Polynomial General Solutions for First Order Autonomous ODEs*

Ruyong Feng and Xiao-Shan Gao

Key Laboratory of Mathematics Mechanization,
Institute of Systems Science,AMSS, Academia Sinica,
Beijing 100080, P. R. China

Abstract. For a first order autonomous ODE, we give a polynomial time algorithm to decide whether it has a polynomial general solution and to compute one if it exists. Experiments show that this algorithm is quite effective in solving ODEs with high degrees and a large number of terms.

1 Introduction

To find elementary function solutions for differential equations could be traced back to the work of Liouville. As a consequence, such solutions of differential equations are called *Liouvillian solutions*. In [16], Risch gave an algorithm for finding Liouvillian solutions for the simplest differential equation $y' = f(x)$, that is, to find elementary function solutions to the integration $\int f(x)\mathrm{d}x$. Kovacic presented a method for solving second order linear homogeneous differential equations [13]. Singer established the general framework to find Liouvillian solutions of general homogeneous linear differential equations [18]. Many interesting results on finding Liouvillian solutions of linear ODEs are given in [1, 2, 3, 6, 11, 20, 19]. In [14], Li and Schwarz gave the first method to find rational solutions for a class of partial differential equations.

All these results are limited to linear cases. There seems no general methods to find Liouvillian solutions of nonlinear differential equations. With respect to ODEs of the form $y' = R(x, y)$ where $R(x, y)$ is a rational function, Poincaré made important contributions [15]. More recently, Carnicer also made important progresses in solving the Poincaré problem [5], which is equivalent to finding the degree bound for the algebraic solutions of $y' = R(x, y)$. For ODEs of this form, other work includes: Cano proposed an algorithm to find polynomial solutions [4]; Singer studied the Liouvillian first integrals [18]. On the other hand, Hubert gave a method to compute a basis of the general solutions of first order ODEs and applied it to study the local behavior of the solutions[10]. Bronstein gave an effective method to compute rational solutions of Ricatti equations [2]. In [9], we propose an algorithm to find rational solutions for first order autonomous ODEs. But this algorithm has exponential complexity.

* Partially supported by NKBRP of China and by a USA NSF grant CCR-0201253.

H. Li, P. J. Olver and G. Sommer (Eds.): IWMM-GIAE 2004, LNCS 3519, pp. 5–17, 2005.

In this paper, we will give a polynomial time algorithm to find polynomial solutions of first order autonomous ODEs. Instead of finding arbitrary polynomial solutions, we will find the general solutions for ODEs of polynomial type. For example, the general solution for $(\frac{\mathrm{d}y}{\mathrm{d}x})^2 - 4y = 0$ is: $y = (x+c)^2$, where c is an arbitrary constant. Three main results are given in this paper. First, we give a sufficient and necessary condition for an ODE to have polynomial general solutions. Second, we give a detailed analysis of the structure of the first order autonomous ODEs which have polynomial general solutions. This leads to an almost *explicit formula* for the polynomial solutions of the first order autonomous ODE. Third, by introducing a novel method of substituting a polynomial solution into a first order ODE, we get a polynomial time algorithm to find polynomial general solutions of first order autonomous ODEs. Our experiments show that this algorithm is quite effective in solving ODEs with high degree and a large number of terms.

The paper is organized as follows. In section 2, a criterion for an ODE to have polynomial general solutions is given. In section 3, we give the degree bound of polynomial solutions of first order autonomous ODEs. In section 4, we analyze the structure of the first order autonomous ODEs which have polynomial solutions. In section 5, we present a polynomial time algorithm to find polynomial general solutions of first order autonomous ODEs. In section 6, we present the conclusion.

2 Polynomial General Solution to ODEs

Let $\mathbf{K} = \mathbf{Q}(x)$ be the differential field of rational functions in x with differential operator $\frac{\mathrm{d}}{\mathrm{d}x}$ and y an indeterminate over $\mathbf{K}$. We denote by y_i the i-th derivative of y. We use $\mathbf{K}\{y\}$ to denote the ring of differential polynomials over the differential field $\mathbf{K}$, which consists of the polynomials in the y_i with coefficients in $\mathbf{K}$. All differential polynomials in this paper are in $\mathbf{K}\{y\}$, if there is no other statement. Let Σ be a system of differential polynomials in $\mathbf{K}\{y\}$. A *zero* of Σ is an element in a universal extension field of $\mathbf{K}$ [17], which vanishes every differential polynomial in Σ. The totality of the zeros in $\mathbf{K}$ is denoted by $\mathrm{Zero}(\Sigma)$. In this paper, we will use $\mathcal{C}$ to denote the constant field of the universal extension of $\mathbf{K}$.

Let $P \in \mathbf{K}\{y\}/\mathbf{K}$. We denote $\mathrm{ord}(P)$ the highest derivative of y in P, called the *order* of P. Let $o = \mathrm{ord}(P) > 0$ be the order of P. We may write P as follows

$$P = a_d y_o^d + a_{d-1} y_o^{d-1} + \ldots + a_0$$

where a_i are polynomials in $y_1, \ldots, y_{o-1}$ for $i = 0, \ldots, d$ and $a_d \neq 0$. a_d is called the *initial* of P and $S = \frac{\partial P}{\partial y_o}$ is called the *separant* of P. The k-th derivative of P is denoted by $P^{(k)}$. Let S be the separant of P, $o = \mathrm{ord}(P)$ and $k > 0$. Then we have

$$P^{(k)} = S y_{o+k} - R_k \tag{1}$$

where R_k is of lower order than $o + k$.

