Algebraic General Solutions of Algebraic Ordinary Differential Equations

J.M. Aroca and J. Cano
Department of Algebra, Geometry and Topology
Fac. Ciencias. Univ. de Valladolid
Valladolid 47011, Spain
(aroca,jcano)@agt.uva.es

R. Feng and X.S. Gao
Key Laboratory of Mathematics Mechanization
Institute of Systems Science, AMSS,
Academia Sinica, Beijing 100080, China
ryfeng@amss.ac.cn
xgao@mmrc.iss.ac.cn

ABSTRACT

In this paper, we give a necessary and sufficient condition for an algebraic ODE to have an algebraic general solution. For a first order autonomous ODE, we give an optimal bound for the degree of its algebraic general solutions and a polynomial-time algorithm to compute an algebraic general solution if it exists. Here an algebraic ODE means that an ODE given by a differential polynomial.

Categories and Subject Descriptors

I.1.2 [**SYMBOLIC AND ALGEBRAIC MANIPULATION**]: Algorithms—*Algebraic algorithms*

General Terms

Algorithms, Theory

Keywords

Algebraic general solution, algebraic differential equation, first order autonomous ODE, algebraic curve, Hermite-Padé approximants

1. INTRODUCTION

Finding the close form solution of an ODE can be traced back to the work of Liouville. For the algorithm consideration, the pioneer work is due to Risch. In [17, 18], Risch described a method to find the elementary integral of $\int udx$ where u is an elementary function. In Trager's Ph.D thesis [22], he gave a method to compute the integral of algebraic functions based on Risch's ideas. In [1], Bronstein generalized Trager's results to elementary functions. For higher order linear homogeneous ODEs, Kovacic presented an effective method to find the Liouvillian solutions for second order ODEs [14]. In [20], Singer established a general framework for finding the Liouvillian solutions for general linear homogeneous ODEs. Many other interesting results on finding the Liouvillian solutions of linear ODEs were reported in [2, 6, 23, 24].

Most of these results are limited to the linear case or some special type nonlinear equations. Work on finding closed form solutions for nonlinear differential equations is not as systematic as that for linear equations. With respect to the particular ODEs of the form $y' = R(x, y)$ where $R(x, y)$ is a rational function, Darboux and Poincaré made important contributions [16]. More recently, Cerveau, Carnicer and Corral et al also made important progresses [4, 3, 7]. In particular, Carnicer gave the degree bound of algebraic solutions in the nondicritical case. In [21], Singer studied the Liouvillian first integrals of differential equations. In [12], 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. In [9, 10], Feng and Gao gave a necessary and sufficient condition for an algebraic ODE to have a rational type general solution and a polynomial-time algorithm to compute a rational general solution if it exists.

In this paper, the idea proposed in [9] is generalized to compute algebraic function solutions. In Section 2, we give a sufficient and necessary condition for an algebraic ODE to have an algebraic general solution, by constructing a class of differential equations whose solutions are all algebraic functions. In Section 3, by treating the variable and its derivative as independent variables, a first order autonomous ODE defines a plane algebraic curve. Using the Riemann-Hurwitz formula, we give a degree bound of algebraic function solutions of the equation. This degree bound is optimal in the sense that there is a class of first order autonomous ODEs, whose algebraic function solutions reach this bound. In Section 4, based on the above results and the theory of Hermite-Padé approximants, we give a polynomial-time algorithm to find an algebraic general solution for a first order autonomous ODE.

A first order autonomous ODE $F(y, \frac{dy}{dx}) = 0$ can be reduced to the form $G(y, \frac{dx}{dy}) = 0$, where G is also a polynomial(see the section 3.2.1, (7)). Then to find the solution of $F = 0$, we may first find $x = \phi(y)$ as a function in y by computing the integral of an algebraic function, and then compute the inversion $y = \phi^{-1}(x)$. For an algebraic function $\phi(x)$ which satisfies $G(x, \phi(x)) = 0$, let $y = \int \phi(x)dx$ be the integral of $\phi(x)$. Then we have $G(x, \frac{dy}{dx}) = 0$. By the same way, $G(x, \frac{dy}{dx}) = 0$ can be converted into a first order autonomous ODE $F(x, \frac{dx}{dy}) = 0$. Then to find the integral y

ISSAC'05, July 24–27, 2005, Beijing, China.

of $\phi(x)$, we may first find $x = \varphi(y)$ by computing a solution of $F(x, \frac{dx}{dy}) = 0$ and then compute the inversion. Hence, our algorithm is equivalent to a polynomial-time algorithm for finding an algebraic integral for an algebraic function.

2. ALGEBRAIC GENERAL SOLUTIONS OF ALGEBRAIC ODES

2.1 Definition of algebraic general solutions

In the following, 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 $\mathbf{K}$. Let $\bar{\mathbf{Q}}$ be the algebraic closure of the rational number field $\mathbf{Q}$. 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 $\mathbf{K}\{y\}$. 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 $\mathbf{K}$, which vanishes every differential polynomial in Σ [19]. In this paper, we also assume that the universal extension field of $\mathbf{K}$ contains an infinite number of arbitrary constants. We will use $\mathcal{C}$ to denote the constant field of the universal extension field of $\mathbf{K}$.

Let $P \in \mathbf{K}\{y\} \setminus \mathbf{K}$. We denote by $\mathrm{ord}(P)$ the highest derivative of y in P, called the *order* of P. Let $o = \mathrm{ord}(P) > 0$. 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 $y, y_1, \ldots, y_{o-1}$ 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 an integer $k > 0$. 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 [13, 19]

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

where J is a product of certain powers of the initial and separant of Q and B_i, R are differential polynomials. Moreover, R is reduced with respect to Q. For a differential polynomial P of 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 $P \in \mathbf{K}\{y\}\setminus\mathbf{K}$ be an irreducible differential polynomial and

$$\Sigma_P = \{A \in \mathbf{K}\{y\} | SA \equiv 0 \bmod \{P\}\}, \tag{2}$$

where$\{P\}$ is the perfect differential ideal generated by P [13, 19]. Ritt proved that [19]

LEMMA 2.1. *Σ_P is a prime differential ideal and a differential polynomial Q belongs to Σ_P iff* $\mathrm{prem}(Q, P) = 0$.

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 [19].

As a consequence of Lemma 2.1, we have

LEMMA 2.2. *Let $F \in \mathbf{K}\{y\} \setminus \mathbf{K}$ be an irreducible differential polynomial with a generic solution η. Then for a differential polynomial P we have $P(\eta) = 0$ iff* $\mathrm{prem}(P, F) = 0$.

The following definition of the general solution is due to Ritt.

DEFINITION 2.3. *Let $F \in \mathbf{K}\{y\} \setminus \mathbf{K}$ be an irreducible differential polynomial. A* general solution *of $F = 0$ is defined as a generic zero of Σ_F. An* algebraic general solution *of $F = 0$ is defined as a general solution $\hat{y}$ which satisfies the following equation*

$$G(x, y) = \sum_{j=0}^{n} \sum_{i=0}^{m_j} a_{i,j} x^i y^j = 0 \tag{3}$$

where $a_{i,j}$ are in $\mathcal{C}$ and $\sum_{j=0}^{n} \sum_{i=0}^{m_j} a_{i,j} x^i y^j$ is irreducible in $\mathcal{C}[x, y]$. When $n = 1$, $\hat{y}$ is called a rational general solution *of $F = 0$.*

For algebraic solutions of a differential equation $F = 0$, we have the following lemma.

