Elimination Theory in Differential and Difference Algebra*

LI Wei · YUAN Chun-Ming

Dedicated to the memories of Professor Wen-Tsün Wu

DOI: 10.1007/s11424-019-8367-x
Received: 15 October 2018 / Revised: 10 December 2018

Abstract Elimination theory is central in differential and difference algebra. The Wu-Ritt characteristic set method, the resultant and the Chow form are three fundamental tools in the elimination theory for algebraic differential or difference equations. In this paper, the authors mainly present a survey of the existing work on the theory of characteristic set methods for differential and difference systems, the theory of differential Chow forms, and the theory of sparse differential and difference resultants.

Keywords Differential Chow forms, differential resultants, sparse differential resultants, Wu-Ritt characteristic sets.

1 Introduction

Algebraic differential equations and difference equations frequently appear in numerous mathematical models and are hot research topics in many different areas. Differential algebra, founded by Ritt and Kolchin, aims to study algebraic differential equations in a way similar to how polynomial equations are studied in algebraic geometry[1, 2]. Similarly, difference algebra, founded by Ritt and Cohn, mainly focus on developing an algebraic theory for algebraic difference equations[3]. Elimination theory, starting from Gaussian elimination, forms a central part of both differential and difference algebra.

For the elimination of unknowns in algebraic differential and difference equations, there are several fundamental approaches, for example, the Wu-Ritt characteristic set theory, the theory of Chow forms, and the theory of resultants.

The characteristic set method is a fundamental tool for studying systems of polynomial or algebraic differential equations[1, 2]. However, the algorithmic study of the characteristic set

LI Wei · YUAN Chun-Ming
KLMM, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190*, China; University of Chinese Academy of Sciences, Beijing* 100049*, China.*
Email: liwei@mmrc.iss.ac.cn; cmyuan@mmrc.iss.ac.cn.

*This research was supported by the National Natural Science Foundation of China under Grant Nos. 11688101, 11301519, 11671014.

◇ *This paper was recommended for publication by Editor LI Hongbo.*

was in stagnation for quite a long time until Wu's work on zero decomposition for polynomial equations and automated geometry theorem proving appeared in the late 1970s[4–6], the method can be viewed as an extended Gaussian elimination method for polynomial systems. Since then, many efficient algorithms and new properties for characteristic sets were proposed for algebraic equation systems and differential equation systems[6–12]. The idea of the method is to privilege systems which have been put in a special "triangular form", also called an ascending chain or simply a chain. The zero-set of any finite system of polynomials equations or differential polynomial equations can be decomposed into the union of the zero-sets represented by chains. With this method, solving a system of equations can be reduced to solving successive univariate equations. It can also be applied to determine the dimension, the degree, and the order of a finitely generated system of polynomials or differential polynomials, to solve the radical ideal membership problem, and to prove theorems from elementary and differential geometries.

The notion of characteristic set for difference polynomial systems was proposed by Ritt and Doob[13], Titt and Raudenbush[14]. The general theory of difference algebra was established by Cohn[3]. Algorithms and properties for ordinary difference chains were well studied in [15–17], zero decomposition algorithms were provided to solve the perfect ideal membership problem. Some basic properties and zero decomposition algorithm are also extended to the partial difference case[18]. However, it is still an open problem to solve the perfect ideal membership problem in the partial difference case.

For the mixed differential and difference polynomial (DD-polynomial) systems, the theoretical properties of differential algebra (dimension polynomials, finite generation of ideals, etc.) have been generalized to DD-setting[19], and the algorithmic counterparts were developed in [20] for ordinary differential-difference ring.

The Chow form, also known as the Cayley form, is a basic concept in algebraic geometry[21, 22]. In recent decades, it becomes a powerful tool in elimination theory and especially for the computational aspects of algebraic geometry. For instance, Brownawell made a major breakthrough in elimination theory by developing new properties of the Chow form and proving an effective version of the Nullstellensatz with optimal bounds[23]; Gel'fand, et al and Sturmfels started the sparse elimination theory which is to study the Chow form and the resultant associated with toric varieties[21, 24]. It also has important applications in transcendental number theory[25, 26] and algebraic computational complexity theory[27].

Recently, the theory of differential Chow forms in both affine and projective differential algebraic geometry has been developed in [28, 29]. Most of the basic properties of the algebraic Chow form are extended to its ordniary differential counterpart[28] and the theory of differential Chow varieties is established in [30]. For difference varieties, a theory of difference Chow forms is also given in [31]. And in the partial differential case, differential Chow forms are defined for a specific kind of partial differential varieties and a type of partial differential Chow varieties is given in [32].

The multivariate resultant, which gives conditions for an over-determined system of polynomial equations to have common solutions, is also a basic concept in algebraic geometry[21, 24, 33–35]. Due to the ability to eliminate several variables simultaneously without introducing many extraneous solutions, resultants have emerged as one of the most powerful computational tools in elimination theory. Many algorithms with best complexity bounds for problems such as polynomial equation solving and first order quantifier elimination, are strongly based on multivariate resultants[23, 27, 36–38]. As a major advance in algebraic geometry and elimination theory, the concept of sparse resultants was introduced by Gelfand, Kapranov, and Zelevinsky[21] and by Sturmfels[24]. The degree of the sparse resultant is the Bernstein-Kushnirenko-Khovanskii (BKK) bound[39], instead of the Beźout bound[21, 40]. And the sparse resultant has matrix representations and determinant forms[37, 38, 41, 42]. All these make the computation of the sparse resultant more efficient and could be implemented in many computer algebra systems.

The differential resultant problem was first studied for differential operators by Ore[43], Berkovich and Tsirulik[44], Zeilberger[45], Chyzak and Salvy[46], and Carrà-Ferro[47]. The subresultant theory was studied by Chardin[48], Li[49] and Hong[50]. For nonlinear differential polynomials, Ritt introduced the differential resultant for two univariate ordinary differential polynomials in [51, p.47]. Then for the multivariate differential resultant, Zwillinger, Rueda and Sendra Carrà-Ferro tried to define or compute the differential resultant as the algebraic resultants of a certain prolonged (differentiated) system[52–54]. The first rigorous definition for multivariate differential resultant was given by Gao, et al. in [28], where the properties of differential resultants were given too. Then the theory of sparse differential resultants for Laurent ordinary differential polynomials has been developed and a computational algorithm with single-exponential complexity is given in [55]. Matrix representations for differential resultants in special cases were studied in [56, 57]. A theory of sparse difference resultants are introduced in [58–60].

In this paper, we mainly give a survey of the above three main elimination approaches in differential algebra and difference algebra. We should point out that there are other recent important advances in differential and difference elimination theory which are not our theme here, for example, several main contributions are made to both the differential and the difference Nullstellensatz problem[61–65].

The rest of the paper is organised as follows. In Section 2, we will overview general theories of characteristic set methods in polynomial algebra, differential algebra and difference algebra respectively. The theory of differential Chow forms and differential Chow varieties is presented in Section 3. In Section 4, we present the main results in the theory of sparse differential resultants and sparse difference resultants.

2 Characteristic Set Methods

In this section, we will introduce basic notations and results in the characteristic set methods for algebraic, differential, difference and differential-difference systems.

2.1 Characteristic Set Method for Algebraic Polynomial Systems

Let $\mathcal{K}$ be a computable field with characteristic zero. Let $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be indeterminates and $\mathcal{K}[\mathbb{Y}] = \mathcal{K}[y_1, y_2, \cdots, y_n]$ the polynomial ring. We use a natural ordering for the variables $y_1 \prec y_2 \prec \cdots \prec y_n$. For $P \in \mathcal{K}[\mathbb{Y}]$, the class of P, denoted by class(P), is the largest

c such that y_c occurs in P. If $P \in K$, we set class$(P) = 0$. If class$(P) = c$, we called y_c the leading variable, denoted as lvar(P). The leading coefficient of P as a univariate polynomial in lvar(P) is called the initial of P, and is denoted as $\mathrm{I}(P)$. The formal derivative $\frac{\partial P}{\partial y_c}$ is called the separant of P, and is denoted by $\mathrm{S}(P)$. A polynomial Q is reduced with respect to another polynomial P if class$(P) = c > 0$ and $\deg(Q, y_c) < \deg(P, y_c)$.

Definition 2.1 A sequence of nonzero polynomials $\mathcal{A} = A_1, A_2, \cdots, A_p$ is a triangular set if either $p = 1$ or class$(A_1) <$ class$(A_2) < \cdots <$ class(A_p). $\mathcal{A}$ is called an ascending chain, or simply a chain, if A_j is reduced w.r.t. A_i for $i < j$.

For a triangular set $\mathcal{A}$, we denote by $I_{\mathcal{A}}$ and $S_{\mathcal{A}}$ the products of the initials and separants of the polynomials in $\mathcal{A}$ respectively.

For a triangular set $\mathcal{A}$, we can rename the variables $\mathbb{Y}$ as $U = \{u_1, u_2, \cdots, u_q\}$ and $X = \{x_1, x_2, \cdots, x_p\}$ such that $\mathcal{A}$ can be rewritten as the following form

$$\mathcal{A} = \begin{cases} A_1(U, x_1) = I_1 x_1^{d_1} + \text{terms of lower degree in } x_1, \\ \vdots \\ A_p(U, x_1, x_2, \cdots, x_p) = I_p x_p^{d_p} + \text{terms of lower degree in } x_p, \end{cases} \tag{1}$$

where $p + q = n$ and $I_i = \mathrm{I}(A_i)$, $U_{\mathcal{A}} = U$ is called the parametric set (or parameters) of $\mathcal{A}$.

We can introduce a rank between two polynomials and two triangular sets. A polynomial P_1 has higher rank than a polynomial P_2, denoted as $P_2 \prec P_1$, if either class$(P_1) >$ class(P_2), or $c =$ class$(P_1) =$ class(P_2) and $\deg(P_1, y_c) > \deg(P_2, y_c)$. If no one has higher rank than the other for two polynomials, they are said to have the same rank, denoted as $P_1 \sim P_2$. We use $P_1 \preccurlyeq P_2$ to denote the relation of either $P_1 \prec P_2$ or $P_1 \sim P_2$. It is easy to see that $\preccurlyeq$ is a partial order on the polynomial ring. We may extend the rank to triangular sets in a natural way. For two triangular sets $\mathcal{A} = A_1, A_2, \cdots, A_p$ and $\widehat{\mathcal{A}} = \widehat{A}_1, \widehat{A}_2, \cdots, \widehat{A}_s$. We say that $\mathcal{A}$ has higher rank than $\widehat{\mathcal{A}}$, also denoted as $\widehat{\mathcal{A}} \prec \mathcal{A}$, if either there exists a $k \le \min(p, s)$ such that $A_1 \sim \widehat{A}_1, A_2 \sim \widehat{A}_2, \cdots, A_{k-1} \sim \widehat{A}_{k-1}$ and $\widehat{A}_k \prec A_k$, or $p < s$ and $A_i \sim \widehat{A}_i$ for $1 \le i \le p$. If no one has higher rank than the other for two triangular sets, they are said to have the same rank, denoted as $\mathcal{A} \sim \widehat{\mathcal{A}}$. We use $\mathcal{A} \preccurlyeq \widehat{\mathcal{A}}$ to denote the relation of either $\mathcal{A} \prec \widehat{\mathcal{A}}$ or $\mathcal{A} \sim \widehat{\mathcal{A}}$. Then $\preccurlyeq$ is a partial order on the triangular sets.

Definition 2.2 The algebraic saturation ideal of a triangular set $\mathcal{A}$ is defined as follows

$$\mathrm{asat}(\mathcal{A}) = \{f \in \mathcal{K}[\mathbb{Y}] | \exists k \in \mathbb{N}, I_{\mathcal{A}}^k f \in (\mathcal{A})\}.$$

Then asat$(\mathcal{A})$ is an ideal.

For a triangular set $\mathcal{A}$ and a non-zero polynomial G, there is a uniquely determined polynomial R reduced w.r.t.$\mathcal{A}$ such that $JG = \sum_i Q_i A_i + R$ for some polynomials Q_i and some smallest power-product J of initials of A_i.

Definition 2.3 The R obtained above is called the remainder of G w.r.t.$\mathcal{A}$, denoted as $R = \textbf{a-prem}(G, \mathcal{A})$.

Definition 2.4 A characteristic set (CS) of a polynomial set $\mathbb{P}$ is any chain of lowest ranking contained in $\mathbb{P}$.

It is evident that any two characteristic sets of a polynomial set are of the same rank. A polynomial Q is called reduced w.r.t. a chain $\mathcal{A}$ if Q is reduced w.r.t. all the polynomials in $\mathcal{A}$.

Note that the zero set defined by a non-trivial chain may have no zeros. For example, let $\mathcal{A} = \{y_1^2, y_1y_2 - 1\}$, then it is a chain, but $\mathrm{Zero}(\mathcal{A}) = \mathrm{Zero}(\mathrm{asat}(\mathcal{A})) = \emptyset$. Hence, we need to add more constraints for the chain in order to make the zero set represented by $\mathcal{A}$ can be measured by $\mathcal{A}$ in certain sense.

Definition 2.5 Let $\mathcal{A} = A_1, A_2, \cdots, A_p$ be a nontrivial triangular set. A polynomial P is said to be invertible w.r.t. $\mathcal{A}$ if $(P, A_1, \cdots, A_p) \cap \mathcal{K}[U] \neq \{0\}$.

Definition 2.6 A nontrivial triangular set $\mathcal{A}$ is called regular if the initials of A_i are invertible w.r.t. $\mathcal{A}_{i-1}$, where $\mathcal{A}_k = \{A_1, A_2, \cdots, A_k\}$ for any k and $\mathcal{A}_0 = \emptyset$.

The concept of regular sets was introduced independently by Yang, et al.[66] and Kalkbrener[67].

Definition 2.7 A regular triangular set $\mathcal{A} = A_1, A_2, \cdots, A_p$ of form (1) is said to be irreducible if A_1 is an irreducible polynomial in x_1 and A_i is irreducible module $\mathcal{A}_{i-1}$ for $i = 2, 3, \cdots, p$.

Then, we have

Theorem 2.8 (see [7, 67]) *If $\mathcal{A}$ is an irreducible triangular set, then* asat($\mathcal{A}$) *is a prime ideal with dimension $|U|$. Conversely, each characteristic set of a prime ideal is an irreducible chain.*

Moreover, regular sets have nice properties,

Theorem 2.9 (see [67], Theorem 3.1) *Let $\mathcal{A}$ be a regular chain, then* $\mathrm{Zero}(\mathrm{asat}(\mathcal{A})) = \cup_i \mathrm{asat}(C_i)$*, where C_i is an irreducible chain for each i and the parametric set of C_i is the same as $\mathcal{A}$.*

Theorem 2.10 (see [7], Theorem 6.1) *A triangular set $\mathcal{A}$ is a characteristic set of* asat($\mathcal{A}$) *if and only if $\mathcal{A}$ is regular.*

Now, let's describe the routine of the characteristic set method, which is introduced by Wu[4, 6, 11].

