The use of the Special semi-groups for solving differential equations*

Jacques-Arthur Weil
GAGE / Centre de mathématiques
Ecole Polytechnique
F-91128 Palaiseau cedex, France
Email: aweil@ariana.polytechnique.fr

Abstract

In general, there is no method for finding closed form first integrals or solutions of ordinary differential equations with non-constant coefficients. Thus, one usually performs heuristics, but this involves fastidious computations. The aim of this paper is to propose strategies that computerize such heuristics to help the analysis.

In section 1, we formulate our questions in terms of differential algebra. Then, we are able to derive algebraic constructive criteria for the search for closed form solutions of differential equations of the type $s(x, y, \dots, y^{(n-1)})y^{(n)} + t(x, y, \dots, y^{(n-1)}) = 0$ (sections 2 and 3). In particular, we focus on the so-called Special polynomials (or Darboux curves). In Section 4, we show how our tools link the expression of the solutions to that of the first integrals, and how it gives a strategy to compute them. Then, in section 5, we show how these techniques permit to derive algorithmic methods to find solutions of order $n-1$ for linear differential equations of order n; we specifically detail the second order case.

1 Preliminaries

To study differential equations in a computable way, we shall use differential algebra, a generalization of commutative algebra to differential equations.
In this section, we recall its outlines. For a complete exposition, the reader is referred to [10], [4], [11], or [5].

1.1 Differential algebra

Let k be an ordinary differential field, that is a field equipped with a derivation, a linear operation $'$ such that k is stable under $'$ and $\forall a, b \in k,\ (ab)' = a'b + ab'$ (Leibniz's rule). The constant field $\mathcal{C}$ of k is the subfield of elements c of k such that $c' = 0$. As an example, one may check that $\mathbb{C}(x)$ (with the usual derivation $\frac{d}{dx}$ that sends any element of $\mathbb{C}$ to 0 and x to 1) is a differential field. In order to understand better what follows, the unfamiliar reader may think of k as a field of meromorphic functions on some given regions of the complex numbers that are closed under differentiation (see [11]). Unless stated otherwise, we assume in the sequel that $\mathcal{C}$ is algebraically closed.

Consider a countable set $Y^{(i)}$ of indeterminates; if we impose $Y^{(i+1)} = Y^{(i)}{}'$, then we can consider the differential ring $k\{Y\} = k[Y, Y', Y'', \dots]$ of differential polynomials and Y is called a differential indeterminate. In that setting, a (ordinary) differential equation may be viewed as an equation between differential polynomials.

An ideal of $k\{Y\}$ is said to be differential if it is stable under $'$. Let y be an element of a differential extension of k (an extension with a derivation that extends $'$); the set $I(k; y)$ of all differential polynomials in $k\{Y\}$ that vanish at y is a prime differential ideal. Conversely, given I a prime differential ideal of $k\{Y\}$, we may find y in an extension of k (namely, the coset of Y in $k\{Y\}/I$) such that $I = I(k; y)$); such a y is called a generic zero of I.

Let $Q = Q(Y, Y', \dots, Y^{(n)})$ be an algebraically irreducible differential polynomial over k, and $[Q]$ the differential ideal generated by Q. The *separant* $\mathrm{Sep}(Q)$ is defined as $\frac{\partial Q}{\partial Y^{(n)}}$; if Q is of order n and of degree m in $Y^{(n)}$, then the *initial* $\mathrm{In}(Q)$ is the coefficient of ${Y^{(n)}}^m$.

If we call H the multiplicative semi-group generated by $(\mathrm{Sep}(Q), \mathrm{In}(Q))$, then the ideal $I(Q) := [Q] : H = \{P \in k\{Y\}$ s.t $\exists n_I, n_S \in \mathbb{N} : \mathrm{In}(Q)^{n_I} \mathrm{Sep}(Q)^{n_S} P \in [Q]\}$ is prime. The converse is true: if I is prime, then there exists a Q such that $I = [Q] : H$. For proofs, one may consult [10] pp 30,31,45,57 and [5] lemma 2 pp 167.

1.2 Zeroes of differential polynomials

The notion of zero of a differential polynomial can be confusing, so let us explain what we search for and settle algebraically what we mean by closed form solution.

We say that an element η of a differential extension of k is a *zero* of Q if $Q \in I(k; \eta)$; a generic zero y of $I(Q)$ is called a *generic zero* of Q (roughly, a zero of Q that is not a zero of any lower polynomial). Any zero of Q is a specialization of y: any (differential) relation satisfied by y will be satisfied by any zero of Q.

In the sequel, the notation P will stand for a quasi-linear differential polynomial, which means that it is linear in its highest derivative:

$$P = s(Y, \dots, Y^{(n-1)})Y^{(n)} + t(Y, \dots, Y^{(n-1)}).$$

*Research supported by the CNRS GDR 1026 (MEDICIS) the GDR-PRC 967 (Math-Info), and the CEC ESPRIT BRA contract 6846 (POSSO).

