Linear Differential Equations and Products of Linear Forms

Michael F. Singer [1]

North Carolina State University, Department of Mathematics, Raleigh, N.C. 27695-8205, USA

Felix Ulmer [2]

IRMAR, Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

Abstract

We show that liouvillian solutions of an n-th order linear differential equation $L(y) = 0$ are related to semi-invariant forms of the differential Galois group of $L(y) = 0$ which factor into linear forms. The logarithmic derivative of such a form F, evaluated in the solutions of $L(y) = 0$, is the first coefficient of a polynomial $P(u)$ whose zeros are logarithmic derivatives of solutions of $L(y) = 0$. Together with the Brill equations, this characterisation allows one to efficiently test if a semi-invariant corresponds to such a coefficient and to compute the other coefficients of $P(u)$ via a factorization of the form F.

1 Introduction

In this paper k is a differential field whose field of constants $\mathcal{C}$ is algebraically closed of characteristic 0 (e.g. $\overline{\mathbb{Q}}(x)$ with the usual derivation d/dx). For the derivation δ of k and $a \in k$ we write $\delta^k(a) = a^{(k)}$ and also $a^{(1)} = a'$, $a^{(2)} = a''$, ... Let

$$L(y) = a_n \frac{d^n y}{dx^n} + a_{n-1} \frac{d^{n-1} y}{dx^{n-1}} + \ldots + a_0 y = 0, \qquad a_i \in k \tag{1}$$

be a linear differential equation of order n over k. We denote by $\{y_1, \ldots, y_n\}$ a fundamental set of solutions of (1). We refer to [11,15,17] for definitions of

[1] Partially supported by NSF Grant CCR 9322433
[2] Partially supported by CNRS GDR 1026 (MEDICIS)

a *Picard-Vessiot extension* (PVE) of k , of the *differential Galois group* $\mathcal{G}(L)$ and of *liouvillian solutions* of for (1). A PVE K of k for (1) is a differential field extension $K = k < y_1, \ldots, y_n >$ with no new constants which is the equivalent of a splitting field for (1). Under our assumptions a PVE exists and is unique up to differential automorphisms. The group $\mathcal{G}(L)$, which consists of the differential automorphisms of K/k, is a linear algebraic group over $\mathcal{C}$ which sends a solution of (1) into a solution of (1). This action gives a faithful representation of $\mathcal{G}(L)$ as a subgroup of $GL(n, \mathcal{C})$ which will be the representation of $\mathcal{G}(L)$ in what follows. There is a Galois correspondence between algebraic subgroups of $\mathcal{G}(L)$ and differential subfields of the PVE of (1) and the fixed field of $\mathcal{G}(L)$ is k. A solution of (1) in k is a *rational solution*, a solution in an algebraic extension of k is an *algebraic solution*, a solution whose logarithmic derivative is in k is an *exponential solution* and a solution belonging to a field obtained by successive adjunctions of exponentials, exponentials of integrals and algebraic functions is a *liouvillian solution*. Algorithms for computing liouvillian solutions of (1) are presented in [6,10,15]. In [10], it is shown that if $L(y) = 0$ has a liouvillian solution, then there is a solution z_1 whose logarithmic derivative $u_1 = z_1'/z_1$ is algebraic and whose algebraic degree can be bounded independently of the equation $L(y) = 0$ [10,17]. All conjugates u_i of u_1 under $\mathcal{G}(L)$ are also logarithmic derivatives of solutions z_i of $L(y) = 0$ and the minimal polynomial $P(u)$ of u_1 can be written as

$$P(u) = \prod_{i=1}^{m} \left(u - \frac{\delta(z_i)}{z_i} \right) \tag{2}$$

$$= u^m - \frac{\delta\left(\prod_{i=1}^{m} z_i\right)}{\prod_{i=1}^{m} z_i} u^{m-1} + \ldots + (-1)^m \prod_{i=1}^{m} \frac{\delta(z_i)}{z_i} \tag{3}$$