Let $\mathbb{P}$ be a polynomial set. We set $\mathbb{P}_0 = \mathbb{P}$ and choose a characteristic set $\mathcal{B}_0$ of $\mathbb{P}_0$. Let $\mathbb{R}_0$ be the nonzero remainders of polynomials in $\mathbb{P}_0 \backslash \mathcal{B}_0$ w.r.t. $\mathcal{B}_0$. Suppose that $\mathbb{R}_0 \neq \emptyset$. Then we form a new polynomial set $\mathbb{P}_1 = \mathbb{P}_0 \cup \mathbb{R}_0$. Choose now a characteristic set $\mathcal{B}_1$ of $\mathbb{P}_1$. Then, $\mathcal{B}_1$ is of lower order than $\mathcal{B}_0$. Continuing in this way, we will obtain successively $\mathbb{P}_i, \mathcal{B}_i, \mathbb{R}_i, i = 1, 2, \cdots$, for which

$$\mathcal{B}_0 \succ \mathcal{B}_1 \succ \mathcal{B}_2 \succ \cdots.$$

This sequence can only be a finite one, hence there exists an m, such that $\mathbb{R}_m = \emptyset$. The above procedure can be exhibited in the form of the scheme as follows:

$$\begin{array}{lll} \mathbb{P}=\mathbb{P}_0\ \mathbb{P}_1 & \cdots\ \mathbb{P}_i\ \cdots\ \mathbb{P}_m & \\ \quad\ \mathcal{B}_0\ \mathcal{B}_1 & \cdots\ \mathcal{B}_i\ \cdots\ \mathcal{B}_m = CS & \qquad (S) \\ \quad\ \mathbb{R}_0\ \mathbb{R}_1 & \cdots\ \mathbb{R}_i\ \cdots\ \mathbb{R}_m = \emptyset, & \end{array}$$

where

$$\mathbb{P}=\mathcal{B}_i = \text{a characteristic set of }\ \mathbb{P}_i$$
$$\mathbb{R}_i = \textbf{a-prem}(\mathbb{P}_i/\mathcal{B}_i, \mathcal{B}_i)/\{0\},$$
$$\mathbb{P}_i = \mathbb{P}_0 \cup \mathcal{B}_{i-1} \cup \mathbb{R}_{i-1}.$$

Definition 2.11 The CS obtained above is called a Wu-characteristic set of $\mathbb{P}$.

Then, we have the following properties of Wu-characteristic set CS.

Theorem 2.12 (see [11], Well-ordering principal) *Let CS be a Wu-characteristic set of $\mathbb{P}$, then*

$$\begin{aligned} &\mathrm{Zero}(CS/I) \subset \mathrm{Zero}(\mathbb{P}) \subset \mathrm{Zero}(CS), \\ &\mathrm{Zero}(\mathbb{P}/I) = \mathrm{Zero}(CS/I) \\ &\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(CS/I) + \bigcup_i \mathrm{Zero}(\mathbb{P}+\{I_i\}), \end{aligned} \tag{2}$$

where I_i is the initial of the polynomial $C_i \in CS$, I is the initial product of CS.

Using the well ordering principal again for each component $(\mathbb{P}+\{I_i\})$ in the above theorem, we may obtain a zero decomposition algorithm for the polynomial system $\mathbb{P}$.

Theorem 2.13 (see [11], Zero decomposition theorem) *For $\mathbb{P} \subset \mathcal{K}[\mathbb{Y}]$, there exists an algorithm, which can compute finite Wu-characteristic sets CS_j, such that*

$$\begin{aligned} &\mathrm{Zero}(\mathbb{P}) = \bigcup_j \mathrm{Zero}(CS_j/I_j), \\ &\textbf{a-prem}(\mathbb{P}/CS_j) = \{0\}, \end{aligned} \tag{3}$$

where I_j is the initial product of CS_j.

In [68], Gallo and Mishra showed that the complexity of computing a characteristic set for a given ideal generated by a polynomial system is single exponential.

Theorem 2.14 (see [68], Theorem 4.14) *Let $I=(f_1, f_2, \cdots, f_s)$ be an ideal in $\mathcal{K}[X]$, and* $\deg(f_i) \leq d, 1 \leq i \leq s$. *Then under any ordering on the indeterminants $x_1 \prec x_2 \prec \cdots \prec x_n$, where the first* $\dim(I)$*-many variables are independent, one can compute a characteristic set of I, in $O(s^{o(n)}(d+1)O(n^3))$ sequential time or* $O(n^7\log^2(s+d+1))$ *parallel time. The polynomials in the computed characteristic set are of degree $O(s(d+1)^{O(n^2)})$.*

Unfortunately, as we mentioned before, the zero set $\mathrm{Zero}(CS_j/I_j)$ may be empty even if CS_j is non-trivial, then, one need to give some restriction on the Wu-characteristic sets. The following theorem gives irreducible decomposition for the zero set of $\mathbb{P}$, that is, restrict CS_j to be irreducible ones.

Theorem 2.15 (see [11, 69], Irreducible decomposition) *For $\mathbb{P} \subset \mathcal{K}[\mathbb{Y}]$, there exists an algorithm, which can compute a finite number of irreducible ascending chains $\mathcal{A}_k$ in finite steps, and polynomials G_k which are reduced* w.r.t. *$\mathcal{A}_k$, such that*

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_k \mathrm{Zero}(\mathcal{A}_k/I_kG_k) \tag{4}$$

or

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_k \mathrm{Zero}(\mathcal{A}_k/I_k) = \bigcup_k \mathrm{Zero}(\mathrm{asat}(\mathcal{A}_k)), \tag{5}$$

where I_k is the initial product of $\mathcal{A}_k$ for any k.

There are also triangular decomposition algorithms in different types, one can also decompose the zero set of the polynomial system into the union of the zero sets of regular sets[67, 70–73].

There are also fruitful applications for various zero decomposition algorithms[74–77]. The most successful area is the automated theorem proving for elemental geometry. The routine to prove theorems from elemental geometry is as follows[11]:

Step 1 Introduce a coordinate system, using indeterminates $x_1, x_2, \cdots, x_n$ to denote the points or other geometric quantities, then the assumptions in the theorem can be represented by a set of polynomial equations, say $HS = 0$. Also, the conclusion of the theorem can be represented by a polynomial equation, say $G = 0$.

Step 2 Using zero decomposition algorithm to decompose the zero set of HS into a set of zeros which is represented by triangular sets, say $\mathcal{C}_1, \mathcal{C}_2, \cdots, \mathcal{C}_t$.

Step 3 Computing $R_i = \textbf{a-prem}(G, \mathcal{C}_i)$, $1 \le i \le t$, then if $R_i = 0, 1 \le i \le t$, we conclude that the theorem is true (sometimes, we may get rid of the initial conditions), and if there exists an h, such that $R_h \neq 0$, then the theorem is not true at the component defined by $\mathcal{C}_h$.

Another way to prove theorems from elemental geometry is to translate the problem into determining whether a polynomial system has zeros or not. That is, to determine whether $G = 0$ is true under the assumption $HS = 0$ is equivalent to decide whether $G \in \sqrt{(HS)}$, or $\mathrm{Zero}(HS) \subseteq \mathrm{Zero}(G)$, this is a radical ideal membership problem. One can reduce this problem to determining whether a new polynomial system $\{HS, Gz + 1\}$ has zeros or not, where z is a new indeterminate. Then, the theorem is true (without any initial condition) if and only if the zero decomposition of $\{HS, G * z + 1\}$ provides no nontrivial component.

Since the work of Wu[4–6, 11], there are extensive work studies the characteristic set method, see [8, 67, 69–71, 76, 78–81]. Using these methods, one can decompose the zero set of a polynomial system into the zero sets represented by triangular systems. When we do not restrict that the characteristic of $\mathcal{K}$ is zero, that is, $\mathrm{char}(\mathcal{K}) = p > 0$, then one can have stronger properties[82–85].

2.2 Characteristic Set Method for Differential Polynomial Systems

The results of the characteristic set method for algebraic polynomial systems can be naturally extended to the differential case[8–10, 86–88].

Let $\mathcal{K}$ be a computable field equipped with a finite set $\delta = \{\delta_1, \delta_2, \cdots, \delta_s\}$ of derivations on this field.

Let Ω be the commutative semigroup of elements generated by δ. Let $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be indeterminates and $\mathcal{K}\{\mathbb{Y}\} = \mathcal{K}[\Omega\mathbb{Y}]$ the differential polynomial ring, where $\Omega\mathbb{Y} = \{\theta y_i | \theta \in \Omega, 1 \leq i \leq n\}$. For a differential polynomial system $\mathbb{P} = \{P_1, P_2, \cdots, P_s\} \subset \mathcal{K}\{\mathbb{Y}\}$, we denote by $[\mathbb{P}]$ the differential ideal generated by $\mathbb{P}$.

Definition 2.16 A rank over the set of derivatives θy_j is said to be admissible if it is a total and compatible with the differentiations:

1) $\delta_i \theta y_j > \theta y_j$ for any $i, \theta \in \Omega, j$;

2) $\theta_1 y_i > \theta_2 y_j \Rightarrow \theta\theta_1 y_i > \theta\theta_2 y_j$ for any $\theta, \theta_1, \theta_2, i, j$.

Let P be a differential polynomial of $\mathcal{K}\{\mathbb{Y}\}$. The leader u_P is the highest ranking derivative appearing in P. The initial $I(P)$ and separant $S(P)$ of P is defined as the algebraic case when regarding P as a univariate polynomial in u_P. Let $Q \in \mathcal{K}\{\mathbb{Y}\}$, we say that Q has higher rank than P when its leader has higher ranking than u_P or is equal but with a higher degree in u_P. The ranking on the derivatives induces a partial order on the differential polynomials in $\mathcal{K}\{\mathbb{Y}\}$. A differential polynomial Q is said to be reduced w.r.t. P if no proper derivatives of u_P appears in Q and $\deg(Q, u_P) < \deg(P, u_P)$.

Let $\mathcal{A} = \{A_1, A_2, \cdots, A_m\}$ be a set of differential polynomials, we say $\mathcal{A}$ is a differential chain if $u_1 < u_2 < \cdots < u_m$ and A_i is reduced w.r.t. A_j for any $1 \leq i, j \leq m, i \neq j$, where $u_i = \text{lead}(A_i)$. For a differential chain $\mathcal{A}$, we denote by $H_{\mathcal{A}}$ the product of the initials and separants of $\mathcal{A}$, that is $H_{\mathcal{A}} = I(\mathcal{A})S(\mathcal{A})$. We say $\mathcal{A}$ is saturated if both $I_{\mathcal{A}}$ and $S_{\mathcal{A}}$ is invertible w.r.t. $\mathcal{A}$. For details of these definitions, please refer to [8, 10, 87].

Note that, for any $P \in \mathcal{K}\{\mathbb{Y}\}$, the initial of $\delta_i P$ is just the separant of P and $\text{lvar}(\delta_i P) = \delta_i \text{lvar}(P)$ and the leading degree of $\delta_i P$ is just one. And for the pseudo-remainder procedure, one need to reduce the polynomial w.r.t. a differential chain not only for the leading variables but also the derivatives of the leading variables.

Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a differential chain. We denote by $L_{\mathcal{A}}$ the leading variables and their derivatives, and $P_{\mathcal{A}} = \Omega\mathbb{Y} \setminus L_{\mathcal{A}}$. Then, $P_{\mathcal{A}}$ form a parametric set of $\mathcal{A}$.

Let $\mathcal{A}$ be a differential chain, $\mathbb{P}$ a set differential polynomials. We say $P \in \mathbb{P}$ is reduced w.r.t. $\mathcal{A}$ if P is reduced w.r.t. each element in $\mathcal{A}$. Now, we define a pseudo-remainder procedure for a differential polynomial $P \in \mathbb{P}$ w.r.t. a differential chain $\mathcal{A}$, see **Algorithm 1**.

Algorithm 1 — d-prem$(P, \mathcal{A})$

```
While $P$ is not reduced w.r.t. $\mathcal{A}$ do
$Q$ = an element of $\mathcal{A}$, s.t. $P$ is not reduced w.r.t. $Q$;
$\theta u_Q$ = the highest ranking derivative of $u_Q$ in $P$;
$P$ = a-prem($P, \theta Q, \theta u_P$);
od;
```

This procedure terminates in finite steps and there exists an $h \in H_{\mathcal{A}}^{\infty}$, such that $hP = \textbf{d-prem}(P, \mathcal{A}) \mod [\mathcal{A}]$.

According to the differential structure, if P is not reduced w.r.t. $\mathcal{A}$, then the $Q \in \mathcal{A}$ such that P is not reduced w.r.t. Q may not unique, hence one need to verify the consistence of the choice of Q.

Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a differential chain in $\mathcal{K}\{y_1, y_2, \cdots, y_n\}$ and $\theta_i y_{k_i} = \mathrm{lvar}(A_i)$, $i = 1, 2, \cdots, m$. For any $1 \le i < j \le m$, if $\mathrm{class}(A_i) = \mathrm{class}(A_j) = t$, then $\theta_i \prec \theta_j$. Let $\theta_{i,j}$ be the least common multiple of θ_i and θ_j in Ω, let $\Delta_{ij} = \textbf{a-prem}(\frac{\theta_{i,j}}{\theta_i}A_i, \frac{\theta_{i,j}}{\theta_j}A_j, \theta_{i,j}y_t)$ be the algebraic pseudo-remainder of $\frac{\theta_{i,j}}{\theta_i}A_i$ w.r.t. $\frac{\theta_{i,j}}{\theta_j}A_j$ in variable $\theta_{i,j}y_t$; otherwise, let $\Delta_{ij} = 0$.

Definition 2.17 If $\textbf{d-prem}(\Delta_{ij}, \mathcal{A}) = \textbf{a-prem}(\Delta_{ij}, \mathcal{A}_{\Delta_{ij}}) = 0$, we call $\mathcal{A}$ a coherent differential chain.