A zero η of P will be said to be of order r if the lowest order differential polynomial Q such that $Q(\eta, \eta', \dots) = 0$ is of order r. For example, if $k = \mathbb{C}(x)$ and $P = Y'' + Y$, then the generic zero will be of order 2 whereas $\sin x$ will be of order 1, for it is a transcendental zero of $Y'^2 + Y^2 - 1$. Conversely, $\sin x$ is a generic zero of $Y'^2 + Y^2 - 1$ but not of $Y'' + Y$.

Now, to solve a differential equation means to characterize the zeroes of the associated differential polynomial. In some sense, this means that we want to classify the zeroes of P by their order over k.

The link with the classical notion of solution of a differential equation is the following. A function f is usually characterized by the property of being a zero of some prime differential ideal I and a set of initial conditions. Now, given some differential polynomial Q, to check if $Q(f) = 0$, one has to consider the composition of the two successive morphisms: $k\{Y\} \xrightarrow{\phi_1} k\{Y\}/I \xrightarrow{\phi_2} \mathcal{F}$, with $\mathcal{F}$ some functional space which f belongs to. We will not consider the morphism ϕ_2, but we focus on the kernel of ϕ_1.

A method due to Ritt for testing if a differential polynomial Q belongs to $\mathrm{Ker}(\phi_1)$ is applied in section 2. In the remaining sections, we deal with the inverse problem, that is: given Q, find a prime differential ideal I properly containing $I(Q)$ (so $Q \in \mathrm{Ker}(\phi_1)$). Suppose such an I exists; then, there is an R such that $I = I(R)$ (see previous section) and Q is said to be soluble in closed form. This is equivalent to saying that there exists $R \in k\{Y\}$ whose generic zero is a zero of Q.

For example, the Airy polynomial $Y'' - xY$ is not soluble in closed form over $\mathbb{C}(x)$, whereas $Y'' + Y$ is (e.g take $I = [Y' + iY]$, with $i^2 + 1 = 0$). This motivates the following definition:

Definition 1.1 *We say that a differential polynomial Q is r-soluble over k if there exists $R \in k\{Y\}$ of order r such that a generic zero of R is a zero of Q.*

2 The singular zeroes

For further considerations, we shall need an order on the monomials of $k\{Y\}$. In the sequel, we consider the lexicographic order with $i > j \Rightarrow Y^{(i)} > Y^{(j)}$. Two monomials m_1 and m_2 which just differ by multiplication by some element of k are called equivalent ($m_1 \sim m_2$). Then, we extend this order to the differential polynomials: any polynomials $Q, R \in k\{Y\}$ have leading monomials $\mathrm{lm}(Q)$ and $\mathrm{lm}(R)$ and we say that $Q \gtrsim R$ if $\mathrm{lm}(Q) \gtrsim \mathrm{lm}(R)$.

If we are given two differential polynomials $Q \gtrsim R$ with $\mathrm{ord}(Q) = n$, $\mathrm{ord}(R) = r$ and $n \geq r$, then we can reduce Q with respect to R as follows (see [10]): We have $R^{(n-r)} = \mathrm{Sep}(R)Y^{(n)}$+lower terms. So, we get $\mathrm{Sep}(R)Q = \alpha_{n-r}R^{(n-r)} +$ terms in $Y^{(n-1)}$ and lower ones (with $\alpha_{n-r} \in k\{y\}$). Proceeding repeatedly, we reduce again until the remainder is of order r. Then we perform an algebraic reduction, to obtain the following relation:

$$\mathrm{In}(R)^m \mathrm{Sep}(R)^{n-r} Q = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} + R_1$$

with $Q \gtrsim R > R_1$ and m some integer. The polynomial R_1 is the *reductum* of Q by R.

Though simple, this reduction process will prove powerful on the two forthcoming results. A zero of a differential polynomial Q is said to be *singular* if it is also a zero of $\mathrm{Sep}(Q)$ or $\mathrm{In}(Q)$.

Theorem 2.1 *Suppose we take $P = s(Y, \dots, Y^{(n-1)})Y^{(n)} + t(Y, \dots, Y^{(n-1)})$. Then one can, in a finite number of steps, decide if P has singular zeroes and produce their minimum polynomial.*

Proof. - Due to the form of P, the question is just to decide whether s and t have a zero in common, which can be done the following way. Suppose $s \gtrsim t$ (else, switch them); reducing s with respect to t, we get another polynomial t_1. A key point is that a common zero of s and t is still a zero of t_1. We reduce s and t with respect to t_1 and produce again other polynomials. If the process produces 1 (or any element of k), then s and t have no zero in common; if not, as the reductums are always lower and lower, the process stops at some point. Set t_0 to be the lowest among our collection of polynomials. By minimality of t_0, s and t reduce to 0 by t_0. So a non-singular zero of t_0 is a common zero to s and t of minimal order. If all zeroes of t_0 are singular, then t_0 is not algebraically irreducible, so we reduce s and t with respect to each factor of t_0 and iterate the process. ∎

This being settled, we can focus our attention on the non-singular zeroes of P.

3 The non-singular zeroes

3.1 A general criterion

Use of the method of the previous section allows for a general (theoretical) criterion for testing if P is soluble.

