, Chinese Academy of Sciences, Beijing* 100190, *China.* Email: huyouren14@mails.ucas.ac.cn; xgao@mmrc.iss.ac.cn.
*This research was supported by NKRDPC under Grant No. 2018YFA0306702 and the National Natural Science Foundation of China under Grant No. 11688101.
◇ *This paper was recommended for publication by Editor LI Hongbo.*

In the work on difference binomial ideals and difference toric varieties[25, 26], the Ritt-Wu characteristic set method in the Laurent case plays a key role. This motivates the study of the Ritt-Wu characteristic set method for Laurent polynomial systems and Laurent ordinary differential polynomial systems[27]. In this paper, we develop the characteristic set method for Laurent partial differential polynomial systems.

Let $\mathcal{F}$ be a partial differential field with differential operators $\varDelta = \{\delta_1, \delta_2, \cdots, \delta_m\}$ and $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ a set of differential indeterminates. Then the Laurent differential polynomial ring $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ is the polynomial ring in $\delta_j y_i$ and $(\delta_j y_i)^{-1}$ for $y_i \in \mathbb{Y}$ and $j \in \mathbb{N}$. Comparing to the differential polynomial ring, the major difference is that y_i and its derivatives are invertible in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. In the polynomial case and the difference polynomial case[23], this does not lead to major difficulties in developing the characteristic set method[27]. But, in the differential polynomial case, essential difficulties arise as illustrated by the following example.

Example 1.1 Let $f = x\delta y - ky$ be an ordinary differential polynomial in $\mathbb{Q}(x)\{y^{\pm}\}$, where y is a differential variable, the differential operator is $\delta = \frac{\partial}{\partial x}$, and $k \in \mathbb{N}$. Then $\delta^i f = x\delta^{i+1}y + (i-k)\delta^i y$ for $i = 1, 2, \cdots, k$. Hence, $\delta^k f = x\delta^{k+1}y$ which is invertible in $\mathbb{Q}(x)\{y^{\pm}\}$. Therefore, in the Laurent case, $f = 0$ has no solutions and the differential ideal generated by f is $\mathbb{Q}(x)\{y^{\pm}\}$, that is, $[f] = [1]$ in $\mathbb{Q}(x)\{y^{\pm}\}$. To check these facts, we need to differentiate f for "sufficiently" many times and the main difficulty is how to give a bound for the number of such differentiations.

In this paper, we give a partial answer to the questions proposed in the above example by developing a Ritt-Wu characteristic set method for Laurent partial differential polynomial systems. The main contributions of this paper are: 1) The concept of Laurent partial differential regular chain is defined and its basic property is proved. 2) We show that deciding whether an irreducible partial differential chain is Laurent regular can be reduced to deciding whether a univariate partial differential chain is Laurent regular. 3) A partial method is given to decide whether a univariate differential chain is Laurent regular. It is clear that if we can decide whether a chain is Laurent regular, then a complete Ritt-Wu characteristic set method can be given similar to the non-Laurent case[17–21]. Therefore, in this paper, we will concentrate on the decision problem for Laurent regular differential chains.

A differential chain $\mathcal{A}$ in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ is called Laurent regular if $\mathcal{A}$ is regular and all the derivatives of y_i are invertible w.r.t. $\mathcal{A}$. A Laurent regular chain $\mathcal{A}$ has the following basic property: $\mathcal{A}$ is the characteristic set of the Laurent saturation ideal of $\mathcal{A}$ if and only if $\mathcal{A}$ is Laurent regular and coherent (refer to Theorem 3.5 for details).

We give partial results on deciding whether a differential chain is Laurent regular. We first show that deciding whether an irreducible partial differential chain is Laurent regular can be reduced to deciding whether a univariate partial differential chain is Laurent regular, and then give partial results on deciding whether a univariate differential chain is Laurent regular.

For a univariate differential chain $\mathcal{A}_1$, we give a criterion for whether $\mathcal{A}_1$ is Laurent regular in terms of its generic zeros. Furthermore, for a partial differential operator $\delta_u \in \varDelta$ and $k \in \mathbb{N}$, we give a method to decide whether $\delta_u^k y$ is invertible with respect to a single differential polynomial f in $\mathcal{F}\{y\}$ and the method is complete when f is of order one. The method is based on a parameterized version of the work of Cano[28, 29] and Grigoriev-Singer[30], where a special Newton polygon was introduced to find the minimal monomial of the series solution to an ordinary differential equation.

The paper is organized as follows. In Section 2, we give some notations and definitions about Laurent partial differential polynomial rings. In Section 3, we define the concept of Laurent regular differential chain and prove its basic properties. In Section 4, we prove that deciding whether an irreducible, coherent and regular chain is Laurent regular can be reduced to deciding whether an irreducible, coherent and regular chain in one differential indeterminate is Laurent regular. In Section 5, we present partial results for the decision of whether a univariate differential polynomial is Laurent regular. In Section 6, conclusions are presented.

2 Preliminaries

Let $\mathcal{F}$ be a differential field with the set of differential operators $\varDelta = \{\delta_1, \delta_2, \cdots, \delta_m\}$ and $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be a set of differential indeterminates. Let $\varTheta = \{\delta_1^{a_1}\delta_2^{a_2}\cdots\delta_m^{a_m}, a_i \in \mathbb{N}, i = 1, 2, \cdots, m\}$ and $\varTheta(\mathbb{Y}) = \{\theta y_j : j = 1, 2, \cdots, n, \theta \in \varTheta\}$. We denote $R = \mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[\varTheta(\mathbb{Y})]$ to be the differential polynomial ring in $\mathbb{Y}$ over $\mathcal{F}$. The order of an element $\theta = \delta_1^{a_1}\delta_2^{a_2}\cdots\delta_m^{a_m} \in \varTheta$ is defined as $\mathrm{ord}(\theta) = \sum_{i=1}^m a_i$.

Let $f \in \mathcal{F}\{\mathbb{Y}\}$. The order of f in y_i is the maximal order of $\theta \in \varTheta$ such that θy_i occurs in f, denoted by $\mathrm{ord}(f, y_i)$. If y_i does not appear in f, denote $\mathrm{ord}(f, y_i) = -\infty$. Denote $\mathrm{ord}(f) = \max_{j=1}^n \mathrm{ord}(f, y_j)$. A ranking $\mathfrak{R}$ is a total order over $\varTheta(\mathbb{Y})$ which satisfies

1) $\delta_i(\alpha) > \alpha$, for any $\alpha \in \varTheta(\mathbb{Y}), i = 1, 2, \cdots, m$ and

2) $\alpha_1 > \alpha_2 \Rightarrow \delta_i(\alpha_1) > \delta_i(\alpha_2)$, for any $\alpha_1, \alpha_2 \in \varTheta(\mathbb{Y}), i = 1, 2, \cdots, m$.

Here we introduce two special rankings:

1) A ranking is said to be orderly if the inequality $\mathrm{ord}(u) < \mathrm{ord}(v)$ implies $u < v$, where $u, v \in \varTheta(\mathbb{Y})$.

2) A ranking is called elimination ranking if $i < j$ implies that $\theta_1 y_i \prec \theta_2 y_j$, for any $\theta_1, \theta_2 \in \varTheta$.

In what follows, if there is no special explanation, we assume that an orderly ranking $\mathfrak{R}_0$ of $\varTheta(\mathbb{Y})$ is fixed.

For $f \in \mathcal{F}\{\mathbb{Y}\}$, the leader of f is the greatest element in $\varTheta(\mathbb{Y})$ occurring in f w.r.t. $\mathfrak{R}_0$, denoted by ld_f. Regarding f as a univariate polynomial in ld_f, its leading coefficient is called the initial of f, denoted by I_f, and its partial derivative w.r.t. ld_f is called the separant of f, denoted by S_f.

For any $f, g \in \mathcal{F}\{\mathbb{Y}\}$, f is said to be of lower ranking than g if 1) $\mathrm{ld}_f < \mathrm{ld}_g$ or 2) $\mathrm{ld}_f = \mathrm{ld}_g$ and $\deg(f, \mathrm{ld}_f) < \deg(g, \mathrm{ld}_g)$, which is denoted as $f \prec g$. If $\mathrm{ld}_f = \mathrm{ld}_g$ and $\deg(f, \mathrm{ld}_f) = \deg(g, \mathrm{ld}_g)$, we denote $f \equiv g$. We say that f is partially reduced w.r.t. g if every proper derivative of ld_g does not appear in f. f is said to be reduced w.r.t. g if it is partially reduced w.r.t. g and $\deg(f, \mathrm{ld}_g) < \deg(g, \mathrm{ld}_g)$. We say f is (partially) reduced w.r.t. a subset S of R if it is (partially) reduced w.r.t. each element of S.

Let $S \subseteq \mathcal{F}\{\mathbb{Y}\}$. S is called an autoreduced set if every element in S is reduced w.r.t.

all the others. Distinct elements of S have distinct leaders and S must be finite[31]. If $\mathcal{A} = \{A_1, A_2, \cdots, A_l\}$ is an autoreduced set with $A_1 \prec A_2 \prec \cdots \prec A_l$, then we denote $\mathcal{A}$ by $\mathcal{A} = A_1, A_2, \cdots, A_l$, which is also called a (differential) chain.