In particular, the coefficient of u^{m-1} is the negative logarithmic derivative of a product of m solutions of $L(y) = 0$. It is possible [9] to construct a differential equation whose solutions are the products of length m of solutions of $L(y) = 0$:

Definition 1 *Let $L(y) = 0$ be a homogeneous linear differential equation of order n and let $\{y_1, \cdots, y_n\}$ be a fundamental system of solutions. The differential equation $L^{\circledS m}(y)$ whose solution space, denoted V_m, is spanned by the monomials of degree m in $y_1, \cdots, y_n$ is called the m-th* symmetric power *of $L(y) = 0$.*

An algorithm to construct $L^{\circledS m}(y)$ is given in [15]. From (3) we get that the coefficient of u^{m-1} in the minimal polynomial $P(u)$ is the negative logarithmic derivative of a solution whose logarithmic derivative is rational, i.e. an exponential solution of $L^{\circledS m}(y) = 0$. Let $\{y_1, \ldots, y_n\}$ be a fundamental system of solutions of $L(y) = 0$ and V the solution space of $L(y) = 0$. The solution space V_m of $L^{\circledS m}(y)$ is, if the solutions satisfy a homogeneous polynomial of degree m over $\mathbb{C}$, a quotient of the m^{th} symmetric power $\mathcal{S}^m(V)$ ([8], p. 586) of V on which the group $\mathcal{G}(L)$ acts in the natural way [3]. If $\mathcal{G}(L)$ is a reductive group, then V_m is a direct summand of $\mathcal{S}^m(V)$ ([14], Lemma 3.5). If we denote the basis of V by new variables $Y_1, \ldots, Y_n$, then $\mathcal{S}^m(V)$ is the vector space of forms of degree m in $Y_1, \ldots, Y_n$ over $\mathcal{C}$ while V_m is the vector space of forms of degree m in $y_1, \ldots, y_n$ over $\mathcal{C}$. The natural homomorphism ψ_m mapping $\mathcal{S}^m(V)$ to V_m is an evaluation homomorphism which maps a homogeneous polynomial $p(Y_1, \ldots, Y_n)$ of degree m into the polynomial $p(y_1, \ldots, y_n)$. For $m > 2$ the homomorphism ψ_m is not always an isomorphism. But ψ_1 is an isomorphism, and the action of $\mathcal{G}(L)$ on forms of degree one is the same in $\mathcal{C}[y_1, \ldots, y_n]$ and $\mathcal{C}[Y_1, \ldots, Y_n]$.

Definition 2 *Let V be a $\mathcal{C}$-vector space, call $\{Y_1, \ldots, Y_n\}$ a basis for V, and let $G \subseteq GL(V)$ be a linear group. Define an action of $g \in G$ on $\mathcal{C}[Y_1, \ldots, Y_n]$ by $g \cdot (p(Y_1, \ldots, Y_n)) = p(g(Y_1), \ldots, g(Y_n))$. A polynomial with the property that*

$$\forall g \in G, \quad g\left(p(Y_1, \ldots, Y_n)\right) = \psi_p(g) \cdot \left(p(Y_1, \ldots, Y_n)\right), \ \textit{with } \psi(g) \in \mathcal{C}$$

is called a semi-invariant of G. If $\forall g \in G$ we have $\psi_p(g) = 1$, then $p(Y_1, \ldots, Y_n)$ is called an invariant of G.

If a polynomial is invariant, then its homogeneous components are invariant. If $p \in \mathcal{S}^m(V)$ is an invariant (resp. semi-invariant) of $\mathcal{G}(L)$, then $\psi_m(p)$ is a rational function (resp. an exponential solution, a function whose logarithmic derivative is rational) which is a solution of $L^{\circledS m}(y)$. Note that if p is a product of linear forms, then $\psi_m(p) \neq 0$.

