

# Mechanized Methods for Differential and Difference Equations\*

Xiaoshan Gao, Ziming Li

*Key Laboratory of Mathematics Mechanization*

*Institute of Systems Science, AMSS*

*Academia Sinica, Beijing 100080, China*

*Email: {xgao, zml} @mmrc.iss.ac.cn*

## Abstract

Some recent results on the mechanized methods for differential and difference equations are surveyed. The results include: the characteristic set method for differential and difference equation systems, algorithms for computing closed-form solutions of differential and difference equations, and algorithms for solving and factoring finite-dimensional linear functional systems.

## 1 Introduction

This paper provides a survey of some recent work on differential and difference equations by researchers at the Key Laboratory of Mathematics Mechanization and their collaborators. The work under review is greatly stimulated by Wu's method for mechanical theorem-proving in differential geometries, finding closed-form solutions of differential (difference) equations, and handling analytic and discrete mathematical objects by computers.

Differential equations describe physical laws in mechanics and geometric properties of manifolds. The characteristic set method for differential equations enables us to search for physical laws and geometric properties by computers [52]. For example, Newton's gravitational law is automatically derived from Kepler's laws [51], and "Theorema Egregium" is rediscovered by computing a characteristic set of the fundamental equations of surface theory [30].

The notion of characteristic sets for differential ideals was introduced by Ritt [42]. It plays a fundamental role in differential algebra, because

---

\*Partially supported by a National Key Basic Research Project of China (2004CB318000).

the Hilbert Basissatz does not hold for differential ideals. The notion and algorithm of characteristic sets for polynomial and differential polynomial sets were introduced by Wu [48, 50] to prove theorems in geometries and to manipulate systems of differential and algebraic equations [48, 49]. Wu's work inspired a great deal of research in the communities of symbolic computation and automated reasoning. Later on, the success of Gröbner bases for polynomial ideals led to methods to characterizing radical differential ideals [4]. The reader may consult [44] for more details on the recent developments of the differential characteristic set method. In this paper we briefly review Wu's scheme for differential characteristic sets and point out its recent extension to difference polynomial systems.

Integrals, special functions and combinatorial sequences are often considered as "infinite" objects. To specify them in terms of a finite amount of information on computers, one uses the differential (difference) equations annihilating these objects. For instances, automatic proofs of combinatorial identities need to find hypergeometric solutions of difference equations [37], while algorithms for symbolic integration need to compute elementary functions satisfying Risch's equation [7]. Great efforts have been made to compute closed-form solutions of linear ordinary differential (difference) equations (see, [26, 39] and the references therein). There are two ways to go further: one is to look for closed-form solutions of nonlinear ordinary differential (difference) equations of some kind; the other is to develop symbolic algorithms for linear partial differential (difference) equations. We will summarize recent theoretical and algorithmic results concerning this subject.

Nonlinear differential equations arise from physics. Their analytic solutions are important for the understanding of the physical phenomena. Interesting methods to search for analytic solutions of nonlinear PDEs are given in [16, 53].

Factoring polynomials helps us to solve algebraic equations. Likewise, we want to decompose differential and difference equations into those of lower orders. There have been efficient algorithms for decomposing linear ordinary differential operators [6, 24, 25, 43]. Recent work on extending these methods to linear partial differential and difference equations [33] will be surveyed. We also mention that a decomposition algorithm for nonlinear ordinary differential equations is presented in [23].

The rest of this paper is organized as follows. In Section 2, we outline the differential characteristic method. Methods for computing rational and algebraic solutions of first-order ordinary differential and difference equations are presented in Section 3. An algebraic setting and a factorization algorithm for finite-dimensional linear functional systems are described in Sections 4 and 5, respectively.

## 2 The characteristic set method

The characteristic set method plays a central role in the theory and applications of mathematics mechanization. In this section, we will introduce its main features and applications in automated reasoning.

### 2.1 Properties of ascending chains

Let  $\mathbb{K}$  be an ordinary differential field,  $\mathbb{X} = \{x_1, \dots, x_n\}$  a set of differential indeterminates, and  $\mathbb{K}\{\mathbb{X}\}$  the set of *differential polynomials* in  $\mathbb{X}$  with coefficients in  $\mathbb{K}$ . We denote  $x_{i,j}$  to be the  $j$ -derivative of  $x_i$ . The *universal field*  $\mathbb{E}$  over  $\mathbb{K}$  is a differentially closed field containing  $\mathbb{K}$  and infinitely many indeterminates. For a polynomial  $D$  and a polynomial set  $\mathbb{P} \subset \mathbb{K}\{\mathbb{X}\}$ ,

$$\text{Zero}(\mathbb{P}) = \{\eta \in \mathbb{E}^n \mid P(\eta) = 0, \forall P \in \mathbb{P}\}$$

is called a *variety*, and  $\text{Zero}(\mathbb{P}/D) = \text{Zero}(\mathbb{P}) \setminus \text{Zero}(D)$  is called a *quasi variety*.

A set  $\mathcal{A}$  of differential polynomials is called an *ascending chain* (triangular set), or simply a chain, if after renaming the indeterminates in  $\mathbb{X}$  as  $\mathbb{U} = \{u_1, \dots, u_q\}$  and  $\mathbb{Y} = \{y_1, \dots, y_p\}$ , we can write  $\mathcal{A}$  in the following form:

$$\begin{aligned} A_1(\mathbb{U}, y_1) &= I_1 y_{1,o_1}^{d_1} + \text{terms of lower orders and degrees in } y_1, \\ &\dots \\ A_p(\mathbb{U}, y_1, \dots, y_p) &= I_p y_{p,o_p}^{d_p} + \text{terms of lower orders and degrees in } y_p. \end{aligned} \tag{1}$$

As a matter of terminologies,  $o_i$  is called the order of  $A_i$ ;  $I_i$  is called the *initial* of  $A_i$ ,  $S_i = \frac{\partial A_i}{\partial y_{i,o_i}}$  is called the *separant* of  $A_i$ . Write  $\mathbf{I}_{\mathcal{A}} = \prod_i I_i S_i$ . The *dimension* of  $\mathcal{A}$  is defined to be  $|\mathbb{U}| = q$ , which is denoted  $\dim(\mathcal{A})$ . The *order* of  $\mathcal{A}$  is defined to be  $\text{ord}(\mathcal{A}) = \sum_{i=1}^p o_i$ . The *degree* of  $\mathcal{A}$  is defined to be  $\text{deg}(\mathcal{A}) = \prod_{i=1}^p d_i$ .

We could say that the formal solutions for a chain is basically determined. Intuitively, for a set of given values of the parameters  $\mathbb{U}$ , the  $y_i$  can be determined iteratively by solving univariate equations  $A_i = 0$ . In order to show the properties of chains, we first introduce several concepts. The *saturation ideal* of  $\mathcal{A}$  is defined to be

$$\text{sat}(\mathcal{A}) = \{P \in \mathbb{K}\{\mathbb{X}\} \mid \exists k \in \mathbb{N}, \mathbf{I}_{\mathcal{A}}^k P \in (\mathcal{A})\}.$$

We may define a partial ordering among the chains in a nature way [42, 52]. It is known that any set of chains contains one with lowest order. A *characteristic set* of a differential polynomial set  $\mathbb{P}$  is any chain of lowest ordering contained in  $\mathbb{P}$ .

A chain  $\mathcal{A}$  is called *irreducible* if  $A_1$  is an irreducible polynomial in  $y_{1,o_1}$  and  $A_k$  is an irreducible polynomial modulo  $A_1, \dots, A_{k-1}$ .

**Theorem 2.1.** [42, 52] *Let  $\mathcal{A}$  be an irreducible chain. Then  $\text{sat}(\mathcal{A})$  is a prime ideal of dimension  $\dim(\mathcal{A})$ , order  $\text{ord}(\mathcal{A})$  wrt  $\mathbb{U}$ , and degree  $\deg(\mathcal{A})$  wrt  $\mathbb{U}$ . Conversely, a characteristic set of a prime ideal is irreducible.*

The following result shows that the dimension, order and degree of a chain are intrinsic properties.

**Theorem 2.2.** [19, 22] *Let  $\mathcal{A}$  be a chain of form (1). If  $\text{Zero}(\text{sat}(\mathcal{A})) \neq \emptyset$ ,  $\text{Zero}(\text{sat}(\mathcal{A}))$  and  $\text{Zero}(\mathcal{A}/\mathbb{I}_{\mathcal{A}})$  are unmixed. More precisely, write  $\text{Zero}(\text{sat}(\mathcal{A}))$  as an irredundant decomposition:  $\text{Zero}(\text{sat}(\mathcal{A})) = \cup_{i=1}^r \text{Zero}(\text{sat}(\mathcal{C}_i))$ . Then*

- (1)  $\mathcal{C}_i$  is also of form (1). As a consequence,  $\dim(\text{sat}(\mathcal{C}_i)) = \dim(\mathcal{A})$  and  $\text{ord}(\mathcal{C}_i) = \text{ord}(\mathcal{A})$ .
- (2)  $\deg(\mathcal{A}) \geq \sum_{i=1}^r \deg(\mathcal{C}_i)$ . Furthermore,  $\deg(\mathcal{A}) = \sum_{i=1}^r \deg(\mathcal{C}_i)$  iff  $\mathcal{A}$  is saturated, that is, the initials and seprants of  $\mathcal{A}$  are invertible wrt  $\mathcal{A}$ .