If $\mathcal{A} = A_1, A_2, \cdots, A_s$ and $\mathcal{B} = B_1, B_2, \cdots, B_t$ are two chains, we say that $\mathcal{A}$ has lower rank than $\mathcal{B}$, denoted by$\mathcal{A} \prec \mathcal{B}$ if there exists $i \leq \min\{s, t\}$ such that $A_j \equiv B_j$ for $j < i$ and $A_i \prec B_i$ or $s > t$ and $A_j \equiv B_j$ for $j = 1, 2, \cdots, t$. If $s = t$ and $A_j \equiv B_j$ for $i = 1, 2, \cdots, t$, then $\mathcal{A}$ is said to have the same rank as $\mathcal{B}$, which is denoted by $\mathcal{A} \equiv \mathcal{B}$. In every nonempty set of autoreduced subsets of $F\{\mathbb{Y}\}$, there exists an autoreduced subset of the lowest rank[31]. Let S be a subset of $F\{\mathbb{Y}\}$, the autoreduced set of S of the lowest rank is called a characteristic set of S.

Let $\mathcal{A} = A_1, A_2, \cdots, A_t$ be an autoreduced set with $A_1 \prec A_2 \prec \cdots \prec A_t$. Denote $I_{\mathcal{A}}$ and $S_{\mathcal{A}}$ to be the product of the initials and the product of separants of $\mathcal{A}$ respectively and $H_{\mathcal{A}} = I_{\mathcal{A}} S_{\mathcal{A}}$. Let ld_{ij} be the lowest common derivative of ld_{A_i} and ld_{A_j}, if it exists. (Evidently, it exists provided both ld_{A_i} and ld_{A_j} are derivatives of the same y_t for some $t \in \{1, 2, \cdots, m\}$). Let A_i and A_j be two differential polynomials in $\mathcal{A}$. Suppose that $\mathrm{ld}_{A_i} = \theta_i y_k$ and $\mathrm{ld}_{A_j} = \theta_j y_k$ for some indeterminate y_k, where $\theta_i, \theta_j \in \Theta$. Then, there exist $\phi_i, \phi_j \in \Theta$ such that $\mathrm{ord}(\phi_i) > 0$, $\mathrm{ord}(\phi_j) > 0$, and $\mathrm{ld}_{ij} = \phi_i \mathrm{ld}_{A_i} = \phi_j \mathrm{ld}_{A_j}$. Let $\Delta_{i,j} = S_{A_j} \phi_i A_i - S_{A_i} \phi_j A_j$ and $\Delta(\mathcal{A}) = \{\Delta_{i,j} : 1 \leq i, j \leq t\}$. $\mathcal{A}$ is said to be coherent[32] if $\Delta(\mathcal{A})$ is empty or for every $\Delta_{i,j} \in \Delta(\mathcal{A})$, there exists an $l \in \mathbb{N}$ such that $H_{\mathcal{A}}^l \Delta_{i,j} \in (\{\phi g : \phi \in \Theta, g \in \mathcal{A}, \mathrm{ld}_{\phi g} \prec \mathrm{ld}_{ij}\})$.

3 Laurent Regular Differential Chains

In this section, we introduce the concept of Laurent regular differential chain and prove its basic properties. We first introduce some basic facts about characteristic set method in the algebraic case.

Let k be a field and $\mathbb{W} = \{w_1, w_2, \cdots, w_n\}$ a set of indeterminates. We let $k[\mathbb{W}] = k[w_1, w_2, \cdots, w_n]$ denote the ring of polynomials in $\mathbb{W}$ over k. Note that ld_f is now the leading variable for $f \in k[\mathbb{W}]$. $\mathcal{A} = A_1, A_2, \cdots, A_p$ in $k[\mathbb{W}]$ is called a triangular set if $\mathrm{ld}_{A_1} < \mathrm{ld}_{A_2} < \cdots < \mathrm{ld}_{A_p}$. Let $v_i = \mathrm{ld}_{A_i}$, $\mathbb{V} = \{v_1, v_2, \cdots, v_p\}$ and $\mathbb{U} = \mathbb{W} - \mathbb{V}$. $\mathbb{U}$ and $\mathbb{V}$ are called the parameter set and the leading variable set of $\mathcal{A}$, respectively. We denote $k[\mathbb{W}]$ as $k[\mathbb{U}, \mathbb{V}]$. A polynomial $f \in k[\mathbb{U}, \mathbb{V}]$ is said to be invertible w.r.t $\mathcal{A}$ if either $f \in k[\mathbb{U}]$ or $(f, A_1, A_2, \cdots, A_s) \bigcap k[\mathbb{U}] \neq \{0\}$ where $\mathrm{ld}_f = \mathrm{ld}_{A_s}$. $\mathcal{A}$ is called regular if its initials are invertible w.r.t. $\mathcal{A}$. A polynomial P is called reducible module $\mathcal{A}$ if there exist $0 \neq M \in k[\mathbb{U}]$, $P_1, P_2 \in k[\mathbb{W}]$ with the same leading variable as P and the initials of $P_i, i = 1, 2$ are invertible w.r.t $\mathcal{A}$ such that $MP = P_1 P_2 \bmod(\mathcal{A})$. If such M, P_1, P_2 do not exist, P is called irreducible module $\mathcal{A}$. $\mathcal{A}$ is called irreducible if A_1 is irreducible as a polynomial in $k[\mathbb{U}][v_1]$ and A_i is irreducible module $\mathcal{A}_{i-1} = \{A_1, A_2, \cdots, A_{i-1}\}$, $i = 2, 3, \cdots, p$. For instance, $A_1 = w_2^2 + w_1, A_2 = w_3^2 + w_1$ is a reducible chain, because $A_2 = (w_3 - w_2)(w_3 + w_2) + A_1$ is reducible module A_1. There exist algorithms to decompose a chain into several irreducible chains[4].

Lemma 3.1 (see [18]) *Let $\mathcal{A}$ be a regular chain in $k[\mathbb{W}]$. A polynomial f is not invertible w.r.t. $\mathcal{A}$ if and only if there exists a non-zero polynomial N reduced w.r.t. $\mathcal{A}$ such that $Nf \in$*

$(\mathcal{A})$.

Let $\mathcal{A}$ be a differential chain in $\mathcal{F}\{\mathbb{Y}\}$ and $\mathbb{U}$ be the set of differential indeterminates not occurring in the leaders of $\mathcal{A}$, which is called the parameter set of $\mathcal{A}$. Then $\mathcal{A}$ can be written as

$$\begin{array}{l} f_{11}(\mathbb{U},x_1), f_{12}(\mathbb{U},x_1),\cdots,f_{1s_1}(\mathbb{U},x_1),\\ \vdots \\ f_{p1}(\mathbb{U},x_1,x_2,\cdots,x_p), f_{p2}(\mathbb{U},x_1,x_2,\cdots,x_p),\cdots,f_{ps_p}(\mathbb{U},x_1,x_2,\cdots,x_p), \end{array} \tag{1}$$

where $\{x_1,x_2,\cdots,x_p\}=\mathbb{Y}-\mathbb{U}$ and $\mathrm{ld}_{f_{ij}}=\theta_{ij}x_i,\theta_{ij}\in\Theta$ and $f_{i,1}\prec f_{i,2}\prec\cdots\prec f_{i,s_i}$. For $\theta_1,\theta_2\in\Theta$, if there exists no $\theta\in\Theta$ such that $\theta_2=\theta_1\theta$, we denote $\theta_1\nmid\theta_2$. Let $\mathfrak{n}(\mathcal{A})=\bigcup_{i=1}^p\{\theta x_i:\theta_{ij}\nmid\theta, j=1,2,\cdots,s_i\}$.

Let $o_{ij}=\mathrm{ord}(f_{ij})=\mathrm{ord}(\theta_{ij})$ and $o\in\mathbb{N}$. Then denote

$$\mathcal{A}^{(o)}=\{\theta f_{ij}:\theta\in\Theta,\mathrm{ord}(\theta f_{ij})\le\widehat{o}\}, \tag{2}$$

where $\widehat{o}=\max\{o,o_{ij}:j=1,2,\cdots,s_i,i=1,2,\cdots,p\}$. It may happen that $\mathcal{A}^{(o)}$ contains $\theta_1 f_{ij}$ and $\theta_2 f_{ik}$ with the same leader. Since $\mathcal{A}$ is coherent, $\theta_1 f_{ij}$ and $\theta_2 f_{ik}$ are equivalent module $\mathcal{A}$ and we can delete one of them from $\mathcal{A}^{(o)}$.

Since the orderly ranking is used, $\mathcal{A}^{(o)}$ is a triangular set in the polynomial ring $\mathcal{F}[\{v:v\in\Theta(\mathbb{Y}),\mathrm{ord}(v)\le\widehat{o}\}]$ and $\mathfrak{n}(\mathcal{A})$ is the parameter set of $\mathcal{A}^{(o)}$.

Let $f\in\mathcal{F}\{\mathbb{Y}\}$. Then f is said to be invertible w.r.t. $\mathcal{A}$ if f is invertible w.r.t. $\mathcal{A}^{(\mathrm{ord}(f))}$ in the polynomial ring $\mathcal{F}[\Theta(\mathbb{Y})]$. Also, the pseudo-remainder $\mathrm{prem}(f,\mathcal{A})$ for differential polynomial f is defined to be the pseudo-remainder $\mathrm{prem}(f,\mathcal{A}^{\mathrm{ord}(f)})$ in the algebraic case[1].