Let P be a differential polynomial of order o. A differential polynomial Q is said to be *reduced* with respect to P if $\mathrm{ord}(Q) < o$ or $\mathrm{ord}(Q) = o$ and $\deg(Q, y_o) < \deg(P, y_o)$. For two differential polynomials P and Q, let $R = \mathrm{prem}(P, Q)$ be the differential pseudo-remainder of P with respect to Q. We have the following *differential remainder formula* for R (see [12, 17])

$$JP = \sum_i B_i Q^{(i)} + R$$

where J is a product of certain powers of the initial and separant of Q and B_i are differential polynomials. For a differential polynomial P with order o, we say that P is *irreducible* if P is irreducible when P is treated as a polynomial in $\mathbf{K}[y, y_1, \ldots, y_o]$.

Let $P \in \mathbf{K}\{y\}/\mathbf{K}$ be an irreducible differential polynomial and

$$\Sigma_P = \{A \in \mathbf{K}\{y\} | \mathrm{prem}(A, P) = 0\}. \tag{2}$$

In [17], Ritt proved that

Lemma 1. *Σ_P is a prime differential ideal.*

Let Σ be a non-trivial prime ideal in $\mathbf{K}\{y\}$. A zero η of Σ is called *a generic zero* of Σ if for any differential polynomial P, $P(\eta) = 0$ implies that $P \in \Sigma$. It is well known that an ideal Σ is prime iff it has a generic zero [17].

A *universal constant extension* of $\mathbf{Q}$ is obtained by first adding an infinite number of arbitrary constants to $\mathbf{Q}$ and then taking the algebraic closure. We further assume that the universal field in this paper contains a universal constant extension of $\mathbf{Q}$.

Definition 1. *Let $F \in \mathbf{K}\{y\}/\mathbf{K}$ be an irreducible differential polynomial. A general solution of $F = 0$ is defined as a generic zero of Σ_F. A polynomial general solution of $F = 0$ is defined as a general solution of $F = 0$ of the form*

$$\hat{y} = \sum_{i=0}^{n} a_i x^i, \; (a_n \neq 0) \tag{3}$$

where a_i are in a universal constant extension of $\mathbf{Q}$.

Example 1. In this example, we give three ODEs $E_i = 0$ which have polynomial general solutions $S_i = 0$ respectively.

$$\begin{array}{ll} E_1 = y_1^2 - 4y & S_1 = (x - c)^2 \\ E_2 = xy_1 - ny & S_2 = cx^n \\ E_3 = y_1(y_1 - 1)(y_1 - 2) - (xy_1 - y)^2 & S_3 = cx + \sqrt{c(c-1)(c-2)} \end{array}$$

where c is an arbitrary constant and n is a fixed positive integer.

In the literature in general, a *general solution* of $F(y) = 0$ is defined as a family of solutions with o independent parameters in a loose sense where $o = \mathrm{ord}(F(y))$. From Theorem 6 in [12] (Chapter 2, section 12), we can see that the above definition of general solutions are essentially the same to the definition in the literature. But, the definition given by Ritt is more precise.

Theorem 1. *Let $F(y)$ be an irreducible differential polynomial. Then $F(y) = 0$ has a polynomial general solution of degree n iff n is the least integer such that $\mathrm{prem}(y_{n+1}, F(y)) = 0$.*

Proof. ($\Longrightarrow$) Suppose that $F(y) = 0$ has a polynomial general solution $\hat{y}$ with degree n. Since $y_{n+1}(\hat{y}) = 0$, $y_{n+1} \in \Sigma_F$ which means that $\mathrm{prem}(y_{n+1}, F(y)) = 0$ by Lemma 1.

($\Longleftarrow$) Assume that there exists an n such that $\mathrm{prem}(y_{n+1}, F(y)) = 0$ and n is the least. If $n = -1$, then $F(y) = y$. It is obvious. Now we suppose that $n \geq 0$. From Lemma 1, $y_{n+1} \in \Sigma_F$. Hence, all the elements in the zero set of Σ_F must have the form: $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$. In particularly, the generic zero $\hat{y}$ has the form: $\hat{y} = \sum_{i=0}^{n} a_i x^i$. If $a_n = 0$, then $y_n(\hat{y}) = 0$ which implies that $y_n \in \Sigma_F$. Hence $\mathrm{prem}(y_n, F(y)) = 0$, a contradiction. ∎

3 A Criterion for First Order Autonomous ODEs

In what follows, if there is no other statement, $F(y)$ will always be a non-zero first order irreducible differential polynomial with coefficients in $\mathcal{C}$ which are not arbitrary constants.

Lemma 2. *Let $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$ be a solution of $F(y) = 0$, where $\bar{a}_i \in \mathcal{C}$, $n > 0$ and $\bar{a}_n \neq 0$. Then for an arbitrary constant c,*

$$\hat{y} = \sum_{i=0}^{n} \bar{a}_i (x + c)^i \tag{4}$$

is a polynomial general solution for $F(y) = 0$.