Rosenfeld's Lemma[89] show that if a differential chain is coherent, then the differential chains can be regarded as algebraic ones in some sense. Moreover, we have

Theorem 2.18 (see [10], Theorem 4.4, Theorem 6.2) *Let $\mathcal{A}$ be a coherent differential chain in $\mathcal{K}[\mathbb{Y}]$. Then $[A] : H_{\mathcal{A}}^{\infty}$ is a radical differential ideal. Let $(A) : H_{\mathcal{A}}^{\infty} = \cap_{i=1}^{r}(C_i) : I_{C_i}^{\infty}$ is a characteristic irredundant decomposition in $\mathcal{K}[P_{\mathcal{A}}, L_{\mathcal{A}}]$ then C_i is coherent, $1 \le i \le r$, and $[\mathcal{A}] : H_{\mathcal{A}}^{\infty} = \cap_{i=1}^{r}[C_i] : H_{C_i}^{\infty}$ is a characteristic irredundant decomposition of $[\mathcal{A}] : H_{\mathcal{A}}^{\infty}$ in $\mathcal{K}[\mathbb{Y}]$.*

Based on the above theorem, one may design an algorithm to compute the zero-decomposition algorithm for differential polynomial system analog to algebraic one.

Theorem 2.19 (see [9], Theorem 3.4.1) *Let $\mathbb{P}$ be a set of differential polynomials in $\mathcal{K}[\mathbb{Y}]$. Then, we can compute a set of saturated coherent ascending chains $\{\mathcal{B}_1, \mathcal{B}_2, \cdots, \mathcal{B}_k\}$, such that*

$$\mathrm{Zero}(\mathbb{P}) = \cup_{i=1}^{k}\mathrm{Zero}(\mathcal{B}_i/S(\mathcal{B}_i)) = \cup_{i=1}^{k}\mathrm{Zero}(\mathcal{B}_i : S(\mathcal{B}_i)^{\infty}).$$

With this theorem, one can solve the radical ideal membership problem, and hence the mechanical theorem proving for differential polynomial systems.

2.3 Characteristic Set Method for Ordinary Difference Polynomial Systems

Let $\mathcal{K}$ be a computable field considered with an automorphism σ of $\mathcal{K}$. Let Ω be the semigroup generated by σ. Let $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be indeterminates and $\mathcal{K}\{\mathbb{Y}\} = \mathcal{K}[\Omega\mathbb{Y}]$ the difference polynomial ring. Here, $\Omega\mathbb{Y} = \{\theta y_i | \theta \in \Omega, 1 \le i \le n\}$ is the set of transforms of indeterminates. We denote by $[\mathbb{P}]$ the difference ideal generated by $\mathbb{P}$, $\{\mathbb{P}\}$ the perfect ideal generated by $\mathbb{P}$. Then, $\{\mathbb{P}\}$ is the intersection of the prime difference ideals which contain $\mathbb{P}$.

Due to the work of Gao and his collaborators[15–17, 90], the theory and algorithms have been well developed.

Similar to the differential case, one may define a rank on the set of $\Omega\mathbb{Y}$. Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a difference chain in $\mathcal{K}\{y_1, y_2, \cdots, y_n\}$. We denote by $L_{\mathcal{A}}$ the leading variables and their transforms, and $P_{\mathcal{A}} = \Omega\mathbb{Y} \setminus L_{\mathcal{A}}$ the parametric set of $\mathcal{A}$. We denote by $V(S)$ the set of variables occur in S for $S \subset \mathcal{K}\{\mathbb{Y}\}$.

Definition 2.20 Let $\mathcal{A}$ be a difference chain, $\mathbb{P}$ a set of difference polynomials. Let $\mathcal{A}_{\mathbb{P}}$ be an algebraic system with elements θA, where $\theta \in \Omega$ and $A \in \mathcal{A}$. We say an algebraic triangular set $\mathcal{A}_{\mathbb{P}}$ is an extension of $\mathcal{A}$ w.r.t. $\mathbb{P}$ if any variable occurs in $V(\mathcal{A}_P \cup \{P\}) \cap L_{\mathcal{A}}$ must be the leading variable of some polynomial in $\mathcal{A}_{\mathbb{P}}$.

We simply denote $\mathcal{A}_P = \mathcal{A}_{\{P\}}$ for a difference chain with a single polynomial P. For details of this definition, please refer to [17]. Then, the difference remainder for P w.r.t. $\mathcal{A}$ can be defined as follows

$$\textbf{r-prem}(P, \mathcal{A}) = \textbf{a-prem}(P, \mathcal{A}_P).$$

Similar to the differential case, one need to check the consistence of the difference extension. The main difference between the difference case and the differential case is that σP need not to be linear in its leading variable.

Definition 2.21 Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a difference chain in $\mathcal{K}\{y_1, y_2, \cdots, y_n\}$ and $k_i = \mathrm{ord}(A_i, \mathrm{lvar}(A_i))$, $i = 1, 2, \cdots, m$. For any $1 \leq i < j \leq m$, if $\mathrm{class}(A_i) = \mathrm{class}(A_j) = t$, then $k_i < k_j$, let $\Delta_{ij} = \textbf{a-prem}(\sigma^{k_j - k_i} A_i, A_j, y_{t,k_j})$ be the algebraic pseudo-remainder of $\sigma^{k_j-k_i} A_i$ w.r.t. A_j in variable y_{t,k_j}; otherwise, let $\Delta_{ij} = 0$. If $\textbf{r-prem}(\Delta_{ij}, \mathcal{A}) = \textbf{a-prem}(\Delta_{ij}, \mathcal{A}_{\Delta_{ij}}) = 0$, where **a-prem** is the algebraic pseudo-remainder, we call $\mathcal{A}$ a coherent difference chain.

Definition 2.22 Let $\mathcal{A}$ be a difference chain and f be a difference polynomial. We say that f is invertible w.r.t. $\mathcal{A}$ if it is invertible w.r.t. $\mathcal{A}_f$, when f and $\mathcal{A}_f$ are treated as algebraic polynomials.

Definition 2.23 Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a difference chain and $I_i = \mathrm{I}(A_i)$. The chain $\mathcal{A}$ is said to be (difference) regular if $\sigma^i I_j$ is invertible w.r.t. $\mathcal{A}$ for any non-negative integer i and $1 \leq j \leq m$.

Then, we have

Theorem 2.24 (see [17], Theorem 2.11) *A difference chain $\mathcal{A}$ is the characteristic set of* $\mathrm{sat}(\mathcal{A})$ *iff $\mathcal{A}$ is coherent and difference regular.*

Unfortunately, one does not know whether the zero set given by a coherent and regular chain is empty or not. It may happen that a nontrivial coherent and difference regular has no difference zero.

Example 2.25 $\mathcal{A} = \{y_1^2 + 1, \sigma y_1 + y_1, y_2^2 + 1, \sigma y_2 - y_2\}$, then one can check that $\mathcal{A}$ is coherent and difference regular, but the zero set of $\mathrm{sat}(\mathcal{A}) = [\mathcal{A}]$ is empty.

Hence, we introduce a new type of chains.

Definition 2.26 A chain $\mathcal{A}$ is said to be proper irreducible if

- $\mathcal{A}^* = \mathcal{A}_{\mathcal{A}}$ is an algebraic irreducible triangular set; and
- If $f = \sigma g \in \mathrm{asat}(\mathcal{A}^*)$ then $g \in \mathrm{asat}(\mathcal{A}^*)$.

For coherent and irreducible chains, thanks to the difference kernel introduced by Cohn[3], we have

Theorem 2.27 (see [17], Theorem 3.7,3.8) *A coherent and proper irreducible chain is difference regular. Moreover,* $\mathrm{Zero}(\mathrm{sat}(\mathcal{A})) \neq \emptyset$.

A proper irreducible chain $\mathcal{A}$ is said to be strong irreducible if $\mathcal{A}_P$ is an irreducible algebraic triangular set for any difference polynomial P.

Theorem 2.28 (see [17], Theorem 3.10) *Let $\mathcal{A}$ be a coherent and strong irreducible difference chain. Then* $\mathrm{sat}(\mathcal{A})$ *is a reflexive prime difference ideal.*

Up to now, we do not know how to decompose the zero set of a difference polynomial system into the union of coherent and strong irreducible difference chains (prime decomposition). Fortunately, we can test and compute the proper irreducible chains, and we have

Theorem 2.29 (see [17], Theorem 4.2) *Let $\mathbb{P}$ be a finite set of difference polynomials in $\mathcal{K}\{y_1, y_2, \cdots, y_n\}$, then there exists an algorithm to compute coherent and proper irreducible difference chains $\mathcal{A}_i$, $i = 1, 2, \cdots, k$, such that*

$$\mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathcal{A}_i/J_i), \quad \mathrm{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \mathrm{Zero}(\mathrm{sat}(\mathcal{A}_i)), \quad \{\mathbb{P}\} = \bigcap_{i=1}^{k} \{\mathrm{sat}(\mathcal{A}_i)\}. \tag{6}$$

Moreover, $\mathrm{Zero}(\mathbb{P}) = \emptyset$ *iff $k = 1$ and $\mathcal{A}_1$ is trivial.*

Using this theorem, one can solve the perfect ideal membership problem for difference polynomial systems[15], and hence the mechanical theorem proving for difference polynomial systems.

Remark 2.30 One can also extend the above results to the ordinary DD-settings. Let $\mathcal{K}$ be a computable field equipped with an automorphism σ and a derivation δ of $\mathcal{K}$. Note that σ and δ need not to commute. Then, similar as the ordinary difference case, one can define the chain, the regularity, the coherence, the proper irreducible chain, the strong irreducible chain in this setting. Then, Theorems 2.24, 2.27, 2.28, 2.29 can also be extended to the DD-case, for details see [20].

2.4 Characteristic Set Method for Partial Difference Polynomial Systems

Let $\mathcal{K}$ be a field of characteristic zero. We say that $\mathcal{K}$ is an inversive partial difference field with transforming operators $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ over $\mathcal{K}$ if $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$ are automorphisms of $\mathcal{K}$ which commute pairwise on $\mathcal{K}$.

Let Θ be the semigroup generated by $\{\sigma_1, \sigma_2, \cdots, \sigma_m\}$, that is, $\Theta = \{\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_m^{k_m} | k_i \in \mathbb{N}, 1 \le i \le m\}$. Let $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be indeterminates and $\mathcal{K}\{\mathbb{Y}\} = \mathcal{K}[\Theta\mathbb{Y}]$ the partial difference polynomial ring. Here, $\Theta\mathbb{Y} = \{\theta y_i | \theta \in \Theta, 1 \le i \le n\}$ is the set of transforms of indeterminates. We denote by $[\mathbb{P}]$ the partial difference ideal generated by $\mathbb{P}$, $\{\mathbb{P}\}$ the perfect partial difference ideal generated by $\mathbb{P}$. Then, $\{P\}$ is the intersection of the prime partial difference ideals that contain $\mathbb{P}$.

One can also extend the characteristic set method to the partial difference case. One may treat Θ as a set of monomials of the difference operators, then we can define an admissible ordering on these monomial[91], this ordering induce a total ordering for $\Theta\mathbb{Y}$. Then, for any partial difference polynomial f, according to this ordering, we can define the leading variable, the class, the initial and the separant of f, which can be denoted by $\mathrm{lvar}(f), \mathrm{class}(f), I(f), S(f)$, respectively.

Definition 2.31 A partial difference polynomial f is said to be reduced w.r.t. another polynomial g if $\deg(f, \eta\mathrm{lvar}(g)) < \deg(g, \mathrm{lvar}(g))$, for any $\eta \in \Theta$.

Definition 2.32 A subset $\mathcal{A} = A_1, A_2, \cdots, A_p$ of $\mathcal{K}\{\mathbb{Y}\}/\mathcal{K}$, where every element is reduced w.r.t. all the others, is called an autoreduced set. A chain is an autoreduced set where the polynomials are listed in the ascending ordering: $A_1 < A_2 < \cdots < A_p$.

Similar to the ordinary difference case, one may define main variables and parameters of a chain $\mathcal{A}$ as follows.

$$L_{\mathcal{A}} = \{\eta y_c \in \Theta\mathbb{Y} \quad s.t. \quad \exists\ A \in \mathcal{A}, \mathrm{lvar}(A) = \theta y_c, \text{ and } \ \eta \text{ is a multiple of } \theta\},$$
$$P_{\mathcal{A}} = \Theta\mathbb{Y} \setminus L_{\mathcal{A}}.$$

Then, we can define an extension of $\mathcal{A}$ w.r.t. a partial difference polynomial set $\mathbb{P}$ similar to the ordinary case[18].

Definition 2.33 Let $\mathcal{A}$ be a partial difference chain, $\mathbb{P}$ a set of partial difference polynomials. Let $\mathcal{A}_{\mathbb{P}}$ be an algebraic system with elements θA, where $\theta \in \Theta$ and $A \in \mathcal{A}$. We say an algebraic triangular set $\mathcal{A}_{\mathbb{P}}$ is an extension of $\mathcal{A}$ w.r.t. $\mathbb{P}$ if any variable occurs in $V(\mathcal{A}_{\mathbb{P}} \cup \{\mathbb{P}\}) \cap L_{\mathcal{A}}$ must be the leading variable of some polynomial in $\mathcal{A}_{\mathbb{P}}$.

Then, one can define the pseudo-remainder of a polynomial w.r.t. a chain, $\mathbf{prem}(f, \mathcal{A}) = \mathbf{a\text{-}prem}(f, \mathcal{A}_f)$ for any partial difference polynomial f and a partial difference chain $\mathcal{A}$.

Let $\mathcal{A} = A_1, A_2, \cdots, A_l$ be a chain in $\mathcal{K}\{\mathbb{Y}\}$ and $\theta_i y_{t_i} = \mathrm{lvar}(A_i)$, $i = 1, 2, \cdots, l$. For any $1 \le i < j \le m$, if $t_i = t_j = t$, let the least common multiple transform of θ_i and θ_j be $\theta_{i,j}$. We define the Δ-polynomials of A_i and A_j as $\Delta_{j,i} = \frac{\theta_{i,j}}{\theta_j} A_j$ and $\Delta_{i,j} = \frac{\theta_{i,j}}{\theta_i} A_i$.

Definition 2.34 If $\mathbf{p\text{-}prem}(\Delta_{i,j}, \mathcal{A}) = 0$ and $\mathbf{p\text{-}prem}(\Delta_{j,i}, \mathcal{A}) = 0$, we call $\mathcal{A}$ a coherent chain.

Definition 2.35 Let $\mathcal{A}$ be a chain and f be a polynomial. f is said to be partial difference invertible, (or invertible) w.r.t. $\mathcal{A}$ if it is invertible w.r.t. $\mathcal{A}_f$ when f and $\mathcal{A}_f$ are treated as algebraic polynomials.

Definition 2.36 Let $\mathcal{A} = A_1, A_2, \cdots, A_m$ be a chain and $I_i = \mathrm{I}(A_i)$. $\mathcal{A}$ is said to be (partial difference) regular if θI_j is invertible w.r.t. $\mathcal{A}$ for any $\theta \in \Theta$ and $1 \le j \le m$.