Lemma 3.1 *The polynomial P is r-soluble if and only if there is an algebraically irreducible differential polynomial R of order r, an integer m, and some elements $\alpha_i \in k\{Y\}$, $i = 0, \dots, n-r$ such that*

$$\mathrm{In}(R)^m Sep(R)^{n-r} P = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} \tag{1}$$

Proof. - The identity (1) clearly implies that a generic zero of R is a zero of P (because $\mathrm{In}(R)$ and $\mathrm{Sep}(R)$ are lower than R). Conversely, suppose that P is r-reducible. Then, there exists some minimum $R \in k\{Y\}$ of order r such that the generic zero ρ of R is a zero of P. The minimality of R implies that it is algebraically irreducible. Reduce P by R: we obtain $\mathrm{In}(R)^m \mathrm{Sep}(R)^{n-r} P = \sum_{i=0}^{i=n-r} \alpha_i R^{(i)} + Q$ with Q lower than R. But $Q(\rho) = 0$; so, as ρ is generic for R, we get $Q = 0$. ∎

Note that this is just a rewriting of the properties that we recalled in section 1.

At this point, it would be illusory to hope to directly extract from this criterion a practical algorithm for finding a candidate for the polynomial R. So, in the sequel, we particularly study a specific case of this lemma, that is the case when $r = n - 1$.

3.2 The special semi-group

Consider $P = s(Y, \dots, Y^{(n-1)})Y^{(n)} + t(Y, \dots, Y^{(n-1)})$ and let y be as usual a generic zero of P. We introduce a convenient notational abuse: we shall write $k\{y\} := k\{Y\}/I(P)$. This is a non-integral algebraic extension of $k[y, \dots, y^{(n-1)}]$. So, every time that $y^{(n)}$ appears in a computation, we will multiply it by $s(y,\ldots,y^{(n-1)})$ and replace that product by $t(y,\ldots,y^{(n-1)})$. This way, we always reduce computations with y to computations in $k[y,\ldots,y^{(n-1)}]$. As y is generic for P, this latter ring behaves as an algebraic ring in n independent indeterminates.

As theorem 3.1 will soon show, applying criterion 1 for $r = n-1$ motivates the study of the set $\mathcal{S}_P$ of all the polynomials f in $k\{y\}$ such that f formally divides sf'.

Lemma 3.2 *If $f,g \in \mathcal{S}_P$, then $fg \in \mathcal{S}_P$. Moreover, if we have $f \in \mathcal{S}_P$, then any irreducible factor of f is in $\mathcal{S}_P$*

Proof. - These are easy consequences of Leibniz's rule. Up to immediate rewriting, the proofs (and additional properties) at order 1 of [2] or [9] apply here. ∎

Therefore, it follows that we may focus on the irreducible elements of $\mathcal{S}_P$. Note that they are at most of order $n-1$.

Definition 3.3 *The set $\mathcal{S}_P$ is called the special semi-group associated with P. An element f of $\mathcal{S}_P$ satisfying $sf' = af$ is called* special for P with factor a. *We will omit the mention "for P" when the context is clear. Furthermore, f will be said to be trivial if it belongs to k.*

Remark. - The terminology "special" was introduced by Bronstein ([2]) to understand how the theory of integration in finite terms extends to extensions of type $y' = H(y)$, $H \in k[y]$ (see [9] for extensions of type $s(y)y' = t(y)$). However, the concept is rather classic; such polynomials are also called "Darboux curves" in the literature (see [13, 7]). They were (up to my knowledge) mainly used in the search for first integrals

Lemma 3.4 *Suppose $f \in \mathcal{S}_P$ is an irreducible special polynomial. Then, either f divides s, or f is of order $n-1$.*

Proof. - The elements in $\mathcal{S}_P$ are of order at most $n-1$. Suppose f is of order $i < n-1$; then, f' is a true polynomial (no terms in $y^{(n)}$). Consider the identity $sf' = \alpha f$ between algebraic polynomials in n variables; then the irreducibility of f implies that it divides s or f'. Suppose that f divides f'; then, as f' is order $i+1$ (multiplication by s doesn't change anything in that case), f must divide $\frac{\partial f}{\partial y^{(i)}}$. Since f is of higher degree in $y^{(i)}$, this is impossible. So f divides s. ∎

Let us take an example: let $P = YY'' - nY'^2$. We then have two special polynomials: $f_1 = y'$ (because $s = y$ and $sf_1' = ny'f_1$), and $f_2 = y^n$ (because $sf_2' = ny'f_2$). Note that, in that case, f_1 and f_2 have the same factor, so $\frac{f_1}{f_2}$ is a (new) constant in the fraction field of $k\{y\}$ (see section 4).

Theorem 3.1 *Suppose f is a special polynomial of order $n-1$. Then any non-singular zero η of f is a zero of P.*

Conversely, if P admits a zero η of order $n-1$, then the minimum polynomial f of η is special for P.