LEMMA 2.4. *Let $G(y) \in \mathcal{C}(x)[y]$ and irreducible in $\bar{\mathcal{C}}(x)[y]$ where $\bar{\mathcal{C}}$ is the algebraic closure of $\mathcal{C}$. If one solution of $G(y) = 0$ is a solution of $F = 0$, then every solution of $G(y) = 0$ is the solution of $F = 0$.*

PROOF. Since $G(y)$ is irreducible in $\bar{\mathcal{C}}(x)[y]$, every solution of $G(y) = 0$ is a generic zero of $G(y) = 0$. By Lemma 2.2, $\mathrm{prem}(F, G) = 0$. That is,

$$S^k I^l F = PG' + QG \tag{4}$$

where $S = \frac{\partial G}{\partial y}$, I is the initial of G and $k, l \in \mathbb{Z}$. Since every solution of $G(y) = 0$ is a generic zero, S or I do not vanish at it. Hence every solution of $G(y) = 0$ is a solution of $F = 0$. ∎

A general solution of $F = 0$ is usually defined as a family of solutions with o independent parameters in a loose sense where $o = \mathrm{ord}(F)$. The definition given by Ritt is more precise. Theorem 6 in Section 12, Chapter 2 in [13] tells us that Ritt's definition of general solutions is equivalent to the definition in the classical literature.

2.2 A criterion for existence of algebraic general solutions

For non-negative integers h, α, k, let $\mathcal{A}_{(h,\alpha;k)}(y)$ be the following $(h+1) \times (\alpha+1)$ matrix:

$$\begin{pmatrix} \binom{k+1}{0} y_{k+1} & \binom{k+1}{1} y_k & \cdots & \binom{k+1}{\alpha} y_{k+1-\alpha} \\ \binom{k+2}{0} y_{k+2} & \binom{k+2}{1} y_{k+1} & \cdots & \binom{k+2}{\alpha} y_{k+2-\alpha} \\ \vdots & \vdots & \cdots & \vdots \\ \binom{k+h+1}{0} y_{k+h+1} & \binom{k+h+1}{1} y_{k+h} & \cdots & \binom{k+h+1}{\alpha} y_{k+h+1-\alpha} \end{pmatrix}.$$

Let $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha_0 \in \mathbb{Z}_{\geq 0}$ where $\mathbb{Z}_{\geq 0}$ means the set of non-negative integers. Let $\mathcal{A}_{(\alpha_0;\underline{\alpha})}(y)$ be the $(h+1) \times (h+1)$ matrix

$$(\mathcal{A}_{(h,\alpha_1;\alpha_0)}(y) | \mathcal{A}_{(h,\alpha_2;\alpha_0)}(y^2) | \cdots | \mathcal{A}_{(h,\alpha_n;\alpha_0)}(y^n))$$

where $n + \alpha_1 + \cdots + \alpha_n = h + 1$. Let $\mathcal{D}_{(\alpha_0;\underline{\alpha})}$ be the determinant of $\mathcal{A}_{(\alpha_0;\underline{\alpha})}(y)$. Note that if $n = 1$, $\mathcal{D}_{(\alpha_0,\underline{\alpha})}$ is just equal to $\mathcal{D}_{n,m}$ in [9].

LEMMA 2.5. *An element $\bar{y}$ in the universal extension of* $\mathbf{K}$ *is a solution of* $\mathcal{D}_{(\alpha_0;\underline{\alpha})} = 0$ *iff it satisfies the equation (3) with* $m_j \leq \alpha_j$ *for* $j = 0, \cdots, n$.

PROOF. Assume that $\bar{y}$ satisfies the equation (3) with $m_j \leq \alpha_j$ where $j = 0, \cdots, n$. Then we have

$$\sum_{j=1}^{n} \sum_{i=0}^{\alpha_j} a_{i,j} (x^i \bar{y}^j)^{(\alpha_0+1)} = 0$$

where $(x^i \bar{y}^j)^{(\alpha_0+1)}$ means the (α_0+1)-th derivative of $x^i \bar{y}^j$ with respect to x and if $i > m_j$ then $a_{i,j} = 0$. Since $a_{i,j}$ are constants, $(x^i \bar{y}^j)^{(\alpha_0+1)}$ $(i = 0, \cdots, \alpha_j, j = 1, \cdots, n)$ are linearly dependent over $\mathcal{C}$. That is, the Wronskian determinant $W((x^i \bar{y}^j)^{(\alpha_0+1)})$ for $(x^i \bar{y}^j)^{(\alpha_0+1)}$ vanishes where $j = 0, \cdots, n, i = 0, \cdots, \alpha_j$ [19]. Then $\bar{y}$ satisfies the equation (3) with $m_j \leq \alpha_j$ iff $W((x^i \bar{y}^j)^{(\alpha_0+1)}) = 0$. By the computation process,

$$W((x^i \bar{y}^j)^{(\alpha_0+1)}) = \mathcal{D}_{(\alpha_0;\underline{\alpha})}(\bar{y}) * |\mathrm{diag}(B_0, \cdots, B_n)|$$

where $\mathrm{diag}(B_0, \cdots, B_n)$ is the diagonal matrix of B_j and

$$B_j = \begin{pmatrix} 1 & x & \cdots & x^{\alpha_j} \\ 0 & 1 & \cdots & \alpha_j x^{\alpha_j - 1} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & \alpha_j! \end{pmatrix}$$

for $j = 0, \cdots, n$. Hence $W((x^i \bar{y}^j)^{(\alpha_0+1)}) = 0$ if and only if $\mathcal{D}_{(\alpha_0;\underline{\alpha})}(\bar{y}) = 0$. ∎

By the above Lemma, we can prove the following criteria theorem easily.

THEOREM 2.6. *Let* F *be an irreducible differential polynomial. Then* $F = 0$ *has an algebraic general solution* $\hat{y}$ *iff there exist* $\underline{\alpha} = (\alpha_1, \cdots, \alpha_n) \in \mathbb{Z}^n_{\geq 0}$, $\alpha_0 \in \mathbb{Z}_{\geq 0}$ *such that* $\mathrm{prem}(\mathcal{D}_{(\alpha_0;\underline{\alpha})}, F) = 0$.

PROOF. ($\Rightarrow$) Let $\hat{y}$ be an algebraic general solution of $F = 0$ which satisfies the equation (3). Let $\underline{\alpha} = (m_1, m_2, \cdots, m_n)$ and $\alpha_0 = m_0$. Then from Lemmas 2.1, 2.2 and 2.5

$$\mathcal{D}_{(\alpha_0,\underline{\alpha})}(\hat{y}) = 0 \Rightarrow \mathcal{D}_{(\alpha_0,\underline{\alpha})} \in \Sigma_F \Rightarrow \mathrm{prem}(\mathcal{D}_{(\alpha_0,\underline{\alpha})}, F) = 0.$$

($\Leftarrow$) $\mathrm{prem}(\mathcal{D}_{(\alpha_0,\underline{\alpha})}, F) = 0$ implies that $\mathcal{D}_{(\alpha_0,\underline{\alpha})} \in \Sigma_F$ by Lemma 2.1. Then all the zeros of Σ_F must satisfy the equation (3). In particular, the generic zero of Σ_F satisfies the equation (3). ∎

Given an algebraic differential equation $F = 0$, if we know the degree bound of the equation (3) with respect to x and y which perhaps defines an algebraic general solution of $F = 0$, then we can decide whether it has an algebraic general solution by computing $\mathrm{prem}(\mathcal{D}_{(\alpha_0,\underline{\alpha})}, F)$ step by step. However for ODEs of order greater than one or with variate coefficients, we do not know this bound. Even for the case $y' = \frac{P(x,y)}{Q(x,y)}$ where $P(x,y), Q(x,y) \in \mathbf{Q}[x,y]$, we have no effective method to get the bound [3, 16]. In the following, for the first order autonomous ODEs, we give a degree bound for algebraic function solutions.