Proof. It is easy to show that $\hat{y}$ is still a zero of Σ_F. For any $G(y) \in \mathbf{K}\{y\}$ satisfying $G(\hat{y}) = 0$, let $R(y) = \mathrm{prem}(G(y), F(y))$. Then $R(\hat{y}) = 0$. Suppose that $R(y) \neq 0$. Since $F(y)$ is irreducible and $\deg(R(y), y_1) < \deg(F(y), y_1)$, there are two differential polynomials $P(y), Q(y) \in \mathbf{K}(c_{k,l})\{y\}$ such that $P(y)F(y) + Q(y)R(y) \in \mathbf{K}(c_{k,l})[y]$ and $P(y)F(y) + Q(y)R(y) \neq 0$ where $c_{k,l}$ are the coefficients of F as a polynomial in y, y_1. Thus $(PF + QR)(\hat{y}) = 0$. Because c is an arbitrary constant which is transcendental over $\mathbf{K}(c_{k,l})$ and $n > 0$, we have $P(y)F(y) + Q(y)R(y) = 0$, a contradiction. Hence $R(y) = 0$ which means that $G(y) \in \Sigma_F$. So $\hat{y}$ is a generic zero of Σ_F. ∎

The above theorem reduces the problem of finding a polynomial general solution to the problem of finding a polynomial solution. In what below, we will show how to find such a solution.

Lemma 3. *Suppose that* $deg(F(y), y_1) = m > 0$*. If* $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$ $(\bar{a}_i \in \mathcal{C}, \bar{a}_n \neq 0)$ *is a solution of* $F(y) = 0$*, then* $n \leq m$*.*

Proof. Assume that $F(y) = \sum_{i=0}^{l} c_{\alpha_i\beta_i} y^{\alpha_i} y_1^{\beta_i}$, where $c_{\alpha_i\beta_i} \neq 0$ and $(\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ if $i \neq j$. Substituting y in $F(y)$ by $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$, we get a polynomial $F(\bar{y})$ in x. Assume that $n > m > 0$. Then $n \geq 2$. We consider the highest degree of x in $F(\bar{y})$ which is the largest number in $\{n\alpha_i + (n-1)\beta_i \quad \text{for } i = 0, \cdots, l\}$. If $\bar{y}$ is a solution of $F(y) = 0$, all the coefficients of $F(\bar{y})$ are zero. Hence the number of the terms $y^{\alpha_i} y_1^{\beta_i}$ such that $n\alpha_i + (n-1)\beta_i$ is the largest is at least two. Without loss of generality, we suppose that two of them are $n\alpha_1 + (n-1)\beta_1$ and $n\alpha_2 + (n-1)\beta_2$. Then we have $n(\alpha_1 - \alpha_2) = (n-1)(\beta_2 - \beta_1)$. Assume that $\beta_2 \geq \beta_1$. Since $(n, n-1) = 1$, we have $n|(\beta_2 - \beta_1)$. But $0 \leq \beta_2 - \beta_1 \leq m < n$, which implies that $\beta_1 = \beta_2$. Hence $\alpha_1 = \alpha_2$. This contradicts $(\alpha_1, \beta_1) \neq (\alpha_2, \beta_2)$. Hence $n \leq m$. ▮

The following theorem gives a criterion for $F(y) = 0$ to have polynomial general solutions.

Theorem 2. *Let* $F(y)$ *be a first order autonomous and irreducible differential polynomial and* $n = \deg(F(y), y_1)$*. Then* $F(y) = 0$ *has a polynomial general solution iff* $prem(y_{n+1}, F(y)) = 0$*.*

Proof. From Lemma 2, we need only to consider polynomial solutions of $F(y) = 0$ with coefficients in $\mathcal{C}$. Now the result is a direct consequence of Lemma 3 and Theorem 1. ▮

Algorithm 1. *The input is a first order autonomous ODE* $F(y) = 0$*. The output is a polynomial general solution of* $F(y) = 0$ *if it exists.*

1. Let n be the degree of $F(y)$ in y_1. If $\text{prem}(y_{n+1}, F(y)) \neq 0$ then $F(y) = 0$ has no polynomial solutions and the algorithm exists; otherwise goto the next step.
2. Let d be the smallest number such that $\text{prem}(y_{d+1}, F(y)) = 0$. By Theorem 1, the polynomial solution of $F(y) = 0$ is of degree d.
3. Substitute $z = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$ into $F(y) = 0$ and let **PS** be the set of the coefficients of $F(z)$ as polynomials in x.
4. Solve equations $\mathbf{PS} = 0$ with Wu's method [22]. Any solution with $a_d \neq 0$ of $\mathbf{PS} = 0$ will provide a polynomial general solution of $F(y) = 0$. If $\mathbf{PS} = 0$ has no solutions, then $F(y) = 0$ has no polynomial general solutions.

Now we give a simple example to show how the algorithm works.

Example 2. Consider the equation

$$F(y) = 31 - 54y + 27y^2 - 3y_1^2 - y_1^3.$$

1. $n := 3$. Since four is the smallest number k such that $\text{prem}(y_k, F(y)) = 0$, $F(y) = 0$ has a polynomial general solution with degree three.

2. $y := a_0 + a_1x + a_2x^2 + a_3x^3$. Substituting y into $F(y)$, we get $PS =$

$$\{\ 27a_3^2 - 27a_3^3, 54a_2a_3 - 54a_2a_3^2,\\ 54a_1a_3 + 27a_2^2 - 27a_3^2 - 9a_1a_3^2 - 24a_2^2a_3 - 3a_3(6a_1a_3 + 4a_2^2),\\ -54a_3 + 54a_0a_3 + 54a_1a_2 - 36a_2a_3 - 24a_1a_2a_3 - 2a_2(6a_1a_3 + 4a_2^2),\\ -54a_2 + 54a_0a_2 + 27a_1^2 - 18a_1a_3 - 12a_2^2 - a_1(6a_1a_3 + 4a_2^2) - 8a_2^2a_1 - 3a_3a_1^2,\\ -54a_1 + 54a_0a_1 - 12a_1a_2 - 6a_1^2a_2, 31 - 54a_0 + 27a_0^2 - 3a_1^2 - a_1^3\ \}.$$

3. Solve $PS = 0$. We have the solutions

$$\{a_3 = 1, a_1 = \frac{a_2^2}{3} + 1, a_0 = 1 + \frac{a_2}{3} + \frac{a_2^3}{27}, a_2 = a_2\}.$$

   Let $a_2 = 0$. Then $F(y) = 0$ has a polynomial general solution

$$\hat{y} = (x + c)^3 + (x + c) + 1$$

   by Lemma 2.