Proof. - An identity between polynomials in y of order $n-1$ or less is still valid for Y. Let $f_2 := s(f' - y^{(n)}\frac{\partial f}{\partial y^{(n-1)}}) - t\frac{\partial f}{\partial y^{(n-1)}}$; f_2 is of order $n-1$. As $f \in \mathcal{S}_P$, $f_2 = \alpha f$; now, $sf'(Y) = f_2(Y) + \frac{\partial f}{\partial y^{(n-1)}}(Y) \times (sY^{(n)} + t)$ in $k\{Y\}$. But, as $f_2 = \alpha f$ as polynomials of order $n-1$, this implies that $sf' - \alpha f = \frac{\partial f}{\partial y^{(n-1)}}(Y) \times P$ in $k\{Y\}$; thus, a non-singular zero η of f is a zero of P.

To prove the converse, we reduce sf' (which is of order $n-1$) by f. We get that, for some integer m and $\beta \in k\{y\}$, $\mathrm{In}(f)^m sf' - \beta f = g$ with $g < f$. But f is minimum for η so g has to be identically zero. Thus, $\mathrm{In}(f)^m sf' = \beta f$. But f is irreducible, so $\mathrm{In}(f)^m$ divides β and $f \in \mathcal{S}_P$ ∎

Up to now, the computation of the special polynomials is in general an open problem. The first difficult step is to bound the degree m of the possible candidates. Secondly, given m, pick a (differential) polynomial f of degree m with unknown coefficients. Reducing sf' by f, we get a first order differential system for the coefficients of f (with as many equations as coefficients). But, the process of reduction induces non-linear terms in the system, so finding its rational solutions is in general a matter of skill. Yet, it appears to be an interesting heuristics for low orders and degrees. Prelle and Singer have proposed a method for $n = 1$ (see [8], and [7],[13] for references to alternative approaches) that is implemented (at least) in MACSYMA.

In the next section, we show how the knowledge of only one element of $\mathcal{S}_P$ helps finding first integrals. Then, in section 5, she show how (modulo the question of the degree) one can compute elements of the special semi-group.

4 Generic constants

It is classic, when studying differential equations, to search for first integrals in order to integrate the differential equation. Following the previous formalism, we will concentrate on a special kind of first integrals.

We say that the pair $f,g \in k\{y\}$ is in canonical form if $\gcd(f,g) = 1$, g is monic, and $f \gtrsim g$.

Definition 4.1 *The polynomial P is said to admit a generic constant if there is a pair $f,g \in k\{y\}$ in canonical form such that $s(f'g - fg') = 0$.*

This definition is equivalent to saying that there are new constants in the fraction field of $k\{y\}$; it is also equivalent to saying that the polynomial P admits a rational first integral: for any zero η of P, $\frac{f}{g}(\eta)$ is a constant. Note that, again, we cannot cancel the multiplication by s if we want to keep a polynomial equality to zero.

Lemma 4.2 *If the polynomial P admits a generic constant (f,g) in canonical form, then the order of f is $n-1$. Thus, for any constant c, any non-singular zero of $f - cg$ is also a zero of P.*

Proof. - This result is a consequence of theorem 3.1. As f is prime with g, $s(f'g - fg') = 0$ implies that f divides sf'. So, f and g are both special with the same factor; this remains true for $f - cg$ (in fact, the generic constants of P form a $\mathcal{C}$-algebra).

Theorem 3.1 applies if $f - cg$ is of order $n-1$, so suppose f and g were factors of s, both of order $< n-1$. Then we would have $f'g - fg' = 0$; as f could not divide f' (it is of higher order), it would have to have a factor in common with g, a contradiction. Therefore, the order of f is $n-1$ and we are done. ∎

It follows from this lemma that techniques for finding special polynomials can bring us two things. First, they show the link between rational first integrals and zeroes, and secondly they provide a technique for finding rational first integrals. To do that, the key point will be the following simple lemma:

Lemma 4.3 *Let m be an integer and $\alpha \in k\{y\}$. Then, one can decide in a finite number of steps if there exists $f \in k\{y\}$ of degree m such that $sf' = \alpha f$. If so, the decision procedure provides the coefficients of f.*

Proof. - Let f have unknown coefficients; as y is generic for P, the relation $sf' - \alpha f = 0$ implies that all coefficients of the (differential) polynomial $sf' - \alpha f$ are equal to zero; as we know s and α, this yields a first order linear differential system for the coefficients of f. Finding rational solutions (and deciding their existence) of such a system is algorithmically well-known, (see, for example, proposition 3.2 pp 669 in [12]): this gives the coefficients of f. $\square$

Remark. - Suppose we are given a polynomial $g \in \mathcal{S}_P$ with factor α and we want to find f such that f/g is a generic constant. In some cases, one can retrieve from g a bound on the degree of f; in this case, the above heuristics is transformed into an algorithm (see proposition 5.6 below).

This is the method that we used in the example following lemma 3.4. Here is another example (provided by Bob Caviness). Consider the first order differential equation over $\mathbb{Q}(x)$:

$$P := x\,(2\,y + x - 1)\,y' - y\,(y + 2\,x + 1) = 0.$$

We have an obvious solution y=0, so $y \in \mathcal{S}_P$. In fact, $sy' = \alpha y$ with $\alpha = y + 2\,x + 1$. So, to find a generic constant, we pick a degree m, take a generic polynomial $f := \sum f_i y^i$ of degree m in y, and consider the relation $sf' - \alpha f = 0$.