3. DEGREE BOUND FOR FIRST ORDER AUTONOMOUS ODES

In the following, we will always assume that $F = 0$ is a first order autonomous ODE in $\mathbf{Q}\{y\}$ and irreducible in $\bar{\mathbf{Q}}\{y\}$ and $G(x,y) \in \bar{\mathbf{Q}}[x,y]$ which is irreducible. We say $G(x,y)$ is *nontrivial* if $\deg(G,x) > 0$ and $\deg(G,y) > 0$. From now on, we always assume that $G(x,y)$ is nontrivial. When we say that $G(x,y) = 0$ *is an algebraic solution of* $F = 0$, we mean that one of the algebraic functions $\hat{y}(x)$ defined by $G(x, \hat{y}(x)) = 0$ is a solution of $F = 0$.

3.1 Structure for algebraic general solutions

It is a trivial fact that for an autonomous ODE, the solution set is invariant by a translation of the independent variable x. Moreover, we have the following fact.

LEMMA 3.1. *Let* $G(x,y) = 0$ *be an algebraic solution of* $F = 0$. *Then* $G(x+c, y) = 0$ *is an algebraic general solution of* $F = 0$, *where* c *is an arbitrary constant.*

PROOF. Assume that $\bar{y}(x)$ is a formal power series solution of $G(x,y) = 0$. Then $\bar{y}(x+c)$ will be a solution of $G(x+c, y) = 0$. Because $\bar{y}(x)$ is a solution of $F = 0$, $\bar{y}(x+c)$ is still a solution of $F = 0$. Hence $G(x+c, y) = 0$ is an algebraic solution of $F = 0$. For any $T \in \mathbf{K}\{y\}$ satisfying $T(\bar{y}(x+c)) = 0$, let $R = \mathrm{prem}(T, F)$. Then $R(\bar{y}(x+c)) = 0$. Suppose that $R \neq 0$. Since F is irreducible and $\deg(R, y_1) < \deg(F, y_1)$, there are two differential polynomials $P, Q \in \mathbf{K}\{y\}$ such that $PF + QR \in \mathbf{K}[y]$ and $PF + QR \neq 0$. Thus $(PF+QR)(\bar{y}(x+c)) = 0$. Because $\bar{y}(x+c) \notin \bar{\mathbf{Q}}$ and c is an arbitrary constant which is transcendental over $\mathbf{K}$, we have $PF + QR = 0$, a contradiction. Hence $R = 0$ which means that $T \in \Sigma_F$. So $\bar{y}(x+c)$ is a generic zero of Σ_F. Hence $G(x+c, y) = 0$ is an algebraic general solution. ∎

Lemma 3.1 reduces the problem of finding an algebraic general solution to the problem of finding a nontrivial algebraic solution. In what follows, we will show how to find a nontrivial algebraic solution in $\bar{\mathbf{Q}}[x,y]$. First of all, we decide the degree of an algebraic solution.

3.2 Degree bound of an algebraic solution

Assume that $G(x,y) = 0$ is an algebraic solution of the differential equation $F = 0$. In this subsection, we will give a bound for $\deg(G,x)$ and $\deg(G,y)$. First, we introduce some concepts concerning the algebraic function fields in one variable.

DEFINITION 3.2. $\bar{\mathbf{Q}}(x,\alpha)$ *is called an algebraic function field in one variable, if* x *is transcendental over* $\bar{\mathbf{Q}}$ *and* α *is algebraic over* $\bar{\mathbf{Q}}(x)$ *[11].*

An irreducible algebraic curve $G(x,y) = 0$ where $G(x,y) \in \bar{\mathbf{Q}}[x,y]$ corresponds to an algebraic function field $\bar{\mathbf{Q}}(\alpha,\beta)$ which is unique under an isomorphism where α, β satisfies $G(\alpha,\beta) = 0$ and α or β is transcendental over $\bar{\mathbf{Q}}$. It is well known that two algebraic curves with isomorphic function fields have the same genus.

3.2.1 Parametrization of a curve

Let $\bar{\mathbf{Q}}((t))$ be the quotient field of the ring of formal power series $\bar{\mathbf{Q}}[[t]]$. Let $G(x,y)$ be a nontrivial irreducible polynomial in $\bar{\mathbf{Q}}[x,y]$. If $x(t), y(t) \in \bar{\mathbf{Q}}((t))$ satisfy $G(x(t), y(t)) = 0$, we say that they are the coordinates of a *parametrization* provided $x(t)$ or $y(t)$ does not belong to $\bar{\mathbf{Q}}$. There exist $x_0, y_0 \in \bar{\mathbf{Q}}$, nonzero integers q and p, and units $u(t), v(t)$ in $\bar{\mathbf{Q}}[[t]]$, such that

$$\begin{aligned} x(t) - x_0 &= t^q\, u(t), \\ y(t) - y_0 &= t^p\, v(t). \end{aligned} \tag{5}$$

The *center* of the parametrization is the point $P \in \mathbb{P}^1 \times \mathbb{P}^1$ defined accordingly the following cases: (a) If $q > 0$ and $p > 0$, then $P = (x_0, y_0)$; (b) If $q > 0$ and $p < 0$, then $P = (x_0, \infty)$; (c) If $q < 0$ and $p > 0$, then $P = (\infty, y_0)$; (d) If $q < 0$ and $p < 0$, then $P = (\infty, \infty)$. If $p < 0$ (resp. $q < 0$) we agree to take $y_0 = 0$ (resp. $x_0 = 0$).

If there exists an integer $k \geq 2$ such that $x(t), y(t) \in \bar{\mathbf{Q}}((t^k))$, the parametrization will be called *reducible*, otherwise *irreducible*. If $\bar{t} \in \bar{\mathbf{Q}}[[t]]$ with order with respect to t greater than zero, then $x(\bar{t}), y(\bar{t})$ is another parametrization with the same center. If the order of $\bar{t}$ is equal to one, the two parametrizations will be said to be *equivalent*. An equivalence class of irreducible parametrizations will be called a *place* B of the curve $G = 0$ with center the center of one of its parametrizations. Two equivalent parametrizations have the same integers q and p as defined above. Then given a place B, we define nonzero integers $\nu_x(B)$ and $\nu_y(B)$ as the integers q and p of any of its irreducible parametrizations.

Let g be the genus of $G(x, y) = 0$ and $n = \deg(G, y)$. By the Riemann-Hurwitz formula [15] we have that

$$g = 1 - n + \frac{1}{2}\sum_B (|\nu_x(B)| - 1)$$

where B runs over all places of the curve $G = 0$.

Each place B with center (α, β) corresponds to exactly q_B fractional power series $y(x^{1/q_B})$ which are the solutions of $G(x, y(x)) = 0$. Let $\alpha \in \bar{\mathbf{Q}} \cup \{\infty\}$. Hence, by the Puiseux theorem we have that

$$\sum_B |\nu_x(B)| = \deg(G, y), \tag{6}$$

where the sum runs over all places B of the curve $G = 0$ with center (α, β).