It is known that the general methods of equation solving are exponential algorithms. Therefore, the above algorithm might be ineffective. In the next section, we will analyze the structure of the first order autonomous ODEs which have polynomial solutions. After doing so, we can obtain a polynomial time algorithm.

4 Structure of the First Order Autonomous ODEs with Polynomial General Solutions

If $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$ is a polynomial solution of $F(y) = 0$, we regard x, y, y_1 as independent indeterminants and eliminate x in the polynomial set $\{\sum_{i=0}^{n} \bar{a}_i x^i - y, \sum_{i=1}^{n} i\bar{a}_i x^{i-1} - y_1\}$. Then we will obtain a new differential polynomial $R(y)$. Theorem 3 below will give the relation between $R(y)$ and $F(y)$.

Lemma 4. *Let $f_1(y) = \sum_{i=0}^{n} \bar{a}_i x^i - y$, $f_2(y) = \sum_{i=1}^{n} i\bar{a}_i x^{i-1} - y_1$ $(n \geq 1, \bar{a}_n \neq 0, \bar{a}_i \in \mathcal{C})$. If $n \geq 2$, let $R(y)$ be the Sylvester-resultant of $f_1(y)$ and $f_2(y)$ with respect to x and if $n = 1$, let $R(y) = f_2(y)$. Then $R(y)$ is an irreducible polynomial in $\mathcal{C}[y, y_1]$ and has the form*

$$R(y) = (-1)^n \bar{a}_n^{n-1} y_1^n + (-1)^{n-1} n^n \bar{a}_n^n y^{n-1} + G(y, y_1) \qquad (5)$$

where tdeg(G) (the total degree of G) $\leq n - 1$ and G does not contain the term y^{n-1}.

Proof. When $n = 1$, it is clear. Assume that $n \geq 2$. We know that $R(y)$ is the following determinant which has 2n-1 columns and rows:

$$\begin{vmatrix} \bar{a}_n & \bar{a}_{n-1} & \bar{a}_{n-2} & \cdots & \bar{a}_1 & \bar{a}_0 - y & & & \\ & \bar{a}_n & \bar{a}_{n-1} & \cdots & \bar{a}_2 & \bar{a}_1 & \bar{a}_0 - y & & \\ & & \cdots & \cdots & \cdots & & & & \\ & & & \bar{a}_n & \bar{a}_{n-1} & \bar{a}_{n-2} & \cdots & \bar{a}_1 & \bar{a}_0 - y \\ n\bar{a}_n & (n-1)\bar{a}_{n-1} & (n-2)\bar{a}_{n-2} & \cdots & \bar{a}_1 - y_1 & & & & \\ & n\bar{a}_n & (n-1)\bar{a}_{n-1} & \cdots & \bar{a}_2 & \bar{a}_1 - y_1 & & & \\ & & \cdots & \cdots & \cdots & & & & \\ & & & n\bar{a}_n & (n-1)\bar{a}_{n-1} & (n-2)\bar{a}_{n-2} & \cdots & \bar{a}_2 & \bar{a}_1 - y_1 \end{vmatrix}.$$

Regard $\bar{a}_i$ in the above determinant as indeterminants. Let $R = \sum c_{\alpha_i \beta_i} y^{\alpha_i} y_1^{\beta_i}$, where $(\alpha_i, \beta_i) \neq (\alpha_j, \beta_j)$ if $i \neq j$ and $c_{\alpha_i \beta_i}$ are non-zero polynomials in $\bar{a}_0, \cdots, \bar{a}_n$. We define a weight

$$w : \mathcal{C}[x, y, y_1, \bar{a}_i] \to \mathcal{Z}$$

which satisfies $w(x) = 1$, $w(\bar{a}_i) = n - i$, $w(y) = n$, $w(y_1) = n - 1$, $w(st) = w(s) + w(t)$ and $w(k) = 0$ for $k \in \mathcal{C}$. Then f_1 and f_2 are the isobaric polynomials with the weight n and $n-1$. From [7], we know that the resultant of two homogeneous polynomials is still homogeneous. By the same way, we can show that the resultant of two isobaric polynomials with the weight n and $n-1$ is still an isobaric polynomial with weight $n(n-1)$. Hence $R(y)$ is an isobaric polynomial with the weight $n(n-1)$. We have $w(y^{\alpha_i} y_1^{\beta_i}) = n\alpha_i + (n-1)\beta_i = \alpha_i + (n-1)(\alpha_i + \beta_i) \leq n(n-1)$, which implies if $\alpha_i > 0$ then we have $\alpha_i + \beta_i < n$. By the computation of the above determinant, the coefficients of y_1^n and y^{n-1} in $R(y)$ are $(-1)^n \bar{a}_n^{n-1}$ and $(-1)^{n-1} n^n \bar{a}_n^n$. Then the form of $R(y)$ is as (5).