Another important property for chains is

**Theorem 2.3.** [52] *An irreducible chain admits a formal power series solution which can be computed algorithmically.*

In order to make the paper shorter, we limit to the ordinary differential case. Similar results for the partial differential case were also established, where we need to assume that the chains are either passive [49, 52] or coherent [4, 5, 27].

Similar results are also proved in the case of algebraic difference polynomials [21, 22]. However, in the difference case, we do not have algorithms to decide whether a chain is irreducible. In order to have a constructive theory, proper irreducible chains are introduced [21]. Also, Theorem 2.2 is proved only for proper irreducible chains.

## 2.2 Characteristic set method

The characteristic set method decomposes the zero set for a differential polynomial system in general form into the union of zero sets for chains. Since the zero set of a chain is considered to be known, this method gives a general tool to deal with differential equation systems.

Let  $\mathbb{P}$  be a finite set of differential polynomials. Then we can perform the following operations:

$$\begin{aligned} \mathbb{P} &= \mathbb{P}_0 \ \mathbb{P}_1 \ \cdots \ \mathbb{P}_i \ \cdots \ \mathbb{P}_m, \\ \mathcal{B}_0 \ \mathcal{B}_1 \ \cdots \ \mathcal{B}_i \ \cdots \ \mathcal{B}_m &= \mathcal{C}, \\ \mathbb{R}_0 \ \mathbb{R}_1 \ \cdots \ \mathbb{R}_i \ \cdots \ \mathbb{R}_m &= \emptyset, \end{aligned} \quad (2)$$

where  $\mathcal{B}_i$  is a lowest chain in  $\mathbb{P}_i$  with respect to a pre-selected partial ordering;  $\mathbb{R}_i$  is the set of nonzero remainders of the polynomials in  $\mathbb{P}_i$  wrt  $\mathcal{B}_i$ ; and  $\mathbb{P}_{i+1} = \mathbb{P}_0 \cup \mathcal{B}_i \cup \mathbb{R}_i$ . In scheme (2),  $\mathcal{B}_m = \mathcal{C}$  verifies

$$\text{prem}(\mathbb{P}, \mathcal{C}) = \{0\} \text{ and } \text{Zero}(\mathbb{P}) \subset \text{Zero}(\mathcal{C}), \quad (3)$$

where  $\text{prem}$  denotes the differential pseudo-remainder. Any chain  $\mathcal{C}$  verifying the property (3) is called a *Wu characteristic set* of  $\mathbb{P}$ .

**Theorem 2.4** (Wu's Well-ordering Principle). [49, 52] *Let  $\mathcal{C}$  be a Wu characteristic set of a finite set  $\mathbb{P}$  of differential polynomials. Then:*

$$\begin{aligned} \text{Zero}(\mathbb{P}) &= \text{Zero}(\mathcal{C}/\mathbf{I}_{\mathcal{C}}) \bigcup \bigcup_i \text{Zero}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}), \\ \text{Zero}(\mathbb{P}) &= \text{Zero}(\text{sat}(\mathcal{C})) \bigcup \bigcup_i \text{Zero}(\mathbb{P} \cup \mathcal{C} \cup \{I_i\}), \end{aligned}$$

where  $I_i$  are the initials and separants of the polynomials in  $\mathcal{C}$ .

Using the well-ordering principle recursively, we obtain the following key result.

**Theorem 2.5** (Ritt-Wu's Zero Decomposition Theorem). [42, 52] *There is an algorithm which permits to determine, for a given finite set  $\mathbb{P}$  of differential polynomials, a finite set of (irreducible) chains  $\mathcal{A}_j$  such that*

$$\text{Zero}(\mathbb{P}) = \bigcup_j \text{Zero}(\mathcal{A}_j/\mathbf{I}_{\mathcal{A}_j}) = \bigcup_j \text{Zero}(\text{sat}(\mathcal{A}_j)).$$

Let  $\mathbb{P}$  be a finite subset of  $\mathbb{K}\{\mathbb{U}, \mathbb{X}\}$ , and  $D \in \mathbb{K}\{\mathbb{U}, \mathbb{X}\}$ , where  $\mathbb{U} = \{u_1, \dots, u_m\}$  and  $\mathbb{X} = \{x_1, \dots, x_n\}$ . The projection of  $\text{Zero}(\mathbb{P}/D)$  to  $\mathbb{U}$  is defined as follows:

$$\text{Proj}_{\mathbb{X}} \text{Zero}(\mathbb{P}/D) = \{e \in \mathbb{E}^m \mid \exists a \in \mathbb{E}^n \text{ s.t. } (e, a) \in \text{Zero}(\mathbb{P}/D)\}.$$

Projection for quasi-varieties can be computed with the characteristic set method.

**Theorem 2.6** (Projection Theorem). [19] *For a finite subset set  $\mathbb{P} \subset K\{\mathbb{U}, \mathbb{X}\}$  and  $D \in K\{\mathbb{U}, \mathbb{X}\}$ , we can compute chains  $\mathcal{A}_i$  and polynomials  $D_i$  in  $\mathbb{K}[\mathbb{U}]$  such that*

$$\text{Proj}_{\mathbb{X}} \text{Zero}(\mathbb{P}/D) = \bigcup_{i=1}^l \text{Zero}(\mathcal{A}_i/D_i \mathbf{I}_{\mathcal{A}_i}).$$

The concept of characteristic sets for prime ideals was introduced by Ritt [42]. The notion of characteristic sets given above, the well-ordering principle, and the current form of zero decomposition theorems were introduced by Wu [48,49,52]. An implementation of the method can be found in [46]. In order to improve the efficiency, new characteristic set methods were proposed [4, 5, 9, 10, 18, 27, 40, 45]. The characteristic set method was used to solve certain problems for analytical functions [41].

A characteristic set method for algebraic difference equation systems was proposed in [21, 22]. It is quite surprising that there are no essential progresses for the theory and algorithms of difference characteristic set methods since the early work of Ritt and his colleagues in the 1930s. In [21], an algorithm was proposed to decompose the zero set a difference polynomial system into the union of unmixed zero sets of difference polynomial systems represented by proper irreducible chains. In [22], a new resolvent theory for difference polynomial systems was proposed.

To solve a set of equations in triangular form, we need to solve univariate equations in a cascade form. The resolvent methods were introduced to reduce the solving of equation systems into the solving of one univariate equation plus a set of linear equations [13, 22].

### 2.3 Wu's method of automated geometry theorem proving and discovering

A geometry theorem is called a *theorem of equality type*, if after introducing coordinates, the theorem can be expressed in the following form

$$\forall x_i[(H_1 = 0 \wedge \cdots \wedge H_s = 0 \wedge D_1 \neq 0 \wedge \cdots \wedge D_t \neq 0) \implies (C = 0)], \quad (4)$$

where  $H_i, D_i, C$  are in  $\mathbb{K}\{\mathbb{X}\}$ .

For theorems of equality type, we have the following principles of mechanical theorem proving, which are consequences of Theorems 2.1 and 2.4.

**Theorem 2.7.** [49] *For a geometry statement of form (4), let  $\mathcal{A}$  be a Wu-characteristic set of  $\{H_1, \dots, H_s\}$ . If  $\text{prem}(C, \mathcal{A}) = 0$ , then the statement is valid under the non-degenerate condition  $\mathbf{I}_{\mathcal{A}} \neq 0$ .*

Note that the non-degenerate condition  $\mathbf{I}_{\mathcal{A}} \neq 0$  is generated automatically by the algorithm.

**Theorem 2.8.** [52] *Let  $D = \prod_i D_i$ . By Theorem 2.5, we have*

$$\text{Zero}(\{H_1, \dots, H_s\}/D) = \cup_{i=1}^l \text{Zero}(\text{sat}(\mathcal{A}_i)/D).$$

*If  $\text{prem}(C, \mathcal{A}_i) = 0, i = 1, \dots, l$ , then the statement is true. If  $\mathcal{A}_i$  is irreducible and  $\text{prem}(C, \mathcal{A}_i) \neq 0$ , then the statement is not valid on  $\text{Zero}(\text{sat}(\mathcal{A}_i)/D)$ .*

As an example, let us show how to prove Newton's gravitational law with Kepler's laws. The first and second Kepler laws state that each planet describes an ellipse with the sun in one focus and the radius vector drawn from the sun to a planet sweeps out equal areas in equal times. The Newton's law states that the acceleration is reversely proportional to the distance from the planet to the sun. We may use differential equations  $K_1 = 0, K_2 = 0$ , and  $N_1 = (ar^2)' = 0$  to represent these laws:

$$\begin{aligned} h_1 &= r^2 - x^2 - y^2 = 0, \\ h_2 &= a^2 - x'^2 - y'^2 = 0, \\ K_1 &= r - p - ex = 0 \wedge p' = 0 \wedge e' = 0, \\ K_2 &= y'x - yx' - h = 0 \wedge h' = 0, \\ d_1 &= p \neq 0 \quad (\text{The ellipse is not a line.}) \end{aligned}$$

Then, we need to show

$$\forall x, y, p, e, a, r [(K_1 = 0 \wedge K_2 = 0 \wedge h_1 = 0 \wedge h_2 = 0 \wedge d_1 \neq 0) \Rightarrow N_1 = 0].$$

By Theorem 2.5 ( $p < e < x < y < r < a$ ),

$$\text{Zero}(\{K_1, p', e', h_1, h_2, n_2\}/p) = \text{Zero}(\text{sat}(\mathcal{A}_1)p),$$

where  $\mathcal{A}_1$  is a chain. By computation, we have  $\text{prem}(n_1, ASC_1) = 0$ , which proves Newton's law.