LEMMA 3.3. *Let $G(x, y)$ be a nontrivial irreducible polynomial of $\bar{\mathbf{Q}}[x, y]$. Let $(x(t), y(t))$ be the coordinates of a parametrization $G = 0$. Then, for any nonzero constant $c \in \bar{\mathbf{Q}}$, $(x(t) + c, y(t))$ are not the coordinates of a parametrization of $G = 0$.*

PROOF. By Gauss's lemma, we know $G(x, y)$ is irreducible in $\bar{\mathbf{Q}}(y)[x]$. Since $y(t) \notin \bar{\mathbf{Q}}$, $\bar{\mathbf{Q}}(y(t))$ is isomorphic to $\bar{\mathbf{Q}}(y)$ which implies that $G(x, y(t)) \in \bar{\mathbf{Q}}(y(t))[x]$ is irreducible too. Now assume that $x(t)$ is a root of $G(x + c, y(t)) = 0$. Then we have $G(x, y(t))$ divides $G(x + c, y(t))$. It is clear that $\deg(G(x+c, y(t)), x) = \deg(G(x, y(t)), x)$ and $G(x, y(t))$ and $G(x + c, y(t))$ have the same leader coefficients. Hence, $G(x, y(t) = G(x + c, y(t))$. Since $c \neq 0$, we have that $\deg(G(x, y), x) = \deg(G(x, y(t)), x) = 0$, in contradiction with the nontriviality of $G(x, y)$. ∎

Now we are ready to give the degree bound of the algebraic solution of $F = 0$. First, we could determine the degree $\deg(G, x)$ exactly from the degree of F.

THEOREM 3.4. *Let $G(x, y) \in \bar{\mathbf{Q}}[x, y]$ be irreducible and let $G(x, y) = 0$ be an algebraic solution of $F = 0$. Then we have*

$$\deg(G, x) = \deg(F, y_1).$$

PROOF. Assume that $\deg(G, x) = s$ and $\deg(F, y_1) = d$. Let us write

$$\begin{aligned} G(x, y) &= A_0(y) + A_1(y)x + \cdots + A_s(y)x^s, \\ F &= F_0(y) + F_1(y)y_1 + \cdots + F_d(y)y_1^d \end{aligned}$$

where $A_i(y), F_j(y) \in \bar{\mathbf{Q}}[y]$. We use $\mathrm{Res}(A, B, z)$ to denote the Sylvester-resultant of A and B with respect to z and $\mathcal{Z}$ stands for "the zero set of". Let $S = \mathcal{Z}(A_s(y)) \cup \mathcal{Z}(F_d(y)) \cup \mathcal{Z}(\mathrm{Res}(G, \frac{\partial G}{\partial x}, x)) \cup \mathcal{Z}(\mathrm{Res}(G, \frac{\partial G}{\partial y}, x)) \cup \mathcal{Z}(\mathrm{Res}(F, \frac{\partial F}{\partial y_1}, y_1))$. Then S is a finite set. Hence we can choose a $c \in \bar{\mathbf{Q}}$ such that $c \notin S$. Then we have the following results:

(a) the set $\{z \in \bar{\mathbf{Q}} | F(c, z) = 0\} = \{z_1, z_2, \cdots, z_d\}$ has exactly d elements;

(b) the set $\{x \in \bar{\mathbf{Q}} | G(x, c) = 0\} = \{x_1, x_2, \cdots, x_s\}$ has exactly s elements;

(c) since $\frac{\partial G}{\partial y}(x_i, c) \neq 0$, there exists a unique formal power series

$$\varphi_i(x) = c + g_{i,1}(x - x_i) + g_{i,2}(x - x_i)^2 + \cdots$$

such that $G(x, \varphi_i(x)) = 0$ for each $i = 1, \cdots, s$.

From Lemma 2.4, $\varphi_i(x)$ is a solution of $F = 0$. Then we have $F(\varphi_i(x), \varphi_i'(x)) = 0$ which implies that $F(c, g_{i,1}) = 0$. Suppose that $s > d$. Then there exist at least two of $g_{i,1}$ which are equal to each other. Without lost of generalization, assume that $g_{1,1} = g_{2,1} = c_1$. Since $\frac{\partial F}{\partial y_1}(c, c_1) \neq 0$, there exists only one solution $\varphi(x)$ of $F(y, y_1) = 0$ such that $\varphi(0) = c$ and $\varphi'(0) = c_1$. Hence $\varphi_1(x) = \varphi_2(x + x_2 - x_1) = \varphi(x - x_1)$. So $(x, \varphi_1(x))$ and $(x + x_2 - x_1, \varphi_1(x))$ are two coordinates of a parametrizations of $G = 0$. This is a contradiction by the above lemma. Hence $s \leq d$. Let $G' = y_1 \frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}$ and $H(y, y_1) = \mathrm{Res}(G, G', x)$. Then

$$H(y, y_1) = y_1^s \mathrm{Res}(G, \frac{\partial G}{\partial y}, x) + \text{terms of lower order in } y_1.$$

Since $\mathrm{Res}(G, \frac{\partial G}{\partial y}, x) \neq 0$, we have $\deg(H, y_1) = s$. Assume that $\bar{y}(x)$ is a solution of $G(x, y) = 0$. Then we have $H(\bar{y}(x), \bar{y}'(x)) = F(\bar{y}(x), \bar{y}'(x)) = 0$. Because F is irreducible, we have that $\deg(H, y_1) \geq \deg(F, y_1)$. In the other words, $s \geq d$. ∎

Since F is first order and autonomous, we can regard $F = 0$ as an algebraic curve and we will use $F(y, y_1)$ to denote F.

LEMMA 3.5. *Assume that $G(x, y) = 0$ is an algebraic solution of $F = 0$. Then the genus of $G(x, y) = 0$ equals to that of $F(y, y_1) = 0$.*

PROOF. Let α satisfy $G(x, \alpha) = 0$. It is clear that α is transcendental over $\bar{\mathbf{Q}}$. Then $\bar{\mathbf{Q}}(x, \alpha)$ and $\bar{\mathbf{Q}}(\alpha, \alpha')$ are the algebraic function fields of $G(x, y) = 0$ and $F(y, y_1) = 0$ respectively. We only need to prove $\bar{\mathbf{Q}}(x, \alpha) = \bar{\mathbf{Q}}(\alpha, \alpha')$. From Theorem 3.4, we have $[\bar{\mathbf{Q}}(x, \alpha) : \bar{\mathbf{Q}}(\alpha)] = [\bar{\mathbf{Q}}(\alpha, \alpha') : \bar{\mathbf{Q}}(\alpha)]$. Since $G(x, \alpha) = 0$, $\alpha' = -\frac{\partial G}{\partial x}(x, \alpha)/\frac{\partial G}{\partial y}(x, \alpha)$. which implies that $\alpha' \in \bar{\mathbf{Q}}(x, \alpha)$. Hence $\bar{\mathbf{Q}}(x, \alpha) = \bar{\mathbf{Q}}(\alpha, \alpha')$. ∎

For convenience, we consider a new differential equation

$$\bar{F}(x_1, y) = x_1^{\deg(F, y_1)} F(y, \frac{1}{x_1}) = 0 \tag{7}$$

where $x_1 = \frac{dx}{dy} = \frac{1}{y_1}$. $\bar{F}$ is irreducible in $\bar{\mathbf{Q}}[x_1, y]$ and $\deg(\bar{F}, y) = \deg(F, y)$, $\deg(\bar{F}, x_1) = \deg(F, y_1)$. Then we have the following lemma.