Let $\mathcal{F}\{\mathbb{Y}\}$ be the differential polynomial ring as above. Define $\delta_j((\theta y_i)^{-1})=-(\theta y_i)^{-2}\delta_j\theta y_i$ and $\theta_1\theta_2((\theta y_i)^{-1})=\theta_1(\theta_2((\theta y_i)^{-1})), i=1,2,\cdots,n,\ j=1,2,\cdots,m$ and $\theta_1,\theta_2,\theta\in\Theta$. Denote $\Theta(\mathbb{Y}^{\pm})=\{\theta y_i,(\theta y_i)^{-1}:\theta\in\Theta,i=1,2,\cdots,n\}$. Then $\mathcal{F}[\Theta(\mathbb{Y}^{\pm})]$ forms a differential ring and we call $\mathcal{F}\{\mathbb{Y}^{\pm}\}=\mathcal{F}[\Theta(\mathbb{Y}^{\pm})]$ the Laurent differential polynomial ring in $\mathbb{Y}$ over $\mathcal{F}$.

A differential polynomial $f\in\mathcal{F}\{\mathbb{Y}\}$ is said to be monomial-primitive if no $\theta y_i\in\Theta(\mathbb{Y})$ divides f. Let f be a Laurent differential polynomial in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ of the form $f=\sum_{i=1}^s a_i m_i n_i^{-1}$, where m_i,n_i are monomials in $\mathcal{F}\{\mathbb{Y}\}$ and $\gcd(m_i,n_i)=1$. Then the normal form of f is defined to be the monomial primitive differential polynomial $\widetilde{f}=\frac{\mathrm{lcm}(n_1,n_2,\cdots,n_s)f}{\gcd(m_1,m_2,\cdots,m_s)}$, denoted by $\widetilde{f}$. Let $\mathbb{P}\subseteq\mathcal{F}\{\mathbb{Y}\}$, we denote $\widetilde{\mathbb{P}}=\{\widetilde{f}:f\in\mathbb{P}\}$.

Definition 3.2 A Laurent differential chain $\mathcal{A}$ in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ is defined to be a differential chain in $\mathcal{F}\{\mathbb{Y}\}$ such that every differential polynomial in $\mathcal{A}$ is monomial primitive. A characteristic set of a subset $\mathbb{P}\subseteq\mathcal{F}\{\mathbb{Y}^{\pm}\}$ is defined to be a Laurent differential chain which is a characteristic set of $\widetilde{\mathbb{P}}$.

A Laurent differential polynomial f is said to be reduced w.r.t. a Laurent differential chain $\mathcal{A}$ if $\widetilde{f}$ is reduced w.r.t. $\mathcal{A}$. $\mathcal{A}$ is a characteristic set of a differential ideal I in $\mathcal{F}\{\mathbb{Y}^{\pm}\}$ if and only if I contains no Laurent differential polynomial reduced w.r.t. $\mathcal{A}$. We define the pseudo-remaider of a Laurent differential polynomial f w.r.t. a Laurent differential chain $\mathcal{A}$ as $\mathrm{lprem}(f,\mathcal{A})=\mathrm{prem}(\widetilde{f},\mathcal{A})$.

Let $\mathcal{A} = A_1, A_2, \cdots, A_p$ be an autoreduced set of $\mathcal{F}\{\mathbb{Y}\}$, $Y_i = \mathrm{ld}_{A_i}$ and $V = \{V_1, V_2, \cdots, V_q\}$ be the set of the other indeterminates which are present in $\mathcal{A}$. With these replacements, $\mathcal{A}$ can be regarded as a chain in polynomial ring $\mathcal{F}[V_1, V_2, \cdots, V_q, Y_1, Y_2, \cdots, Y_p]$. Then $\mathcal{A}$ is called regular if the initials and separants of $\mathcal{A}$ regarded as algebraic polynomial are invertible w.r.t. $\mathcal{A}$ in $\mathcal{F}[V_1, V_2, \cdots, V_q, Y_1, Y_2, \cdots, Y_p]$ and $\mathcal{A}$ is called irreducible if $\mathcal{A}$ is irreducible as an algebraic chain in $\mathcal{F}[V_1, V_2, \cdots, V_q, Y_1, Y_2, \cdots, Y_p]$. It is easy to see that this definition coincides with that of invertibility in differential sense.

Definition 3.3 A Laurent differential chain $\mathcal{A}$ is called Laurent regular if $\mathcal{A}$ is a regular chain in $\mathcal{F}\{\mathbb{Y}\}$ and all the elements in $\Theta(\mathbb{Y})$ are invertible w.r.t. $\mathcal{A}$. If a Laurent regular chain $\mathcal{A}$ consists of one differential polynomial f, then f is called a Laurent regular differential polynomial.

Let $\mathcal{A}$ be a Laurent differential chain and $H_{\mathcal{A}}$ be the product of the initials and separants of $\mathcal{A}$. We define the saturated ideal of $\mathscr{A}$ in $\mathcal{F}\{Y\}$ and $\mathcal{F}\{Y^{\pm}\}$ to be

$$\mathrm{dsat}(\mathcal{A}) = [\mathscr{A}] : H_{\mathcal{A}}^{\infty} = \{f \in \mathcal{F}\{\mathbb{Y}\} \,|\, \exists m \in \mathbb{N}, \text{s.t.}\, H_{\mathcal{A}}^{m} f \in [\mathcal{A}]_{\mathcal{F}\{\mathbb{Y}\}}\}$$

and

$$\mathrm{ldsat}(\mathcal{A}) = [\mathcal{A}]_{\mathcal{F}\{\mathbb{Y}^{\pm}\}} : H_{\mathcal{A}}^{\infty} = \{f \in \mathcal{F}\{\mathbb{Y}^{\pm}\} \,|\, \exists m \in \mathbb{N}, \text{s.t.}\, H_{\mathcal{A}}^{m} f \in [\mathcal{A}]_{\mathcal{F}\{\mathbb{Y}^{\pm}\}}\}$$

respectively, where $[\mathcal{A}]_{\mathcal{F}\{\mathbb{Y}\}}$ ($[\mathcal{A}]_{\mathcal{F}\{\mathbb{Y}^{\pm}\}}$) is the differential ideal generated by $\mathcal{A}$ in $\mathcal{F}\{\mathbb{Y}\}$ ($\mathcal{F}\{\mathbb{Y}^{\pm}\}$). In the rest of this paper, we use $[P]$ to represent $[P]_{\mathcal{F}\{\mathbb{Y}\}}$ for any $P \subset \mathcal{F}\{\mathbb{Y}\}$. A basic fact about regular chains is:

Theorem 3.4 (see [20], Lemma 6.1) *Let $\mathcal{A} \subset \mathcal{F}\{\mathbb{Y}\}$ be a chain. Then $\mathcal{A}$ is the characteristic set of* $\mathrm{dsat}(\mathcal{A})$ *if and only if $\mathcal{A}$ is regular and coherent.*

The following theorem shows that similar property holds for Laurent regular chains.

Theorem 3.5 *Let $\mathcal{A}$ be a Laurent differential chain. Then $\mathcal{A}$ is a characteristic set of* $\mathrm{ldsat}(\mathcal{A})$ *if and only if $\mathcal{A}$ is Laurent regular and coherent.*

Proof First, suppose that $\mathcal{A}$ is a characteristic set of $\mathrm{ldsat}(\mathcal{A})$. Then $\mathcal{A}$ is a characteristic set of $\mathrm{dsat}(\mathcal{A})$. By Theorem 3.4, $\mathcal{A}$ is regular and coherent. If there exist $\theta \in \Theta$ and i such that θy_i is not invertible w.r.t. $\mathcal{A}$, then by Lemma 3.1, there exists a differential polynomial Q reduced w.r.t. $\mathcal{A}$ such that $(\theta y_i)Q \in [\mathcal{A}]$, which implies that $Q \in \mathrm{ldsat}(\mathcal{A})$, a contradiction.

For the converse implication, assume $\mathcal{A}$ is Laurent regular and coherent of form (1). Then by Theorem 3.4, $\mathcal{A}$ is the characteristic set of $\mathrm{dsat}(\mathcal{A})$. Now suppose that $f \in \mathrm{ldsat}(\mathcal{A})$ is reduced w.r.t. $\mathcal{A}$. Then there exists a differential monomial $M \in \mathcal{F}\{\mathbb{Y}\}$ such that $M\widetilde{f} \in \mathrm{dsat}(\mathcal{A})$. Because M is invertible w.r.t. $\mathcal{A}$, then by definition there exists a differential polynomial $P \in \mathcal{F}\{\mathbb{U}\}[\mathfrak{n}(\mathcal{A})]$ such that $P \in [\mathcal{A}, M]$, where $\mathbb{U}$ and $\mathfrak{n}(\mathcal{A})$ are defined as before. So $P\widetilde{f} \in \mathrm{dsat}(\mathcal{A})$. However $P\widetilde{f}$ is reduced w.r.t. $\mathcal{A}$, which is a contradiction. ∎

4 Reductions for the Decision Problem of Laurent Regularity

In this section, we reduce the problem of deciding whether an irreducible and coherent regular chain is Laurent regular from the multivariate case to the univariate case.

4.1 Reducing the Multivariate Case to the Univariate Case

In this section, let $\mathcal{A} \subset \mathcal{F}\{\mathbb{Y}\}$ be a Laurent differential chain, which is irreducible, coherent and regular. We want to know whether $\mathcal{A}$ is Laurent regular. We first prove a lemma.