There are two kinds of problems in differential geometry other than theorem proving. One is finding locus equations, the other is deriving geometry formulas. For a geometric configuration given by a set of polynomial equations  $h_1(\mathbb{U}, x_1, \dots, x_p) = 0, \dots, h_r(\mathbb{U}, x_1, \dots, x_p) = 0$ , we want to find a relation between arbitrarily chosen variables  $\mathbb{U}$  (parameters) and a dependent variable, say,  $x_1$ . Wu pointed out that the characteristic set method can be used to discover such unknown geometric formulas [51]. Actually, Newton's law can be deduced from Kepler's laws automatically in this way. More detailed accounts can be found in [10, 11, 30, 45].

The characteristic set method can be used to prove a much wider class of geometry theorems. Let  $\mathbb{E}$  be a differentially closed extension of  $\mathbb{K}$ , say, the field of meromorphic functions [42]. A *first order formula* over  $\mathbb{E}$  can be defined as follows.

1. If  $P \in \mathbb{K}[\mathbb{X}]$ , then  $P(\mathbb{X}) = 0$  is a formula.
2. If  $f, g$  are formulas, then  $\neg f$ ,  $f \wedge g$ , and  $f \vee g$  are formulas.
3. If  $f$  is a formula, then  $\exists x_i \in \mathbb{E}(f)$  and  $\forall x_i \in \mathbb{E}(f)$  are formulas.

A formula can always be written as a prefix canonical form

$$\phi = Q_1 y_1 \dots Q_m y_m \psi(u_1, \dots, u_d, y_1, \dots, y_m), \quad (5)$$

where  $Q_k$  is a quantifier  $\exists$  or  $\forall$  and  $\psi$  a formula free of quantifiers. For a first order formula  $\phi$  of form (5), there exists a fundamental problem:

**Quantifier Elimination:** Find a formula  $\theta(u_1, \dots, u_d)$  such that  $\theta$  is equivalent to  $\phi$ . If  $d = 0$ , we need to decide whether  $\phi$  is valid or not.

As a consequence of Theorem 2.6, we have

**Theorem 2.9.** *There exists a decision procedure for the first order theory over a differentially closed field.*

### 3 Rational and algebraic solutions of ODEs and OΔEs

For brevity we abbreviate ordinary difference equations as OΔE.

By decomposing the zero set of a differential polynomial system into the zero sets of chains, the characteristic set method gives a complete way to describe the structure for the zero sets of equation systems. In particular, finding the solutions of differential polynomial systems can be reduced to finding those of a single differential equation or a system of equations in a single variable.

Closed-form solutions of linear ODEs and OΔEs were widely studied. On the other hand, similar results to nonlinear ODEs are very limited. In this section, we summarize some recent results on finding rational and algebraic solutions to nonlinear ODEs and OΔEs. It is interesting to see whether these results can be treated uniformly with the differential Galois theory [35].

#### 3.1 Rational and algebraic solutions of algebraic ODEs

Let  $P \in \mathbb{K}\{y\} \setminus \mathbb{K}$  be an irreducible differential polynomial in an indeterminate  $y$  and

$$\Sigma_P = \{A \in \mathbb{K}\{y\} \mid SA \equiv 0 \pmod{\{P\}}\},$$

where  $S$  is the separant of  $P$  and  $\{P\}$  is the radical differential ideal generated by  $P$ . Then  $\Sigma_P$  is a prime ideal [42]. A generic zero of  $\Sigma_P$  is defined to be a *general solution* of  $P = 0$ . In particular, an *algebraic general solution* of  $P = 0$  is a general solution  $\hat{y}$  which satisfies the following equation

$$G(x, y) = \sum_{i=0}^n a_i(x)y^i = 0, \quad (6)$$

where  $a_i$  is a polynomial in  $x$  with degree  $\alpha_i$  and with constant coefficients, and  $G(x, y)$  is an irreducible polynomial in  $x, y$ . When  $n = 1$ ,  $\hat{y}$  is called a *rational general solution* of  $P = 0$ .

For  $\alpha_0, \alpha_1, \dots, \alpha_n \in \mathbb{Z}_{\geq 0}$ , we define the differential polynomial

$$\mathbb{D}_{(\alpha_0; \alpha_1, \dots, \alpha_n)} := \det(\mathcal{A}_{(h, \alpha_1; \alpha_0)}(y) | \mathcal{A}_{(h, \alpha_2; \alpha_0)}(y^2) | \dots | \mathcal{A}_{(h, \alpha_n; \alpha_0)}(y^n)),$$

where

$$\mathcal{A}_{(h, \alpha; k)}(y) := \begin{pmatrix} \binom{k+1}{0} y_{k+1} & \binom{k+1}{1} y_k & \dots & \binom{k+1}{\alpha} y_{k+1-\alpha} \\ \binom{k+2}{0} y_{k+2} & \binom{k+2}{1} y_{k+1} & \dots & \binom{k+2}{\alpha} y_{k+2-\alpha} \\ \vdots & \vdots & \dots & \vdots \\ \binom{k+h+1}{0} y_{k+h+1} & \binom{k+h+1}{1} y_{k+h} & \dots & \binom{k+h+1}{\alpha} y_{k+h+1-\alpha} \end{pmatrix}.$$

We have

**Lemma 3.1.** [1]  $y(x)$  satisfies an equation of the type (6) if and only if  $\mathbb{D}_{(\alpha_0; \alpha_1, \dots, \alpha_n)}(y(x)) = 0$ . As a consequence, we give a defining differential equation for algebraic functions.

When  $n = 2, \alpha_1 = \alpha_2 = 1$  and  $\alpha_0 = 2$ ,

$$\mathbb{D}_{(2; 1, 1)} = \begin{vmatrix} y_3 & 3y_2 & (y^2)''' & 3(y^2)'' \\ y_4 & 4y_3 & (y^2)^{(4)} & 4(y^2)''' \\ y_5 & 5y_4 & (y^2)^{(5)} & 5(y^2)^{(4)} \\ y_6 & 6y_5 & (y^2)^{(6)} & 6(y^2)^{(5)} \end{vmatrix}.$$

We have  $\mathbb{D}_{(2; 1, 1)}(y(x)) = 0$  if and only if

$$(a_{2,1}x + a_{2,0})y^2(x) + (a_{1,1}x + a_{1,0})y(x) + a_{0,2}x^2 + a_{0,1}x + a_{0,0} = 0$$

for constants  $a_{i,j}$ .

The key to find a rational and algebraic function solutions is to give a degree bound for the solution. We can give these degree bounds for first order autonomous ODEs. In what follows, let  $F(y, y_1) = 0$  be a first order autonomous ODE. Then we have

**Theorem 3.2.** [1] If  $G(x, y) = 0$  defines a nontrivial algebraic solution of  $F = 0$ , then

- (1)  $\deg(G(x, y), x) = \deg(F, y_1)$ ,
- (2)  $\deg(G(x, y), y) \leq \deg(F, y) + \deg(F, y_1)$ .

The following example shows that the bound in (2) is optimal. Let  $n > m > 0$  and  $(n, m) = 1$ . Then  $G = y^n - x^m$  is irreducible.  $y^n - x^m = 0$  is an algebraic solution of  $F = y^{n-m}y_1^m - (m/n)^m = 0$ . Here,  $\deg(G(x, y), y) = \deg(F, y) + \deg(F, y_1)$ .

For rational solutions, we could give the exact degree bound [17].

**Theorem 3.3.** *If  $y = P(x)/Q(x)$  is a rational solution of  $F(y, y_1) = 0$ , then  $\deg(y(x)) = \deg(F, y_1)$ .*

These degree bounds are obtained by treating  $F(y, y_1) = 0$  as an algebraic curve and the solution as a parametrization of the curve. This idea also leads to the following algorithm to find a rational solution to a first order autonomous ODE [17].

**Theorem 3.4.** *Let  $y = r(x), y_1 = s(x)$  be a proper rational parametrization of  $F(y, y_1) = 0$ , where  $r(x), s(x)$  are rational functions in  $x$  with constant coefficients. Then  $F = 0$  has a rational general solution iff we have the following relations*

$$ar(x)' = s(x) \quad \text{or} \quad a(x-b)^2r(x)' = s(x),$$

where  $a, b$  are constants and  $a \neq 0$ . If one of the above relations is true, then replacing  $x$  by  $a(x+c)$  (or  $b - \frac{1}{a(x+c)}$ ) in  $y = r(x)$ , we obtain a rational general solution of  $F = 0$ , where  $c$  is an arbitrary constant.

The above algorithm depends on the rational parametrization of algebraic curves. A more efficient algorithm is based on Hermite-Padé approximation.