In the following, we take $\bar{a}_i$ as complex numbers. If $R(y)$ is reducible, we assume that $R(y) = F_1(y)F_2(y)$, where $0 < \operatorname{tdeg}(F_1(y)), \operatorname{tdeg}(F_2(y)) < n$. Since $R(y) = P(y)f_1(y) + Q(y)f_2(y)$, where $P(y)$, $Q(y)$ are two differential polynomials, we have $R(\bar{y}) \equiv 0$ which implies that $F_1(\bar{y}) = 0$ or $F_2(\bar{y}) = 0$. But we know that it is impossible by Lemma 3, because $\deg(F_1(y), y_1)$, $\deg(F_2(y), y_1) < n$, a contradiction. ∎

Theorem 3. *Use the same notations as in Lemma 4. If $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$ is a polynomial solution of $F(y) = 0$, then $R(y) | F(y)$. Since $F(y)$ is irreducible, $F(y) = \lambda R(y)$, where $\lambda \in \mathcal{C}$ and $\lambda \neq 0$.*

Proof. From Lemma 3 and Lemma 4, we know $\deg(F(y), y_1) \geq n = \deg(R(y), y_1)$. Let $T(y) = \operatorname{prem}(F(y), R(y))$. Then we have the remainder formula $J(y)^k F(y) = Q(y)R(y) + T(y)$, where $Q(y), T(y) \in \mathcal{C}[y, y_1]$, $J(y)$ is the initial of $R(y)$ and $\deg(T(y), y_1) < \deg(R(y), y_1)$. Since $F(\bar{y}) = 0$ and $R(\bar{y}) = 0$, we have $T(\bar{y}) = 0$. By Lemma 3, $T(y) = 0$. That is $J(y)^k F(y) = Q(y)R(y)$ which implies that $R(y)|F(y)$ because $R(y)$ is irreducible. Since $F(y)$ is irreducible, it is clear that $F(y) = \lambda R(y)$ where $\lambda \in \mathcal{C}$ and $\lambda \neq 0$. ∎

From Lemma 4 and Theorem 3, if $F(y)$ has a polynomial solution $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$, it must be of the following form

$$F(y) = a y_1^n + b y^{n-1} + G(y, y_1) \tag{6}$$

where $a, b \in \mathcal{C}$ are not zero, $\mathrm{tdeg}(G) \leq n-1$ and G does not contain the term y^{n-1}.

As a consequence of Theorem 3 and Lemma 4, we have

Corollary 1. *Let $F(y)$ be of the form (6) and have a polynomial solution of the form (4). Then*

$$\bar{a}_n = -\frac{b}{n^n a}. \tag{7}$$

Lemma 5. *Let $F(y)$ be of the form (6) and have a polynomial general solution of the form (4). Then we may construct a new general solution of the following form for $F(y) = 0$*

$$\hat{y} = \bar{a}_n (x+c)^n + \sum_{i=0}^{n-2} \tilde{a}_i (x+c)^i. \tag{8}$$

In other words, we may assume that $\bar{a}_{n-1} = 0$ in the general solution of $F(y) = 0$.

Proof. It is clear that

$$\hat{y} = \bar{a}_n (x + c - \frac{\bar{a}_{n-1}}{n\bar{a}_n})^n + \sum_{i=0}^{n-2} \tilde{a}_i (x + c - \frac{\bar{a}_{n-1}}{n\bar{a}_n})^i.$$

Since $c - \frac{\bar{a}_{n-1}}{n\bar{a}_n}$ is still an arbitrary constant, replacing $c - \frac{\bar{a}_{n-1}}{n\bar{a}_n}$ by c in the above equation, we get the form (8) and it is still a general solution of $F(y) = 0$. ∎

The following theorem tells us that the value of $\bar{a}_k$ only depends on the values of $\bar{a}_i$ for $i \geq k$ if $F(y) = 0$ has polynomial general solutions.

Lemma 6. *Let $F(y)$ be of the form (6) and $z = (-b/n^n a)x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ where a_i are indeterminants. Substituting y by z in $F(y)$, the coefficients of $x^{(n-1)^2+i-1}$ in $F(z)$ are of the following form*

$$(\frac{-b}{n^n a})^{n-2}(n-1-i)ba_i + h_i(a_{n-1}, \cdots, a_{i+1}), \quad \textit{for } i = n-2, \cdots, 0 \tag{9}$$

where $h_i(a_{n-1}, \cdots, a_{i+1})$ are the polynomials in $a_{n-1}, \cdots, a_{i+1}$.

Proof. Let $\mathcal{C}_i$ be the coefficient of $x^{(n-1)^2+i-1}$ in $F(z)$ for $i = 0, \cdots, n-2$ where

$$F(z) = az_1^n + bz^{n-1} + G(z, z_1).$$

As in the proof of Lemma 4, we define a weight w. Then $z = (-b/n^n a)x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is an isobaric polynomial with the weight n. Hence $z^{\alpha_j} z_1^{\beta_j}$ is still an isobaric polynomial with the weight $n\alpha_j + (n-1)\beta_j$. Now we consider $\mathcal{C}_i$. By computation, we know that the highest weight of the terms in $F(z)$ is $n(n-1)$. Hence the highest weight in $\mathcal{C}_i$ is not greater than $n - i$. So a_k can not appear in $\mathcal{C}_i$ for $k \leq i-1$ and if a_i appears in $\mathcal{C}_i$, then it must be linear and its coefficient must be constant. In the coefficients of $x^{(n-1)^2+i-1}$ in $az_1^n + bz^{n-1}$, the term in which a_i appears are $(\frac{-b}{n^n a})^{n-1} i n^n a a_i + (\frac{-b}{n^n a})^{n-2}(n-1)ba_i$. In the coefficients of $x^{(n-1)^2+i-1}$ in $G(z, z_1)$, since the weight of each term is less than $n - i$ (for $\mathrm{tdeg}(G) < n$), a_i can not appear. Therefore $\mathcal{C}_i$ has the form (9). ∎

5 A Polynomial-Time Algorithm

From the results in section 4, we have the following algorithm.