Lemma 4.1 *A differential polynomial f is not invertible w.r.t. $\mathcal{A}$ if and only if* $\mathrm{prem}(f, \mathcal{A}) = 0$.

Proof Assume f is not invertible w.r.t. $\mathcal{A}$. By Lemma 3.1, there exists a differential polynomial N reduced w.r.t. $\mathcal{A}$ such that $Nf \in [\mathcal{A}]$. Let $g = \mathrm{prem}(f, \mathcal{A})$. Then $Ng \in \mathrm{dsat}(\mathcal{A})$. Since $\mathcal{A}$ is irreducible, we have $N \in \mathrm{dsat}(\mathcal{A})$ or $g \in \mathrm{dsat}(\mathcal{A})$. So $g = 0$ by Theorem 3.4. On the other hand, assume $\mathrm{prem}(f, \mathcal{A}) = 0$. Then there is an integer $m \in \mathbb{N}$ such that $H_{\mathcal{A}}^m f \in [\mathcal{A}]$. Since $\mathcal{A}$ is regular, $H_{\mathcal{A}}$ is invertible w.r.t. $\mathcal{A}$. Then there exists a differential polynomial $g' \in \mathcal{F}\{\mathbb{U}\}[\mathfrak{n}(\mathcal{A})]$ such that $g'f \in [\mathcal{A}]$. By Lemma 3.1, f is not invertible w.r.t. $\mathcal{A}$. ∎

Corollary 4.2 *An irreducible, coherent and regular chain $\mathcal{A}$ is not Laurent regular if and only if there exist $\theta \in \Theta, i \in [1, n]$ such that* $\mathrm{prem}(\theta y_i, \mathcal{A}) = 0$.

Corollary 4.3 *Let $\mathcal{A}$ be defined as in Lemma* 4.1 *and $\theta \in \Theta$. If θy_i is not invertible w.r.t. $\mathcal{A}$, then* $\mathrm{dsat}(\mathcal{A}) \bigcap \mathcal{F}\{y_i\} \neq \{0\}$.

Proof By Lemma 4.1, $\mathrm{prem}(\theta y_i, \mathcal{A}) = 0$, which implies $\theta y_i \in \mathrm{dsat}(\mathcal{A}) \bigcap \mathcal{F}\{y_i\}$. ∎

Lemma 4.4 *Let $f \in \mathcal{F}\{\mathbb{Y}\}$ be irreducible and there exist more than one indeterminates in f. Then f is Laurent regular.*

Proof Since $f \in \mathcal{F}\{\mathbb{Y}\}$ is an irreducible differential polynomial, f is the characteristic set of $\mathrm{dsat}(f)$ under any ranking. We will show that for any y_i, $\mathrm{dsat}(f) \bigcap \mathcal{F}\{y_i\} = \{0\}$ and hence f is Laurent regular by Corollary 4.3. If y_i does not occur in f, it is clear that $\mathrm{dsat}(f) \bigcap \mathcal{F}\{y_i\} = \{0\}$. Otherwise, we choose an elimination ranking with y_i as the smallest variable. Then, $\mathrm{ld}(f) = \theta y_k$ for $k \neq i$ and $\theta \in \Theta$. Then for any $g \in \mathcal{F}\{y_i\} \setminus \{0\}$, we have $\mathrm{prem}(g, f) = g \neq 0$ and hence $\mathrm{dsat}(f) \bigcap \mathcal{F}\{y_i\} = \{0\}$. The lemma is proved. ∎

Theorem 4.5 *Let $\mathcal{A}$ be an irreducible, coherent and regular differential chain in $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}\{\mathbb{U}, \mathbb{X}\}$ defined as in* (1). *Then deciding whether $\mathcal{A}$ is Laurent regular can be reduced to deciding whether an irreducible, coherent and regular differential chain in $\mathcal{F}\{y_i\}$ is Laurent regular, for $i = 1, 2, \cdots, n$.*

Proof First, it is easy to see that $\mathrm{dsat}(\mathcal{A}) \bigcap \mathcal{F}\{u\} = \{0\}$, where $u \in \mathbb{U}$. So by Corollary 4.3, $\theta u \in \Theta(\mathbb{Y})$ is invertible w.r.t. $\mathcal{A}$ for any $u \in \mathbb{U}$. Then using the algorithm given in [17] converting a characteristic set of a prime differential ideal from one ranking into another, we can compute an irreducible, coherent and regular chain $\mathcal{A}_i$ under the elimination ranking satisfying that x_i is of the lowest ranking. Note that $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_i)$. By Lemma 4.1, θx_i is invertible w.r.t. $\mathcal{A}_i$ if and only if θx_i is invertible w.r.t. $\mathcal{A}$. We denote $\mathcal{A}_i$ as the following form:

$$g_{11}, g_{12}, \cdots, g_{1l_1}, g_{21}, g_{22}, \cdots, g_{2l_2}, \cdots, g_{p1}, g_{p2}, \cdots, g_{pl_p},$$

where $\mathrm{ld}_{g_{j1}}, \mathrm{ld}_{g_{j2}}, \cdots, \mathrm{ld}_{g_{jl_j}} \in \Theta(y_{s_j})$ and $g_{i1} \prec g_{i2} \prec \cdots \prec g_{il_i}$. If $\mathrm{ld}_{g_{11}}$ is not in $\Theta(x_i)$, then no $\mathrm{ld}_{g_{kl}}$ is in $\Theta(x_i)$ by the definition of the ranking. So in this case, $\mathrm{dsat}(\mathcal{A}) \bigcap \mathcal{F}\{x_i\} =$

$\{0\}$, which implies that θx_i is invertible w.r.t. $\mathcal{A}_i$ by Corollary 4.3. Thus we need only to consider the case that $\mathrm{ld}_{g_{11}} \in \Theta(x_i)$, that is $g_{11}, g_{12}, \cdots, g_{1l_1} \in \mathcal{F}\{x_i\}$. Then $\mathrm{dsat}(\mathcal{A}) \bigcap \mathcal{F}\{x_i\} = \mathrm{dsat}(\mathcal{A}_i) \bigcap \mathcal{F}\{x_i\} = \mathrm{dsat}(\{g_{11}, g_{12}, \cdots, g_{1l_1}\})$. By Theorem 4.1 , θx_i is invertible w.r.t. $\mathcal{A}_i$ if and only if it is invertible w.r.t. $g_{11}, g_{12}, \cdots, g_{1l_1}$. So deciding whether θx_i is invertible w.r.t. $\mathcal{A}$ can be reduced to deciding whether an irreducible, coherent and regular chain $g_{11}, g_{12}, \cdots, g_{1l_1}$ in $\mathcal{F}\{x_i\}$ is Laurent regular. The theorem is proved. ∎

Remark 4.6 We assume that $\mathcal{A}$ is irreducible for two reasons. First, irreducible chains have nice properties which are necessary for our results. Second, even in this special case, it is still open to decide whether $\mathcal{A}$ is Laurent regular. If $\mathcal{A}$ is not irreducible, then Theorem 4.5 is not valid.

4.2 Reducing the Univariate Case to the Single Polynomial Case

Now we consider an irreducible, coherent and regular differential chain $\mathcal{A}$ in one differential indeterminate and show that the problem of deciding whether $\mathcal{A}$ is Laurent regular can be reduced to that of deciding whether a single differential polynomial is Laurent regular in certain cases. Let y be a new differential indeterminate and $\mathcal{F}\{y\}$ the differential polynomial ring in y over $\mathcal{F}$.

Lemma 4.7 *Let $\mathcal{A} = f_1(y), f_2(y), \cdots, f_r(y)$ in $\mathcal{F}\{y\}$ be an irreducible, coherent and regular differential chain under the ranking satisfying $\delta_1^{i_1}\delta_2^{i_2}\cdots\delta_m^{i_m}y \prec \delta_1^{j_1}\delta_2^{j_2}\cdots\delta_m^{j_m}y$ if and only if $(i_1, i_2, \cdots, i_m) \prec_{lex} (j_1, j_2, \cdots, j_m)$. If $\mathrm{ld}_{f_1} = \delta_1^{k_1}\delta_2^{k_2}\cdots\delta_m^{k_m}y$ and $k_i \neq 0$ for certain $i < m$, then $\delta_m^t y$ is invertible w.r.t. $\mathcal{A}$, for any $t \in \mathbb{N}$.*

Proof We first show that $\delta_m^t y$ is reduced w.r.t. $\mathcal{A}$, for any $t \in \mathbb{N}$. Assume the contrary: There exists an $s \in \mathbb{N}$ such that $\delta_m^s y$ is not reduced w.r.t. $\mathcal{A}$. Then there exist $j \in [1, r]$ and $\theta \in \Theta$ such that $\delta_m^s y = \theta \mathrm{ld}_{f_j}$. Then $\mathrm{ld}_{f_j} = \delta_m^u y$ for some nonnegative integer u. By the definitions of lexicographical rank and the differential chain, this may happen only if $j = 1$, which is a contradiction to the hypothesis. Now, the lemma follows from Lemma 4.1. ∎