One may check that there are no candidates for $m = 1$ or $m = 2$. For $m = 3$, we get the following first order linear differential system in the coefficients of f:

$$\begin{aligned}
x\,(x-1)\frac{\partial}{\partial x}f_0(x) - f_0(x)\,(2\,x+1) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_1(x) + 2\,x\frac{\partial}{\partial x}f_0(x) - f_0(x) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_2(x) + 2\,x\frac{\partial}{\partial x}f_1(x) + (2\,x+1)\,f_2(x) &= 0,\\
x\,(x-1)\frac{\partial}{\partial x}f_3(x) + (4\,x+2)\,f_3(x) + f_2(x) + 2\,x\frac{\partial}{\partial x}f_2(x) &= 0,\\
2\,f_3(x) + 2\,x\frac{\partial}{\partial x}f_3(x) &= 0.
\end{aligned}$$

We easily find the rational solutions of this linear differential differential system, so:

$$f = \frac{-c_0y^3 + 3(x-1)c_0y^2 + \left((-3x^2-3)c_0 + xc_1\right)y + (x-1)^3c_0}{x}$$

where c_0 and c_1 are arbitrary constants, and f/y is a generic constant for P. In particular, for $c1 = 6c0$, we find the first integral that MACSYMA provides (type USAGE(ODEFI) under MACSYMA):

$$\frac{(-y + x - 1)^3}{xy}.$$

This example shows that, to compute an $f \in \mathcal{S}_P$ such that $sf' = \alpha f$, one should first focus on finding candidates for the factor α. Note that, then, our method works at any order (whereas MACSYMA seems to treat only the first order case).

An interest of these results lies in the fact that the study of the constant field of a differential extension provides informations on the extension itself ([16]).

We now turn to a case where we can explicitly compute elements of $\mathcal{S}_P$.

5 The case of linear differential equations

In this section, we suppose that $k = \mathcal{C}(x)$, where $\mathcal{C}$ is some computable number field. Let $L(Y) = Y^{(n)} + a_{n-2}Y^{(n-2)} + \ldots + a_0Y = 0$ be a linear differential equation on k (it can always be reduced to this form, see e.g [14]), and y a generic zero of L. The extension $k\{y\}$ can be identified with $k[y, y', \ldots, y^{(n-1)}]$ with the derivative of $y^{(n-1)}$ being $-\sum_{i=0}^{n-2} a_i y^{(i)}$. The main feature of these linear equations that we shall use here is the fact that the derivation on $k[y, y', \ldots, y^{(n-1)}]$ is homogeneous of degree zero, which means that the derivative of a monomial of degree m is a homogeneous polynomial of the same degree m.

5.1 Computing the special semigroup

Lemma 5.1 *Suppose L admits a special polynomial f with factor a ($f' = af$). Then, $a \in k$ and each homogeneous component of f is itself a special polynomial with same factor a.*

Proof. - Write $f = \sum_{i=0}^m f_i$ with each f_i homogeneous. As f is special, we have:

$$\sum_{i=0}^{m} f_i' = a \sum_{i=0}^{m} f_i. \qquad (2)$$

As the derivation is homogeneous, f_i' is still homogeneous and has the same degree as f_i. Suppose a has a term a_+ of degree superior to 0. Then, comparing degrees on the two sides of (2), we get that $a_+ f_m = 0$. As $f_m \neq 0$, $a_+ = 0$ and $a \in k$. Now, comparing the terms in (2) at each total degree, we get that for all i, $f_i' = af_i$. $\square$

It follows that we may focus our study of $\mathcal{S}_L$ to the study of its monic homogeneous elements, which is the key to the following:

Theorem 5.1 *Given any integer m, one can decide in a finite number of steps if L admits a special polynomial of degree m.*

Proof. - For this proof, let us write y_i in place of $y^{(i)}$. Suppose $f = y_{n-1}^m + f_{\nu-1}y_{n-1}^{m-1}y_{n-2} + \ldots$, where the f_i, $i = 0, \ldots, \nu - 1$ are the coefficients of f. differentiating, we get $f' = \frac{\partial}{\partial x}f + \sum_{i=0}^{n-1} y_{i+1}\frac{\partial f}{\partial y_i}$.

So, $f' = (-\sum_{i=0}^{n-2} a_i y_i)\frac{\partial f}{\partial y_{n-1}} + f_{\nu-1}y_{n-1}^m +$ lower terms. A term in y_{n-1}^m can only come from differentiating a term in y_{n-2}: as there is no term in y_{n-1} in L, differentiating with respect to y_{n-1} strictly lowers the degree in y_{n-1}. Thus, $f' = f_{\nu-1}y_{n-1}^m +$ lower terms. So, equating to zero the coefficients of $f' - f_{\nu-1}f$ produces the conditions for f to be special. If V is a vector in k^ν whose entries are the unknown f_i, then these conditions can be rewritten as the system (NL) in the lemma just below. So, the proof the following lemma yields the desired algorithm.