Algorithm 2. *The input is* $F(y)$. *The output is a polynomial general solution of* $F(y) = 0$ *if it exists.*

1. If $F(y)$ can be written as the form (6), then goto step 2. Otherwise, by Theorem 3, $F(y) = 0$ has no polynomial general solutions and the algorithm terminates.
2. Let $F(y)$ be of degree n in y_1. Let $\bar{a}_n = -\frac{b}{n^n a}$, $\bar{a}_{n-1} = 0$, $\bar{a}_i = -\frac{h_i(\bar{a}_{n-1},\cdots,\bar{a}_{i+1})}{(-b/n^n a)^{n-2}(n-1-i)b}$, $i = n-2, \cdots, 0$, where h_i are from Lemma 6. We have $\bar{a}_i \in \mathcal{C}$.
3. Let $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$. If $F(\bar{y}) \equiv 0$ then $\hat{y} = \sum_{i=0}^{n} \bar{a}_i (x+c)^i$ is a polynomial general solution of $F(y) = 0$. Otherwise, $F(y) = 0$ has no polynomial general solutions.

The correctness of Step 3 is due to the following facts. By Corollary 1, Lemmas 5 and 6, if $F(y) = 0$ has polynomial general solutions, then $\hat{y} = \sum_{i=0}^{n} \bar{a}_i (x+c)^i$ must be such a solution. By Lemma 2, to check wether $\hat{y}$ is a polynomial general solution we need only to check whether $\bar{y}$ is a solution of $F(y) = 0$.

Now we give some examples.

Example 3. Consider the differential polynomial:

$$F(y) = {y_1}^4 - 8\,{y_1}^3 + (6 + 24\,y)\,{y_1}^2 + 257 + 528\,y^2 - 256\,y^3 - 552\,y.$$

1. $F(y)$ can be written as the form:

   $$F(y) = {y_1}^4 - 256\,y^3 + G(y, y_1)$$

   where

   $$G(y, y_1) = -8\,{y_1}^3 + (6 + 24\,y)\,{y_1}^2 + 257 + 528\,y^2 - 552\,y,$$

   $tdeg(G) \leq 3$.
2. If $F(y) = 0$ has a polynomial general solution, then its degree is four and the coefficient of x^4 must be $a_4 = \frac{256}{4^4} = 1$.
3. Let $z = x^4 + a_2x^2 + a_1x + a_0$. Replacing y by z in $F(y)$ and collecting the coefficients of x^8, x^9, x^{10}, we obtain the following equations:

   $$\begin{aligned} &768\,a_2 + 528 - 384\,{a_2}^2 - 768\,a_0 = 0,\\ &-512 - 512\,a_1 = 0,\\ &384 - 256\,a_2 = 0. \end{aligned}$$

   Solving the above equations, we have $a_0 = \frac{17}{16}, a_1 = -1, a_2 = \frac{3}{2}$.

4. Let $\bar{y} = x^4 + \frac{3}{2}x^2 - x + \frac{17}{16}$. Substituting y by $\bar{y}$ in $F(y)$, $F(y)$ becomes zero. Hence a polynomial general solution of $F(y) = 0$ is

$$\bar{y} = (x+c)^4 + \frac{3}{2}(x+c)^2 - (x+c) + \frac{17}{16}.$$

In Step 2 of Algorithm 2, we need to compute $F(z)$ where $z = -\frac{b}{n^n a}x^n + a_{n-1}x^{n-1} + \cdots + a_0$ and a_i are indeterminants. A naive method of doing this evaluation is very costly. In order to give a polynomial-time algorithm, we need to give an efficient algorithm for Step 2. From Theorem 6, to compute the value of $\bar{a}_k$, we need only to compute $h_k(\bar{a}_{n-1}, \cdots, \bar{a}_{k+1})$. In other words, we need only to compute $F(\bar{z})$ where $\bar{z} = \sum_{k+1}^{n} \bar{a}_i x^i$ and $\bar{a}_i \in \mathcal{C}$. Moreover, we need only to compute the coefficient of $x^{(n-1)^2+k-1}$ in $F(\bar{z})$. To compute $F(\bar{z})$, we need to compute multiplication of two univariate polynomials which can be computed by the classical Karatsuba method ([21]).

Algorithm 3. *The inputs are $F(y)$ as the form (6) and $\bar{z} = \bar{a}_n x^n + \cdots + \bar{a}_0$ where $\bar{a}_i \in \mathcal{C}$. The output is the coefficient of $x^{(n-1)^2+k-1}$ in $F(\bar{z})$ for some k.*

1. Compute $\bar{z}^n$ and $\bar{z}_1^{n-1}$ where $\bar{z}_1$ is the derivative of $\bar{z}$ wrt x. We compute $\bar{z}^n$ step by step. That is, we compute $\bar{z}^2$ first, then compute the multiplication of $\bar{z}^2$ and $\bar{z}$, and so on. Note that, after we computed $\bar{z}^n$, we have also obtained $\bar{z}^i$ for $i < n$. For $\bar{z}_1^{n-1}$, we compute it in the same way.
2. Write $F(y)$ as the form: $F(y) = \sum_{i=0}^{n}(d_{0,i} + d_{1,i}y + \cdots + d_{n-i,i}y^{n-i})y_1^i$ where $d_{i,j} \in \mathcal{C}$.
3. For i from 0 to n, compute $p_i = d_{0,i} + d_{1,i}\bar{z} + \cdots + d_{n-i,i}\bar{z}^{n-i}$.
4. result:=0.
   For j from 0 to n
   For i from 0 to $(n-1)^2 + k - 1$
   result:=result+coeff$(p_j, x, i)*$coeff$(y_1^j, x, (n-1)^2 + k - 1 - i)$
   where coeff(p, x, k) means the coefficient of x^k in p.
5. return(result).