Theorem 4.8 *Let $\mathcal{A} = f_1(y), f_2(y), \cdots, f_r(y)$ be an irreducible, coherent and regular differential chain in $\mathcal{F}\{y\}$. Then for a fixed $i \in [1, m]$ and $t \in \mathbb{N}$, deciding whether $\delta_i^t y$ is invertible w.r.t. $\mathcal{A}$ can be reduced to deciding whether $\delta_i^t y$ is invertible w.r.t. a differential polynomial in $\mathcal{F}[y, \delta_i y, \cdots, \delta_i^q y]$ for some $q \in \mathbb{N}$.*

Proof Using the algorithm given in [17] converting a characteristic set of a prime differential ideal from one ranking into another, we can compute an irreducible, regular and coherent chain $\mathcal{A}_i$ under the ranking satisfying that $\delta_1^{a_1}\delta_2^{a_2}\cdots\delta_i^{a_i}\cdots\delta_m^{a_m}y \prec \delta_1^{b_1}\delta_2^{b_2}\cdots\delta_i^{b_i}\cdots\delta_m^{b_m}y, k = 1, 2, \cdots, p$ if and only if $(a_1, a_2, \cdots, a_{i-1}, a_{i+1}, \ldots, a_m, a_i) \prec_{lex} (b_1, b_2, \cdots, b_{i-1}, b_{i+1}, \cdots, b_m, b_i)$, where $\prec_{lex}$ is the lexicographic order in $\mathbb{N}^m$. Note that $\mathrm{dsat}(\mathcal{A}) = \mathrm{dsat}(\mathcal{A}_i)$. So $\delta_i^t y$ is invertible w.r.t. $\mathcal{A}$ if and only if $\delta_i^t y$ is invertible w.r.t. $\mathcal{A}_i$ by Lemma 4.1. Let $\mathcal{A}_i = g_1(y), g_2(y), \cdots, g_s(y)$. Suppose that $\mathrm{ld}_{g_1} = \theta y$ for some $\theta \in \Theta$. If δ_d appears in θ for some $d \neq i$, then $\delta_i^t y$ is invertible w.r.t. $\mathcal{A}_i$ by Lemma 4.7. So we just consider the case that $\mathrm{ld}_{g_1} = \delta_i^q y$ for some $q \in \mathbb{N}$. It is easy to see that for this case, ld_{g_k} is not of the form $\delta_i^{s_k} y, k > 1$ by the definition of a chain. So deciding whether $\delta_i^t y$ is invertible w.r.t. $\mathcal{A}$ can be reduced to deciding whether $\delta_i^t y$ is invertible w.r.t. g_1 in $\mathcal{F}[y, \delta_i y, \cdots, \delta_i^q y]$. The theorem is proved. ∎

5 Deciding Laurent Regularity for Univariate Differential Polynomial

In this section, we give a partial method to decide whether an irreducible univariate differential polynomial is Laurent regular. Precisely, we consider whether $\delta_i^s y$ is invertible with respect to a differential polynomial $f \in K\{y\}$ for $\delta_i \in \Delta$ and $s \in \mathbb{N}$. Following Theorem 4.8, decision of whether a differential chain is Laurent regular can be reduced to this problem in certain cases.

In this section, we assume that $\mathcal{F} = \mathbb{Q}(t_1, t_2, \cdots, t_m)$ and the differential operators are $\delta_i = \frac{\partial}{\partial t_i}$ for $i = 1, 2, \cdots, m$. Let y be a differential indeterminate and all differential polynomials in this section are in $\mathcal{F}\{y\}$.

5.1 Laurent Regularity and Structure of Solutions

The following lemma gives a connection between the fact that f is Laurent regular and the structure of the generic zeros of (f). We need the following facts. Let I be a differential prime ideal. Then I has a generic zero η with the following property: A differential polynomial f is in I if and only if $f(\eta) = 0$[1]. Also, if $\mathcal{A}$ is an irreducible, coherent and regular differential chain, then dsat$(\mathcal{A})$ is a prime ideal and hence has a generic zero[1].

Lemma 5.1 *Let $\mathcal{A}$ be an irreducible, coherent and regular differential chain in $\mathcal{F}\{y\}$. Then $\widetilde{y} = \sum_{i=0}^{o_1-1} a_{1i}(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} a_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_m-1} a_{mi}(\widehat{t_m})t_m^i$ is a generic zero of* dsat$(\mathcal{A})$ *if and only if* $\mathrm{prem}(\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}y,\ \mathcal{A}) = 0$*, where $\widehat{t_i}$ is the set $\{t_1, t_2, \cdots, t_{i-1}, t_{i+1}, \cdots, t_m\}$ and $a_{ij}(\widehat{t_i})$ is a differentiable function in $\widehat{t_i}$. In other words, $\mathcal{A}$ is not Laurent regular if and only if* dsat$(\mathcal{A})$ *has a generic zero of the form $\widetilde{y} = \sum_{i=0}^{o_1-1} a_{1i}(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} a_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_m-1} a_{mi}(\widehat{t_m})t_m^i$.*

Proof If $\widetilde{y} = \sum_{i=0}^{o_1-1} a_{1i}(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} a_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_m-1} a_{mi}(\widehat{t_m})t_m^j$ is a generic zero of dsat$(\mathcal{A})$, then $\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}\widetilde{y} = 0$. So $\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}y \in$ dsat$(\mathcal{A})$, which implies that $\mathrm{prem}(\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}y, \mathcal{A}) = 0$ by Theorem 3.4. For the other direction, assume that prem $(\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}y, \mathcal{A}) = 0$. Then $\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}y \in$ dsat$(\mathcal{A})$. If $\widetilde{y}$ is a generic solution of dsat$(\mathcal{A})$, then $\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}\widetilde{y} = 0$. We claim that $\widetilde{y}$ must be of the form $\widetilde{y} = \sum_{i=0}^{o_1-1} a_1(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} a_2(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_m-1} a_{mi}(\widehat{t_m})t_m^i$ and $a_{ij}(\widehat{t_i})$ is a differentiable function in $\widehat{t_i}$, where $j = 0, 1, \cdots, o_i - 1, i = 1, 2, \cdots, n$. We use the inductive method to prove this claim. Indeed, it is easy to see that $\delta_m^{o_m}\widetilde{y} = 0$ implies that $\widetilde{y} = \sum_{i=0}^{o_m-1} a_i(\widehat{t_m})t_m^i$, where $a_i(\widehat{t_m})$ is a differentiable function in $\widehat{t_m}$. Then $\delta_1^{o_1}\delta_2^{o_2}\cdots\delta_m^{o_m}\widetilde{y} = \delta_1^{o_1}\delta_2^{o_2}\cdots\delta_{m-1}^{m-1}(\delta_m^{o_m}\widetilde{y}) = 0$ implies that $\delta_m(\delta_m^{o_m-1}\widetilde{y}) = \delta_m^{o_m}\widetilde{y} = \sum_{i=0}^{o_1-1} c_{1i}(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} c_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_{m-1}-1} c_{m-1,i}(\widehat{t_{m-1}})t_{m-1}^j$ by induction, where $c_{ij}(\widehat{t_i})$ is a differentiable function in $\widehat{t_i}$. So

$$\delta_m^{o_m-1}\widetilde{y} = \sum_{i=0}^{o_1-1} c'_{1i}(\widehat{t_1})t_1^i + \sum_{i=0}^{o_2-1} c'_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_{m-1}-1} c'_{m-1,i}(\widehat{t_{m-1}})t_{m-1}^i + c'_{m,o_m-1}(\widehat{t_m}), \quad (3)$$

where $\delta_m c'_{ij}(\widehat{t_i}) = c_{ij}(\widehat{t_i})$ and $c'_{m,o_m-1}(\widehat{t_m})$ is a differentiable function in $\widehat{t_m}$. Then integral each side of the equation (3) $o_m - 1$ times with respect to t_m, we obtain that $\widetilde{y} = \sum_{i=0}^{o_1-1} a_{1i}(\widehat{t_1})t_1^i +$

$\sum_{i=0}^{o_2-1} a_{2i}(\widehat{t_2})t_2^i + \cdots + \sum_{i=0}^{o_m-1} a_{mi}(\widehat{t_m})t_m^j$, where $\delta_m^{o_m-1} a_{ij}(\widehat{t_i}) = c'_{ij}(\widehat{t_i})$, $i = 1, 2, \cdots, m-1, j = 0, 1, \cdots, o_m - 1$ and $\delta_m^{o_m-1} a_{m,o_m-1}(\widehat{t_m}) = c'_{m,o_m-1}(\widehat{t_m})$ and $a_{m,j}(\widehat{t_m})$ is a differentiable function in $\widehat{t_m}$, $j = 0, 1, \cdots, o_m - 2$. Then this lemma is proved. ∎

Corollary 5.2 *The generic zero of* $\mathrm{dsat}(\mathcal{A})$ *is a polynomial in* $t_1, t_2, \cdots, t_m$ *if and only if for* $i = 1, 2, \cdots, m$, *there exists* $a_i \in \mathbb{N}$ *such that* $\mathrm{prem}(\delta_i^{a_i} y, \mathcal{A}) = 0$.