Lemma 5.2 *Let $V = (f_{\nu-1}, \ldots, f_0)^t$ be a column vector of unknowns in k^ν, B a known column vector of k^ν and $A \in \mathcal{M}_\nu(k)$ a square $\nu \times \nu$ matrix of known elements of k. Then, one can compute the rational solutions of the (slightly) non-linear system*

$$(NL): \qquad V' = f_{\nu-1}V + AV + B.$$

Proof. - Let δ be some unknown verifying $\delta' = -f_{\nu-1}\delta$. The idea will be to express the f_j linearly in terms of δ (and its derivatives) and then find conditions on δ for the system to have a rational solution.

We have $\delta'' = (-f'_{\nu-1} + f^2_{\nu-1})\delta$; if we replace $f'_{\nu-1}$ by its expression in (NL), the term $f^2_{\nu-1}$ is canceled and we get:

$$\delta'' = (-f'_{\nu-1} + f^2_{\nu-1})\delta = (-A_1 V - B_1)\delta$$

where A_1 (resp B_1) denotes the first row in A (resp B). The recursion is now easy. Suppose that $\delta^{(i)} = (\Delta_i V + c_i)\delta$, with Δ_i a row vector in k^ν and $c_i \in k$. Then:

$$\begin{aligned} \delta^{(i+1)} &= \left(\Delta'_i V + \Delta_i V' + c'_i - f_{\nu-1}\Delta_i V - f_{\nu-1}c_i\right)\delta \\ &= \left(\Delta'_i V + \Delta_i A V + \Delta_i B + c'_i - c_i f_{\nu-1}\right)\delta \end{aligned}$$

and so we get recurrence formulas:

$$\begin{aligned} \Delta_{i+1} &= \Delta'_i + \Delta_i A - (c_i, 0, \ldots, 0) \\ c_{i+1} &= \Delta_i B + c'_i \end{aligned}$$

Now, there is a number ν of f_j, and so the expressions $\Delta_1 V, \ldots, \Delta_{\nu+1} V$ are linearly dependent. Performing Gaussian elimination, we find the lowest integer ν_0 such that $\Delta_1 V, \ldots, \Delta_{\nu_0}$ are linearly dependent. Then, the $\delta^{(i)} - c_i\delta$ $(i = 1, \ldots, \nu_0)$ are linearly dependent, and δ satisfies a system (CC) of homogeneous linear differential equations L_{ν_i} of orders $\nu_0, \ldots, \nu+1$: these are the compatibility conditions for the linear system in the f_j to have solutions.

At this point, finding rational solutions to (NL) is equivalent to finding a solution of (CC) whose logarithmic derivative is rational. Making successive reductions as in section 2 between the L_{ν_i}, one easily finds a single linear differential equation L_{ν_1} of order $\nu_1 \leq \nu_0$ such that (CC) has a solution δ if and only if $L_{\nu_1}(\delta)$=0.

So, our problem is reduced to finding a zero δ of L_{ν_1} whose logarithmic derivative is in k. This problem is algorithmically well-known; for example, we may use the algorithm that Bronstein ([3]) has implemented in AXIOM to solve it. Knowing δ, we know f_{m-1} and we solve the remaining linear system to find the other coefficients. ∎

Remark. - A rationality result follows from lemma 4.1 of [15]: if $\mathcal{C}$ is not algebraically closed and our problem has a solution in $\overline{\mathcal{C}}(x)$, then it has a solution in $\mathcal{C}_1(x)$ where $\mathcal{C}_1$ is an extension of $\mathcal{C}$ of degree at most ν_1; however, it is not clear yet whether the algorithm in [3] will produce such a solution.

There exists a theoretical bound on the possible degrees for f. However, it is not constructive (see [7],[13]). So, the above procedure does not yield a complete algorithm for computing the whole of $\mathcal{S}_L$.

Remark. - If the degree is one, then the procedure just described yields the adjoint equation to L (that is the equation that admits a right factor whenever L, taken as a differential operator, admits a left factor, see e.g [12])

5.2 The second order case

Suppose $L(Y) = Y'' + rY$. It is classic that the change of variables $Y' = UY$ induces the Riccati equation $Ri(U) = U' - r + U^2 = 0$. The study of L can therefore be reduced to that of Ri.

One efficient point in the previous algorithm is that the knowledge of the first coefficient linearly determines the remaining ones. This sheds light on a specificity of the second order case when one searches for liouvillian solutions of differential equations (see e.g [6] or [14]): in that case, the minimum special polynomials agree with the minimum polynomials of algebraic solutions to the associated Riccati equation.

Theorem 3.1 helps us find again the usual classification of zeroes of L, that is: L admits a non-generic zero if and only if Ri admits an algebraic solution, which is summed up in the following known lemma:

Lemma 5.3 *Suppose f is a non-trivial homogeneous irreducible element of $\mathcal{S}_L$, and let $f(y, y') = y^m \tilde{f}(u)$ then: the equation $Ri(U) = 0$ admits an algebraic solution v and the polynomial $\tilde{f}$ is the minimum polynomial for v.*

Moreover, for any algebraic solution u of $Ri(u) = 0$ with minimum polynomial $\tilde{g}$ of degree n, the polynomial $g := y^n \tilde{g}(\frac{y'}{y})$ is special for L.