2 Liouvillian solutions and products of linear forms

Theorem 3 *Let $L(y) = 0$ be an n-th order linear differential equation over k with differential Galois group $\mathcal{G}(L) \subseteq GL(n, \mathcal{C})$.*

(i) If $L(y) = 0$ has a liouvillian solution whose logarithmic derivative is algebraic of degree m, then there is a $\mathcal{G}(L)$-semi-invariant of degree m in $\mathcal{C}[Y_1, \ldots, Y_n]$ which factors into linear forms.

(ii) If there is a $\mathcal{G}(L)$-semi-invariant of degree m in $\mathcal{C}[Y_1, \ldots, Y_n]$ which factors into linear forms, then $L(y) = 0$ has a liouvillian solution whose logarithmic derivative is algebraic of degree $\leq m$.

[3] For a cyclic vector of a differential module M, the m-th symmetric power of the vector is not always a cyclic vector of the m-th symmetric power of M

Proof. Let $z_1 = \sum_{i=1}^n a_{i,1} y_i$ be a liouvillian solution of $L(y) = 0$ whose logarithmic derivative z_1'/z_1 is algebraic of degree m over k. The conjugates of z_1'/z_1 under $\mathcal{G}(L)$ are also logarithmic derivatives of solutions $z_j = \sum_{i=1}^n a_{i,j} y_i$ of $L(y) = 0$ ([17], Theorem 1.5) and $\forall \sigma \in \mathcal{G}(L)$ we have that $\sigma(z_i) = c_{\sigma,i} z_j$ where $c_{\sigma,i} \in \mathcal{C}$ ([17], Proof of Theorem 2.3). Since the action of $\mathcal{G}(L)$ on forms of degree one is the same in $\mathcal{C}[y_1, \ldots, y_n]$ and $\mathcal{C}[Y_1, \ldots, Y_n]$, the forms $\sum_{i=1}^n a_{i,j} Y_i$ will be sent to constant multiples of each other by the elements of $\mathcal{G}(L)$ and thus $\prod_{j=1}^m \left(\sum_{i=1}^n a_{i,j} Y_i\right)$ is a $\mathcal{G}(L)$-semi-invariant form which factors into linear forms.
Let $F = F(Y_1, \ldots, Y_n) \in \mathcal{C}[Y_1, \ldots, Y_n]$ be a $\mathcal{G}(L)$-semi-invariant form of degree m over $\mathcal{C}$ which factors into a product of linear forms:

$$F(Y_1, Y_2, \ldots, Y_n) = \prod_{j=1}^m \left(\sum_{i=1}^n a_{i,j} Y_i \right)$$

For $\sigma \in \mathcal{G}(L)$ we have $\sigma(F) = c_\sigma \cdot F$ with ($c_\sigma \in \mathcal{C}$). Thus

$$\prod_{j=1}^m \sigma \left(\left(\sum_{i=1}^n a_{i,j} Y_i \right) \right) = c_\sigma \cdot \left(\prod_{j=1}^m \left(\sum_{i=1}^n a_{i,j} Y_i \right) \right)$$

Since $\mathcal{C}[Y_1, \ldots, Y_n]$ is a unique factorization domain and the elements of $\mathcal{C}$ are the only units, we must have $\sigma\left(\sum_{i=1}^n a_{i,j} Y_i\right) = c_{\sigma,j} \cdot \left(\sum_{i=1}^n a_{i,j'} Y_i\right)$, where $c_{\sigma,j} \in \mathcal{C}$. Since the action of $\mathcal{G}(L)$ on forms of degree one is the same in $\mathcal{C}[y_1, \ldots, y_n]$ and $\mathcal{C}[Y_1, \ldots, Y_n]$, we get that the m solutions $\sum_{i=1}^n a_{i,j} y_i$ of $L(y) = 0$ are sent to constant multiples of each other. In particular the logarithmic derivatives are permuted by $\mathcal{G}(L)$. The length of the orbit of any of these logarithmic derivatives under $\mathcal{G}(L)$ is at most m, which shows that all of these logarithmic derivatives are algebraic of degree at most m. $\square$