LEMMA 3.6. *Let $\bar{F}$ be defined as in (7) and $G(x, y) = 0$ an algebraic solution of $F = 0$. Then $G(x, y) = 0$ also defines an algebraic function (in y) solution of $\bar{F}(x_1, y) = 0$.*

PROOF. From the proof of Theorem 3.4, we know that

$$\mathrm{Res}(G, G', x) = A(y)F(y, y_1)$$

where $G' = y_1 \frac{\partial G}{\partial y} + \frac{\partial G}{\partial x}$. In the other words, there exist two polynomials $P, Q \in \bar{\mathbf{Q}}[x, y, y_1]$ such that $PG + QG' = A(y)F(y, y_1)$. Replacing y_1 by $\frac{1}{x_1}$ and multiplying some power of x_1, we have

$$\bar{P}G + \bar{Q}(\frac{\partial G}{\partial y} + x_1 \frac{\partial G}{\partial x}) = x_1^k A(y)\bar{F}(x_1, y) \tag{8}$$

where $\bar{P}, \bar{Q} \in \bar{\mathbf{Q}}[x, y, x_1]$ and $k \in \mathbb{Z}_{\geq 0}$. Suppose that β satisfies $G(\beta, y) = 0$. Replacing x by β and x_1 by β' in (8) where $\beta' = \frac{d\beta}{dy}$, we have that $\bar{F}(\beta', y) = 0$. Hence $G(x, y) = 0$ is an algebraic solution of $\bar{F} = 0$. ∎

LEMMA 3.7. *Let $(x(t), y(t))$ be an irreducible parametrization of $G = 0$. Then $(\frac{x'(t)}{y'(t)}, y(t))$ is an irreducible parametrization of $\bar{F}(x_1, y) = 0$.*

PROOF. Let us denote $x_1(t) = \frac{x'(t)}{y'(t)}$ where $'$ means the derivative with respect to t. Since $x_1(t) = \frac{dx}{dy}(t)$, we have $\bar{F}(x_1(t), y(t)) = 0$. Assume that $(x_1(t), y(t))$ is a reducible parametrization. Let $k \geq 2$, such that $x_1(t), y(t) \in \bar{\mathbf{Q}}((t^k))$. Then $x_1(t)y'(t) = \sum_{j \geq j_0} c_j t^{kj-1}$. Since $x'(t) = x_1(t)y'(t)$, then we have that $c_0 = 0$ and $x(t) = c + \sum_{j \geq j_0} \frac{c_j t^{kj}}{kj}$, for some constant c. Hence we get a contradiction because $x(t), y(t) \in \bar{\mathbf{Q}}((t^k))$. ∎

THEOREM 3.8. *Assume that $G(x, y) = 0$ is a nontrivial algebraic solution of $F = 0$. Then we have that*

$$\deg(G, y) \leq \deg(F, y) + \deg(F, y_1).$$

PROOF. Let $\bar{F}$ be as in (7). Let g_G and $g_{\bar{F}}$ be the genus of $G(x, y) = 0$ and $\bar{F}(x_1, y) = 0$ respectively. Let B be a place of $G = 0$ with center $P = (\alpha, \beta)$. Let $(x(t), y(t))$ be an irreducible parametrization of B. Let us denote by $\tilde{B}$ the place of the algebraic curve $\bar{F}(x_1, y) = 0$ given by the irreducible parametrization $(x_1(t), y(t))$, where $x_1(t) = x'(t)/y'(t)$. Let $\tilde{P} = (\tilde{\alpha}, \tilde{\beta})$ be the center of $\tilde{B}$. It is obvious that $\nu_y(B) = \nu_y(\tilde{B})$ and $\beta = \tilde{\beta}$. If $\nu_x(B) \neq \nu_y(B)$ then we have that $\nu_{x_1}(\tilde{B}) = \nu_x(B) - \nu_y(B)$. Hence, if $\nu_x(B) > \nu_y(B)$, then $\tilde{\alpha} = 0$; if $\nu_x(B) < \nu_y(B)$, then $\tilde{\alpha} = \infty$; if $\nu_x(B) = \nu_y(B)$, then $\tilde{\alpha} \in \bar{\mathbf{Q}}$.

The map that sends each place B of $G = 0$ to the place $\tilde{B}$ of $\bar{F} = 0$ is injective. Let B and B' be two places of $G = 0$ such that $\tilde{B} = \widetilde{B'}$. Let $(x(t), y(t))$ and $(z(t), v(t))$ be the parametrizations of B and B' respectively. We may assume that $y(t) = y_0 + t^p$ and $v(t) = v_0 + t^{p'}$ (see [26], Chap. 4, Theorem 2.2). Since $\tilde{B} = \widetilde{B'}$ we have that $p = p'$, $y(t) = v(t)$ and $x'(t) = z'(t)$. Hence $z(t) = x(t) + c$, for some constant c. By lemma 3.3 we have that $c = 0$, so $B = B'$.

By the Riemann-Hurwitz formula we have that

$$2(g_G + \deg(G, y) - 1) = \sum_B (|\nu_x(B)| - 1), \tag{9}$$

where B runs over all places of $G = 0$.

We will split the right hand side of the above equation in four cases: We say that $B \in (1)$ if $\nu_x(B) > 0$ and $\nu_y(B) > 0$; that $B \in (2)$ if $\nu_x(B) > 0$ and $\nu_y(B) < 0$; $B \in (3)$ if $\nu_x(B) < 0$ and $\nu_y(B) > 0$; and that $B \in (4)$ if $\nu_x(B) < 0$ and $\nu_y(B) < 0$. Moreover, we say that $B \in (1)'$ if $B \in (1)$ and $\nu_x(B) > \nu_y(B)$; and we say that $B \in (4)'$ if $B \in (4)$ and $\nu_x(B) < \nu_y(B)$. In the following inequalities B_x, B_y $\tilde{B}_{x_1}$ and $\tilde{B}_y$ will stand for $\nu_x(B)$, $\nu_y(B)$, $\nu_{x_1}(\tilde{B})$ and $\nu_y(\tilde{B})$ respectively.

For $k = 1$ and $k = 4$, we have that

$$\sum_{B \in (k)} (|B_x| - 1) \leq \sum_{B \in (k)'} |\tilde{B}_{x_1}| + \sum_{B \in (k)} (|B_y| - 1). \tag{10}$$

For $k = 2$ and $k = 3$, we have that

$$\sum_{B \in (k)} (|B_x| - 1) \leq \sum_{B \in (k)} |\tilde{B}_{x_1}|. \tag{11}$$

If $B \in (1)' \cup (2)$, then the center of $\tilde{B}$ is over $x_1 = 0$. If $B \in (3) \cup (4)'$, then the center of $\tilde{B}$ is over $x_1 = \infty$. Hence, using the formula (6), we have that

$$\sum_{B \in (1)', (2), (3), (4)'} |\tilde{B}_{x_1}| \leq 2 \deg(\bar{F}, y). \tag{12}$$

By the Riemann-Hurwitz formula, we have that

$$\sum_{B \in (1), (4)} (|\tilde{B}_y| - 1) \leq 2(g_{\bar{F}} + \deg(\bar{F}, x_1) - 1). \tag{13}$$

We remark that in the inequalities (12,13) we have used the fact that the map $B \mapsto \tilde{B}$ between the places of $G = 0$ and places of $\bar{F} = 0$ is injective. By the inequalities ((9)-(13)), we have that

$$2(g_G + \deg(G, y) - 1) \leq 2(g_{\bar{F}} + \deg(\bar{F}, x_1) + \deg(\bar{F}, y) - 1).$$

Using the above inequalities, and the facts that $\deg(\bar{F}, x_1) = \deg(F, y_1)$, $\deg(\bar{F}, y) = \deg(F, y)$ and that $g_G = g_{\bar{F}}$, gives the required inequality. ∎

The following example shows that the degree bound given in Theorem 3.8 is optimal.