Let  $A(x)$  be a formal power series. If a polynomial  $G(x, y)$  satisfies

$$G(x, A(x)) = O\left(x^{(n+1)(m+1)+1}\right),$$

where  $m = \deg(G, x), n = \deg(G, y)$ , then we call  $G(x, y) = 0$  Hermite-Padé approximant to  $A(x)$ . We could find the algebraic solution for an first order autonomous ODEs as follows [1].

- (1) Find the first  $N$  terms  $f(x)$  of formal power series solution of  $F(y, y_1) = 0$ , where

$$N = 2(\deg(F, y) + \deg(F, y_1)).$$

- (2) Let  $d = \deg(F, y_1)$ . Construct the  $(d, d, \dots, d)$  Hermite-Padé approximant  $G(x, y) = 0$  to  $f(x)$ .
- (3) We need only to check whether  $G = 0$  is a nontrivial algebraic solution of  $F = 0$ .

The complexity of this algorithm is polynomial in terms of the number of the multiplications in the number field.

## 3.2 Rational solutions of algebraic OΔEs

The result about rational solutions of ODEs can be extended to OΔEs. Let  $\mathbb{K} = \mathbb{Q}(x)$  be the difference field with the difference operator  $\mathbf{E}(x) = x + 1$ ,  $y$  an indeterminate, and  $y_n = \mathbf{E}^n y$ .

Let  $P \in \mathbb{K}\{y\} \setminus \mathbb{K}$  be an irreducible difference polynomial in  $y$ , and

$$\Sigma_P = \{A \in \mathbb{Q}(x)\{y\} \mid SA \equiv 0 \pmod{\{P\}}\},$$

where  $S$  is the separant of  $P$ . Cohn proved that  $\Sigma_P$  is a perfect difference ideal and it could be decomposed into the intersection of the principle components of  $P$  [14]. Let  $\Lambda$  be one of the principle components of  $P$ . A general solution of  $P = 0$  is defined as a generic zero of one of the principle components of  $\Sigma_P$ . A *rational general solution* of  $P(y) = 0$  is defined as a general solution of  $P = 0$  with the following form:

$$\hat{y}(x) = \frac{a_n x^n + a_{n-1} x^{n-1} + \dots + a_0}{x^m + b_{m-1} x^{m-1} + \dots + b_0}, \quad (7)$$

where  $a_i, b_j$  are constants. In particular, if  $m = 0$ , we call  $\hat{y}(x)$  polynomial general solution. For instance, the difference equation  $(y - y_1)^2 - 2(y + y_1) + 1 = 0$  has two general solutions:  $y(x) = (x + c)^2$  and  $y(x) = (ce^{i\pi x} + \frac{1}{2})^2$  where  $c$  is an arbitrary constant.

The defining difference equations for polynomial and rational functions are given by the following lemmas [20].

**Lemma 3.5.** *Let  $\mathcal{P}_n = \sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} y_i$ . Then  $y(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  ( $\mathbf{E}(a_i) = a_i$ ) if and only if  $\mathcal{P}_n(y(x)) = 0$ .*

Let

$$\mathcal{R}_{n,m} = \det\left(\sum_{i=0}^{n+1} (-1)^i \binom{n+1}{i} Y_i * M_i\right),$$

where  $Y_i = \text{diag}(y_i, y_{i+1}, \dots, y_{m+i})$ ,  $M_i = (H_{k,l}(i))_{(m+1) \times (m+1)}$ ,

$$H_{k,l}(i) = \frac{(i+k-n)(i+k-n-1) \dots (i+k-n-l)(i+k-n-l-2) \dots (i+k-n-m)}{(-1)^{m-l} (m+1-l)! (l-1)!}.$$

**Lemma 3.6.**  $y(x) = \frac{a_n x^n + a_{n-1} x^{n-1} + \dots + a_0}{b_m x^m + b_{m-1} x^{m-1} + \dots + b_0} \Leftrightarrow \mathcal{R}_{n,m}(y(x)) = 0$  where  $\mathbf{E}(a_i) = a_i$ ,  $\mathbf{E}(b_j) = b_j$ .

Using properties of the proper parametrization of algebraic curves, the degree bound for the rational solution can be given [20].

**Theorem 3.7.** *Let  $F(y, y_1) = 0$  be a first order autonomous OΔE. If  $y(x) \in \mathbb{Q}(x) \setminus \mathbb{Q}$  is a rational solution of  $F = 0$ , then  $\deg(y(x)) = \deg(F, y_1) = \deg(F, y)$ .*

Similar to the differential case, the rational solutions can be found with the help of rational parametrization of algebraic curves [20].

**Theorem 3.8.** *Let  $y = r(t), y_1 = s(t)$  be a proper parametrization of  $F(y, y_1) = 0$ . Then  $F = 0$  has a nontrivial rational solution iff  $r(t), s(t)$  satisfy one of the following relations:*

- (1) *There exists a nonzero  $a \in \mathcal{C}$  such that  $r(\frac{t+1}{a}) = s(\frac{t}{a})$ .*
- (2) *There exist  $a \neq 0, b \in \mathcal{C}$  such that  $r(\frac{a}{t+1} - b) = s(\frac{a}{t} - b)$ .*

It is obvious that if (1) is true,  $\bar{y}(x) = r(\frac{x+c}{a})$  is a rational general solution of  $F = 0$  where  $c$  is an arbitrary constant. If (2) is true,  $\bar{y}(x) = r(\frac{a}{x+c} - b)$  is a rational general solution of  $F = 0$  where  $c$  is an arbitrary constant.

## 4 Finite-dimensional partial linear functional systems

A finite-dimensional partial linear functional system consists of linear partial differential, shift, and  $q$ -shift operators, or any mixture thereof, and has a finite-dimensional solution space. The following is an example:

$$\begin{cases} P''(x, k) - \frac{2x}{1-x^2}P'(x, k) + \frac{k(k+1)}{1-x^2}P(x, k) = 0, \\ P(x, k+2) - \frac{(2k+3)x}{k+2}P(x, k+1) + \frac{k+1}{k+2}P(x, k) = 0. \end{cases} \quad (8)$$

The sequence of the Legendre polynomials  $\{P(x, k)\}_{k=1}^{\infty}$  is a solution of (8) with the initial conditions  $\{P(0, 0) = 0, P'(0, 0) = 0, P(0, 1) = 0, P'(0, 1) = 1\}$ .

For brevity, finite-dimensional linear functional systems will be called  $\partial$ -finite systems in the sequel. They are also called over-determined systems in the literature.  $\partial$ -finite systems arise from symmetry analysis of nonlinear ordinary differential equations, theory of special functions, and combinatorics.

In this section we review a purely algebraic setting for  $\partial$ -finite systems, including modules of formal solutions and Picard-Vessiot extensions. The former captures the notion of  $\partial$ -finiteness, and makes it possible to compute the dimension of the solution space of a  $\partial$ -finite system; while the latter contains “all” solutions of a  $\partial$ -finite system, and paves a way to introduce Galois groups.

### 4.1 An algebraic setting

Let  $R$  be a ring and  $\Delta$  be a finite set of commuting maps from  $R$  to itself. A map in  $\Delta$  is assumed to be either a derivation or an automorphism. Recall that a derivation  $\delta$  is an additive map satisfying the multiplicative

rule  $\delta(ab) = a\delta(b) + \delta(a)b$  for all  $a, b \in R$ . The pair  $(R, \Delta)$  is called a  $\Delta$ -ring, and it is a  $\Delta$ -field when  $R$  is a field.

For a derivation  $\delta \in \Delta$ , an element  $c$  of  $R$  is called a *constant* with respect to  $\delta$  if  $\delta(c) = 0$ . For an automorphism  $\sigma \in \Delta$ ,  $c$  is called a *constant* with respect to  $\sigma$  if  $\sigma(c) = c$ . An element  $c$  of  $R$  is called a *constant* if it is a constant with respect to all maps in  $\Delta$ . The set of constants of  $R$ , denoted by  $C_R$ , is a subring. The ring  $C_R$  is a subfield if  $R$  is a field.

Let  $(F, \Delta)$  be a  $\Delta$ -field. By reordering the indices, we can always assume that

$$\Delta = \{\delta_1, \dots, \delta_\ell, \sigma_{\ell+1}, \dots, \sigma_m\}$$

for some  $\ell \geq 0$ , where the  $\delta_i$ 's are derivation operators on  $F$  and the  $\sigma_j$ 's are automorphisms of  $F$ . The *Ore algebra* ([12]) over  $F$  is the polynomial ring  $\mathcal{S} := F[\partial_1, \dots, \partial_m]$  in  $\partial_i$  with the usual addition and a multiplication as follows:

$$\partial_i \partial_j = \partial_j \partial_i, \quad \partial_s a = a \partial_s + \delta_s(a), \quad \partial_t a = \sigma_t(a) \partial_t,$$

for any  $1 \leq i, j \leq m$ ,  $1 \leq s \leq \ell$ ,  $\ell < t \leq m$  and  $a \in F$ .

Remark that  $\partial_i(a)$ , where  $a$  is an element of a  $\Delta$ -ring, is meant to be  $\delta_i(a)$  if  $\partial_i$  is associated to a derivation operator  $\delta_i$ , and to be  $\sigma_i(a)$  if  $\partial_i$  is associated to an automorphism  $\sigma_i$ ; while  $\partial_i a$ , where  $a$  is an element of the Ore algebra  $\mathcal{S}$ , means the product of  $\partial_i$  and  $a$ .