As an immediate consequence of the above result we have that if the form $F = \prod_{j=1}^m \left(\sum_{i=1}^n a_{i,j} Y_i\right)$ of degree m is not the product of forms of lower degree which are $\mathcal{G}(L)$-semi-invariant, then $\mathcal{G}(L)$ must act transitively on the logarithmic derivatives of $\sum_{i=1}^n a_{i,j} y_i$. We then get the following representation of the minimal polynomial $P(u)$ of the logarithmic derivatives:

$$P(u) = \prod_{j=1}^m \left(u - \frac{\left(\sum_{i=1}^n a_{i,j} y_i\right)'}{\sum_{i=1}^n a_{i,j} y_i} \right) \tag{4}$$

Thus, not only is the existence of the minimal polynomial equivalent to the existence of a $\mathcal{G}(L)$-semi-invariant form that factors into linear forms, but all coefficients of the minimal polynomial are given by the factorization of the

form. This remark can be found in [7] p. 52.
From the equation (4) we get:

Corollary 4 *If a $\mathcal{G}(L)$-semi-invariant form F which factors into linear forms $F = \prod_{j=1}^{m}(\sum_{i=1}^{n} a_{i,j}Y_i)$ factors into a product $\prod F_j$ of $\mathcal{G}(L)$-invariant (resp. semi-invariant) forms F_j of degree m_j, then the corresponding polynomial $P(u)$ of (4) will be the product of polynomials P_j of degree m_j whose roots are the logarithmic derivatives of solutions $\sum_{i=1}^{n} a_{i,j}y_i$ of $L(y) = 0$.*

The above result is a generalization of Theorem 2.1 of [19] (without the recursion for the other coefficients) which states that for second order equations the existence of a liouvillian solution is equivalent to the existence of an exponential solution of some symmetric power. This follows directly from the fact that a form in two variables over an algebraic closed field always factors into linear forms and that for second order equations the map $\psi_m : \mathcal{S}^m(V) \mapsto V_m$ is an isomorphism for all $m \in \mathbb{N}$ ([14], Lemma 3.5).

3 Bounds on the degree of the forms

For linear differential equations of order ≥ 3 the known algorithm for computing a liouvillian solution will compute the coefficients of the minimal polynomial of a solution or its logarithmic derivative by computing rational and exponential solutions of various symmetric powers $L^{\circledS m}(y) = 0$, i.e. the images under ψ_m of $\mathcal{G}(L)$-invariant forms. The main difficulties of this approach are, first, the combinatorial explosions of the complexity of computing the symmetric powers and, second, the many ways to choose the correct linear combinations among the rational/exponential solutions to get the coefficients. In what follows we show how to:

(i) Choose a first coefficient which *must* correspond to a minimal polynomial, i.e. the evaluation of a semi-invariant form that factors into linear forms.
(ii) Compute the other coefficients from the first in a unique way by factoring the semi-invariant form.

Since we will have to compute rational/exponential solutions of $L(y) = 0$ we will assume that k is a differential field over which such solutions can be computed (e.g. $(\mathbb{C}(x), d/dx)$). Algorithms which compute such solutions are described in [3,12] For $(\mathbb{C}(x), d/dx)$ the computation of an exponential solution is much more difficult than the computation of a rational solution. For irreducible second order equations it is shown in Theorem 4 of [19] that one can use only rational solutions. We will now give a similar result for third order equations using the result of [15].

Theorem 5 *If an irreducible third order linear differential equation $L(y) = 0$ with coefficients in k and $\mathcal{G}(L) \subset SL(3, \mathcal{C})$ has a liouvillian solution, then $L(y) = 0$ has a solution z, such that the logarithmic derivative $u = z'/z$ of z is algebraic over k of degree $m \in \{3, 6, 9, 21, 36\}$ and m is minimal with that property. To such a solution corresponds a $\mathcal{G}(L)$-semi-invariant form $F = \prod_{j=1}^{m} (\sum_{i=1}^{n} a_{i,j} Y_i)$ which factors into linear forms.*

(i) If $m = 3$ then $\mathcal{G}(L)$ is an imprimitive linear group. In this case F or F^2 is an invariant. We have the following possibilities:
   (a) If $\mathcal{G}(L) \cong E_{3,1}$, the extra special group of order 3^3 and exponent 3, or $\mathcal{G}(L) \cong (E_{3,1} \times (\mathbb{Z}/3\mathbb{Z}))$ then there are, up to multiples, 4 semi-invariant forms F.
   (b) Otherwise F is unique up to multiples.