5.2 First Order Differential Polynomials

Let f be an irreducible differential polynomial in $\mathcal{F}\{y\}$ of the form below:

$$f(y) = \sum_{(\alpha,\beta)\in\mathbb{N}\times\mathbb{N}^{o+1}, \sum \beta_i \le D} c_{\alpha,\beta} t_1^{\alpha} \prod_{i=0}^{o} (\delta_1^i y)^{\beta_i}, \tag{4}$$

where $c_{\alpha,\beta} \in \mathbb{Q}[t_2, t_3, \cdots, t_m]$ and $D \in \mathbb{N}$. We want to decide whether there exists a $j \in \mathbb{N}$ such that $\delta_1^j y$ is not invertible w.r.t. f. For $i > 1$, the discussion for $\delta_i^j y$ is similar.

By Lemma 4.1 and Lemma 5.1, $\delta_1^j y$ is not invertible w.r.t. f if and only if $\delta_1^j y \in \mathrm{dsat}(f)$, or equivalently $f(y) = 0$ has a generic solution that is a polynomial in t_1 with coefficients being differentiable functions in $t_2, t_3, \cdots, t_m$. Therefore, we need to give a method to find an upper bound for N such that

$$\widetilde{y} = \sum_{i=0}^{N} a_i(\widehat{t_1}) t_1^i \tag{5}$$

is a solution of $f = 0$, where $a_i(\widehat{t_1})$ is a differentiable function in $\widehat{t_1} = \{t_2, t_3, \cdots, t_m\}$, $i = 0, 1, \cdots, N$.

Definition 5.3 For $f(y)$ given in (4), we set

$$\varepsilon(f(y)) = \{P(\alpha, \beta) = (\alpha - \beta_1 - 2\beta_2 - \cdots - o\beta_o, \beta_0 + \beta_1 + \cdots + \beta_o : c_{\alpha,\beta} \ne 0\}.$$

Define $NP(f(y))$ to be the convex hull of $\varepsilon(f(y))$ in $\mathbb{R}^2$. In the rest of this paper, we use u and v to represent horizontal and vertical axes of $\mathbb{R}^2$, respectively.

Definition 5.4 Given $f(y)$ in (4) and $\mu \in \mathbb{R}$, a line $L(f, \mu)$ in $\mathbb{R}^2$ defined by $u + \mu v = w$ for some $w \in \mathbb{R}$ is called feasible for $f(y)$ if $NP(f(y)) \bigcap L(f, \mu) \ne \varnothing$ and $NP(f(y))$ lies in the left side of $L(f, \mu)$, which means that for any point $(u_0, v_0) \in NP(f(y))$, $u_0 + \mu v_0 \le w$.

Definition 5.5 Let $f(y)$ be defined as in (4). We denote the vertexes of $NP(f)$ from the top-right to the right-most clockwisely as $P_1, P_2, \cdots, P_l$, where $P_i = (u_i, v_i)$. Then the line $P_i P_{i+1}$, $i = 1, 2, \cdots, l-1$, is denoted as l_i and its slope is $\frac{v_{i+1}-v_i}{u_{i+1}-u_i} < 0$. We set $s_i = -\frac{u_{i+1}-u_i}{v_{i+1}-v_i} > 0$, for $i = 1, 2, \cdots, l-1$, $s_0 = +\infty$ and $s_l = 0$, for $l \ge 2$. If $l = 1$, set $s_1 = 0$.

It is easy to see that

Lemma 5.6 *We have* $s_0 > s_1 > \cdots > s_{l-1} > s_l \ge 0$ *and the lines*

$$L(f, \delta_i) : u + \delta_i v = u_i + \delta_i v_i, \quad \delta_i \in [s_i, s_{i-1}), \quad i = 1, 2, \cdots, l-1$$

are all the feasible lines for $f(y)$ *and their slopes are negative.*

For $P_i = (u_i, v_i)$ introduced in Definition 5.5, we define the polynomials

$$\Phi_i(\mu) = \sum_{P(\alpha,\beta)=(u_i,v_i)} c_{\alpha,\beta}(\mu)_1^{\beta_1}(\mu)_2^{\beta_2}\cdots(\mu)_o^{\beta_o} \in \mathbb{Q}[t_2, t_3, \cdots, t_m, \mu], \tag{6}$$

where $i = 1, 2, \cdots, l$ and $(\mu)_k = \mu(\mu-1)\cdots(\mu-k+1)$. Then $\Phi_i(\mu)$ can be written as $\Phi_i(\mu) = \sum_{j=1}^{l_i} a_{ij}M_{ij}$, where a_{ij} is a polynomial in $\mathbb{Q}[\mu]$ and M_{ij} is a monomial in $t_2, t_3, \cdots, t_m$.

We first consider the case that $\text{ord}(f) = 1$. The following theorem gives a complete method of deciding whether there exists a $j \in \mathbb{N}$ such that $\delta_1^j y$ is invertible w.r.t. f.

Theorem 5.7 *Assume that* $f(y) = \sum_{(\alpha,\beta)\in\mathbb{N}\times\mathbb{N}^2} c_{\alpha,\beta_0,\beta_1} t_1^{\alpha} y^{\beta_0}(\delta_1 y)^{\beta_1}$ *and* $P_1, P_2, \cdots, P_l$ *and* $s_1, s_2, \cdots, s_l$ *are defined as in Definition* 5.5. *Then* Φ_i *in* (6) *becomes*

$$\Phi_i = c_{u_i,v_i,0} + c_{u_i+1,v_i-1,1}\mu + \cdots + c_{u_i+v_i,0,v_i}\mu^{v_i} = \sum_{j=1}^{l_i} a_{ij}M_{ij} \neq 0, \tag{7}$$

where $M_{ij} \in \mathbb{Q}[t_2, t_3, \cdots, t_m]$ *and* $a_{ij} \in \mathbb{Q}[\mu]$. *If there exists an* $n \in (s_i, s_{i-1})\bigcap\mathbb{N}$ *such that* $a_{ij}(n) = 0, j = 1, 2, \cdots, l_i$ *we denote* η_i *to be the maximal number satisfying the condition. Otherwise, set* $\eta_i = s_i$. *Let* M *be the first positive integer in the sequence* $\eta_1, \eta_2, \cdots, \eta_l$. *If such an* M *exists and* (5) *is a solution of* $f = 0$, *then* $N \leq M$. *Otherwise, let* $M = -1$ *and* $f(y) = 0$ *has no solution of the form* (5).

Proof If such an M exists, then $\exists i_0 \in \{1, 2, \cdots, l\}$ such that $M = \eta_{i_0} \in [s_{i_0}, s_{i_0-1})$. Suppose that there is a number $\mu_0 \in \mathbb{N}$ such that $M < \mu_0$ and $\widetilde{y} = a_{\mu_0}t_1^{\mu_0} + a_{\mu_0-1}t_1^{\mu_0-1} + \cdots + a_0$ is a solution of $f(y) = 0$, where a_i is a function in $t_2, t_3, \cdots, t_m$ and $a_{\mu_0} \neq 0$. Then μ_0 must be in $[s_i, s_{i-1})$ for some $i \leq i_0$. Substitute $\widetilde{y}$ into $f(y)$ and we have

$$f(\widetilde{y}) = \sum c_{\alpha,\beta_0,\beta_1} t_1^{\alpha}(a_{\mu_0}t_1^{\mu_0} + a_{\mu_0-1}t_1^{\mu_0-1} + \cdots + a_0)^{\beta_0}(\mu_0 a_{\mu_0}t_1^{\mu_0-1} + (\mu-1)a_{\mu_0-1}t_1^{\mu_0-2} + \cdots + a_1)^{\beta_1}.$$

The leading term in the expansion of $c_{\alpha,\beta_0,\beta_1}t_1^{\alpha}y^{\beta_0}\delta_1 y^{\beta_1}$ in $f(\widetilde{y})$ is

$$c_{\alpha,\beta_0,\beta_1} a_{\mu_0}^{\beta_0+\beta_1}\mu_0^{\beta_1} t_1^{\alpha-\beta_1+\mu_0(\beta_0+\beta_1)}.$$

If we choose the maximal number in $\{\alpha - \beta_1 + \mu_0(\beta_0+\beta_1) : c_{\alpha,\beta_0,\beta_1} \neq 0\}$, denoted by $u_0 + \mu_0 v_0$, where $u_0 = \alpha - \beta_1$, $v_0 = \beta_0 + \beta_1$ for some $c_{\alpha,\beta_0,\beta_1} \neq 0$. Then $u + \mu_0 v \leq u_0 + \mu_0 v_0$, for any $(u, v) \in \varepsilon(f)$. So we can define the line $L(f, \mu_0) : u + \mu_0 v = u_0 + \mu_0 v_0$, which is feasible for $f(y)$. Because $\mu_0 \in [s_i, s_{i-1})$, $(u_0, v_0) = (u_i, v_i)$ or (u_{i+1}, v_{i+1}). Then we consider the coefficient of $t_1^{u_0+\mu_0 v_0}$ in the expansion of $f(\widetilde{y})$: $H = \sum_{\alpha-\beta_1+\mu_0(\beta_0+\beta_1)=u_0+\mu_0 v_0} c_{\alpha,\beta_0,\beta_1}\mu_0^{\beta_1}a_{\mu_0}^{\beta_0+\beta_1} = \sum_{(\alpha-\beta_1,\beta_0+\beta_1)\in L(f,\mu_0)} c_{\alpha,\beta_0,\beta_1}\mu_0^{\beta_1}a_{\mu_0}^{\beta_0+\beta_1}$, and it must be zero. Now we consider two cases.