EXAMPLE 3.9. *Assume that $n > m > 0$ and $(n, m) = 1$. Let $G(x, y) = y^n - x^m$ which is irreducible. We have that $G(x, y) = 0$ is an algebraic solution of $F = y^{n-m} y_1^m - (\frac{m}{n})^m = 0$. In this case, we have that* $\deg(G, y) = \deg(F, y) + \deg(F, y_1)$.

4. A POLYNOMIAL-TIME ALGORITHM

The simple degree bounds given in the preceding section allow us to give a polynomial-time algorithm to compute algebraic function solutions of a first order autonomous ODE.

4.1 Algebraic approximant

Algebraic approximant is a special type of Hermite-Padé approximant. It uses an algebraic function to approximate a given function.

DEFINITION 4.1. *Let $G(x, y)$ be an irreducible polynomial in $\bar{\mathbf{Q}}[x, y]$. An algebraic function $\bar{y}(x)$ satisfying $G(x, \bar{y}(x)) = 0$ is called an algebraic approximant to a function $f(x)$ if*

$$G(x, f(x)) = O(x^{(m+1)(n+1)-1})$$

where $m = \deg(G, x)$ and $n = \deg(G, y)$.

More generally, we will find $G(x, y)$ such that

$$G(x, f(x)) = O(x^{N+1}) \tag{14}$$

where N is a positive integer. We can get the coefficients of $G(x,y)$ with respect to x and y by solving linear equations. Let $G(x,y) = \sum_{j=0}^{n}\sum_{i=0}^{m} b_{i,j}x^i y^j$ and $f(x) = a_0 + a_1 x + \cdots + a_N x^N + O(x^{N+1})$. Let

$$M_0 = \begin{pmatrix} I_{(m+1)\times(m+1)} \\ \\ 0_{(N-m)\times(m+1)} \end{pmatrix} \tag{15}$$

where $I_{(m+1)\times(m+1)}$ is an $m+1$ unit square matrix and $0_{(N-m)\times(m+1)}$ is an $(N-m)\times(m+1)$ zero matrix. Let $M_i = TM^i * M_0$ for $i = 1, \cdots, n$ where

$$TM = \begin{pmatrix} a_0 & 0 & 0 & \cdots & 0 \\ a_1 & a_0 & 0 & \cdots & 0 \\ a_2 & a_1 & a_0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_N & a_{N-1} & a_{N-2} & \cdots & a_0 \end{pmatrix} \tag{16}$$

and a_i are the coefficients of $f(x)$. Then by the computation process, we can write (14) as the matrix form

$$(M_0|M_2|\cdots|M_n) \begin{pmatrix} B_0 \\ B_1 \\ \vdots \\ B_n \end{pmatrix} = 0 \ , \ B_i = \begin{pmatrix} b_{0,i} \\ b_{1,i} \\ \vdots \\ b_{m,i} \end{pmatrix} \tag{17}$$

for $i = 1, \cdots, n$.

Let $\bar{y}(x) = a_0 + a_1 x + \cdots$ be a formal power series. When we say $\varphi(x)$ is *the first* $N+1$ *terms* of $\bar{y}(x)$, we mean that $\varphi(x) = a_0 + a_1 x + \cdots + a_N x^N$. The following lemma will be used in our algorithm.

LEMMA 4.2. *Let $\bar{y}(x)$ be a formal power series such that $G(x,\bar{y}(x)) = 0$. Assume that $m = \deg(G,x)$ and $n = \deg(G,y)$. Let $\varphi(x)$ be the first $2mn+1$ terms of $\bar{y}(x)$. If $Q_0(x), Q_1(x), \cdots, Q_n(x) \in \bar{\mathbf{Q}}[x]$ such that*

$$Q_0(x) + Q_1(x)\varphi(x) + \cdots + Q_n(x)\varphi(x)^n = O(x^{2mn+1})$$

where $\deg(Q_i(x),x) \le m$ and not all of them are zero. Then

$$G(x,y) = \lambda(Q_0(x) + Q_1(x)y + \cdots + Q_n(x)y^n) \tag{18}$$

where $\lambda \in \bar{\mathbf{Q}}$ does not equal to zero.

PROOF. Let $Q(x,y) = Q_0(x) + Q_1(x)y + \cdots + Q_n(x)y^n$. There exist $S, T \in \bar{\mathbf{Q}}[x,y]$ such that

$$SG(x,y) + TQ(x,y) = \mathrm{Res}(G,Q,y) \tag{19}$$

where $\deg(S,y) < n$ and $\deg(T,y) < n$. If $Q(x,\bar{y}(x)) = 0$, then (18) is true. Assume that $Q(x,\bar{y}(x)) \neq 0$ and $\mathrm{Res}(G,Q,y) \neq 0$. Then it is not difficult to know that $\deg(\mathrm{Res}(G,Q,y),x) \le 2mn$. However, substituting $\bar{y}(x)$ to the left side of (19), the left side will become a series with order greater than $2mn$, a contradiction. Hence $\mathrm{Res}(G,Q,y) = 0$ which implies (18) is true, because $G(x,y)$ is irreducible. ∎

4.2 An algorithm to compute algebraic solutions

First, we give an algorithm to compute the first $N+1$ terms of a formal power series solution of $F = 0$ for a given positive integer N. Regarding $F = 0$ as an algebraic curve, find a point (z_0, z_1) on it such that the separant $S(y, y_1)$ of $F(y, y_1)$ does not vanish at (z_0, z_1). Then we can compute $y_i = z_i$ step by step from (1). Then $\bar{y}(x) = z_0 + z_1 x + \frac{z_2}{2!}x^2 + \cdots$ is a formal power series solution of $F = 0$. Moreover, if $z_1 \neq 0$, then $\bar{y}(x) \notin \bar{\mathbf{Q}}$.

ALGORITHM 4.3. *Input: $F = 0$ and a positive integer N. Output: the first $N+1$ terms of a formal power series solution of $F = 0$ which is not in $\bar{\mathbf{Q}}$.*

1. *Find a point $(z_0, z_1) \in \bar{\mathbf{Q}}^2$ on $F(y, y_1) = 0$ such that $S(z_0, z_1) \neq 0$ and $z_1 \neq 0$.*
2. *$i := 2$ and $\varphi(x) := z_0 + z_1 x$.*
3. *while $i \le N$ do*
   (a) *Replace y by $\varphi(x)$ and y_1 by $\varphi'(x)$ in $F(y, y_1)$.*
   (b) *$c :=$ the coefficient of x^{i-1} in $F(\varphi(x), \varphi'(x))$.*
   (c) *$z_i := -\frac{(i-1)!c}{S(z_0,z_1)}$ and $\varphi(x) := \varphi(x) + \frac{z_i x^i}{i!}$.*
   (d) *$i := i + 1$.*
4. *Return($\varphi(x)$).*