(ii) If $m \neq 3$, then $\mathcal{G}(L)$ is a finite primitive linear group. There are, up to multiples, only finitely many possibilities for F and a unique one for $m = 9$ or $m = 21$. For $m \neq 6$, the semi-invariant F is an invariant. For $m = 6$ either F or F^2 is an invariant.

Proof. The existence of a solution z whose logarithmic derivative $u = z'/z$ of z is algebraic over k of degree $m \in \{36, 21, 9, 6, 3\}$ follows from [15], Theorem 3.3 where the minimality of m is also proven. From Theorem 3 we can associate to this solution a $\mathcal{G}(L)$-semi-invariant form F which factors into linear forms.
If $m = 3$ then $\mathcal{G}(L)$ is a monomial subgroup of $SL(3, \mathcal{C})$ and from [14], Proposition 3.6 we get that there exists a form F of degree 3 which is either a $\mathcal{G}(L)$-invariant form or whose square is a $\mathcal{G}(L)$-invariant form. From [18] Theorem 3.1 we get the result in the imprimitive case.
If $m \neq 3$, then $\mathcal{G}(L)$ must be a finite primitive group [14,15]. The stabilizer of the logarithmic derivative is a subgroup having a common eigenvector, i.e. a 1-reducible subgroup. From [15] we get that the finitely many 1-reducible subgroups of $\mathcal{G}(L)$ of minimal index (corresponding to an algebraic logarithmic derivative of minimal degree) are non abelian for each of the 8 finite primitive groups and thus have, up to multiples, one eigenvector. There are thus only finitely many minimal polynomials of degree m and thus, up to multiples, only finitely many forms of degree m that factor into linear forms. Decomposing the m-th symmetric power of the faithfull primitive characters of degree 3 of the 8 finite primitive subgroups of $SL(3, \mathbb{C})$ we get, except for $\mathcal{G}(L) \cong F_{36}^{SL_3}$, that all linear characters are trivial (for $m = 9, 21$ there is a unique trivial summand). For $\mathcal{G}(L) \cong F_{36}^{SL_3}$ the linear characters in the decomposition are of order 1 or 2. $\square$

A similar result holds for linear differential equations of any prime[4] order ([6,10,15,17]).

4 Computation of a liouvillian solution

We will present a general method, but focus on third order equations in the presentation. The existence of a liouvillian solution of a differential equation whose differential Galois group is unimodular is equivalent to the existence of a $\mathcal{G}(L)$-invariant form whose degree m belongs to a finite set determined by the order of the equation and which factors into linear forms. In order to transform this into an algorithm which computes liouvillian solutions we need to:

(i) Perform a variable transformation in order to get a differential equation whose differential Galois group is unimodular and which has a non trivial liouvillian solution if and only if the original equation does. One can also perform a second transformation with the property that, for given m, the kernel of ψ_m is trivial for the new equation.
(ii) Compute the invariant forms of given degree m.
(iii) Find among the invariant forms of degree m those that factors into a product of linear forms (for imprimitive groups and $F_{36}^{SL_3}$ we consider the square of the semi-invariant)
(iv) Factor the forms over $\mathbb{C}$ into linear factors and compute the other coefficients of the minimal polynomial of the logarithmic derivative corresponding to the form.