Example 4. Let $F(y)$ be as in Example 3 and $\bar{z} = x^4$. Now we compute the coefficient of x^{10} in $F(\bar{z})$.

1. $\bar{z} := x^4, \bar{z}^2 := x^8, \bar{z}^3 := x^{12}$.
   $\bar{z}_1 := 4x^3, \bar{z}_1^2 := 16x^6, \bar{z}_1^3 := 64x^9, \bar{z}_1^4 := 256x^{12}$.
2.

$$p_0 := 257 + 528\,\bar{z}^2 - 256\,\bar{z}^3 - 552\,\bar{z} = 257 - 552x^4 + 528x^8 - 256x^{12},$$
$$p_1 := 0, \quad p_2 := 6 + 24\bar{z} = 6 + 24x^4, \quad p_3 := -8, \quad p_4 := 1.$$

3. result:=coeff$(p_2, x, 4)$*coeff$(\bar{z}_1^2, x, 6)$=24*16=384. Because for other i, j, coeff(p_j, x, i)*coeff$(\bar{z}_1^j, x, 10 - i)$= 0.

Since multiplication is the dominant factor for the running time of the algorithm, we will use the number of multiplications of rational numbers to measure the complexity of the algorithm. In Algorithm 3, the complexity of Step 1 is $O(n^4)$. The complexity of Step 2 is $O(n^2)$. The complexity of Step 3 is $O(n^4)$. The complexity of Step 4 is $O(n^3)$. Hence the complexity of Algorithm 3 is $O(n^4)$.

Algorithm 4. *The inputs are $F(y)$ as the form (6) and $z = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ where a_i are interminates. The output is $\bar{a}_i$ for $i = n, \cdots, 0$ in Step 2 of Algorithm 2.*

1. Let $\bar{a}_n = -\frac{b}{n^n a}$, $\bar{a}_{n-1} = 0$.
2. Let $i = n - 2$.
   while $i \geq 0$ do
   (a) $\bar{y} := \bar{a}_n x^n + \cdots + \bar{a}_{i+1}x^{i+1}$.
   (b) C_i :=the coefficient of $x^{(n-1)^2+i-1}$ in $F(\bar{y})$ by Algorithm 3.
   (c) $\bar{a}_i := -\frac{C_i}{(-b/n^n a)^{n-2}(n-1-i)b}$.
   (d) $i := i - 1$.

Example 5. (Example 3 continued)

1. $n := 4, a := 1, b := -256$.
2. $\bar{a}_4 := 1, \bar{a}_3 := 0$.
3. $\bar{y} := x^4$. Substitute $\bar{y}$ into $F(y)$.
4. Then by Algorithm 3, the coefficient of x^{10} in $F(x^4)$ equals to 384. That is, $C_2 = 384$.
5. $\bar{a}_2 := -\frac{384}{-256} = \frac{3}{2}$ which equals to a_2 in Example 3. The other coefficients can be computed similarly.

It is easy to know that the complexity of Algorithm 4 is $O(n^5)$. In Step 3 of Algorithm 2, we verify whether $\bar{y}$ is a polynomial solution of $F(y) = 0$. If $\bar{y}$ is not a polynomial solution of $F(y) = 0$, that is $F(\bar{y}) \neq 0$, then $F(\bar{y})$ will be a polynomial in x with degree not greater than $n(n-1)$. Hence, if $F(\bar{y}) \neq 0$, then $F(\bar{y}) = 0$ as an equation in x has $n(n-1)$ roots at most. So we can verify it by numerical computation. If $F(\bar{y})(k) = 0$ for $k = -\frac{n(n-1)}{2}, -\frac{n(n-1)}{2}+1, \cdots, \frac{n(n-1)}{2}$, then $F(\bar{y}) = 0$. Otherwise, $F(\bar{y}) \neq 0$.

Algorithm 5. *The inputs are $F(y)$ as the form (6) and $\bar{y} = \sum_{i=0}^{n} \bar{a}_i x^i$ as in Algorithm 2. The output is "Yes" or "No" where "Yes" means $\bar{y}$ is a solution of $F(y) = 0$ and "No" means $\bar{y}$ is not a solution of $F(y) = 0$.*

1. Write $F(y)$ as the form: $F(y) = \sum_{j=0}^{n}(d_{0,j} + d_{1,j}y + \cdots + d_{n-j,j}y^{n-j})y_1^j$ where $d_{i,j} \in \mathcal{C}$.
2. For k from $-n(n-1)/2$ to $n(n-1)/2$
   (a) Substitute x^i by k^i in $\bar{y}$ and $\bar{y}_1$. Then we get the values of $\bar{y}$ and $\bar{y}_1$ at k, which are denoted by $\bar{y}(k)$ and $\bar{y}_1(k)$. Compute $\bar{y}_1(k)^i$ and $\bar{y}(k)^i$ for $i = 1 \cdots n$ in the same way as Step 1 of Algorithm 3.

(b) result:=0.
For j from 0 to n, compute $p_j(k) = d_{0,j} + d_{1,j}\bar{y}(k) + \cdots + d_{n-j,j}\bar{y}(k)^j$,
result:=result+$p_j(k)\bar{y}_1(k)^j$.
(c) If result$\neq 0$ then return(No).
3. return(Yes).