1) If there exists only one vertex $(u_0, v_0) \in L(f, \mu_0)\bigcap NP(f)$, then H can be written as $H = \sum_{k=0}^{v_0} c_{u_0+k,v_0-k,k}\mu_0^k a_{\mu_0}^{v_0} = a_{\mu_0}^{v_0}\Phi_i(\mu_0)$. So μ_0 must be a positive integer such that $\Phi_i \equiv 0$, which implies $a_{ij}(\mu_0) = 0, j = 1, 2, \cdots, l_1$. Thus, if $i < i_0$, we have $M < \mu_0 \leq \eta_i \in \mathbb{N}$, a contradiction to the choice of m. Otherwise, $i = i_0$ implies $M \geq \mu_0$, a contradiction to the choice of μ_0.

2) If $L(f, \mu_0)\bigcap NP(f)$ is an edge of $NP(f)$, $\mu_0 = s_i$. If $i = i_0$, $\mu_0 = s_{i_0} \leq M < \mu_0$, a contradiction. If $i < i_0$, $M < \mu_0 \leq \eta_i \in \mathbb{N}$, a contradiction to the choice of M. ∎

As a direct consequence, we have

Corollary 5.8 *Let f be an irreducible differential polynomial of order* 1 *in the ordinary differential ring $\mathcal{F}\{y\}$ ($m = 1$). Then we can decide whether f is Laurent regular.*

Example 5.9 Assume that $f(y) = t_1^2\delta_1^2 y - 3t_1\delta_1 y + 3y - 3t_2^2$ is a partial differential polynomial in $\mathbb{Q}(t_1, t_2)\{y\}$. Then $\varepsilon(f) = \{(0,\ 1), (0,\ 0)\}$ and $NP(f)$ is a segment connecting two points in $\varepsilon(f)$. Then $P_1 = (0, 1), P_2 = (0, 0), s_0 = +\infty, s_1 = 0$ and $\Phi_1 = \mu^2 - 4\mu + 3$. We have $\eta_1 = 3$ and $\eta_2 = 0$. By Theorem 5.7, an upper bound for the degrees of the polynomial solutions of $f(y) = 0$ is 3. Because $\text{prem}(\delta_1^4 y, f) = 0$, $\delta_1^4 y$ is not invertible w.r.t. f. Thus f is not a Laurent regular polynomial. A generic solution of $f(y) = 0$ is $a_3(t_2)t_1^3 + a_1(t_2)t_1 + t_2^2$, where $a_3(t_2)$ and $a_1(t_2)$ are arbitrary differential functions in t_2.

Example 5.10 Assume that $f(y) = t_2^2(\delta_1 y)^2 - 2t_2\delta_1 y - 4y + 4t_1$ is a partial differential polynomial in $\mathbb{Q}(t_1, t_2)\{y\}$. Then $\varepsilon(f) = \{(-2,\ 2), (-1,\ 1), (0,\ 1), (1,\ 0)\}$ and $NP(f)$ is given in Figure 1. Then $P_1 = (-2, 2), P_2 = (0, 1), P_3 = (1, 0), s_0 = +\infty, s_1 = 2, s_2 = 1, s_3 = 0$ and $\Phi_1 = \mu^2 t_2^2$, $\Phi_2 = -4$, $\Phi_3 = 4$. We have $\eta_1 = 2, \eta_2 = 1, \eta_3 = 0$. By Theorem 5.7, an upper bound for the degrees of the polynomial solutions of $f(y) = 0$ is 2. Because $\text{prem}(\delta_1^3 y, f) \neq 0$, $\delta_1^i y$ is invertible w.r.t. f, for any $i \in \mathbb{N}$.

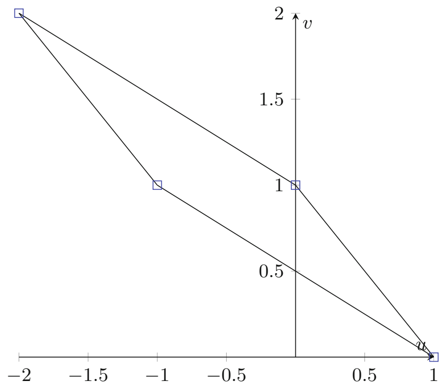

Figure 1 $NP(f)$ for f in Example 5.10

5.3 Higher Order Differential Polynomial

We now consider the general case and a partial solution is given to decide whether $\delta_1^j y$ is not invertible w.r.t. a given f.

Theorem 5.11 *For $f(y) \in \mathcal{F}\{y\}$ of order o as defined in* (4),

$$\Phi_1(\mu) = \sum_{P(\alpha,\beta)=(u_1,v_1)} c_{\alpha,\beta}(\mu)_1^{\beta_1}(\mu)_2^{\beta_2}\cdots(\mu)_o^{\beta_o} = \sum_{j=1}^{l_1} a_{1j}M_{1j}.$$

Use the notations in Definition 5.5*. Then*

1) *If Φ_1 is not the zero polynomial and $l \geq 2$, let $M \in [s_1, +\infty)$ be the maximal integer such that $a_{1j}(M) = 0, j = 1, 2, \cdots, l_1$. Assume that $f = 0$ has solution of the form* (5)*. If such a number exists, then $N \leq M$. Otherwise, $N \leq M = \lfloor s_1 \rfloor$.*

2) If Φ_1 is not the zero polynomial and $l = 1$, let M be the maximal integer root of $a_{1j}(\mu), j = 1, 2, \cdots, l_1$ in $(0, +\infty)$. If such a number exists and $f = 0$ has solutions of the form (5), *then $N \le M$. Otherwise, $f = 0$ has no solutions of the form* (5).

3) If $\Phi_1 \equiv 0$ and $l \ge 2$, let $M = \lfloor s_1 \rfloor$. If $\mathrm{prem}(\delta_1^{M+1} y, f) = 0$, then $f(y) = 0$ has solutions of the form (5) *with $N \le M + 1$.*

Proof 1) If $M_1 \ge s_1$ and $\widetilde{y} = \sum_{i=0}^{M_1} a_i t_1^i$ is a polynomial solution of $f(y) = 0$ with $a_{M_1} \ne 0$ and a_i are functions in $t_2, t_3, \cdots, t_m$, then $u_1 + M_1 v_1 > u + M_1 v$ for any $(u_1, v_1) \ne (u, v) \in \varepsilon(f)$. Indeed, from the line $L(f, s_1) : u + s_1 v = u_1 + s_1 v_1$, we have $u + s_1 v \le u_1 + s_1 v_1$, for any $(u_1, v_1) \ne (u, v) \in \varepsilon(f)$. Then $u_1 + M_1 v_1 = u_1 + s_1 v_1 + (M_1 - s_1) v_1 \ge u + s_1 v + (M_1 - s_1) v_1 > u + s_1 v + (M_1 - s_1) v = u + M_1 v$, for any $(u_1, v_1) \ne (u, v) \in \varepsilon(f)$. So as in the proof of Theorem 5.7, the leading term of $f(\widetilde{y})$ is $\sum_{P(\alpha,\beta)=(u_1,v_1)} c_{\alpha,\beta} (M_1)_1^{\beta_1} (M_1)_2^{\beta_2} \cdots (M_1)_o^{\beta_o} a_{M_1}^{v_1} t_1^{u_1 + M_1 v_1}$. Because $f(\widetilde{y}) = 0$ and $a_{M_1} \ne 0$, we have

$$\Phi_1(M_1) = \sum_{P(\alpha,\beta)=(u_1,v_1)} c_{\alpha,\beta} (M_1)_1^{\beta_1} (M_1)_2^{\beta_2} \cdots (M_1)_o^{\beta_0} = \sum_{j=1}^{l_1} a_{1j}(M_1) M_{1j} = 0.$$

So if $a_{11}(\mu), a_{12}(\mu), \cdots, a_{1l_1}(\mu)$ have no positive integer roots larger than s_1, the degree of the solutions which are polynomials in t_1 of $f(y) = 0$ is not larger than s_1. Otherwise, the number M exists and we have $M_1 < M$ by the choice of M.

2) $t = 1$ implies that $L(f, \delta) : u + \delta v = u_1 + \delta v_1, 0 < \delta < +\infty$ are all the feasible lines and $L(f, \delta) \bigcap NP(f) = \{(u_1, v_1)\}$, which means that for any $(u', v') \in NP(f), (u', v') \ne (u_1, v_1)$ and we thus have $u' + \delta v' < u_1 + \delta v_1$. Then if $y' = \sum_{i=0}^{N} a_i t_1^i$ is a solution of $f(y) = 0$, where $a_N \ne 0$ and a_i are functions in $t_2, t_3, \cdots, t_m$, substituting y' into $f(y)$ and we have that the leading term of $f(y')$ is $a_N^{v_1} \Phi_1 t_1^{u_1 + N v_1}$. So $\Phi_1(N) \equiv 0$, which means $a_{1j}(N) = 0$. Because Φ_1 is not the zero polynomial, we have $N \le M$.

Note that Case 3) is trivial. ∎

5.4 Complexity Analysis

From Theorems 5.7 and 5.11, we can find a bound O in certain cases such that $\delta_1^O y_1$ is invertible w.r.t f if and only if $\mathrm{prem}(\delta_1^O y_1, f) \ne 0$. In this section, we estimate the complexity of computing $\mathrm{prem}(\delta_1^O y_1, f)$. We need the following lemma.