Proof. - The first part is a direct consequence of lemma 5.1 and theorem 3.1. For the second part, the minimality of $\tilde{g}$ implies that $\tilde{g}$ is special for Ri; then, an immediate change of variables shows that g is special for L. ∎

Remark. - We know that the degree m of the minimum polynomial of a solution of the Riccati equation is to be chosen in the list 1,2,4,6,12 (see [6]). Thus, using the algorithm following theorem 5.1 for each of these values of m, we obtain an algorithm for solving second order linear differential equations. It belongs to the same family as the algorithms in [6] and [14]: in the second order case, the equation that we produced for δ is exactly the m-th symmetric power (see [12]) of L.

We now turn to generic constants. The previous results help us refine the link that is shown in [13] between Liouvillian solutions and Liouvillian first integrals:

Lemma 5.4 *Suppose $Ri(U) = 0$ admits an algebraic solution with minimum polynomial $\tilde{f}$ of degree $n \geq 2$, and let Δ be its discriminant; also, set $f(y, y') = y^n \tilde{f}(\frac{y'}{y})$. Then $\frac{f^{2(n-1)}}{\Delta}$ is a generic constant for L.*

Proof. - Write $f = y'^n + a(y')^{n-1}y + \cdots$. We have seen that $f' = af$. Now, the discriminant of $\tilde{f}$ is $\Delta = \prod_{i \neq j}(u_i - u_j)$ (recall that Δ is rational). But, all zeroes of $\tilde{f}$ are zeroes of Ri; so, we have

$$\frac{\Delta'}{\Delta} = \sum_{i \neq j} \frac{u'_i - u'_j}{u_i - u_j} = \sum_{i \neq j} \frac{u_j^2 - u_i^2}{u_i - u_j}$$

Thus, $\frac{\Delta'}{\Delta} = -2(n-1)\sum u_i = 2(n-1)a$. As $f' = af$, we get that $f^{2(n-1)}$ and Δ have the same logarithmic derivative. ∎

Corollary 5.5 *L has a liouvillian first integral if and only if it has liouvillian solutions. In that case, it has a polynomial first integral unless Ri has a rational solution u_0 which is not the logarithmic derivative of an element in k: there, the first integral is $e^{\int u_0}(y' - u_0 y)$.*

Remark. - The Riccati equation can admit a fraction as a generic constant, but it cannot admit a polynomial generic constant: the leading coefficient of a candidate f would be the leading coefficient of the derivative, so it would be zero. This remains obviously true for equations of type $s(u)u' = t(u)$ with $\deg_u t > 1 + \deg_u s$.

Lemma 5.4 illustrates the following idea: The fact of being a first integral is much stronger than that of being a solution, for it defines a whole set of solutions. It is therefore not too surprising that it algebraically induces higher complexity to find a first integral than to find one corresponding solution. However, the degrees of the first integrals derived from lemma 5.4 are highly not sharp (see [14] pp 59-63): we just mean that the complexity of finding first integrals is at least that of finding one single solution.

Last, we show how we can use lemma 4.3 to find generic constants for the Ricatti equation:

Proposition 5.6 *Suppose we are given a polynomial $\tilde{g}$ that is special for Ri. Then, one can decide in a finite number of steps if it can be the denominator of a generic constant of Ri. If so, the decision procedure computes the numerator $\tilde{f}$.*

Proof. - Suppose $\deg_u \tilde{f} = n$ and $\deg_u \tilde{g} = m$; the leading coefficient of $\tilde{f}'\tilde{g} - \tilde{g}'\tilde{f}$ is $(n-m)f_n g_m$ and it is zero; so $n = m$. Thus, as we know $\tilde{g}$, we know the degree m of $\tilde{f}$. Now, defining α by $g' = \alpha g$, we apply the procedure from lemma 4.3 to compute f from m and α. □

5.3 Example

Consider the equation

$$\begin{aligned} L(y) &:= x^2\,(x-1)^2\,(5\,x-2)^2\,(5\,x+4)^2\,(5\,x-1)^2 y'' \\ &+ (5625\,x^6 - 4500\,x^5 + 4800\,x^4 - 5160\,x^3 + 1602\,x^2 \\ &- 192\,x + 12)y = 0 \end{aligned}$$

Computing the second symmetric power of L, we get a rational solution to the Riccati equation and the following special polynomial for L:

$$\begin{aligned} \tilde{f}_* &= x^2(x-1)^2(5x-2)^2(5x+4)^2(5x-1)^2U^2 \\ &- \left(250x^4 - 275x^3 + 35x^2 + 52x - 8\right) \\ &\times (x-1)(5x-2)(5x+4)(5x-1)xU \\ &+ 12 - 144x + 126x^2 + 3360x^3 - 10250x^4 \\ &+ 3875x^5 + 22500x^6 - 34375x^7 + 15625x^8 \end{aligned}$$

Note that, in this example, our method is completely similar to the Kovacik algorithm ([6],[14]).