**Definition 4.1.** *Let  $(F, \Delta)$  be a  $\Delta$ -field. A linear functional system over  $F$  is a system of the form  $A(\mathbf{z}) = 0$  where  $A$  is a  $p \times q$  matrix with entries in the Ore algebra  $\mathcal{S}$  and  $\mathbf{z}$  is a column vector of  $q$  unknowns.*

**Example 4.2.** *The system (8), satisfied by the Legendre polynomials, can be rewritten as  $A(z) = 0$  where*

$$A = \left( \partial_x^2 - \frac{2x}{1-x^2} \partial_x + \frac{k(k+1)}{1-x^2}, \partial_k^2 - \frac{(2k+3)x}{k+2} \partial_k + \frac{k+1}{k+2} \right)^\tau,$$

with  $\partial_x$  the differentiation with respect to  $x$  and  $\partial_k$  the shift operator with respect to  $k$ .

Let  $F$  be a  $\Delta$ -field. A commutative ring  $R$  containing  $F$  is called a  $\Delta$ -extension of  $F$  if all the maps in  $\Delta$  can be extended to  $R$  in such a way that all derivations (resp. automorphisms) of  $F$  become derivations (resp. automorphisms) of  $R$  and the extended maps commute pairwise.

By a solution of a linear functional system  $A(\mathbf{z}) = 0$  over  $F$ , we mean a vector  $(s_1, \dots, s_q)^\tau$  over some  $\Delta$ -extension of  $F$  such that  $A(s_1, \dots, s_q)^\tau = 0$ , i.e., the application of the matrix  $A$  to the vector is zero.

## 4.2 Modules of formal solutions

Let  $F$  be a  $\Delta$ -field and  $\mathcal{S} = F[\partial_1, \dots, \partial_m]$  be the corresponding Ore algebra. In the differential case, an  $\mathcal{S}$ -module is classically associated to a linear functional system [34, 39]. In the difference case, however,  $\mathcal{S}$ -modules may not have appropriate dimensions, as illustrated by the following counterexample.

**Example 4.3.** *Let  $\sigma \neq 1$  be an automorphism of  $F$  and  $\mathcal{S} = F[\partial]$  be the corresponding Ore algebra. The equation  $\partial(y) = 0$  cannot have a fundamental matrix  $(u)$  in any difference ring extension of  $F$ , for otherwise,  $0 = \partial(u) = \sigma(u)$ , thus  $u = 0$ . Therefore  $\partial(y) = 0$  has only trivial solution. However, the  $\mathcal{S}$ -module  $\mathcal{S}/\mathcal{S}\partial$  has dimension one as an  $F$ -vector space.*

In [38, page 56], modules over Laurent algebras are used instead to avoid the above problem. It is therefore natural to introduce the following extension of  $\mathcal{S}$ : let  $\theta_{\ell+1}, \dots, \theta_m$  be indeterminates independent of the  $\partial_i$ . Since the  $\sigma_j^{-1}$  are automorphisms of  $F$ ,  $\overline{\mathcal{S}} = F[\partial_1, \dots, \partial_m, \theta_{\ell+1}, \dots, \theta_m]$  is also an Ore algebra in which the  $\theta_j$  are associated to the  $\sigma_j^{-1}$ . Note that  $\partial_j\theta_j$  is in the center of  $\overline{\mathcal{S}}$ , since

$$(\partial_j\theta_j)a = \partial_j\sigma_j^{-1}(a)\theta_j = \sigma_j(\sigma_j^{-1}(a))\partial_j\theta_j = a\partial_j\theta_j, \text{ for all } a \in F \text{ and } j > \ell.$$

Therefore the left ideal  $T = \sum_{j=\ell+1}^m \overline{\mathcal{S}}(\partial_j\theta_j - 1)$  is a two-sided ideal of  $\overline{\mathcal{S}}$ , and we call the factor ring  $\mathcal{L} = \overline{\mathcal{S}}/T$  the *Laurent-Ore algebra* over  $F$ . Writing  $\partial_j^{-1}$  for the image of  $\theta_j$  in  $\mathcal{L}$ , we can write  $\mathcal{L}$  (by convention) as  $\mathcal{L} = F[\partial_1, \dots, \partial_m, \partial_{\ell+1}^{-1}, \dots, \partial_m^{-1}]$  and view it as an extension of  $\mathcal{S}$ . For linear ordinary difference equations,  $\mathcal{L} = F[\sigma, \sigma^{-1}]$  is the algebra used in [38]. For linear partial difference equations with constant coefficients,  $\mathcal{L}$  is the Laurent polynomial ring used in [36, 54].

When revisiting Example 4.3 with Laurent-Ore algebras, we get that the left ideal generated by  $\partial$  in  $\mathcal{L} = F[\partial, \partial^{-1}]$  is  $\mathcal{L}$ , therefore the dimension of  $\mathcal{L}/(\mathcal{L}\partial)$  over  $F$ , which is zero, equals that of the solution space of  $\partial(y) = 0$  in any difference ring extension.

Let  $F$  be a  $\Delta$ -field, and  $\mathcal{S}$  and  $\mathcal{L}$  be the corresponding Ore and Laurent-Ore algebras. We have the following theorem.

**Theorem 4.4.** *Let  $A \in \mathcal{S}^{p \times q}$  and  $M = \text{coker}_{\mathcal{L}}(A)$ . Then  $\text{sol}_N(A(\mathbf{z})=0)$  and  $\text{Hom}_{\mathcal{L}}(M, N)$  are isomorphic as  $C_F$ -vector spaces for any  $\mathcal{L}$ -module  $N$ .*

The proof of Theorem 4.4 reveals that the vector  $\mathbf{e} := (\mathbf{e}_1, \dots, \mathbf{e}_q)^T \in M^q$  specified above is a “generic” solution of the system  $A(\mathbf{z}) = 0$  in the sense that any solution  $(s_1, \dots, s_q)^T$  of that system in  $N$  is the image of  $\mathbf{e}$  under the map in  $\text{Hom}_R(M, N)$  sending  $\mathbf{e}_i$  to  $s_i$ . Thus  $\text{coker}_{\mathcal{L}}(A)$  describes the properties of all the solutions of  $A(\mathbf{z}) = 0$  “anywhere”. This motivates us to define

**Definition 4.5.** Let  $A \in S^{p \times q}$ . The  $\mathcal{L}$ -module  $M = \mathcal{L}^{1 \times q} / (\mathcal{L}^{1 \times p} A)$  is called the module of formal solutions of the system  $A(\mathbf{z}) = 0$ . The dimension of  $M$  as an  $F$ -vector space is called the linear dimension of the system. The system is said to be of finite linear dimension, or simply,  $\partial$ -finite, if  $0 < \dim_F M < +\infty$ .

Note that we choose to exclude systems with  $\dim_F M = 0$  in the above definition since such system has only trivial solution in any  $\mathcal{L}$ -module, particularly, in any  $\Delta$ -extension of  $F$ .

One can compute the dimension of a module of formal solution by Gröbner bases in Laurent-Ore algebra (see [47, 55]).

### 4.3 Picard-Vessiot extensions

A  $\partial$ -finite system can be reduced to a normal form defined below:

**Definition 4.6.** A system of the form

$$\delta_i(\mathbf{z}) = A_i \mathbf{z}, \quad 1 \leq i \leq \ell, \quad \sigma_i(\mathbf{z}) = A_i \mathbf{z}, \quad \ell + 1 \leq i \leq m, \quad (9)$$

where  $A_i \in F^{n \times n}$  and  $\mathbf{z}$  is a column vector of  $n$  unknowns, is called an integrable system of size  $n$  over  $F$  if the following compatibility conditions are satisfied:

$$\begin{aligned} \delta_i(A_j) &= \delta_j(A_i), & 1 \leq i < j \leq \ell, \\ \sigma_i(A_j)A_i &= \sigma_j(A_i)A_j, & \ell < i < j \leq m, \\ \sigma_j(A_i)A_j &= A_i A_j + \delta_i(A_j), & 1 \leq i \leq \ell < j \leq m. \end{aligned} \quad (10)$$

The integrable system (9) is said to be fully integrable if the matrices  $A_{\ell+1}, \dots, A_m$  are invertible.

Using Ore algebra notation, we write  $\{\partial_i(\mathbf{z}) = A_i \mathbf{z}\}_{1 \leq i \leq m}$  for the system (9) where the action of  $\partial_i$  is again meant to be  $\delta_i$  for  $i \leq \ell$  and to be  $\sigma_i$  for  $i > \ell$ . Observe that the conditions (10) are derived from the condition  $\partial_i(\partial_j(\mathbf{z})) = \partial_j(\partial_i(\mathbf{z}))$  and are exactly the matrix-analogues of the compatibility conditions for first-order scalar equations in [28]. For a linear ordinary difference equation, we often assume that its trailing coefficient is nonzero, while, for a first-order matrix difference equation, we assume that its matrix is invertible. These assumptions lead to the condition on invertibility of  $A_{\ell+1}, \dots, A_m$  in Definition 3.1.