Then, we have

Theorem 2.37 (see [18], Theorem 20) *A chain $\mathcal{A}$ is the characteristic set of* $\mathrm{sat}(\mathcal{A})$ *if and only if $\mathcal{A}$ is coherent and difference regular.*

Definition 2.38 A chain $\mathcal{A}$ is strong irreducible if

- $\mathcal{A}_f$ is an irreducible algebraic triangular set for any $f \in \mathcal{K}\{\mathbb{Y}\}$;
- For $\theta \in \Theta$ and $h \in \mathcal{K}\{\mathbb{Y}\}$, if $\theta h \in \mathrm{asat}(\mathcal{A}_f)$ then $h \in \mathrm{asat}(\mathcal{A}_f)$.

Theorem 2.39 (see [18], Theorem 22) *Let $\mathcal{A}$ be a coherent and strongly irreducible difference chain. Then* $\mathrm{sat}(\mathcal{A})$ *is a reflexive prime difference ideal.*

Theorem 2.40 (see [18], Theorem 25) *Let $\mathcal{I}$ be a reflexive prime difference ideal and $\mathcal{A}$ be a characteristic set of $\mathcal{I}$. Then $\mathcal{A}$ is coherent, strongly irreducible, and* $\mathcal{I} = \mathrm{sat}(\mathcal{A})$.

For the zero decomposition, we have

Theorem 2.41 (see [18], Theorem 27) *Let $\mathbb{P}$ be a finite set of polynomials in $\mathcal{K}\{y_1, y_2, \cdots, y_n\}$, then we can obtain a sequence of coherent chains $\mathcal{A}_i$, $i = 1, 2, \cdots, k$ such that*

$$\operatorname{Zero}(\mathbb{P}) = \bigcup_{i=1}^{k} \operatorname{Zero}(\mathcal{A}_i/I_{\mathcal{A}_i}) = \bigcup_{i=1}^{k} \operatorname{Zero}(\operatorname{sat}(\mathcal{A}_i)). \tag{7}$$

Remark 2.42 Unfortunately, for any proper coherent ascending chain $\mathcal{A}$, one does not know if the zero set of $\operatorname{sat}(\mathcal{A})$ is empty or not. An example shows that even for an ideal generated by one single irreducible polynomial, the zero set of this ideal may be empty[92]. Up to now, the perfect ideal membership problem is still open.

Example 2.43 (see [92]) Let $\mathcal{K} = (\mathbb{Q}(i, b), \{\sigma, \tau\})$, where $\mathbb{Q}$ is the field of rational numbers, $\mathrm{i}^2 + 1 = 0$, $b = \sqrt{2}$, the difference operators σ_1, σ_2 are defined as follows.

$$\sigma_1 \mathrm{i} = \mathrm{i}, \quad \sigma_1 b = -b,$$

$$\sigma_2 \mathrm{i} = -\mathrm{i}, \quad \sigma_2 b = b.$$

Consider the zero set of $x^2 - b$ or equivalently, $\{x^2 - b\}$

$$\begin{aligned}\{x^2 - b\} = \{x^2 - b, \sigma_1 x + ix, \sigma_2 x - x\} \cap \{x^2 - b, \sigma_1 x + ix, \sigma_2 x + x\}\\ \cap\{x^2 - b, \sigma_1 x - ix, \sigma_2 x - x\} \cap \{x^2 - b, \sigma_1 x - ix, \sigma_2 x + x\}.\end{aligned}$$

One can check that each component of the above equations has no zero, that is, $\{x^2 - b\} = [1]$.

3 Differential Chow Forms and Differential Chow Varieties

In this section, we will briefly introduce the definition of differential Chow forms, present basic properties and show the existence of differential Chow varieties. For more details, please refer to [28, 29]. Unless otherwise indicated, all differential varieties under discussion are ordinary differential ones in Sections 3 and 4.

Let K be a fixed differential field of characteristic 0 with derivation δ, and E a universal differential field extension of K[2]. By $\mathbb{A}^n$ and $\mathbb{P}^n$, we mean the affine differential space and the projective differential space defined over E respectively. For a subset $U \subset E$, we use $K\{U\}$, $K\langle U\rangle$ to denote the differential ring $K[(\delta^k u)_{k\in\mathbb{N},u\in U}]$, the differential field $K\big((\delta^k u)_{k\in\mathbb{N},u\in U}\big)$ generated by S over K respectively.

To define differential Chow forms, we first need the generic differential intersection theory. Intersection theory is a fundamental problem in algebraic geometry, and it is well-known that each component of the intersection of two irreducible algebraic varieties in $\mathbb{A}^n$ of dimension r and s is of dimension at least $r + s - n$. However, this result does not hold in differential algebraic geometry. A famous counter-example was given by Ritt[1]:

Example 3.1 Let $n = 3$ and V be the general component of $\mathbb{V}(y_1^5 - y_2^5 + y_3(y_1 y_2' - y_2 y_1')^2) \subset \mathbb{A}^3$. Let $W = \mathbb{V}(y_3)$. Clearly, both V and W are irreducible differential varieties of differential dimension 2. However, $V \cap W = \{(0, 0, 0)\}$ whose differential dimension is $0 < 2 + 2 - 3$.

Example 3.1 is also a counter-example to the differential version of the algebraic intersection formula, which claims that the intersection of an irreducible variety V of dimension d and a hypersurface not containing V is purely of dimension $d-1$. Although in general the intersection formula does not hold in the differential setting, the next result shows that it holds generically.

Definition 3.2 Let $\mathbb{m}_{s,r}$ be the set of all differential monomials in $K\{y_1, y_2, \cdots, y_n\}$ of order $\leq s$ and degree $\leq r$. Let $\mathbb{U} = \{u_M\}_{M\in\mathbb{m}_{s,r}}$ be a subset of elements of a universal differential field containing K that are differential indeterminates over K. Then,

$$f = \sum_{M\in\mathbb{m}_{s,r}} u_M M$$

is called a generic differential polynomial of order s and degree r. A generic differential hypersurface is the set of differential zeros of a generic differential polynomial.

Theorem 3.3 (see [28], Theorem 1.1) *Let $V \subseteq \mathbb{A}^n$ be an irreducible differential variety over K of dimension d and order h. Let P be a generic differential polynomial of order s with the set of its coefficients $\boldsymbol{u}$. Then,*

1) *over $K\langle \boldsymbol{u}\rangle$, $V \cap \mathbb{V}(P) \neq \emptyset$ if and only if $d > 0$.*

2) *if $d > 0$, then the intersection of V and $\mathbb{V}(P)$ is an irreducible differential variety over $K\langle \boldsymbol{u}\rangle$ of differential dimension $d-1$ and order $h+s$.*

Remark 3.4 Theorem 3.3 could be generalized to the partial differential case, as was shown in [32, 93] that $\omega_{V\cap\mathbb{V}(P)}(t)$, the Kolchin polynomial of $V \cap \mathbb{V}(P)$, is equal to $\omega_V(t) - \binom{t+m-s}{m}$ (here m is the number of derivations).

Let $V \subset \mathbb{A}^n$ be an irreducible differential variety defined over K of dimension d and

$$L_i = u_{i0} + u_{i1}y_1 + \cdots + u_{in}y_n, \quad i = 0, 1, \cdots, d$$

be $d+1$ generic linear differential polynomials with the vector of coefficients $\boldsymbol{u}_i = (u_{i0}, \cdots, u_{in})$. Given $\boldsymbol{a}_i = (a_{i0}, \cdots, a_{in}) \in \mathbb{P}^n$, let

$$L_i(\boldsymbol{a}_i) = a_{i0} + a_{i1}y_1 + \cdots + a_{in}y_n, \quad i = 0, 1, \cdots, d$$

denote the defining polynomial of $d+1$ differential hyperplanes. Let

$$Z_0 = \big\{(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_d) \in (\mathbb{P}^n)^{d+1} |\, V \cap \mathbb{V}(L(\boldsymbol{a}_0)) \cap \cdots \cap \mathbb{V}(L(\boldsymbol{a}_d)) \neq \emptyset\big\}. \tag{8}$$

Then by Theorem 3.3, the Kolchin closure of Z_0 (i.e., the smallest differential variety containing Z_0), $\overline{Z_0}^{\text{kol}}$, is an irreducible differential variety of codimension 1. So there exists a unique irreducible differential polynomial $F(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)$ such that $\overline{Z_0}^{\text{kol}}$ is the general component of F, that is,

$$\overline{Z_0}^{\text{kol}} = \mathbb{V}(\text{sat}(F))$$

under any arbitrary ranking.

Definition 3.5 (see [28], Definition 4.2) The unique $F(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)$ (up to appropriate scaling) is defined to be the differential Chow form of V or $\mathbb{I}(V)$.

Differential Chow forms uniquely characterize their corresponding differential varieties. They could be computed using differential characteristic set methods by its definition; and for irreducible differential varieties given by characteristic sets, algorithms with single exponential complexity were designed in [94] to compute their differential Chow forms.

The following theorem gives some basic properties of differential Chow forms.

Theorem 3.6 (see [28], Theorem 1.2) *Let V be an irreducible differential variety defined over K with differential dimension d and order h. Suppose $F(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)$ is the differential Chow form of V. Then F has the following properties.*

1) $\mathrm{ord}(F) = h$. *In particular,* $\mathrm{ord}(F, u_{i0}) = h$ *for each* $i = 0, 1, \cdots, d$.

2) *F is differentially homogenous of the same degree m in each $\boldsymbol{u}_i$. This m is called the* differential degree *of V.*

3) *Let $g = \deg(F, u_{00}^{(h)})$. There exist differential extension fields $K_\tau\,(\tau = 1, 2, \cdots, g)$ of K and $\xi_{\tau j} \in K_\tau\,(j = 1, 2, \cdots, n)$ such that*

$$F = A \prod_{\tau=1}^{g} (u_{00} + u_{01}\xi_{\tau 1} + \cdots + u_{0n}\xi_{\tau n})^{(h)},$$

where A is a differential polynomial free from $u_{00}^{(h)}$. Moreover, each $\xi_\tau = (\xi_{\tau 1}, \xi_{\tau 2}, \cdots, \xi_{\tau n})$ is a generic point of V, and $L_1, L_2, \cdots, L_d$ vanish at ξ_τ.

4) *The points $\xi_1, \xi_2, \cdots, \xi_g$ are the only points of V lying on the differential hyperplanes $L_i = 0\,(i = 1, 2, \cdots, d)$ as well as on the algebraic hyperplanes $L_0^{(k)} = 0\,(k = 0, 1, \cdots, h-1)$. The number g is called the* leading differential degree *of V.*

5) *Given $d+1$ differential hyperplanes $L_i(\boldsymbol{a}_i) = 0\,(i = 0, 1, \cdots, d)$, if V and $L_i(\boldsymbol{a}_i) = 0\ (i = 0, 1, \cdots, d)$ have a point in common, then $F(\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_d) = 0$. Conversely, if $F(\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_d) = 0$ and $\frac{\partial F}{\partial u_{00}^{(h)}}(\boldsymbol{a}_0, \boldsymbol{a}_1, \cdots, \boldsymbol{a}_d) \neq 0$, then the $d+1$ hyperplanes $L_i(\boldsymbol{a}_i) = 0\,(i = 0, 1, \cdots, d)$ and V have a common point.*

Below is a simple example to illustrate these invariants of a differential variety.

Example 3.7 Let $n = 1$ and $V = \mathbb{V}(y^2 y' + 1) \subseteq \mathbb{A}^1$. Then the differential Chow form of V is $F(\boldsymbol{u}_0) = u_{00}^2 u_{01} u_{00}' - u_{00}^3 u_{01}' - u_{01}^4$. The order of V is 1, the differential degree of V is 4 and the leading differential degree of V is 1.

A differential variety is called order-unmixed if all its components have the same differential dimension and order. Let V be an order-unmixed differential variety of dimension d and order h and $V = \bigcup_{i=1}^{l} V_i$ its minimal irreducible decomposition with $F_i(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)$ the Chow form of V_i. Let

$$F(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d) = \prod_{i=1}^{l} F_i(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)^{s_i} \tag{9}$$

with s_i arbitrary nonnegative integers. In [28], a differential algebraic cycle is defined associated to (9) similar to its algebraic analog, that is, $\boldsymbol{V} = \sum_{i=1}^{l} s_i V_i$ is a differential algebraic cycle with s_i as the multiplicity of V_i and $F(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_d)$ is called the differential Chow form of $\boldsymbol{V}$.

Suppose each V_i is of differential degree m_i and leading differential degree g_i, then the leading differential degree and differential degree of $\boldsymbol{V}$ is defined to be $\sum_{i=1}^{l} s_i g_i$ and $\sum_{i=1}^{l} s_i m_i$ respectively. A differential cycle $\boldsymbol{V}$ in the n dimensional affine space with dimension d, order h, leading differential degree g, and differential degree m is said to be of index (d,h,g,m) in $\mathbb{A}^n$.

Definition 3.8 Let $\boldsymbol{V}$ be a differential cycle of index (d,h,g,m) in $\mathbb{A}^n$. The differential Chow coordinate of $\boldsymbol{V}$ is the coefficient vector of the differential Chow form of $\boldsymbol{V}$ considered as a point in a higher dimensional projective space determined by (d,h,g,m) and n.

Definition 3.9 Fix an index (d,h,g,m) and n. Consider the sets

$$\mathbb{V}_{(n,d,h,g,m)} = \{\boldsymbol{V} \big| \boldsymbol{V} \text{ is a differential cycle of index } (d,h,g,m) \text{ in } \mathbb{A}^n\}$$

and

$$\mathcal{C}_{(n,d,h,g,m)} = \big\{\mathrm{c}_{\boldsymbol{V}} \big| \, \mathrm{c}_{\boldsymbol{V}} \text{is the differential Chow coordinate of } \boldsymbol{V}, \boldsymbol{V} \in \mathbb{V}_{(n,d,h,g,m)}\big\}.$$

If $\mathbb{V}_{(n,d,h,g,m)}$ (or equally $\mathcal{C}_{(n,d,h,g,m)}$) has the structure of a differential constructible set in some differential space, then $\mathbb{V}_{(n,d,h,g,m)}$ is called the differential Chow variety of index (d,h,g,m) of $\mathbb{A}^n$, denoted by δ-chow(n,d,h,g,m).

Once the existence of differential Chow varieties is proved, the theory of differential Chow varieties will provide a natural stratification of the parameter spaces of differential cycles via the discrete index invariant. In the case $g=1$, the existence of differential Chow varieties was proved through constructing the defining differential equations and inequations of $\mathcal{C}_{(n,d,h,1,m)}$.