The correctness of the algorithm comes from the following facts. Let $\bar{y}(x)$ be a formal power series solution of $F = 0$. Then by (1),

$$(F(\bar{y}(x), \bar{y}_1(x)))^{(i-1)} = S\bar{y}_i(x) + R(\bar{y}(x), \cdots, \bar{y}_{i-1}(x)) = 0.$$

Since $\bar{y}_k(x)|_{x=0} = z_k$ for $k = 1, 2, \cdots$, we have that

$$S(z_0, z_1)z_i + R(z_0, \cdots, z_{i-1}) = 0.$$

Now assume that $\varphi(x) = z_0 + z_1 x + \cdots + \frac{z_{i-1}}{(i-1)!}x^{i-1}$. Then

$$(F(\varphi(x), \varphi'(x)))^{(i-1)} = R(\varphi(x), \cdots, \varphi^{(i-1)}(x)).$$

Since $\varphi^{(k)}(x)|_{x=0} = z_k$ for $k = 1, \cdots, i-1$ and $\varphi^i(x) = 0$, we have that

$$R(z_0, \cdots, z_{i-1}) = (F(\varphi(x), \varphi'(x)))^{(i-1)}|_{x=0}$$

which equals to $(i-1)!$ times the coefficient of x^{i-1} in $F(\varphi(x), \varphi'(x))$. Let $T = \mathrm{tdeg}(F)$, the total degree of F. Theorem 9 given in [9] shows that the number of the points on $F(y, y_1) = 0$ which make $S(y, y_1)$ or y_1 vanish is at most T^2.

The complexity of Algorithm 4.3 is polynomial in terms of the number of multiplications in $\mathbf{Q}$ needed in the algorithm. In Step 1, we can find a point (z_0, z_1) as follows. We may replace y by the integers $z_0 = 0, \pm 1, \cdots \pm \lceil \frac{T^2}{2} \rceil$ where $T = \mathrm{tdeg}(F)$ and let $L(y_1)$ be a monic irreducible factor of $F(z_0, y_1) \in \mathbf{Q}[y_1]$. We may take z_1 to be a root of $L(y_1) = 0$. Since the number of the points which make $S(y, y_1)$ or y_1 vanish is at most T^2, there always exists an integer $z_0 \in \{0, \pm 1, \cdots \pm \lceil \frac{T^2}{2} \rceil\}$ such that the point (z_0, z_1) satisfies the assumption in Step 1. Hence the complexity of Step 1 is polynomial. Then all the procedures will be executed over the number field $\mathbf{Q}(z_1)$. Let $D = \deg(L(y_1)) \le T = \mathrm{tdeg}(F)$. Then any element of $\mathbf{Q}(z_1)$ can be represented as a polynomial in z_1 with degree $\le T-1$. Let $\beta, \gamma \in \mathbf{Q}(z_1)$. Then there exist $P(z), Q(z) \in \mathbf{Q}[z]$ such that $\beta = P(z_1), \gamma = Q(z_1)$ where $\deg(P) \le T-1, \deg(Q) \le T-1$. To compute $\phi = \beta * \gamma$, we need to compute $R = \mathrm{prem}(PQ, L)$. Therefore, a multiplication of two elements in $\mathbf{Q}(z_1)$ needs $O(T^2)$ multiplications of rational numbers. Since computing the inversion of β can also be done in $O(T^2)$, the division of two elements in $\mathbf{Q}(z_1)$ needs $O(T^2)$ multiplications of rational numbers too. In Step 3, the computation of $(a_0 + a_1 x + \cdots + a_N x^N)^T$ needs at most $O(N^2T^4)$ multiplications in $\mathbf{Q}(z_1)$, and hence at most $O(T^2 \cdot N^2T^4) = O(N^2T^6)$ multiplications in $\mathbf{Q}$.

Now we can give the algorithm to compute an algebraic solution of $F = 0$.

ALGORITHM 4.4. *Input: $F = 0$. Output: an algebraic solution of $F = 0$ if it exists.*

1. $d := \deg(F, y_1)$ and $e := \deg(F, y)$.
2. $k := 1$.
   while $k \leq d + e$ do
   (a) Compute the first $2dk+1$ terms $\varphi(x)$ of a formal power series solution of $F = 0$ by Algoritm 4.3.
   (b) $a_i :=$ the coefficient of x^i in $\varphi(x)$ for $i = 0, \cdots, 2dk$.
   (c) In (15) and (16), let $m = d, n = k$ and $N = 2dk$. We construct the linear equations (17).
   (d) If (17) has no nonzero solution or the dimension of the solution space of (17) is great than one, then go to Step (i).
   (e) Otherwise, choose one of nonzero solutions $\bar{b}_{i,j}$ where $i = 0, \cdots, d$ and $j = 0, \cdots, k$.
   (f) $G(x, y) := \sum_{j=0}^{k} \sum_{i=0}^{d} \bar{b}_{i,j} x^i y^j$, $S := \frac{\partial G}{\partial y}$ and $I :=$ the initial of $G(x, y)$.
   (g) If $\mathrm{GCD}(G, S) \neq 1$ or $\mathrm{GCD}(G, I) \neq 1$, then go to Step (i). Otherwise, go to next step.
   (h) Let $R = \mathrm{prem}(F, G)$.
   If $R = 0$, then return$(G(x, y) = 0)$.
   (i) $k := k + 1$.
3. If the algorithm does not return $G(x, y) = 0$ in Step 2, $F = 0$ has no algebraic solution and the algorithm terminates.

From Theorem 2.6 and Lemma 2.5, we know that if $F = 0$ has a nontrivial algebraic solution, then every formal power series solution is algebraic. From Lemma 4.2, we only need to compute the first $2dk + 1$ terms of a nontrivial formal power series solution to construct the algebraic approximant. From Theorems 3.4, 3.8, if $F = 0$ has an algebraic solution $G(x, y) = 0$, then there is a k which satisfies that $k \geq 1$ and $k \leq d + e$ such that $\deg(G, x) = d$ and $\deg(G, y) = k$. From Lemma 4.2 again, the dimension of the solution space of (17) equals to one. If $G(x, y) = 0$ is an algebraic solution, then $G(x, y)$ is irreducible. Then it is obvious that $\mathrm{GCD}(G, S) = 1$ and $\mathrm{GCD}(G, I) = 1$. Now assume that $\mathrm{GCD}(G, S) = 1$, $\mathrm{GCD}(G, I) = 1$ and $\mathrm{prem}(F, G) = 0$. We will prove that $G(x, y)$ is irreducible. Suppose that $k = h$. Then $G(x, y)$ can not have a factor $u(x) \in \bar{\mathbf{Q}}[x]$, because $\mathrm{GCD}(G, I) = 1$. If $G(x, y) = g(y) \in \bar{\mathbf{Q}}[y]$, then by (14), $g(\varphi(0)) = 0$ and $g'(\varphi(0))\varphi'(0) = 0$. Since $\varphi'(0) = z_1 \neq 0$ and $g'(y) = S$, we have $\mathrm{GCD}(G, S) \neq 1$. Hence $G(x, y) \notin \bar{\mathbf{Q}}[y]$. If $G(x, y)$ is reducible, then $G(x, y)$ has an irreducible factor $\tilde{G}(x, y)$ which is nontrivial and $\deg(\tilde{G}, y) < h$. Since $\mathrm{GCD}(G, S) = 1$, $\mathrm{GCD}(G, I) = 1$ and $\mathrm{prem}(F, G) = 0$, by (4), $\tilde{G}(x, y) = 0$ is an algebraic solution of $F = 0$. Hence, we would have got $\tilde{G}(x, y)$ when k was less than h and the algorithm must terminate before $k = h$, a contradiction with the assumption $k = h$. So $G(x, y)$ is irreducible and $G(x, y) = 0$ is an algebraic solution.