**Example 4.7.** Let  $F = \mathbb{C}(x, k)$ ,  $\delta_x$  be the differentiation with respect to  $x$  and  $\sigma_k$  the shift operator with respect to  $k$ . Then  $\mathcal{A} : \{\delta_x(\mathbf{z}) = A_x \mathbf{z}, \sigma_k(\mathbf{z}) = A_k \mathbf{z}\}$  is a fully integrable system where

$$A_x = \begin{pmatrix} \frac{x^2 - kx - k}{x(x-k)(x-1)} & \frac{x^2 - kx + 3k - 2x}{kx(x-k)(x-1)} \\ \frac{k(kx + x - x^2 - 2k)}{(x-k)(x-1)} & \frac{x^3 + x^2 - kx^2 - 2x + 2k}{x(x-k)(x-1)} \end{pmatrix}$$

and

$$A_k = \begin{pmatrix} \frac{k+1+kx^2-xk^2-x}{(x-k)(x-1)} & -\frac{k+1+kx-k^2-x}{k(x-k)(x-1)} \\ \frac{x(k+1)(k+1+kx-k^2-x)}{(x-k)(x-1)} & \frac{(k+1)(x^2-2kx-x+k^2)}{k(x-k)(x-1)} \end{pmatrix}.$$

We will first define the notion of Picard-Vessiot extensions of fully integrable systems, and then generalize it to  $\partial$ -finite systems. Recall that a square matrix with entries in a commutative ring is said to be *invertible* if its determinant is a unit in that ring.

Let  $F$  be a  $\Delta$ -field and  $\{\partial_i(\mathbf{z}) = A_i\mathbf{z}\}_{1 \leq i \leq m}$  be a fully integrable system of size  $n$  over  $F$ . We define

**Definition 4.8.** *An  $n \times n$  matrix  $U$  with entries in a  $\Delta$ -extension of  $F$  is a fundamental matrix for the system  $\{\partial_i(\mathbf{z}) = A_i\mathbf{z}\}_{1 \leq i \leq m}$  if  $U$  is invertible and  $\partial_i(U) = A_iU$  for each  $i$ , i.e., each column of  $U$  is a solution of the system.*

A two-sided ideal  $I$  of a commutative  $\Delta$ -ring  $R$  is said to be *invariant* if  $\delta_i(I) \subset I$  for  $i \leq \ell$  and  $\sigma_j(I) \subset I$  for  $j > \ell$ . The ring  $R$  is said to be *simple* if its only invariant ideals are  $(0)$  and  $R$ .

**Definition 4.9.** *A Picard-Vessiot ring for a fully integrable system is a ring  $E$  such that:*

- (i)  *$E$  is a simple  $\Delta$ -extension of  $F$ .*
- (ii) *There exists some fundamental matrix  $U$  with entries in  $E$  for the system such that  $E$  is generated by the entries of  $U$  and  $\det(U)^{-1}$  over  $F$ .*

Definitions 4.8 and 4.9 are natural generalizations of their analogues in the purely differential case [39, (pages 12, 415)] and the ordinary difference case [38, (Errata)].

The existence of fundamental matrices and Picard-Vessiot extensions for fully integrable systems is stated in the following [8].

**Theorem 4.10.** *Every fully integrable system over  $F$  has a Picard-Vessiot ring  $E$ . If  $F$  has characteristic 0 and  $C_F$  is algebraically closed, then  $C_E = C_F$ . Furthermore, that extension is minimal, meaning that no proper subring of  $E$  satisfies both conditions in Definition 4.9.*

Consequently, if  $F$  has characteristic zero and an algebraically closed field of constants, then all the solutions of a fully integrable system in its Picard-Vessiot ring form a  $C_F$ -vector space whose dimension equals the size of the system.

**Example 4.11.** Consider the system  $\mathcal{A}$  in Example 4.7. Note that the change of variable<sup>①</sup>  $\mathbf{z} = M\mathbf{y}$  where

$$M = \begin{pmatrix} \frac{x-k}{x} & x^2 \\ (x-k)k & x^2k \end{pmatrix},$$

transforms  $\mathcal{A}$  into another Fsystem  $\mathcal{B} : \{\delta_x(\mathbf{y}) = B_x\mathbf{y}, \sigma_k(\mathbf{y}) = B_k\mathbf{y}\}$  with  $B_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$  and  $B_k = \begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix}$ . It suffices to find a Picard-Vessiot ring of  $\mathcal{B}$ . We get that  $V = \begin{pmatrix} e^x & 0 \\ 0 & \Gamma(k) \end{pmatrix}$  is a fundamental matrix for  $\mathcal{B}$ , and thus  $MV$  is for  $\mathcal{A}$ . Moreover,  $F[e^x, \Gamma(k), e^{-x}, \Gamma(k)^{-1}]$  is a Picard-Vessiot extension for  $\mathcal{A}$ .

Let  $A(\mathbf{z}) = 0$  with  $A \in S^{p \times q}$  be a system of linear dimension  $n$  and  $M$  be its module of formal solutions with an  $F$ -basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ . Suppose that  $\partial_i(\mathbf{b}_1, \dots, \mathbf{b}_n)^\tau = B_i(\mathbf{b}_1, \dots, \mathbf{b}_n)^\tau$  where  $B_i \in F^{n \times n}$  for  $1 \leq i \leq m$ . By a straightforward verification,  $\{\partial_i(\mathbf{x}) = B_i\mathbf{x}\}_{1 \leq i \leq m}$  is a fully integrable system, which is called the *integrable connection* of  $A(\mathbf{z}) = 0$  with respect to the basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  of  $M$ .  $\partial$ -finite and fully integrable systems are connected by the next proposition whose proof is given in [8, Proposition 2] and [47, Proposition 2.4.12].

**Proposition 4.12.** Let  $A, \mathbf{b}_1, \dots, \mathbf{b}_n, B_1, \dots, B_m$  be as above, and  $B$  be the stacking of the blocks  $(\partial_i \cdot \mathbf{1}_n - B_i)$ . Then

- (i)  $\text{coker}_{\mathcal{L}}(A) \cong_{\mathcal{L}} \text{coker}_{\mathcal{L}}(B)$ .
- (ii) Let  $\{\mathbf{e}_1, \dots, \mathbf{e}_q\}$  be the set of  $\mathcal{L}$ -generators of  $M$  satisfying  $A(\mathbf{e}_1, \dots, \mathbf{e}_q)^\tau = 0$  and  $P \in F^{q \times n}$  be given by  $(\mathbf{e}_1, \dots, \mathbf{e}_q)^\tau = P(\mathbf{b}_1, \dots, \mathbf{b}_n)^\tau$ . Then, for any  $\Delta$ -extension  $E$  of  $F$ , the correspondence  $\xi \mapsto P\xi$  is an isomorphism of  $C_E$ -modules between  $\text{sol}_E(\{\partial_i(\mathbf{x}) = B_i\mathbf{x}\}_{1 \leq i \leq m})$  and  $\text{sol}_E(A(\mathbf{z}) = 0)$ .

Remark that the inverse of the correspondence in Proposition 4.3 (ii) is given by  $\eta \mapsto Q\eta$ , where  $Q$  is a matrix in  $\mathcal{L}^{n \times q}$  such that  $(\mathbf{b}_1, \dots, \mathbf{b}_n)^\tau = Q(\mathbf{e}_1, \dots, \mathbf{e}_q)^\tau$ . From Proposition 4.12 (ii), all the solutions of the system  $A(\mathbf{z}) = 0$  can be obtained from those of its integrable connection  $\{\partial_i(\mathbf{x}) = B_i\mathbf{x}\}_{1 \leq i \leq m}$ , and vice versa. Figure 1 illustrates such a relationship, and it also suggests reducing the problem of solving  $\partial$ -finite systems to that of solving fully integrable systems.

Proposition 4.12 allows us to generalize the notion of Picard-Vessiot extensions from fully integrable systems to  $\partial$ -finite ones.

---

<sup>①</sup>Which can be found, for example, by computing the hyperexponential solutions of the system ([28, 47]).

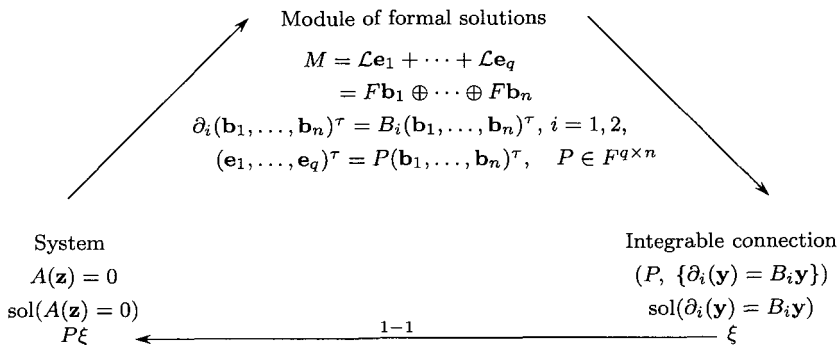


Figure 1 Relationships among Systems, Modules and Solutions

**Definition 4.13.** Let  $A(\mathbf{z}) = 0$  with  $A \in S^{p \times q}$  be a  $\partial$ -finite system,  $M$  be its module of formal solutions,  $\{\mathbf{e}_1, \dots, \mathbf{e}_q\}$  be a set of  $\mathcal{L}$ -generators of  $M$  and  $\mathbf{b}_1, \dots, \mathbf{b}_n$  be an  $F$ -basis of  $M$  such that  $A(\mathbf{e}_1, \dots, \mathbf{e}_q)^\tau = 0$  and  $(\mathbf{e}_1, \dots, \mathbf{e}_q)^\tau = P(\mathbf{b}_1, \dots, \mathbf{b}_n)^\tau$  where  $P \in F^{q \times n}$ .