Theorem 3.10 (see [28], Theorem 5.7) *For each n,d,m and $g=1$, the differential Chow variety δ-chow$(n,d,h,1,m)$ exists.*

But the constructive methods used to prove Theorem 3.10 could not be adapted to prove the general case. The existence of differential Chow varieties in general case was proved with a model-theoretical approach in [30] (refer to [30] for a detailed proof).

Theorem 3.11 (see [30], Theorem 5.1) *For each nonnegative integer n,d,g,m, the differential Chow variety δ-chow(n,d,h,g,m) exists.*

Differential Chow forms are also studied for projective differential varieties[29]. In the partial differential case, the theory of differential Chow forms and differential Chow varieties is not well-developed[32]. Even in the course of defining partial differential Chow forms, an insuperable obstacle is encountered: It is impossible to define differential Chow forms for most of irreducible partial differential varieties. Only for a specific kind of irreducible partial differential varieties, we could manage to define differential Chow forms, and only a specific kind of differential Chow varieties exist.

For the ordinary difference case, the generic intersection theory for difference varieties is proved and Theorem 3.3 is generalised to its difference analog[31]. Also, in [31], the difference Chow form is defined for irreducible difference varieties and its basic properties are proved too. Due to the distinct structures of the differential and difference operators, the theory of difference

Chow forms is far from well-develped compared with their ordinary differential counterparts. In particular, it may happen that two different irreducible difference varieties may have the same difference Chow form (see [31, Example 6.4]). Thus, in general, it is impossible to develop a theory of difference Chow varieties.

4 Differential Resultants and Sparse Differential Resultants

In this section, we introduce the theory of differential resultants and the theory of sparse differential resultants.

4.1 Differential Resultants

Differential resultants were first studied for differential operators, or equivalently, for linear homogenous differential polynomials. Using the analogue between ordinary differential operators and univariate polynomials, differential resultants for two linear ordinary differential operators were implicitly given by Ore[43] and then studied by Berkovich and Tsirulik[44] using Sylvester style matrices. The subresultant theory was first studied by Chardin[48] for two differential operators and then by Li[49] and Hong[50] for more general Ore polynomials. Carrá-Ferro generalized it to the partial differential operators in [47].

The differential resultant for two nonlinear differential polynomials in one variable was defined by Ritt in [51, p.47]. In [52, p.46], Zwillinger proposed to define the differential resultant of two differential polynomials as the determinant of a matrix following the idea of algebraic multivariate resultants, but did not provide the details. General differential resultants were defined by Carrà-Ferro using Macaulay's definition of algebraic resultants[54, 95]. But, the treatment in [54, 95] is not complete. For instance, the differential resultant for two generic differential polynomials with positive orders and degrees greater than one is always identically zero if using the definition in [54]. In [96], Yang, et al. used the idea of algebraic Dixon resultant to compute the differential resultant. Although efficient, this approach is also not complete, because it does not show that the differential resultant can always be computed in this way. Differential resultants for linear ordinary differential polynomials were studied by Rueda-Sendra[53, 57].

The first rigorous definition of the differential resultant of $n+1$ differential polynomials in n variables was given by Gao, et al. in [28], where the properties of differential resultants were proved.

Definition 4.1 Let $\mathbb{P}_i$ $(i=0,1,\cdots,n)$ be generic differential polynomials in n variables $y_1, y_2, \cdots, y_n$ with orders s_i and degrees m_i. For each i, denote $\boldsymbol{u}_i$ to be the set of coefficients of $\mathbb{P}_i$. By Theorem 3.3, there exists a unique (up to a scalar in $\mathbb{Q}$) irreducible differential polynomial $R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) \in \mathbb{Q}\{\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n\}$ such that

$$[\mathbb{P}_0, \mathbb{P}_1, \cdots, \mathbb{P}_n] \cap \mathbb{Q}\{\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n\} = \mathrm{sat}(R).$$

This $R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n)$ is defined to be the differential resultant of $\mathbb{P}_0, \mathbb{P}_1, \cdots, \mathbb{P}_n$.

For a given system of $n+1$ differential polynomials $\overline{P}_i$ in $y_1, y_2, \cdots, y_n$ with orders s_i, degrees m_i and coefficients $\boldsymbol{v}_i$ from some differential field K, their differential resultant is defined to be

$R(\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) \in K$. The vanishing of the differential resultant gives a necessary condition for the system having a common solution. Besides, differential resultants have the following properties which are similar to the classical algebraic case.

Theorem 4.2 (see [28], Theorem 1.3) *Let $\mathbb{P}_i$ $(i = 0, 1, \cdots, n)$ be generic differential polynomials in $y_1, y_2, \cdots, y_n$ with orders s_i, degrees m_i, and degree* 0 *terms u_{i0} respectively. Let $R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n)$ be the differential resultant of $\mathbb{P}_0, \mathbb{P}_1, \cdots, \mathbb{P}_n$, where $\boldsymbol{u}_i$ is the set of coefficients of $\mathbb{P}_i$. Then*

a) *$R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n)$ is differentially homogeneous in each $\boldsymbol{u}_i$ and is of order $h_i = s - s_i$ in $\boldsymbol{u}_i$ $(i = 0, 1, \cdots, n)$ with $s = \sum_{l=0}^{n} s_l$.*

b) *There exist $\xi_{\tau\rho}(\rho = 1, 2, \cdots, n)$ in the differential extension fields $K_\tau(\tau = 1, 2, \cdots, t_0)$ of $\mathcal{F}$ such that*

$$R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) = A(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) \prod_{\tau=1}^{t_0} \mathbb{P}_0(\xi_{\tau 1}, \xi_{\tau 2}, \cdots, \xi_{\tau n})^{(h_0)},$$

where $A(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n)$ is a differential polynomial in $\boldsymbol{u}_i$, $t_0 = \deg(R, u_{00}^{(h_0)})$, $\mathbb{P}_0(\xi_{\tau 1}, \xi_{\tau 2}, \cdots, \xi_{\tau n})^{(h_0)}$ is the (h_0)-th derivative of $\mathbb{P}_0(\xi_{\tau 1}, \xi_{\tau 2}, \cdots, \xi_{\tau n})$, and $(\xi_{\tau 1}, \xi_{\tau 2}, \cdots, \xi_{\tau n})\,(\tau = 1, 2, \cdots, t_0)$ are certain generic points of the zero dimensional prime ideal $[\mathbb{P}_1, \mathbb{P}_2, \cdots, \mathbb{P}_n]$.

c) *The differential resultant can be written as a linear combination of $\mathbb{P}_i$ and their derivatives up to the order $s - s_i\,(i = 0, 1, \cdots, n)$. Precisely, we have*

$$R(\boldsymbol{u}_0, \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n) = \sum_{i=0}^{n} \sum_{j=0}^{s-s_i} h_{ij} \delta^j \mathbb{P}_i.$$

In the above expression, $h_{ij} \in \mathcal{F}\langle \boldsymbol{u} \rangle[y_1, \cdots, y_n, \cdots, y_1^{(s)}, \cdots, y_n^{(s)}]$ have degrees at most $(sn + n)^2 D^{sn+n} + D(sn + n)$, where $\boldsymbol{u} = \cup_{i=0}^{n} \boldsymbol{u}_i \setminus \{u_{00}, \cdots, u_{n0}\}$, and $D = \max\{m_0, m_1, \cdots, m_n\}$.

d) *Suppose that $\boldsymbol{u}_i$ $(i = 0, 1, \cdots, n)$ specialize to sets $\boldsymbol{v}_i$ of specific elements in $\mathcal{E}$ and $\overline{\mathbb{P}}_i\,(i = 0, 1, \cdots, n)$ are obtained by substituting $\boldsymbol{u}_i$ by $\boldsymbol{v}_i$ in $\mathbb{P}_i$. If $\overline{\mathbb{P}}_i = 0$ $(i = 0, 1, \cdots, n)$ have a common solution, then $R(\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) = 0$. On the other hand, if $R(\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) = 0$ and $\frac{\partial R}{\partial u_{00}^{(h_0)}}(\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_n) \neq 0$, then $\overline{\mathbb{P}}_i = 0$ $(i = 0, 1, \cdots, n)$ have a common solution in $\mathcal{E}$.*

If $\boldsymbol{u}_i$ specializes to a set $\boldsymbol{v}_i$ of specific elements in an extension field of $\mathcal{F}$, then either $S_R(\boldsymbol{v}_0, \boldsymbol{v}_1, \cdots, \boldsymbol{v}_d) = 0$ or $\overline{\mathbb{P}}_i\,(i = 0, 1, \cdots, n)$ have a common solution in an extension field of $\mathcal{F}$, where $\overline{\mathbb{P}}_i$ are obtained by substituting $\boldsymbol{u}_i$ by $\boldsymbol{v}_i$.

e) *(BKK-type bound) For each $i \in \{0, 1, \cdots, n\}$,*

$$\deg(R, \boldsymbol{u}_i) \leq \sum_{k=0}^{s-s_i} \mathcal{M}\big((\mathcal{Q}_{jl})_{j \neq i, 0 \leq l \leq s-s_j}, \mathcal{Q}_{i0}, \cdots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \cdots, \mathcal{Q}_{i,s-s_i}\big),$$

where $s = \sum_{i=0}^{n} s_i$, $\mathcal{Q}_{jl}$ is the Newton polytope of $\delta^l \mathbb{P}_j$ as a polynomial in $y_1^{[s]}, y_2^{[s]}, \cdots, y_n^{[s]}$ and $\mathcal{M}(S)$ is the mixed volume of the polytopes in S.

Example 4.3 The simplest nonlinear differential resultant is the case $n = 1, d_0 = d_1 = 2, s_0 = 0, s_1 = 1$. Denote y_1 by y. Let $\mathbb{P}_0 = u_{00} + u_{01}y + u_{02}y^2$, $\mathbb{P}_1 = u_{10} +$

$u_{11}y + u_{12}y' + u_{13}y^2 + u_{14}yy' + u_{15}(y')^2$. Then the differential resultant for $\mathbb{P}_0$ and $\mathbb{P}_1$ is a δ-polynomial $R(\boldsymbol{u}_0, \boldsymbol{u}_1)$ such that $\mathrm{ord}(R, \boldsymbol{u}_0) = 1$, $\mathrm{ord}(R, \boldsymbol{u}_1) = 0$ and R is δ-homogenous of degree 8 in $\boldsymbol{u}_0$ and degree 2 in $\boldsymbol{u}_1$, respectively. Totally, R has 206 terms. Moreover, R has a matrix representation which is a factor of the determinant of the coefficient matrix of $\mathbb{P}_0, y'\mathbb{P}_0, y^2\mathbb{P}_0, yy'\mathbb{P}_0, y'^2\mathbb{P}_0, \mathbb{P}_0', y\mathbb{P}_0', y'\mathbb{P}_0', yy'\mathbb{P}_0', y'^2\mathbb{P}_0, \mathbb{P}_1$, $y\mathbb{P}_1, y'\mathbb{P}_0, yy'\mathbb{P}_1$ w.r.t. the monomials $\{y^{l_0}(y')^{l_1} | 0 \le l_0 \le 4, 0 \le l_1 < 4, l_0 + l_1 \le 4\}$.

In the computational aspect, differential resultants could be computed by the characteristic set method. But to be more efficient, it is desirable to find matrix representation or determinantal formulae for the differential resultants. Note that such a formula was claimed to be given in [54, 95], which are not correct as explained in the beginning of this section. The first matrix representation was given by Zhang, et al.[56] for two generic ordinary differential polynomials f_1 and f_2 in the differential indeterminate y with order 1 and arbitrary degree. It is still an open issue whether differential resultants generally admit matrix representations.

Theorem 4.4 (see [56], Theorem 4.4) *The algebraic sparse resultant of $f_1, f_2, \delta f_1, \delta f_2$ as polynomials in variables y, y', y'' is not identically zero, and contains the differential resultant of f_1 and f_2 as a factor.*

4.2 Sparse Differential Resultants

Similar to the fact that sparse resultants are defined for Laurent polynomial systems and related to solutions in $(\mathbb{C}\backslash\{0\})^n$, sparse differential resultants are related to Laurent differential polynomials and non-polynomial solutions.

Let $\mathbb{Y} = \{y_1, y_2, \cdots, y_n\}$ be the set of n differential variables and (K, δ) is a differential field. A Laurent monomial of the form $\prod_{i=1}^{n}\prod_{k=0}^{s}(y_i^{(k)})^{m_{ik}}$ $(s \in \mathbb{N}, m_{ik} \in \mathbb{Z})$ is called a Laurent differential monomial in $\mathbb{Y}$. A Laurent differential polynomial in $\mathbb{Y}$ over K is a finite linear combination of Laurent differential monomials with coefficients from K. The Laurent differential polynomial ring over K is denoted by $K\{\mathbb{Y}^{\pm}\}$.

To seek solutions for Laurent differential polynomials, the presence of negative exponents requires us to consider non-polynomial solutions. A non-polynomial solution of $f \in K\{\mathbb{Y}^{\pm}\}$ is a point $(a_1, a_2, \cdots, a_n) \in \mathbb{A}^n$ such that $f(a_1, a_2, \cdots, a_n) = 0$ and for each i and k, $\delta^k a_i \neq 0$.

Let $\mathcal{A}_i = \{M_{i0}, M_{i1}, \cdots, M_{il_i}\}$ $(i = 0, 1, \cdots, n)$ be $n+1$ sets of Laurent differential monomials in $\mathbb{Y}$. Consider $n+1$ generic Laurent differential polynomials in $\mathbb{Y}$

$$P_i = \sum_{k=0}^{l_i} u_{ik} M_{ik}, \quad i = 0, 1, \cdots, n \tag{10}$$

defined over $\mathcal{A}_i$ (called the support of P_i), and denote $\boldsymbol{u}_i = (u_{i0}, u_{i1}, \cdots, u_{il_i})$. Given vectors $\boldsymbol{a}_i = (a_{i0}, a_{i1}, \cdots, a_{il_i}) \in \mathbb{P}^{l_i}$, let

$$P_i(\boldsymbol{a}_i, \mathbb{Y}) := \sum_{k=0}^{l_i} a_{ik} M_{ik}, \quad i = 0, 1, \cdots, n \tag{11}$$

denote the specific Laurent differential system with coefficients $\boldsymbol{a}_i$.

The sparse differential resultant should be a differential polynomial in the coefficients $\boldsymbol{u}_i$ which vanishes at $(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n)$ precisely (in certain sense) when the system $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0$ has a non-polynomial solution. For this purpose, let

$$Z_0 = \big\{(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) | P_0(\boldsymbol{a}_i, \mathbb{Y}) = \cdots = P_0(\boldsymbol{a}_n, \mathbb{Y}) = 0 \text{ has a non-polynomial solution}\big\}$$

and Z be the Kolchin closure of Z_0 in $\mathbb{P}^{l_0} \times \cdots \times \mathbb{P}^{l_n}$, that is,

$$Z = \big\{(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) | P_0(\boldsymbol{a}_i, \mathbb{Y}) = \cdots = P_0(\boldsymbol{a}_n, \mathbb{Y}) = 0 \text{ has a non-polynomial solution}\big\}^{\text{kol}}.$$

Then Z is an irreducible differential variety. If Z is of codimension 1, then there exists a unique differential polynomial such that Z is the general component of this polynomial. We need to find a necessary and sufficient condition for Z satisfying such desired property. This is precisely the condition that $\mathcal{A}_0, \cdots, \mathcal{A}_n$ is Laurent differentially essential.