The complexity of Algorithm 4.4 is polynomial in T where $T = \mathrm{tdeg}(F)$. In Step 2(a), the complexity is polynomial. In Step 2(c), we need only to compute $TM^{2T} * M_0$ which needs $O(T^8)$, because TM is an $l \times l$ matrix with $l \leq 2T^2 + 1$ and M_0 is a $p \times q$ matrix with $p \leq 2T^2 + 1, q \leq T + 1$. (Note that in the worst case, we have to do the operations over $\mathbf{Q}(z_1)$. Hence the complexity has to increase by $O(T^2)$.) In Step 2(d), we need only to solve at most $4T^2 + 1$ linear equations with at most $2T^2 + 3T + 1$ variables. Hence its complexity is polynomial. In Step 2(g), from ([25],p152), $\mathrm{GCD}(G, S)$ and $\mathrm{GCD}(G, I)$ can be computed in $O(T^6)$. In Step 2(h), for deciding whether $\mathrm{prem}(F, G) = 0$, we compute $R_1 = \mathrm{prem}(F, G')$ first. Since $R_1 = (\frac{\partial G}{\partial y})^k F(y, -\frac{\partial G}{\partial x}/\frac{\partial G}{\partial y})$ where $k \leq T$, we can compute it in $O(T^{12})$ and have that $\deg(R_1, x) \leq 2T^2$ and $\deg(R_1, y) \leq 4T^2 + T$. Then we compute the $\mathrm{GCD}(R_1, G)$ which can be computed in $O(T^{10})$. If $\mathrm{GCD}(R_1, G) = G$, then $\mathrm{prem}(F, G) = 0$; otherwise $\mathrm{prem}(F, G) \neq 0$. The number of the circulation in Step 2 is at most $2T$. Hence the complexity of Step 2 is also polynomial.

EXAMPLE 4.5. *Consider*

$$F = (y^6+2y+1)y_1^3-(12y^5+9y^4-1)y_1^2+27y^8+54y^7+27y^6+4y^3.$$

1. *Let $d = 3$ and $e = 8$.*
2. *For the case $k = 1$, we get a $G(x, y) = 0$ which is not the solution of $F = 0$. Here we only give the process in the case $k = 2$.*
3. *The first 13 terms of the formal power series solution of $F = 0$ is*

$$\varphi(x) = 1 - 2x + \frac{5}{2}x^2 - \frac{9}{4}x^3 + \frac{1}{2}x^4 + \frac{5}{4}x^5 - \frac{41}{32}x^6 - \frac{65}{64}x^7 + \frac{363}{128}x^8 - \frac{111}{256}x^9 - \frac{2545}{512}x^{10} + \frac{5141}{1024}x^{11} + \frac{5891}{1024}x^{12}.$$

4. *Let $m = 3, n = 2$ and $N = 12$. We construct the linear equations (17). Solving it, we get a nonzero solution*

$$(-1, 1, 0, 0, 0, 3, -3, 1, 1, 0, 0, 0).$$

5. *Let $G(x, y) = -1 + x + 3xy - 3x^2y + x^3y + y^2$ and $S = 2y + 3x - 3x^2 + x^3$, $I = 1$.*
6. *We have $GCD(G, S) = 1$ and $GCD(G, I) = 1$.*
7. *$prem(F, G) = 0$. Hence $G(x, y) = -1 + x + 3xy - 3x^2y + x^3y + y^2 = 0$ is an algebraic solution of $F = 0$.*

5. REFERENCES

[1] Bronstein, M., Integration of elementary functions, *J. Symb. Comput.*, 9, 117-173, 1990.

[2] Bronstein, M. and Lafaille, S., Solutions of linear ordinary differential equations in terms of special functions, *Proc. ISSAC2002*, ACM Press, 2002.

[3] Carnicer, M.M., The Poincaré problem in the nondicritical case, *Ann. of Math.*, 140, 289-294, 1994.

[4] Cerveau, D. and Lins Neto, A., Holomorphic foliations in $\mathbb{C}P(2)$ having an invariant algebraic curve, *Ann. Inst. Fourier*, 41(4), 883-903, 1991.

[5] Cormier, O., Singer, M.F., Trager, B.M. and Ulmer, F., Linear differential operators for polynomial equations, *J. Symb. Comput.*, 34, 355-398, 2002.

[6] Cormier, O., On Liouvillian solutions of linear differential equations of order 4 and 5, *Proc. ISSAC2001*, 93-100, ACM Press, 2001.

[7] Corral, N. and Fernández-Sánchez, P., Isolated invariant curves of a foliation, to apper in *Proc. Amer. Math. Soc.*.

[8] Davenport, J.H., On the integration of algebraic functions, *Lecture Notes in Computer Science*, 102, Springer-Verge, New York, 1981.

[9] Feng, R. and Gao, X.S., Rational general solutions of algebraic ordinary differential equations, *Proc. ISSAC2004*, 155-162, ACM Press, 2004.

[10] Feng, R. and Gao, X.S., A polynomial-time algorithm to compute rational solutions of first order autonomous ODEs, *MM-Preprints*, No.23, 54-65, December, 2004.

[11] Fulton, W., *Algebraic Curves*, Benjamin/Cummings Publishing Company, Inc, 1969.

[12] Hubert, E., The general solution of an ordinary differential equation, *Proc. ISSAC1996*, 189-195, ACM Press, 1996.

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

[14] Kovacic, J.J., An algorithm for solving second order linear homogeneous differential equations, *J. Symb. Comput.*, 2(1), 3-43, 1986.

[15] Lang, S., *Introduction to Algebraic and Abelian Functions*, second edition, Springer-Verlag, New York, 1972.

[16] Poincaré, H., Sur l'intégration algébrique des équations différentielles du premier ordre et du premier degré, *Rend. Circ. Mat. Palermo*, 11, 193-239, 1897.

[17] Risch, R.H., The problem of integration in finite terms, *Trans. Amer. Math. Soc.*, 139, 167-189, 1969.

[18] Risch, R.H., The Solution of the problem of integration in finite terms, *Bull. Amer. Math. Soc.*, 76, 605–608, 1970.

[19] Ritt, J.F., *Differential Algebra*, Amer. Math. Sco. Colloquium, New York, 1950.

[20] Singer, M.F., Liouillian solutions of nth order homogeneous linear differential equations, *Amer. J. Math.*, 103(4), 661-682, 1981.

[21] Singer, M.F., Liouillian first integrals of differential equations, *Trans. Amer. Math. Sco.*, 333(2), 673-688, 1992.

[22] Trager, B., Integration of Algebraic Functions, Ph.D thesis, Dpt. of EECS, Massachusetts Institute of Technology, 1984.

[23] Ulmer, F. and Calmet, J., On liouvillian solutions of homogeneous linear differential equations, *Proc. ISSAC1990*, 236-243, ACM Press, 1990.

[24] Van der Put, M. and Singer, M. *Galois Theory of Linear Differential Equations*, Springer, Berlin, 2003.

[25] von Zur Gathen, J. and Gerhard, J. (1999). *Modern Computer Algebra*, Cambridge University Press, Cambridge.

[26] Walker, R. J., *Algebraic Curves*, Princeton Unv. Press, 1950.