A  $q \times n$  matrix  $V$  with entries in a  $\Delta$ -extension  $E$  of  $F$  is called a fundamental matrix for  $A(\mathbf{z}) = 0$  if  $V = PU$  where  $U \in E^{n \times n}$  is a fundamental matrix of the integrable connection of  $A(\mathbf{z}) = 0$  with respect to  $\mathbf{b}_1, \dots, \mathbf{b}_n$ .

A Picard-Vessiot ring for an integrable connection of  $A(\mathbf{z}) = 0$  is called a Picard-Vessiot ring for  $A(\mathbf{z}) = 0$ .

As a consequence of Theorem 4.10, we have

**Theorem 4.14.** Every  $\partial$ -finite system  $A(\mathbf{z}) = 0$  over  $F$  has a Picard-Vessiot ring  $E$ . If  $F$  has characteristic 0 and  $C_F$  is algebraically closed, then  $C_E = C_F$ .

Assume that  $F$  has characteristic 0 with an algebraically closed field of constants. If  $E$  is a Picard-Vessiot ring for the system  $A(\mathbf{z}) = 0$  then the dimension of  $\text{sol}_E(A(\mathbf{z}) = 0)$  as a  $C_F$ -vector space equals the linear dimension of  $A(\mathbf{z}) = 0$ , whenever the latter is finite.

In summary, by associating a  $\partial$ -finite system to its module of formal solutions, we reduce the system to a fully integrable system, define the notion of Picard-Vessiot extension, and compute the dimension of its solutions space by noncommutative Gröbner basis techniques.

## 5 Determining all submodules of a Laurent-Ore module

A module over a Laurent-Ore algebra that is finite-dimensional over the ground field is called a *Laurent-Ore module*. As seen in Section 4.2, a

$\partial$ -finite system  $S$  has a module of formal solutions, which is a Laurent-Ore module and denoted by  $M_S$ . A submodule of  $M$  corresponds to a subsystem of  $S$ . Thus, determining all submodules of  $M_S$  is equivalent to factoring  $S$ . In this section, we outline an algorithm for determining all submodules of a Laurent-Ore module.

## 5.1 Generalized Beke's method

Recall that  $\mathcal{L} = F[\partial_1, \dots, \partial_m, \partial_{\ell+1}^{-1}, \dots, \partial_m^{-1}]$  is a Laurent-Ore algebra. The  $d$ -th exterior power  $\wedge^d M$  of an  $\mathcal{L}$ -module  $M$  is the  $F$ -vector space  $\wedge_F^d M$  provided with the actions given by the formulas  $\partial_i(\mathbf{w}_1 \wedge \dots \wedge \mathbf{w}_d) = \sum_{s=1}^d \mathbf{w}_1 \wedge \dots \wedge (\partial_i \mathbf{w}_s) \wedge \dots \wedge \mathbf{w}_d$  for  $i \leq \ell$  and  $\partial_j^\nu(\mathbf{w}_1 \wedge \dots \wedge \mathbf{w}_d) = \partial_j^\nu(\mathbf{w}_1) \wedge \dots \wedge \partial_j^\nu(\mathbf{w}_d)$  for  $j > \ell$  and  $\nu \in \{-1, 1\}$ . A decomposable element  $\mathbf{w} \in \wedge^d M$  is an exterior product of  $d$  elements in  $M$ , i.e.,  $\mathbf{w} = \mathbf{w}_1 \wedge \dots \wedge \mathbf{w}_d$ .

The next theorem generalizes Lemma 10 in [15] or the corresponding statement in [39, page 111]:

**Theorem 5.1.** *A Laurent-Ore module  $M$  has a  $d$ -dimensional submodule if and only if  $\wedge^d M$  has a one-dimensional submodule generated by a decomposable element.*

Remark that the operators  $\partial_j^{-1}$  are indispensable in the proof of Theorem 5.1 (see also [47, Theorem 4.3.1]), and this proof yields a correspondence between  $d$ -dimensional submodules and one-dimensional submodules generated by decomposable elements: if a  $d$ -dimensional submodule of  $M$  has an  $F$ -basis  $\mathbf{v}_1, \dots, \mathbf{v}_d$ , then the linear subspace generated by  $\mathbf{v}_1 \wedge \dots \wedge \mathbf{v}_d$  in  $\wedge^d M$  is a one-dimensional submodule; conversely, if a one-dimensional submodule of  $\wedge^d M$  is generated by a decomposable element  $\mathbf{v}_1 \wedge \dots \wedge \mathbf{v}_d$ , then the  $F$ -linear subspace generated by  $\mathbf{v}_1, \dots, \mathbf{v}_d$  in  $M$  is a  $d$ -dimensional submodule.

The original idea of Theorem 5.1 is due to Beke [3]. He shows that finding right factors of a linear ordinary differential operator  $L$  is equivalent to finding exponential solutions of some associated equations which are constructed by Wronskian techniques. His method is generalized to factor  $\partial$ -finite differential systems [31, 32]. Theorem 5.1 may be viewed as a module-theoretic generalization of Beke's method. However, this module-theoretic approach avoids not only constructing complicated Wronskian-like determinants but also guessing leading derivatives of Gröbner bases.

## 5.2 Determining one-dimensional submodules

We outline an algorithm for determining one-dimensional submodules of a Laurent-Ore module in [33]. In a  $\Delta$ -extension  $R$  of  $F$ , a non-zero

element  $h$  is said to be *hyperexponential with respect to a map  $\phi$*  in  $\Delta$  if  $\phi(h)=rh$  for some  $r \in F$ . The element  $r$  is denoted  $\ell\phi(h)$ . The element  $h$  is said to be *hyperexponential over  $F$*  if it is hyperexponential with respect to all the maps in  $\Delta$ . A non-zero vector  $V \in R^n$  is said to be *hyperexponential (with respect to a map  $\phi$ )* if there exist  $h \in R$ , hyperexponential (with respect to  $\phi$ ), and  $W \in F^n$  such that  $V = hW$ .

Let  $M$  be an  $\mathcal{L}$ -module with a finite basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  over  $F$ . The module structure of  $M$  is determined by  $m$  matrices  $A_1, \dots, A_m$  in  $F^{n \times n}$ , where

$$\partial_i(\mathbf{b}_1, \dots, \mathbf{b}_n)^T = A_i(\mathbf{b}_1, \dots, \mathbf{b}_n)^T, \quad i = 1, \dots, m. \quad (11)$$

Note that  $A_{\ell+1}, \dots, A_m$  are invertible because  $\mathcal{L}$  contains  $\partial_{\ell+1}^{-1}, \dots, \partial_m^{-1}$ . We call  $A_1, \dots, A_m$  *the structure matrices* with respect to  $\mathbf{b}_1, \dots, \mathbf{b}_n$ . For a column vector  $Z = (z_1, \dots, z_n)^T$  of unknowns,

$$\delta_i(Z) = -A_i^T Z, \quad i \leq \ell, \quad \sigma_j(Z) = (A_j^{-1})^T Z, \quad j > \ell \quad (12)$$

is called the system associated to  $M$  and the basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$ . Systems associated to different bases are equivalent in the sense that the solutions of one system can be transformed to those of another by a matrix in  $F^{n \times n}$ . The multiplicative rules  $\partial_s \partial_t = \partial_t \partial_s$  for all  $s, t \in \{1, \dots, m\}$  imply that (12) is fully integrable [8, Definition 2]. A detailed verification of this assertion is presented in [47, Lemma 4.1.1]. On the other hand, every fully integrable system is associated to its module of formal solutions [8, Example 4], which is an  $\mathcal{L}$ -module of finite dimension.

The next proposition connects one-dimensional submodules of  $M$  with hyperexponential solutions of its associated systems.

**Proposition 5.2.** *Let an  $\mathcal{L}$ -module  $M$  have a finite  $F$ -basis  $\mathbf{b}_1, \dots, \mathbf{b}_n$  with structure matrices given in (11) and the associated system in (12). Let  $\mathbf{u} = \sum_{i=1}^n u_i \mathbf{b}_i$  with  $u_i \in F$  not all zero.*

- (i) *If there exists a hyperexponential element  $h$  in some  $\Delta$ -extension such that  $h(u_1, \dots, u_n)^T$  is a solution of (12), then  $F\mathbf{u}$  is a submodule of  $M$  with*

$$\partial_i(\mathbf{u}) = -\text{ldeg}_i(h)\mathbf{u}, \quad i \leq \ell \quad \text{and} \quad \partial_j(\mathbf{u}) = \ell\sigma_j(h)^{-1}\mathbf{u}, \quad j > \ell. \quad (13)$$

- (ii) *If  $F\mathbf{u}$  is a submodule of  $M$  then there exists an invertible hyperexponential element  $h$  in some  $\Delta$ -extension such that  $h(u_1, \dots, u_n)^T$  is a solution of (12).*

By Proposition 5.2 we need only to compute hyperexponential solutions of the fully integrable system (12), which can be done by algorithms for computing exponential (resp. hypergeometric) solutions of ordinary differential (resp. difference) matrix equation [2, 26], and a back-substitution process described in [33].