The system $\mathcal{A}_0, \cdots, \mathcal{A}_n$, or $\mathbb{P}_0, \cdots, \mathbb{P}_n$ in 10, is called Laurent differentially essential if there exists $k_i\,(i = 0, 1, \cdots, n)$ with $1 \leq k_i \leq l_i$ such that

$$\delta.\text{tr.deg}\, \mathbb{Q}\left\langle \frac{M_{0k_0}}{M_{00}}, \frac{M_{1k_1}}{M_{10}}, \cdots, \frac{M_{nk_n}}{M_{n0}} \right\rangle = n.$$

There exists a simple criterion based on linear algebraic computations to detect whether $\mathcal{A}_0, \cdots, \mathcal{A}_n$ is Laurent differentially essential. Let $M_{ik}/M_{i0} = \prod_{j=1}^{n} \prod_{l=0}^{s_i} (y_j^{(l)})^{t_{ikjl}}$, where $s_i = \text{ord}(\mathbb{P}_i, \mathbb{Y})$ and $t_{ikjl} \in \mathbb{Z}$. Introduce n algebraic indeterminates $x_1, \cdots, x_n$ and set $d_{ij} = \sum_{k=0}^{l_i} u_{ik} \sum_{l=0}^{s_i} t_{ikjl} x_j^l$ for $i = 0, 1, \cdots, n$ and $j = 1, 2, \cdots, n$.

Proposition 4.1 *For $\mathbb{P}_i$ given in 10, let*

$$\boldsymbol{M}_{\mathbb{P}} = \begin{pmatrix} d_{01} & d_{02} & \cdots & d_{0n} \\ d_{11} & d_{12} & \cdots & d_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ d_{n1} & d_{n2} & \cdots & d_{nn} \end{pmatrix}.$$

Then the following are equivalent.

1) *$\mathcal{A}_0, \cdots, \mathcal{A}_n$ is Laurent differentially essential.*

2) *rank$(\boldsymbol{M}_{\mathbb{P}}) = n$.*

3) *There exist $k_i\,(i = 0, 1, \cdots, n)$ with $1 \leq k_i \leq l_i$ such that rank$(\boldsymbol{M}_{k_0, \cdots, k_n}) = n$ where $\boldsymbol{M}_{k_0, \cdots, k_n} = \big(d'_{ij}\big)_{(n+1)\times(n+1)}$ with $d'_{ij} = \sum_{l=0}^{s_i} t_{ik_ijl} x_j^l$.*

4) *Z is an irreducible differential variety of codimension 1.*

Definition 4.5 Let $\mathcal{A}_0, \cdots, \mathcal{A}_n$ be a Laurent differentially essential system. There exists a unique (up to a scalar in $\mathbb{Q}$) irreducible differential polynomial $\boldsymbol{R} \in \mathbb{Q}\{\boldsymbol{u}_0 \cdots, \boldsymbol{u}_n\}$ such that

$$Z = \mathbb{V}\big(\text{sat}(\boldsymbol{R})\big).$$

This $\boldsymbol{R}$ is defined to be the *sparse differential resultant* of $\mathbb{P}_0, \cdots, \mathbb{P}_n$, denoted by $\text{Res}_{\mathcal{A}_0, \cdots, \mathcal{A}_n}$.

Example 4.6 Let $\mathcal{A}_0 = \{\mathbf{1}, y_1y_2\}$, $\mathcal{A}_1 = \{\mathbf{1}, y_1y_2'\}$ and $\mathcal{A}_2 = \{\mathbf{1}, y_1'y_2'\}$. It is easy to verify that $\mathcal{A}_0, \mathcal{A}_1, \mathcal{A}_2$ form a Laurent differentially essential system. And

$$\mathrm{Res}_{\mathcal{A}_0,\mathcal{A}_1,\mathcal{A}_2} = u_{10}u_{01}u_{21}u_{11}u_{00}' - u_{10}u_{00}u_{11}u_{21}u_{01}' - u_{01}^2u_{21}u_{10}^2 - u_{01}u_{00}u_{11}^2u_{20}.$$

For a specific system of Laurent differential polynomials $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0$ with supports $\mathcal{A}_i$ and coefficents $\boldsymbol{a}_i$, the sparse differential resultant of $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0$ is defined to be the value $\mathrm{Res}_{\mathcal{A}_0,\cdots,\mathcal{A}_n}(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n)$. Similar to the relation between sparse resultants and non-zero solutions (e.g., in $(\mathbb{C}\backslash\{0\})^n$), the vanishing of its sparse differential resultant gives a necessary condition such that the given system has a non-polynomial solution. This is one property of the sparse differential resultant. Besides, it has similar properties as its algebraic countpart.

Theorem 4.7 (see [55], Theorem 1.2) *Let $\mathcal{A}_0, \cdots, \mathcal{A}_n$ be a Laurent differentially essential system. The sparse differential resultant $\boldsymbol{R}(\boldsymbol{u}_0, \cdots, \boldsymbol{u}_n) = \mathrm{Res}_{\mathcal{A}_0,\cdots,\mathcal{A}_n}$ has the following properties:*

1) *If the $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0$ in* (11) *has a common non-polynomial solution, then $\boldsymbol{R}(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) = 0$. Conversely, if $\boldsymbol{R}(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) = 0$ and $\frac{\partial \boldsymbol{R}}{\partial u_{00}^{(h)}}(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) \neq 0$ ($h = \mathrm{ord}(\boldsymbol{R}, u_{00})$), then $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0\,(i = 0, \cdots, n)$ has a common non-polynomial solution.*

2) *$\boldsymbol{R}(\boldsymbol{u}_0, \cdots, \boldsymbol{u}_n)$ is differentially homogenous in each $\boldsymbol{u}_i\,(i = 0, 1, \cdots, n)$.*

3) (Poisson Product Formula) *Let $h = \mathrm{ord}(\boldsymbol{R}, \boldsymbol{u}_0) \geq 0$. Then $t_0 = \deg(\boldsymbol{R}, u_{00}^{(h)}) \geq 1$ and there exist $(\mathbb{Q}_\tau, \delta_\tau)$ and $\xi_{\tau k} \in \mathbb{Q}_\tau$ for $\tau = 1, 2, \cdots, t_0$ and $k = 1, 2, \cdots, l_0$ such that*

$$\boldsymbol{R} = A \prod_{\tau=1}^{t_0} \left(u_{00} + \sum_{k=1}^{l_0} u_{0k}\xi_{\tau k} \right)^{(h_0)},$$

where A is a polynomial in $\mathbb{Q}\langle \boldsymbol{u}_1, \cdots, \boldsymbol{u}_n\rangle[\boldsymbol{u}_0^{[h_0]}\backslash u_{00}^{(h_0)}]$. Furthermore, if additionally the system is normal rank essential (see [55, Definition 5.5]), *then there exist $\eta_\tau = (\eta_{\tau 1}, \cdots, \eta_{\tau n}) \in \mathbb{Q}_\tau^n$ such that*

$$\boldsymbol{R} = A \prod_{\tau=1}^{t_0} \left[\frac{\mathbb{P}_0(\eta_\tau)}{M_{00}(\eta_\tau)} \right]^{(h_0)},$$

And η_τ $(\tau = 1, 2, \cdots, t_0)$ are common non-polynomial solutions of $\mathbb{P}_1, \cdots, \mathbb{P}_n$.

4) (*Differential toric varieties*) *Assume that $\mathcal{A}_i = \mathcal{A}\,(i = 0, 1, \cdots, n)$. The differential toric variety $X_{\mathcal{A}}$ associated with $\mathcal{A}$ is defined and is shown to be an irreducible projective differential variety of dimension n. And the differential Chow form of $X_{\mathcal{A}}$ is $\boldsymbol{R}$.*

5) *$h_i = \mathrm{ord}(\boldsymbol{R}, \boldsymbol{u}_i) \leq \mathrm{J}_i = \mathrm{Jac}(\widehat{\mathbb{P}_{\hat{i}}})$ for $i = 0, 1, \cdots, n$, where $\widehat{\mathbb{P}_{\hat{i}}} = \{\mathbb{P}_0, \cdots, \mathbb{P}_n\}\backslash\{\mathbb{P}_i\}$.*

6) *$\deg(\boldsymbol{R}) \leq \prod_{i=0}^n (m_i+1)^{h_i+1} \leq (m+1)^{\sum_{i=0}^n (J_i+1)} = (m+1)^{J+n+1}$, where m_i is the degree of the norm form of $\mathbb{P}_i$, $m = \mathrm{max}_i\{m_i\}$, and $J = \sum_{i=0}^n J_i$.*

7) *Let $\mathrm{ord}(\mathbb{P}_i, y_j) = e_{ij}$. $\boldsymbol{R}$ has the following representation*

$$\prod_{i=0}^{n} N_{i0}^{(h_i+1)\deg(\boldsymbol{R})} \cdot \boldsymbol{R} = \sum_{i=0}^{n}\sum_{j=0}^{h_i} G_{ij}\left(\mathbb{P}_i\right)^{(j)}$$

where $G_{ij} \in \mathbb{Q}[\boldsymbol{u}_0^{[h_0]}, \cdots, \boldsymbol{u}_n^{[h_n]}, y_1^{[t_1]}, \cdots, y_n^{[t_n]}]$ with $t_j = \mathrm{max}_{i=0}^n\{h_i + e_{ij}\}$ such that $\deg(G_{ij}\mathbb{P}_i^{(j)}) \leq [m + 1 + \sum_{i=0}^n (h_i + 1)\deg(N_{i0})]\deg(\boldsymbol{R})$.

Similar to the differential resultant, in principle, the sparse differential resultant can also be computed with characteristic set methods for differential polynomials via symbolic computation[1, 4, 10]. But in general, differential elimination procedures based on characteristic sets do not have an elementary complexity bound. In [55], based on order and degree bounds given in 5)–7) of Theorem 4.7, a single exponential algorithm **SDResultant** to compute the sparse differential resultant $\boldsymbol{R}$ was proposed.

Theorem 4.8 (see [55], Theorem 6.18) *The sparse differential resultant of* $\mathbb{P}_0, \cdots, \mathbb{P}_n$ *can be computed with at most* $O\big((J+n+2)^{O(lJ+l)}(m+1)^{O(lJ+l)(J+n+2))}/n^n\big)$ $\mathbb{Q}$*-arithmetic operations, where* $l = \sum_{i=0}^{n}(l_i+1)$*,* $m = \max_{i=0}^{n} m_i$*, and* $J = \sum_{i=0}^{n} J_i$*.*

For linear non-homogenous sparse differential polynomials, Rueda[57] gave matrix formulas to compute the sparse linear differential resultants. Precisely, let P be a system of n linear nonhomogeneous ordinary differential polynomials in $n-1$ variables. Linear differential resultant formulas for P are given which are determinants of coefficient matrices of appropriate sets of derivatives of the differential polynomials in P or in a linear perturbation of P. In particular, when P is "super essential", such a formula is the determinant of a matrix without zero columns. It is desirable to give matrix representations for sparse differential resultants for non-linear systems.

4.3 Sparse Difference Resultants

Let $\mathcal{F}$ be a reflexive difference field with a transforming operator σ and $\mathcal{F}\{\mathbb{Y}\} = \mathcal{F}[\sigma^k y_j : k \in \mathbb{N}]$ the ring of difference polynomials in the difference indeterminates $\mathbb{Y} = \{y_1, \cdots, y_n\}$.

Similarly to the differential case, to study sparse difference resultants, we are interested in Laurent difference polynomials. A Laurent difference monomial is a Laurent monomial of the form $\prod_{i=1}^{n}\prod_{k=0}^{s}(\sigma^k y_i)^{b_{ik}}$ for some $s \in \mathbb{N}$ and $b_{ik} \in \mathbb{Z}$. A Laurent difference polynomial over $\mathcal{F}$ is a finite linear combination of Laurent difference monomials with coefficients in $\mathcal{F}$. We denote the difference ring of Laurent difference polynomials over $\mathcal{F}$ by $\mathcal{F}\{y_1, y_1^{-1}, \cdots, y_n, y_n^{-1}\}$, or simply by $\mathcal{F}\{\mathbb{Y}^{\pm}\}$. For $F \in \mathcal{F}\{\mathbb{Y}^{\pm}\}$, an n-tuple $(a_1, \cdots, a_n)$ over $\mathcal{F}$ with each $a_i \neq 0$ is said to be a nonzero difference solution of F if $F(a_1, \cdots, a_n) = 0$.

Suppose $\mathcal{A}_i = \{M_{i0}, M_{i1}, \cdots, M_{il_i}\}\,(i = 0, 1, \cdots, n)$ are finite sets of Laurent difference monomials in $\mathbb{Y}$. Consider $n+1$ *generic Laurent difference polynomials* defined over $\mathcal{A}_0, \cdots, \mathcal{A}_n$:

$$\mathbb{P}_i = \sum_{k=0}^{l_i} u_{ik} M_{ik}, \quad i = 0, 1, \cdots, n, \tag{12}$$

and denote $\boldsymbol{u}_i = (u_{i0}, u_{i1}, \cdots, u_{il_i}),\ i = 0, 1, \cdots, n$. Given vectors $\boldsymbol{a}_i = (a_{i0}, \cdots, a_{il_i}) \in \mathbb{P}^{l_i}$, let

$$\mathbb{P}_i(\boldsymbol{a}_i, \mathbb{Y}) := \sum_{k=0}^{l_i} a_{ik} M_{ik}, \quad i = 0, 1, \cdots, n \tag{13}$$

denote the specific Laurent difference system with coefficients $\boldsymbol{a}_i$.

Sparse difference resultants are used to give conditions on the coefficients $\boldsymbol{a}_i$ to determine whether $P_i(\boldsymbol{a}_i, \mathbb{Y}) = 0$ has a nonzero solution. Let

$$Z_0 = \big\{(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n) | \mathbb{P}_0(\boldsymbol{a}_i, \mathbb{Y}) = \cdots = \mathbb{P}_n(\boldsymbol{a}_n, \mathbb{Y}) = 0 \text{ has a nonzero solution}\big\}$$

and Z be the smallest difference variety in $\mathbb{P}^{l_0}\times\cdots\times\mathbb{P}^{l_n}$ containing Z_0. Then Z is an irreducible difference variety. And Z is of codimension one if and only if $\mathcal{A}_0,\cdots,\mathcal{A}_n$ form a Laurent transformally essential system.