Let us call $\tilde{f}$ the monic polynomial obtained by dividing $\tilde{f}_*$ by its leading coefficient. The discriminant of $\tilde{f}$ is

$$\frac{(-2+5\,x)^2}{x^2\,(5\,x-1)\,(x-1)\,(5\,x+4)^2}$$

Let $f(y, y') = y^m \tilde{f}(u)$; then, by lemma 5.4, f^2/Δ is a polynomial first integral for L.

By lemma 5.4, we can also directly search for rational solutions of the fourth symmetric power of L; it has two independent solutions:

$$\delta_1 = \frac{25\,x\left(64\,x - 224\,x^2 - 540\,x^3 + 200\,x^4 + 500\,x^5\right)}{64\,(5\,x-2)^2}$$

and

$$\delta_2 = \frac{25\,x\left(64 - 424\,x^2 - 5965\,x^3 - 1050\,x^4 + 7375\,x^5\right)}{64\,(5\,x-2)^2}.$$

To each δ_i corresponds a polynomial $f_i \in \mathcal{S}_L$. Computing the logarithmic derivatives, one may check that $\delta_1 f_1$ and $\delta_2 f_2$ are polynomial first integrals of L. Their expression is too big to be given here; However, this last method is much faster than the first one (in our case, the computation took a few seconds with MAPLE).

Also, applying the algorithm in proposition 5.6, one may check that $\tilde{f}_1$ and $\tilde{f}_2$ can both be denominators of generic constants of the Ricatti equation.

6 Conclusion

The missing computer tools to perform the methods and algorithms described along the paper are being implemented (in MAPLE at the present time). Thus, even though there are still no general algorithms to answer the questions that we posed in the introduction, the ability to handle special cases should be enhanced.

The main problem on this topic remains to be the knowledge of bounds on the degree of the monic irreducible special polynomials that we consider (in the same way that it is the main problem when one searches for liouvillian solutions to linear differential equations).

Modulo this central problem, the results in sections 4 and 5 seem to indicate a general strategy: to find polynomials f such that $sf' = \alpha f$, one should first search for conditions on α. For example, the *a priori* knowledge of α is a key point in the Prelle-Singer method ([8]). Also, a reason why the linear case works so well is that we know the shape of α and how to compute candidates for α. Work is in progress in this direction.

Up to now, the method applies best in the linear case. There, we hope that the algorithm provided in theorem 5.1 should generalize to find lower order zeroes. Also, we saw in the second order case that we could sometimes adapt the last step of the method in 5.1 and search directly for rational solutions of some linear differential equation. There is a very fast algorithm to solve this last problem (see [1]), so it may be an interesting strategy.

The author would like to thank Jean Moulin-Ollagnier, Michael Singer, Felix Ulmer, and Manuel Bronstein for fruitful conversations during the preparation of this paper.

References

[1] ABRAMOV S.A, KVANSENKO K.YU *Fast algorithms for the rational solutions of linear differential equations with polynomial coefficients* Proceedings ISSAC 91, ACM Press 1991.

[2] BRONSTEIN M *A unification of liouvillian extensions* AAECC journal **1** (1990) n^o 1, pp 5-24.

[3] BRONSTEIN M *Linear differential equations: breaking through the order two barrier* Proceedings ISSAC 92, ACM Press 1992.

[4] KAPLANSKY I *An introduction to differential algebra* Second edition, Hermann, Paris 1976.

[5] KOLCHIN E.R *Differential algebra and algebraic groups* Academic Press, New-York 1973.

[6] KOVACIK J *An algorithm for solving second order linear homogeneous differential equations* J.Symb.Comp **2** (1986) pp 3-43.

[7] MOULIN-OLLAGNIER J. *Liouvillian first integrals of homogeneous polynomial 3-dimensional vector fields* Prepublication 92-9, Université Paris-XIII, Avril 1992.

[8] PRELLE M.J & SINGER M.F *Elementary first integrals of differential equations* Trans. Amer. Math. Soc, **279** (1983) Number 1, pp 215-229.

[9] RAO N.V *A generalization of the Liouville's theorem on elementary functions* Preprint, University of Toledo Ohio, 1994.

[10] RITT J.F *Differential Algebra* AMS coll. Publications (or Dover, 1966) 1950.

[11] ROSENLICHT M *Integration in finite terms* Amer.Math.Monthly, **79** (1972) pp 963-972.

[12] SINGER M.F *Liouvillian solutions of n-th order homogeneous linear differential equations* Amer.J.Mat. **103** (1981) pp 661-682.

[13] SINGER M.F *Liouvillian first integrals of differential equations* Trans. Amer. Math. Soc, **333** (1992) Number 2, pp 673-687.

[14] SINGER M.F & ULMER F *Liouvillian and algebraic solutions of second and third order linear differential equations* J.Symb.Comp **16** (1993), pp 37-73.

[15] HENDRIKS P & VAN DER PUT M *Galois action on solutions of a differential equation* Preprint, university of Groningen, September 1993.

[16] WEIL J.A *De l'importance d'être constant* Manuscript, Proceedings of the MEDICIS 92 meeting.