Lemma 5.12 (see [33], Lemma 26) *Let $\mathcal{A} = \{A_1, A_2, \cdots, A_p\}$ be a triangular set in a polynomial ring $\mathcal{F}[y_1, y_2, \cdots, y_n]$. Set $M = \max_i\{\deg(A_i)\}$. Then for any $f \in \mathcal{F}[y_1, y_2, \cdots, y_n]$, $\deg(f) = D$, the pseudo-remainder r of f w.r.t. $\mathcal{A}$ can be computed with at most $[2(D+1)^n (M+1)^{n(p+1)}]^{2.376}$ $\mathcal{F}$-arithmetic operations and the degree of r is bounded by $(M+1)^p (D+1)$.*

The following theorem gives the complexity of computing the pseudo remainder of one differential polynomial w.r.t another one.

Theorem 5.13 *Let $f, g \in \mathcal{F}\{y\}$. Set $D = \deg(f)$, $O = \mathrm{ord}(f)$, $M = \deg(g)$, $o = \mathrm{ord}(g)$ and $\widehat{O} = \max\{o, O\}$. Then $\mathrm{prem}(f, g)$ can be computed at most $2^{2.376}[(D+1)(M+1)^{\binom{\hat{O}-o+m}{m}+1}]^{2.376\binom{\hat{O}+m}{m}}$ $\mathcal{F}$-arithmetic operations and its degree is bounded by $(M+1)^{\binom{\hat{O}-o+m}{m}}(D+1)$.*

Proof Let $G = g, \theta_1 g, \cdots, \theta_s g$ be a chain under a fixed orderly ranking with $\mathrm{ord}(\theta_s g) \le \widehat{O}$, where $\theta_1, \theta_2, \cdots, \theta_s \in \Theta$. Note that $\deg(\theta_i g) = \deg(g)$ for each i. Then $s \le \binom{\hat{O}-o+m}{m} - 1$ and the number of the set $\{u \in \Theta(\mathbb{Y}) : \mathrm{ord}(u) \le \widehat{O}\}$ is $\binom{\hat{O}+m}{m}$. Since $\mathrm{prem}(f,g) = \mathrm{prem}(f,G)$, by Lemma 5.12, the remainder of f w.r.t. G is of degree bounded by $(M+1)^{\binom{\hat{O}-o+m}{m}}(D+1)$. And it can be computed with at most

$$2^{2.376}[(D+1)(M+1)^{\binom{\hat{O}-o+m}{m}}+1]^{2.376\binom{\hat{O}+m}{m}}$$

$\mathcal{F}$-arithmetic operations. ∎

The complexity is high because the number of variables and the number of differential polynomials in $G = \{g, \theta_1 g, \theta_2 g, \cdots, \theta_s g\}$ is large due to the existence of the the partial differential operators. As a direct consequence, we have

Corollary 5.14 *Let $g \in \mathcal{F}\{y\}$ with $M = \deg(g)$ and $o = \mathrm{ord}(g)$. For $\theta \in \Theta$ and $\mathrm{ord}(\theta) = O \ge o$, $\mathrm{prem}(\theta y, g)$ can be computed at most $2^{2.376}[2(M+1)^{\binom{O-o+m}{m}}+1]^{2.376\binom{O+m}{m}}$ $\mathcal{F}$-arithmetic operations and its degree is bounded by $2(M+1)^{\binom{\hat{O}-o+m}{m}}$. Moreover, if $g \in \mathcal{F}[y, \delta_1 y, \cdots, \delta_1^o y]$, then $\mathrm{prem}(\delta_1^O y, g)$ can be computed at most $2^{2.376}[2(M+1)^{(O-o+2)}]^{2.376(O+1)}$ $\mathcal{F}$-arithmetic operations and its degree is bounded by $2(M+1)^{O-o+1}$.*

6 Conclusion

In this paper, we present a Ritt-Wu characteristic set method for Laurent partial differential polynomial systems. We define the concept of Laurent differential regular chains and prove that a Laurent differential chain $\mathcal{A}$ is a characteristic set of $\mathrm{ldsat}(\mathcal{A})$ if and only if $\mathcal{A}$ is Laurent regular and coherent. Then we show that deciding whether an irreducible, coherent and regular chain is Laurent regular can be reduced to deciding whether a univariate irreducible differential chain is Laurent regular. For an irreducible differential chain $\mathcal{A}$ in the univariate polynomial ring $\mathcal{F}\{y\}$, we show that deciding whether $\delta_1^j y$ is invertible w.r.t. $\mathcal{A}$ can be reduced to deciding whether $\delta_1^j y$ is invertible w.r.t an irreducible differential polynomial. In the case of first order, we give a complete method of deciding whether $\delta_1^j y$ is invertible w.r.t. f. In the general case, we give a partial method of deciding whether $\delta_1^j y$ is invertible w.r.t. f.

References

[1] Ritt J, *Differential Algebra*, The American Mathematical Society, 1950.

[2] Wu W T, On the decision problem and the mechanization of theorem-proving in elementary geometry, *Science in China Ser. A*, 1978, **29**(2): 117–138.

[3] Wu W T, Basic principles of mechanical theorem proving in elementary geometries, *Journal of Automated Reasoning*, 1986, **2**(3): 221–252.

[4] Wu W T, *Mathematics Mechanization*, Science Press/Kluwer, Beijing, 2001.

[5] Aubry P, Lazard D, and Maza M M, On the theories of triangular sets, *Journal of Symbolic Computation*, 1999, **28**(1–2): 105–124.

[6] Chou S C and Gao X S, Ritt-Wu's decomposition algorithm and geometry theorem proving, *Tenth International Conference on Automated Deduction*, Springer-Verlag, New York, 1990, 207–220.

[7] 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.

[8] Li B H, A method to solve algebraic equations up to multiplicities via Ritt-Wu's characteristic sets, *Acta Analysis Functionalis Applicata*, 2003, **5**(2): 97–109.

[9] Li B H, Hilbert problem 15 and Ritt-Wu method (I), *Journal of Systems Science and Complexity*, 2019, **32**(1): 47–61.

[10] Li X and Maza M M, Fast arithmetic for triangular sets: From theory to practice, *International Symposium*, 2007, 269–276.

[11] Wang D, *Elimination Methods*, Springer, Vienna, 2001.

[12] Yang L, Zhang J Z, and Hou X R, *Non-Linear Algebraic Equations and Automated Theorem Proving*, Shanghai Science and Education Pub., Shanghai, 1996.

[13] Chen C, Davenport J H, May J P, et al., Triangular decomposition of semi-algebraic systems, *Journal of Symbolic Computation*, 2013, **49**: 3–26.

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

[15] Gao X S and Huang Z, Characteristic set algorithms for equation solving in finite fields, *Journal of Symbolic Computation*, 2011, **46**(6): 655–679.

[16] Li X, Mou C, and Wang D, Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case, *Theoretical Computer Science*, 2010, **60**(11): 2983–2997.

[17] Boulier F, Lemaire F, and Maza M M, Computing differential characteristic sets by change of ordering, *Journal of Symbolic Computation*, 2010, **45**(1): 124–149.

[18] Bouziane D, Rody A K, and Maârouf H, Unmixed-dimensional decomposition of a finitely generated perfect differential ideal, *Journal of Symbolic Computation*, 2001, **31**(6): 631–649.

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

[20] Hubert E, Factorization-free decomposition algorithms in differential algebra, *Journal of Symbolic Computation*, 2000, **29**(4): 641–662.

[21] Sit W Y, The Ritt-Kolchin theory for differential polynomials, *Differential Algebra and Related Topics*, 2002, 1–70.

[22] Zhu W and Gao X S, A triangular decomposition algorithm for differential polynomial systems with elementary computation complexity, *Journal of Systems Science and Complexity*, 2017, **30**(2): 464–483.

[23] Gao X S, Luo Y, and Yuan C M, A characteristic set method for ordinary difference polynomial systems, *Journal of Symbolic Computation*, 2009, **44**(3): 242–260.

[24] Wu W T and Gao X S, Mathematics mechanization and applications after thirty years, *Frontiers of Computer Science in China*, 2007, **1**(1): 1–8.

[25] Gao X S, Huang Z, and Yuan C M, Binomial difference ideals, *Journal of Symbolic Computation*, 2017, **80**: 665–706.

[26] Gao X S, Huang Z, Wang J, et al., Toric difference variety, *Journal of Systems Science and Complexity*, 2017, **30**(1): 173–195.

[27] Hu Y and Gao X S, Characteristic set method for Laurent differential polynomial systems, *International Workshop on Computer Algebra in Scientific Computing*, Springer, 2017, 183–195.

[28] Cano J, An extension of the Newton-Puiseux polygon construction to give solutions of Pfaffian forms, *Annales-Institut Fourier*, 1993, **43**(1): 125–142.

[29] Fine H B, On the functions defined by differential equations, with an extension of the Puiseux polygon construction to these equations, *American Journal of Mathematics*, 1889, **11**(4): 317–328.

[30] Grigor'ev D Y and Singer M F, Solving ordinary differential equations in terms of series with real exponents, *Transactions of the American Mathematical Society*, 1991, **327**(1): 329–351.

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

[32] Rosenfeld A, Specializations in differential algebra, *Transactions of the American Mathematical Society*, 1959, **90**(3): 394–407.

[33] Li W and Li Y H, Computation of differential chow forms for ordinary prime differential ideals, *Advances in Applied Mathematics*, 2016, **72**: 77–112.