Definition 4.9 A set of Laurent difference polynomials of the form 12 is called Laurent transformally essential if there exist k_i $(i=0,1,\cdots,n)$ with $1\leq k_i\leq l_i$ such that

$$\sigma.\mathrm{tr.deg}\,\mathbb{Q}\Big\langle\frac{M_{0k_0}}{M_{00}},\frac{M_{1k_1}}{M_{10}},\cdots,\frac{M_{nk_n}}{M_{n0}}\Big\rangle/\mathbb{Q}=n.$$

In this case, we also say that $\mathcal{A}_0,\cdots,\mathcal{A}_n$ form a Laurent transformally essential system.

Now suppose $\{\mathbb{P}_0,\cdots,\mathbb{P}_n\}$ is a Laurent transformally essential system. Then Z is an irreducible difference variety of codimension one. Then there exists a unique irreducible difference polynomial $\boldsymbol{R}\in\mathbb{Q}\{\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n\}$ such that Z is a general component of $\boldsymbol{R}$ (Unlike the differential case, there may be several different general components of an irreducible difference polynomial.) From the point view of ideals, if we denote

$$\mathbb{I}_{\boldsymbol{u}}=\{\mathbb{P}_0,\cdots,\mathbb{P}_n\}_{\mathbb{Q}\{\mathbb{Y}^{\pm},\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n\}}\cap\mathbb{Q}\{\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n\},$$

then $\mathbb{I}_{\boldsymbol{u}}$ is a reflexive prime difference ideal of codimension one. By the difference characteristic method, the above $\boldsymbol{R}$ can serve as the first polynomial in each characteristic set of $\mathbb{I}_{\boldsymbol{u}}$ w.r.t. any ranking endowed on $\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n$, that is,

$$[\mathbb{P}_0,\cdots,\mathbb{P}_n]\cap\mathbb{Q}\{\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n\}=\mathrm{sat}(\boldsymbol{R},R_1,\cdots,R_k).$$

(As pointed out in [59, Problem 23], it is still unknown whether $k=0$ or not).

Definition 4.10 The above $\boldsymbol{R}(\boldsymbol{u}_0,\cdots,\boldsymbol{u}_n)$ is defined to be the *sparse difference resultant* of the Laurent transformally essential system $\mathbb{P}_0,\cdots,\mathbb{P}_n$, denoted by $\mathrm{Res}_{\mathcal{A}_0,\cdots,\mathcal{A}_n}$.

Given a specific system of Laurent difference polynomials $\mathbb{P}_i(\boldsymbol{a}_i,\mathbb{Y})$ $(i=0,1,\cdots,n)$, the sparse difference resultant of the $\mathbb{P}_i(\boldsymbol{a}_i,\mathbb{Y})$ is defined to be $\mathrm{Res}_{\mathcal{A}_0,\cdots,\mathcal{A}_n}(\boldsymbol{a}_0,\cdots,\boldsymbol{a}_n)$.

Example 4.11 Let $n=1$ and $\mathbb{P}_0=u_{00}+u_{01}y_1^2$, $\mathbb{P}_1=u_{10}y_1^{(1)}+u_{11}y_1$. Clearly, $\mathbb{P}_0,\mathbb{P}_1$ are Laurent transformally essential. The sparse difference resultant of $\mathbb{P}_0,\mathbb{P}_1$ is

$$\boldsymbol{R}=u_{10}^2u_{01}u_{00}^{(1)}-u_{11}^2u_{00}u_{01}^{(1)}.$$

Similarly to the differential case, there is a simple criterion to detect whether a Laurent difference system is transformally essential in terms of their supports. Let $M_{ik}/M_{i0}=\prod_{j=1}^{n}\prod_{l=0}^{s}(y_j^{(k)})^{t_{ikjl}}$ and set

$$d_{ikj}=\sum_{l=0}^{s}t_{ikjl}x^l\ (j=1,2,\cdots,n)\in\mathbb{Z}[x],$$

where x is a new algebraic indeterminate. Let $\beta_{ik}=(d_{ik1},d_{ik2},\cdots,d_{ikn})$. Then $\sum_{k=1}^{l_i}u_{ik}\beta_{ik}$ is called the symbolic support vector of $\mathbb{P}_i$. The matrix $M_{\mathbb{P}}$ whose rows are the symbolic support vectors of $\mathbb{P}_i$ is called the symbolic support matrix of the system.

Proposition 4.2 *Let $\mathbb{P}_0, \cdots, \mathbb{P}_n$ be defined in* (12)*. Then $\mathbb{P}_0, \cdots, \mathbb{P}_n$ form a Laurent transformally essential system if and only if* $\mathrm{rank}(M_{\mathbb{P}}) = n$.

Sparse difference resultants have the following properties:

Theorem 4.12 (see [59], Theorems 37, 41, 51) *Let $\mathbb{P}_i\,(i = 0, 1, \cdots, n)$ be a Laurent transformally essential system and $\boldsymbol{R}$ its sparse difference resultant. Then*

1) *$\boldsymbol{R}$ is transformally homogeneous in the coefficient set of each $\mathbb{P}_i$. And*

$$\mathrm{Res}(\sigma\mathbb{P}_0, \cdots, \sigma\mathbb{P}_n) = \sigma\mathrm{Res}(\mathbb{P}_0, \cdots, \mathbb{P}_n).$$

2) *If $\mathbb{P}_i(\boldsymbol{a}_i, \mathbb{Y}) = 0\,(i = 0, 1, \cdots, n)$ has a common nonzero difference solution, then their sparse difference resultant $\boldsymbol{R}(\boldsymbol{a}_0, \cdots, \boldsymbol{a}_n)$ is zero.*

3) $\mathrm{ord}(\boldsymbol{R}, \boldsymbol{u}_i) \leq J_i$*, where J_i is the Jacobi number of the system $\{\mathbb{P}_j : j \neq i\}$.*

4) *The degree of $\boldsymbol{R}$ has a Bezout-type bound and $\boldsymbol{R}$ can be written as a linear combination of the norm form of $\mathbb{P}_i$ and its transforms with given order and degree bounds.*

Based on the order and degree bounds, an algorithm **SDResultant**$(\mathbb{P}_0, \cdots, \mathbb{P}_n)$ was designed to compute the sparse difference resultant, which has single-exponential complexity.

Theorem 4.13 (see [59], Theorem 76) *Let $\mathbb{P} = \{\mathbb{P}_0, \cdots, \mathbb{P}_n\}$ be a Laurent transformally essential system of the form* (12)*. Let $\mathrm{J} = \sum_{i=0}^{n} J_i$ and $m = \max_i \deg(\mathbb{P}_i, \mathbb{Y})$. Algorithm* **SDResultant** *computes the sparse difference resultant $\boldsymbol{R}$ with at most*

$$O\big((J + n + 2)^{O(l\mathrm{J}+l)}(m + 1)^{O((lJ+l)(J+n+2))}/n^n\big)$$

$\mathbb{Q}$*-arithmetic operations.*

When $\mathbb{P}_0, \cdots, \mathbb{P}_n$ are generic differential polynomials (dense in the sense that it contains all terms with respect to bounded order and degree), the sparse difference resultant exists. In this case, $\mathrm{Res}(\mathbb{P}_0, \cdots, \mathbb{P}_n)$ is defined to be the *difference resultant* of $\mathbb{P}_0, \cdots, \mathbb{P}_n$.

We know exact orders and degrees for difference resultants, and also we have determinant formulae to compute difference resultants.

Theorem 4.14 (see [59], Theorem 79) *Let $\mathbb{P}_i\,(i = 0, 1, \cdots, n)$ be generic difference polynomials of the form with order s_i, degree m_i, and coefficients $\boldsymbol{u}_i$. Let $\boldsymbol{R}(\boldsymbol{u}_0, \cdots, \boldsymbol{u}_n)$ be the difference resultant of $\mathbb{P}_0, \cdots, \mathbb{P}_n$. Denote $s = \sum_{i=0}^{n} s_i$. Then $\boldsymbol{R}(\boldsymbol{u}_0, \cdots, \boldsymbol{u}_n)$ is also the algebraic sparse resultant of $\mathbb{P}_0^{[s-s_0]}, \cdots, \mathbb{P}_n^{[s-s_n]}$ treated as polynomials in $\mathbb{Y}^{[s]}$. And for each $i \in \{0, 1, \cdots, n\}$ and $k = 0, \cdots, s - s_i$,*

$$\mathrm{ord}(\boldsymbol{R}, \boldsymbol{u}_i) = s - s_i, \tag{14}$$

$$\deg(\boldsymbol{R}, \boldsymbol{u}_i^{(k)}) = \mathcal{M}\big((\mathcal{Q}_{jl})_{j\neq i, 0\leq l\leq s-s_j}, \mathcal{Q}_{i0}, \cdots, \mathcal{Q}_{i,k-1}, \mathcal{Q}_{i,k+1}, \cdots, \mathcal{Q}_{i,s-s_i}\big), \tag{15}$$

where $\mathcal{Q}_{jl}$ is the Newton polytope of $\mathbb{P}_j^{(l)}$ as a polynomial in $\mathbb{Y}^{[s]}$ and $\boldsymbol{u}_i^{(k)} = (u_{i\alpha}^{(k)})_{u_{i\alpha}\in\boldsymbol{u}_i}$.

Example 4.15 Consider two generic difference polynomials of order one and degree two in one indeterminate y: $\mathbb{P}_i = u_{i0}+u_{01}y+u_{i2}y^{(1)}+u_{i3}y^2+u_{i4}yy^{(1)}+u_{i5}(y^{(1)})^2, i = 0, 1$. Then the degree bound given by Theorem 4.12 is $\deg(\boldsymbol{R}) \leq (2+1)^4 = 81$. By Theorem 4.14, $\deg(\boldsymbol{R}, \boldsymbol{u}_0) = \mathcal{M}(\mathcal{Q}_{10}, \mathcal{Q}_{11}, \mathcal{Q}_{00}) + \mathcal{M}(\mathcal{Q}_{10}, \mathcal{Q}_{11}, \mathcal{Q}_{01}) = 8 + 8 = 16$ and consequently $\deg(\boldsymbol{R}) = 32$, where

$\mathcal{Q}_{00} = \mathcal{Q}_{10} = \mathrm{conv}\{(0,0,0),(2,0,0),(0,2,0)\}$, $\mathcal{Q}_{01} = \mathcal{Q}_{11} = \mathrm{conv}\{(0,0,0),(0,2,0),(0,0,2)\}$, and $\mathrm{conv}(\cdot)$ means taking the convex hull in $\mathbb{R}^3$. By the proof of Theorem 4.14, $\boldsymbol{R}$ is the sparse resultant of $\mathbb{P}_0, \sigma(\mathbb{P}_0), \mathbb{P}_1, \sigma(\mathbb{P}_1)$.

As a direct consequence of the above theorem and the determinant representation for algebraic sparse resultants given in [42], we have the following result.

Corollary 4.15 *The difference resultant for generic difference polynomials* $\mathbb{P}_i$ $(i = 0, 1, \cdots, n)$ *can be written as the form* $\det(D_1)/\det(D_0)$ *where* D_1 *and* D_0 *are matrices whose elements are coefficients of* $\mathbb{P}_i$ *and their transforms up to the order* $s - s_i$ *and* D_0 *is a minor of* D_1.

For sparse difference resultants, it ha been shown in [59] that the sparse difference resultant is equal to the algebraic sparse resultant of certain generic sparse polynomial system (there are procedures to find such a generic sparse polynomial system), which theoretically could also lead to a determinant representation for the sparse difference resultant. The difficulty lies in that we do not know before implementing the procedures that which of the $\sigma^k(\mathbb{P}_i)$ are needed to compute the algebraic sparse resultant. New bounds and an efficient implementation for sparse difference resultant are presented in [60]. Related to the sparse difference resultants, difference toric varieties and binomial ideals are studied in [90, 97].

5 Open Problems

In the paper, we focus on the fundamental algorithmic tools in the elimination theory for differential and difference polynomials, and briefly survey the existing work on the theory of characteristic set methods, the theory of differential Chow forms, and the theory of sparse differential and difference resultants. Despite these significant developments, there are still a number of open problems to be further explored. We will end the paper by proposing four representative problems.

Problem 1 (The Ritt problem) Given an irreducible ordinary differential polynomial $A \in K\{y_1, \cdots, y_n\}$ vanishing at $(0, \cdots, 0)$, decide whether $(0, \cdots, 0)$ is a zero of $\mathrm{sat}(A) = [A] : \mathrm{S}_A^\infty$? More generally, given two prime differential ideals $\mathrm{sat}(\mathcal{A})$ and $\mathrm{sat}(\mathcal{B})$ represented by differential characteristic sets $\mathcal{A}$ and $\mathcal{B}$ respecitively, decide whether $\mathrm{sat}(\mathcal{A}) \subseteq \mathrm{sat}(\mathcal{B})$?

These problems are essential in order to devise algorithms to obtain minimal prime decompositions for finitely generated radical differential ideals. They are far from solved even for the simplest case $n = 1$. And they have several other equivalent formulations[98].

Problem 2 Develop the mechanical theorem proving methods for partial difference polynomial systems, or specifically, to solve the perfect ideal membership problem in the partial difference case.

Problem 3 Give matrix representations or determinantal formulae for (sparse) differential resultants. This is a central problem to be solved to devise efficient algorithms to compute (sparse) differential resultants. However, we do not have such formulae, even in the simplest case of the differential resultant for two generic differential polynomials in one variable. Currently, there are results only in the linear case[57] and in the case when there are two generic differential polynomials of degree two and order one[56].

Problem 4 Develop a theory of resultants for systems of partial differential polynomials.

References

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

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

[3] Cohn R M, *Difference Algebra*, Interscience Publishers John Wiley & Sons, New York-London-Sydeny, 1965.

[4] Wu W T, On the decision problem and the mechanization of theorem-proving in elementary geometry, *Sci. Sinica*, 1978, **21**(2): 159–172.

[5] Wu W T, A constructive theory of differential algebraic geometry based on works of Ritt J F with particular applications to mechanical theorem-proving of differential geometries, *Differential Geometry and Differential Equations* (Shanghai, 1985), volume 1255 of *Lecture Notes in Math.*, Springer, Berlin, 1987, 173–189.

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

[7] Aubry P, Lazard D, and Moreno Maza M, On the theories of triangular sets, *J. Symbolic Comput.*, 1999, **28**(1): 105–124.