It is easy to check that the complexity of Algorithm 5 is $O(n^3)$. So we have the following theorem.

Theorem 4. *We can decide whether $F(y) = 0$ has a polynomial general solution and compute one if it exists with $O(n^5)$ multiplications of rational numbers.*

6 Conclusion

We have implemented the algorithms in Maple. The software is available at http://www.mmrc .iss.ac.cn/~xgao/software.html. In Table 1, we present the statistic results of running our algorithm for twenty differential equations, which could be found in [8]. We only give the total degrees and numbers of terms in these differential equations. In Table 1, F_i and G_i denote the differential equations. Here, the coefficients of F_i and G_j are integers. The coefficients of F_i are less than 10^6 but that of G_j may be very large. The running time is in seconds. The column of "solution" means whether they have a polynomial general solution or not. The running time is collected on a computer with Pentium 4, 2.66GHzCPU and 256M memory.

From the experimental results, we could conclude that the algorithm can be used to find polynomial solutions for very large ODEs efficiently. Recently, we have extended the method proposed in this paper to find rational and algebraic solutions of first order autonomous ODEs. It is interesting to see whether the result can be extended to the case when the coefficients of first order ODEs are not constant.

Table 1. Statistics on Algorithm2

	tdegree	term	time(s)	solution		tdegree	term	time(s)	solution
G_6	6	17	0.077	Y	F_6	6	22	0.063	N
G_7	7	22	0.125	Y	F_7	7	28	0.266	N
G_8	8	30	0.312	Y	F_8	8	37	1.141	N
G_9	9	38	1.468	Y	F_9	9	45	3.500	N
G_{10}	10	47	8.108	Y	F_{10}	10	55	10.656	N
G_{11}	11	57	16.062	Y	F_{11}	11	60	31.345	N
G_{12}	12	68	34.250	Y	F_{12}	12	74	70.438	N
G_{13}	13	80	78.203	Y	F_{13}	13	80	148.984	N
G_{14}	14	93	178.469	Y	F_{14}	14	90	273.065	N
G_{15}	15	106	306.250	Y	F_{15}	15	110	434.514	N

References

1. Boucher, D., About the Polynomial Solutions of Homogeneous Linear Differential Equations Depending on Parameters, *Proc. ISSAC1999*, 261-268, ACM Press, 1999.
2. Bronstein, M., On Solutions of Linear Ordinary Differential Equations in their Coefficient Field, *J. Symb. Comput.*, 13(4), 1992.
3. Barkatou, M. A., Pflgel, E., An Algorithm Computing the Regular Formal Solutions of a System of Linear Differential Equations, *J. Symb. Comput.*, 28(4-5), 569-587, 1999.
4. Cano, J., An Algorithm to Find Polynomial Solutions of $y' = R(x, y)$, private communication, 2003.
5. Carnicer, M.M., The Poincaré Problem in the Nondicritical Case, *Ann. of Math.*, 140, 289-294, 1994.
6. Cormier, O., On Liouvillian Solutions of Linear Differential Equations of Order 4 and 5, *Proc. ISSAC2001*, 93-100, ACM Press, 2001.
7. Cox, D., Little, J. and O'Shea, D., *Ideals, Varieties, and Algorithms*, Springer, New York, 1991.
8. Feng, R.Y. and Gao, X.S., Polynomial General Solution for First Order ODEs with Constant Coefficients, *MM Research Preprints*, No. 22, 24-29, 2003. (Available at http://www.mmrc.iss.ac.cn/pub/mm-pre.html)
9. Feng, R.Y. and Gao, X.S., Rational General Solutions of Algebraic Ordinary Differential Equations, *Proc. ISSAC2004*, 155-162, ACM Press, 2004.
10. Hubert, E., The General Solution of an Ordinary Differential Equation, *Proc. ISSAC1996*, 189-195, ACM Press, 1996.
11. Kean, C., Taylor Polynomial Solutions of Linear Differential Equations, *Appl. Math. Comput.*, V.142, Issue 1, Sep.20, 155-165, 2003.
12. Kolchin, E.R., *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1950.
13. Kovacic, J.J., An Algorithm for Solving Second Order Linear Homogeneous Differential Equations, *J. Symb. Comput.*, 2(1), 3-43, 1986.
14. Li, Z.M. and Schwarz, F., Rational Solutions of Riccati-like Partial Eifferential Equations, *J. Symb. Comput.*, 31(6), 691-716, 2001.
15. Poincaré, H., Sur L'intégration Algébrique des Équations Différentielles du Premier Ordre et du Premier Degré, *Rend. Circ. Mat. Palermo*, 11, 193-239, 1897.
16. Risch, R.H., The Problem of Integration in Finite Terms, *Trans. Amer. Math. Soc*, 139, 167-189, 1969.
17. Ritt, J.F., *Differential Algebra*, Amer. Math. Sco. Colloquium, New York, 1950.
18. Singer, M.F., Liouillian First Integrals of Differential Equations, *Trans. Amer. Math. Soc.*, 333(2), 673-688, 1992.
19. Ulmer, F. and Calmet, J., On Liouvillian Solutions of Homogeneous Linear Differential Equations, *Proc. ISSAC1990*, 236-243, ACM Press, 1990.
20. Van der Put, M. and Singer, M., *Galois Theory of Linear Differential Equations*, Springer, Berlin, 2003.
21. Winkler, F., *Polynomial Algorithm in Computer Algebra*, Spring Verlag, 1996.
22. Wu, W.T., *Mathematics Mechanization*, Science Press/Kluwer, Beijing, 2000.