## References

- [1] J.M. Aroca, J. Cano, R. Feng and X.S. Gao. Algebraic general solutions of algebraic ODEs. *Proceedings of ISSAC 2005*, 29-36, ACM Press, 2005.
- [2] M.A. Barkatou. Rational solutions of matrix difference equations: the problem of equivalence and factorization. *Proceedings of ISSAC 1999*, 277-282, ACM Press, 1999.
- [3] E. Beke. Die Irreducibilität der homogenen Differentialgleichungen. *Math. Annal.* **45**, 278-294, 1894.
- [4] F. Boulier, D. Lazard, F. Ollivier and M. Petitiot. Representation for the radical of a finitely generated differential ideal, *Proceedings of ISSAC 1995*, 158-166, ACM Press, 1995.
- [5] D. Bouziane, A. Kandri Rody and H. Maârouf. Unmixed decomposition of a finitely generated perfect differential ideal. *Journal of Symbolic Computation* **31**, 631-649, 2001.
- [6] M. Bronstein. An improved algorithm for factoring linear ordinary differential operators. *Proceedings of ISSAC 1994*, 336-347, ACM Press, 1994.
- [7] M. Bronstein. *Symbolic Integration I*, Springer, 1997.
- [8] M. Bronstein, Z. Li and M. Wu. Picard-Vessiot extensions for linear functional systems. *Proceedings of ISSAC 2005*, 68-75, ACM Press, 2005.
- [9] Y. Chen and X. S. Gao. Involutive characteristic set of partial differential polynomial systems. *Science in China (A)*, **33**(2), 97-113, 2003.
- [10] S.C. Chou and X.S. Gao. Automated reasoning in differential geometry and mechanics. *Journal of Automated Reasoning* **10**, 161-172, 1993.
- [11] S.C. Chou and X.S. Gao. Automated reasoning in geometry. *Handbook of Automated Reasoning*, (eds. A. Robinson and A. Voronkov), 709-749, Elsevier, Amsterdam, 2001.
- [12] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *Journal of Symbolic Computation* **26**, 187-228, August 1998.
- [13] T. Cluzeau and E. Hubert. Resolvent representation for regular differential ideals. *AAECC* **29**, 395-425, 2003.
- [14] R.M. Cohn. *Difference Algebra*. Tracts in Mathematics 17, Interscience, New York, 1965.

- [15] E. Compoint and J.A. Weil. Absolute reducibility of differential operators and Galois groups. *J. of Algebra*, 275(1): 77-105, 2003.
- [16] E.G. Fan. *Integrable Systems and Computer Algebra* (in Chinese), Science Press, 2004.
- [17] R.Y. Feng and X.S. Gao. A polynomial time algorithm to find rational general solutions Of first order autonomous ODEs, *Journal of Symbolic Computation* **41**, 739-762, 2006.
- [18] X.S. Gao. Implicitization for differential rational parametric equations, *J. of Symbolic Computation*, 811-824, 36(5), 2003.
- [19] X.S. Gao and S.C. Chou. A zero structure theorem for differential parametric systems, *Journal of Symbolic Computation* **16**, 585-595, 1994.
- [20] R. Feng, X.S. Gao and Z. Huang. Rational general solutions of algebraic ordinary difference equations. *MM-Preprints*, KLMM, CAS, 2005.
- [21] X.S. Gao and Y. Luo. A characteristic set method for difference polynomial systems. *Inter Conf on Poly Sys. Sol.* Nov. 24-26, Paris, 2004.
- [22] X.S. Gao and C. Yuan. Resolvent systems of difference polynomial ideals. *Proceedings of ISSAC, 2006*, 101-108, ACM Press, 2006.
- [23] X.S. Gao and M. Zhang. Decomposition of differential polynomials with constant coefficients. *Proceedings of ISSAC 2004*, 175-182, ACM Press, New York, 2004.
- [24] M. van Hoeij. Formal solutions and factorization of differential operators. *Journal of Symbolic Computation* **24**, 1-30, 1997.
- [25] M. van Hoeij. Factorization of differential operators with rational function coefficients. *Journal of Symbolic Computation* **24**, 537-561, 1997.
- [26] M. van Hoeij. Finite singularities and hypergeometric solutions of linear recurrence equations. *J. Pure Appl. Algebra* **139**, 109-131 1999.
- [27] E. Hubert. Factorization-free decomposition algorithms in differential algebra. *Journal of Symbolic Computation* **29**, 641-662, 2000.
- [28] G. Labahn and Z. Li. Hyperexponential solutions of finite-rank ideals in orthogonal Ore algebras. In *Proceedings of ISSAC 2004*, 213-220. ACM Press, 2004.
- [29] H. Li and M. Cheng. Clifford algebraic reduction method for mechanical theorem proving in differential geometry. *Journal of Automated Reasoning* **21**, 1-21, 1998.

- [30] Z. Li. Mechanical theorem proving of the local theory of surfaces. *Ann. Math. Artif. Intell.* **13**, 25-46, 1995.
- [31] Z. Li, F. Schwarz and S. Tsarev. Factoring zero-dimensional ideals of linear partial differential operators. In *Proceedings of ISSAC 2002*, 168-175, ACM Press, 2002.
- [32] Z. Li, F. Schwarz and S. Tsarev. Factoring systems of linear PDE's with finite-dimensional solution spaces. *Journal of Symbolic Computation* **36**, 443-471, 2003.
- [33] Z. Li, M.F. Singer, M. Wu and D. Zheng. A recursive method for determining the one-dimensional submodules of Laurent-Ore modules. *Proceedings of ISSAC 2006*, 220-227, ACM Press, 2006.
- [34] B. Malgrange. Motivations and introduction to the theory of  $D$ -modules. *Computer Algebra and Differential Equations*, vol. 193, *LMS LNS*, 3-20, Cambridge Univ. Press, 1994.
- [35] B. Malgrange. On nonlinear differential Galois theory, *Chinese Annals of Mathematics, Series B*, 23(2), 219-226, 2002.
- [36] F. Pauer and A. Unterkircher. Gröbner bases for ideals in Laurent polynomial rings and their applications to systems of difference equations. *AAECC* **9**, 271-291, 1999.
- [37] M. Petkovšek, H. Wilf and D. Zeilberger.  $A=B$ . A K Peters, Ltd, 1996.
- [38] M. van der Put and M.F. Singer. *Galois Theory of Difference Equations, Lecture Notes in Mathematics 1666*. Springer, 1997.
- [39] M. van der Put and M.F. Singer. *Galois Theory of Linear Differential Equations, Grundlehren der Mathematischen Wissenschaften* **328**. Springer, Heidelberg, 2003.
- [40] G. Reid. Algorithms for reducing a system of PDEs to standard form. *European J. of Appl. Math.* **2**, 293-318, 1991.
- [41] D. Richardson. Wu's method and the Khovanskii finiteness theorem. *Journal of Symbolic Computation* **12**, 127-141, 1991.
- [42] J.F. Ritt. *Differential Algebra*. Amer. Math. Soc. Colloquium, 1950.
- [43] M.F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *AAECC* **7**, 77-104, 1996.
- [44] W. Sit. The Ritt-Kolchin theory for differential polynomials. *Differential Algebra and related Topics, Proceedings of the International Workshop*, 1-70, World Scientific, 2002.
- [45] D. Wang. A method for proving theorems in differential geometry and mechanics. *J. Univ. Comput. Sci.* **9**, 658-673, 1995.

- [46] D.K. Wang. *Polynomial Equations Solving and Mechanical Geometric Theorem Proving*. PhD Thesis, KLMM, Academia Sinica, 1993.
- [47] M. Wu. *On Solutions of Linear Functional Systems and Factorization of Modules over Laurent-Ore Algebras*. PhD thesis, Chinese Academy of Sciences and Université de Nice, 2005.
- [48] W.T. Wu. On the decision problem and the mechanization of theorem-proving in elementary geometry. *Scientia Sinica* **21**, 159-172, 1978.
- [49] W.T. Wu. Mechanical theorem proving in elementary differential geometry (in Chinese). *Scientia Sinica*, 94-102, 1979.
- [50] W.T. Wu. *Basic Principle of Mechanical Theorem Proving in Geometries*. (in Chinese) Science Press, Beijing, 1984; Springer, Wien, 1994.
- [51] W.T. Wu. Mechanical derivation of Newton's Gravitational Laws from Kepler's Laws. *MM-Preprints* **1**, 53-61, 1987.
- [52] W.T. Wu. On the Foundation of Algebraic Differential Geometry. *Sys.Sci. & Math.Scis.* **2**, 289-312, 1989.
- [53] Z.Y. Yan. *Constructive Methods for Complex Nonlinear Waves* (in Chinese), Science Press, 2006.
- [54] S. Zampieri. A solution of the Cauchy problem for multidimensional discrete linear shift-invariant systems. *Linear Algebra and Its Applications* **202**, 143-162, 1994.
- [55] M. Zhou and F. Winkler. Gröbner bases in difference-differential modules. *Proceedings of ISSAC 2006*, 353-360, ACM Press, 2006.