[8] Boulier F, Lazard D, Ollivier F, et al., Representation for the radical of a finitely generated differential ideal, *Proceedings of the* 1995 *International Symposium on Symbolic and Algebraic Computation*, ISSAC'95, Montreal, Canada, July 10–12, 1995, 158–166. ACM Press, New York, NY, 1995.

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

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

[11] Wu W T, *Mathematics Machenization*, Science Press/Kluwer, Beijing, 2001.

[12] Yang L, Zhang J Z, and Hou X R, *Non-linear Algebraic Equations and Automated Theorem Proving*, Shanghai Science and Technological Education Pub., 1996 (in Chinese).

[13] Ritt J F and Doob J L, Systems of algebraic difference equations, *Amer. J. Math.*, 1933, **55**(1–4): 505–514.

[14] Ritt J F and Raudenbush H W, Ideal theory and algebraic difference equations, *Trans. Amer. Math. Soc.*, 1939, **46**: 445–452.

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

[16] Gao X S and Yuan C M, Resolvent systems of difference polynomial ideals, *ISSAC* 2006, ACM, New York, 2006, 100–108.

[17] Gao X S, Yuan C M, and Zhang G L, Ritt-Wu's characteristic set method for ordinary difference polynomial systems with arbitrary ordering, *Acta Math. Sci. Ser. B* (*Engl. Ed.*), 2009, **29**(4): 1063–1080.

[18] Zhang G L and Gao X S. Properties of ascending chains for partial difference polynomial systems, *Computer Mathematics 8th Asian Symposium*, ASCM 2007, Singapore, December 15–17, 2007. Revised and invited papers, 307–321. Springer, Berlin, 2008.

[19] Kondratieva M V, Levin A B, Mikhalev A V, et al., *Differential and Difference Dimension Polynomials*, volume 461 of *Mathematics and Its Applications*, Kluwer Academic Publishers, Dordrecht, 1999.

[20] Gao X S, Van der Hoeven J, Yuan C M, et al., Characteristic set method for differential-difference polynomial systems, *J. Symbolic Comput.*, 2009, **44**(9): 1137–1163.

[21] Gel'fand I M, Kapranov M M, and Zelevinsky A V, *Discriminants, Resultants, and Multidimensional Determinants*, Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 1994.

[22] Hodge W V D and Pedoe D, *Methods of Algebraic Geometry, Vol. II*, Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1994.

[23] Brownawell W D, Bounds for the degrees in the nullstellensatz, *Ann. Math.*, 1987, **126**(3): 577–591.

[24] Sturmfels B, Sparse elimination theory, *Computational Algebraic Geometry and Commutative Algebra* (Cortona, 1991), Sympos. Math., XXXIV, Cambridge University Press, Cambridge, 1993, 264–298.

[25] Nesterenko Y V, Estimates for the orders of zeros of functions of a certain class and applications in the theory of transcendental numbers, *Izv. Akad. Nauk SSSR Ser. Mat.*, 1977, **41**: 253–284.

[26] Philippon P, Critères pour l'indpendance algbrique, *Inst. Hautes Ètudes Sci. Publ. Math.*, 1986, **64**: 5–52.

[27] Jeronimo G, Krick T, Sabia J, et al., The computational complexity of the Chow form, *Found. Comput. Math.*, 2004, **4**(1): 41–117.

[28] Gao X S, Li W, and Yuan C M, Intersection theory in differential algebraic geometry: Generic intersections and the differential Chow form, *Trans. Amer. Math. Soc.*, 2013, **365**(9): 4575–4632.

[29] Li W and Gao X S, Chow form for projective differential variety, *J. Algebra*, 2012, **370**: 344–360.

[30] Freitag J, Li W, and Scanlon T, Differential chow varieties exist, *J. Lond. Math. Soc.*, 2017, **95**(1): 128–156.

[31] Li W and Li Y H, Difference Chow form, *J. Algebra*, 2015, **428**: 67–90.

[32] Li W, Partial differential chow forms and a type of partial differential chow varieties, ArXiv: 1709.02358v1, 2017.

[33] Macaulay F S, *The Algebraic Theory of Modular Systems*, Cambridge University Press, Cambridge, 1994.

[34] Eisenbud D, Schreyer F, and Weyman J, Resultants and Chow forms via exterior syzygies, *J. Amer. Math. Soc.*, 2003, **16**(3): 537–579.

[35] Jouanolou J P, Le formalisme du résultant, *Adv. Math.*, 1991, **90**(2): 117–263.

[36] Canny J, Generalised characteristic polynomials, *J. Symb. Comput.*, 1990, **9**(3): 241–250.

[37] Emiris I Z and Canny J F, Efficient incremental algorithms for the sparse resultant and the mixed volume, *J. Symb. Comput.*, 1995, **20**(2): 117–149.

[38] Emiris I Z and Pan V Y, Improved algorithms for computing determinants and resultants, *J. Complexity*, 2005, **21**(1): 43–71.

[39] Bernstein D N, The number of roots of a system of equations, *Functional Anal. Appl.*, 1975, **9**(3): 183–185.

[40] Sturmfels B, On the Newton polytope of the resultant, *J. Algebraic Combin.*, 1994, **3**(2): 207–236.

[41] Emiris I Z, On the complexity of sparse elimination, *J. Complexity*, 1996, **12**(2): 134–166.

[42] D'Andrea C, Macaulay style formulas for sparse resultants, *Trans. Amer. Math. Soc.*, 2002, **354**(7): 2595–2629.

[43] Ore O, Formale theorie der linearen differentialgleichungen (Zweiter Teil), *J. Reine Angew. Math.*, 1932, **168**: 233–252.

[44] Berkovich L M and Tsirulik V G, Differential resultants and some of their applications, *Differ. Equations*, 1986, **22**: 530–536.

[45] Zeilberger D, A holonomic systems approach to special functions identities, *J. Comput. Appl. Math.*, 1990, **32**(3): 321–368.

[46] Chyzak F and Salvy B, Non-commutative elimination in Ore algebras proves multivariate identities, *J. Symbolic Comput.*, 1998, **26**(2): 187–227.

[47] Carrà Ferro G, A resultant theory for systems of linear partial differential equations, *Lie Groups Appl.*, 1994, **1**(1): 47–55.

[48] Chardin M, Differential resultants and subresultants, *Fundamentals of computation theory* (Gosen, 1991), volume 529 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 1991, 180–189.

[49] Li Z M, A subresultant theory for linear differential, linear difference and Ore polynomials, with applications, PhD thesis, Johannes Kepler University, 1996.

[50] Hong H, Ore subresultant coefficients in solutions, *Appl. Algebra Engrg. Comm. Comput.*, 2001, **12**(5): 421–428.

[51] Ritt J F, *Differential Equations from the Algebraic Standpoint*, American Mathematical Society, New York, 1932.

[52] Zwillinger D, *Handbook of Differential Equations,* Academic Press, San Diego, CA, 3rd Ed., 1998.

[53] Rueda S L and Sendra J R, Linear complete differential resultants and the implicitization of linear DPPEs, *J. Symbolic Comput.*, 2010, **45**(3): 324–341.

[54] Carrà-Ferro G, A resultant theory for the systems of two ordinary algebraic differential equations, *Appl. Algebra Engrg. Comm. Comput.*, 1997, **8**(6): 539–560.

[55] Li W, Yuan C M, and Gao X S, Sparse differential resultant for Laurent differential polynomials, *Found. Comput. Math.*, 2015, **15**(2): 451–517.

[56] Zhang Z Y, Yuan C M, and Gao X S, Matrix formulae of differential resultant for first order generic ordinary differential polynomials, *Computer Mathematics* 9*th Asian Symposium*, ASCM 2009, Fukuoka, Japan, December 14–17, 2009, 10th Asian symposium, ASCM 2012, Beijing, China, October 26–28, 2012, Contributed papers and invited talks, Springer, Berlin, 2014, 479–503.

[57] Rueda S L, Linear sparse differential resultant formulas, *Linear Algebra Appl.*, 2013, **438**(11): 4296–4321.

[58] Li W, Yuan C M, and Gao X S. Sparse difference resultant, *ISSAC* 2013 — *Proceedings of the* 38*th International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2013, 275–282.

[59] Li W, Yuan C M, and Gao X S, Sparse difference resultant, *J. Symbolic Comput.*, 2015, **68**(1): 169–203.

[60] Yuan C M and Zhang Z Y, New bounds and efficient algorithm for sparse difference resultant, arXiv: 1810.00057, 2018.

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

[62] D'Alfonso L, Jeronimo G, and Solernó P, Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients, *J. Complexity*, 2014, **30**(5): 588–603.

[63] Gustavson R, Kondratieva M, and Ovchinnikov A, New effective differential Nullstellensatz, *Adv. Math.*, 2016, **290**: 1138–1158.

[64] Ovchinnikov A, Pogudin G, and Scanlon T, Effective difference elimination and Nullstellensatz, ArXiv: 1712.01412V2, 2017.

[65] Ovchinnikov A, Pogudin G, and Vo T N, Bounds for elimination of unknowns in systems of differential-algebraic equations, ArXiv: 1610.0422v6, 2018.

[66] Yang L, Zeng Z B, and Zhang W N, Search dependency between algebraic equations: An algorithm applied to automated reasoning, *Technical Report ICTP/*91/6*, International Center For Theoretical Physics*, International Atomic Energy Agency, Miramare, Trieste, 1991.

[67] Kalkbrener M, A generalized Euclidean algorithm for computing triangular representations of algebraic varieties, *J. Symbolic Comput.*, 1993, **15**(2): 143–167.

[68] Gallo G and Mishra B, Efficient algorithms and bounds for Wu-Ritt characteristic sets, *Effective Methods in Algebraic Geometry* (Castiglioncello, 1990), volume 94 of *Progr. Math.*, Birkhäuser Boston, Boston, MA, 1991, 119–142.

[69] Wang D M, An elimination method for polynomial systems, *J. Symbolic Comput.*, 1993, **16**(2): 83–114.

[70] Wang D M, Decomposing polynomial systems into simple systems, *J. Symbolic Comput.*, 1998, **25**(3): 295–314.

[71] Wang D M, Computing triangular systems and regular systems, *J. Symbolic Comput.*, 2000, **30**(2): 221–236.

[72] Hubert E, Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems, *Symbolic and Numerical Scientific Computation* (Hagenberg, 2001), volume 2630 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2003, 1–39.

[73] Li Z M and Wang D M, Some properties of triangular sets and improvement upon algorithm charser, Eds. by Calmet J, Ida T, Wang D, *Artificial Intelligence and Symbolic Computation, Lecture Notes of Comput. Sci.*, 2006, **4120**: 82–93.

[74] Chou S C, *Mechanical Geometry Theorem Proving*, volume 41 of *Mathematics and Its Applications*, D. Reidel Publishing Co., Dordrecht, 1988.

[75] Chou S C and Gao X S, Ritt-Wu's decomposition algorithm and geometry theorem proving, 10*th International Conference on Automated Deduction* (Kaiserslautern, 1990), volume 449 of *Lecture Notes in Comput. Sci.*, 207–220, Springer, Berlin, 1990.

[76] Chen C B, Davenport J H, May J P, et al., Triangular decomposition of semi-algebraic systems, *J. Symb. Comput.*, 2013, **49**: 3–26.

[77] Chen C B, Moreno Maza M, Xia B C, et al., Computing cylindrical algebraic decomposition via triangular decomposition, *ISSAC* 2009 *— Proceedings of the* 2009 *International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2009, 95–102.

[78] Wang D M, *Elimination Methods*, Texts and Monographs in Symbolic Computation, Springer-Verlag, Vienna, 2001.

[79] Mou C Q and Bai Y, On the chordality of polynomial sets in triangular decomposition in top-down style, *ISSAC'*18 *— Proceedings of the* 2018 *ACM International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2018, 287–294.

[80] Chen C B and Moreno Maza M, Algorithms for computing triangular decompositions of polyno-

mial systems, *ISSAC 2011 — Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation*, ACM, New York, 2011, 83–90.

[81] Wang D M, On the connection between ritt characteristic sets and buchberger-gröbner bases, *Math. Comput. Sci.*, 2016, **10**(4): 479–492.

[82] Chai F J, Gao X S, and Yuan C M, A characteristic set method for solving Boolean equations and applications in cryptanalysis of stream ciphers, *J. Syst. Sci. Complex.*, 2008, **21**(2): 191–208.

[83] Li X L, Mou C Q, and Wang D M, Decomposing polynomial sets into simple sets over finite fields: The zero-dimensional case, *Comput. Math. Appl.*, 2010, **60**(11): 2983–2997.

[84] Mou C Q, Wang D M, and Li X L, Decomposing polynomial sets into simple sets over finite fields: The positive-dimensional case, *Theoret. Comput. Sci.*, 2013, **468**: 102–113.

[85] Gao X S and Huang Z Y, Characteristic set algorithms for equation solving in finite fields, *J. Symbolic Comput.*, 2012, **47**(6): 655–679.

[86] Li Z M and Wang D M, Coherent, regular and simple systems in zero decompositions of partial differential systems, *Sys. Sci. Math. Sci.*, 1999, **12**: 43–60.

[87] Hubert E, Notes on triangular sets and triangulation-decomposition algorithms. II. Differential systems, *Symbolic and Numerical Scientific Computation* (Hagenberg, 2001), volume 2630 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 2003, 40–87.

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

[89] Rosenfeld A, Specializations in differential algebra, *Trans. Amer. Math. Soc.*, 1959, **90**: 394–407.

[90] Gao X S, Huang Z, and Yuan C M, Binomial difference ideals, *J. Symbolic Comput.*, 2017, **80**(3): 665–706.

[91] Mishra B, *Algorithmic Algebra*, Springer, Boston, MA, 2001.

[92] Bentsen I, The existence of solutions of abstract partial difference polynomials, *Trans. Amer. Math. Soc.*, 1971, **158**: 373–397.

[93] Freitag J, Bertini theorems for differential algebraic geometry, ArXiv: 1211.0972v3, 2015.

[94] Li W and Li Y H, Computation of differential Chow forms for ordinary prime differential ideals, *Adv. in Appl. Math.*, 2016, **72**: 77–112.

[95] Carrà Ferro G, A resultant theory for ordinary algebraic differential equations, *Applied algebra, algebraic algorithms and error-correcting codes* (*Toulouse,* 1997), volume 1255 of *Lecture Notes in Comput. Sci.*, Springer, Berlin, 1997, 55–65.

[96] Yang L, Zeng Z B, and Zhang W N, Differential elimination with Dixon resultants, *Appl. Math. Comput.*, 2012, **218**(21): 10679–10690.

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

[98] Golubitsky O D, Kondrat'eva M V, and Ovchinnikov A I, On the generalized Ritt problem as a computational problem, *Fundam. Prikl. Mat.*, 2008, **14**(4): 109–120.