All points can be solved algorithmically for $k \subseteq \mathbb{C}(x)$:

4.1 Transformations

If the differential equation is not unimodular, then the transformation $z = y \cdot exp\left(-\frac{\int a_{n-1}}{n}\right)$ is a solution to the first problem (cf. [14], p. 18). We denote the new equation again by $L(y) = 0$. In order to compute the invariants of degree m we want $\psi_m : \mathcal{S}^m(V) \mapsto V_m$ to be an isomorphism. If $L^{\circledS m}(y) = 0$ is not of maximal order $\binom{n+m-1}{n-1}$, then we modify the equation $L(y) = 0$ into an equation $\tilde{L}(y)$ so that the groups $\mathcal{G}(L)$ and $\mathcal{G}(\tilde{L})$ are equivalent and so that the $\tilde{L}^{\circledS m}(y) = 0$ is of maximal order, i.e. so that $\psi_m : \mathcal{S}^m(V) \mapsto V_m$ is an isomorphism. This can be done by constructing an equation $\tilde{L}(y) = L^{(b_0,\ldots,b_{n-1})}(y)$

[4] For non prime order, the non-monomial imprimitive linear groups must be considered

where $b_i \in k$ and whose solution space is $\{z = \sum_{i=0}^{n-1} b_i y^{(i)} \mid L(y) = 0\}$. One can apriori choose the degree of the b_i so that the equation $L^{(b_0,\ldots,b_{n-1})}(y)$ will have the required properties ([16], Proof of Theorem 3.5 and [13], Example 3.3 and after). By construction $\tilde{L}(y) = 0$ will have a liouvillian solution whose logarithmic derivative is algebraic of degree m if and only if $L(y) = 0$ does.

Example 6 *For the equation*

$$L(y) = \frac{d^3 y}{dx^3} + \frac{32x^2 - 27x + 27}{36x^2(x-1)^2}\frac{dy}{dx} - \frac{64x^3 - 81x^2 + 135x - 54}{72x^3(x-1)^3}\, y = 0 \quad (5)$$

the map $\psi_3 : \mathcal{S}^3(V) \mapsto V_3$ is not an isomorphism, because $L^{\circledS 3}(y)$ is of order 7 and thus has a solution space which is of dimension 7 over $\mathbb{C}$, while $\mathcal{S}^3(V)$ is of dimension 10. We thus need to modify the equation by setting for example $z = y + y'$. The linear differential equation $\tilde{L}(y) = L^{(1,1,0)}(y)$ of lowest order whose solution space is $\{z = y + y' \mid L(y) = 0\}$ is:

$$\frac{d^3 y}{dx^3} + \frac{128x^5 - 98x^4 + 108x^3 + 378x^2 - 486x + 162}{x(x-1)(72x^6 - 216x^5 + 280x^4 - 126x^3 + 27x^2 + 81x - 54)}\frac{d^2 y}{dx^2} +$$

$$\frac{9477x - 13464x^7 + 2106x^4 + 29565x^3 - 26514x^2 - 1458 + 2304x^8 - 24840x^5 + 24872x^6}{36x^2(72x^6 - 216x^5 + 280x^4 - 126x^3 + 27x^2 + 81x - 54)(x-1)^2}$$

$$\frac{dy}{dx} + \frac{-4608x^6 + 28872x^5 - 67240x^4 + 115560x^3 - 131166x^2 + 78165x - 27135}{72x(72x^6 - 216x^5 + 280x^4 - 126x^3 + 27x^2 + 81x - 54)(x-1)^2}\, y$$

We thus have that $\mathcal{G}(L)$ is equivalent to $\mathcal{G}(\tilde{L})$. Computing $\tilde{L}^{\circledS 3}(y)$ we get that this equation is of order 10 and thus that $\psi_3 : \mathcal{S}^3(V) \mapsto V_3$ is an isomorphism for $\tilde{L}(y)$.

4.2 Computing the invariants

We propose to compute the invariants of degree m of $\mathcal{G}(L)$ by computing the m-th symmetric power of $L(y)$.
We will assume (eventually after a transformation described above) that ψ_m is an isomorphism. In this case there is a bijection between rational solution of $L^{\circledS m}(y) = 0$ and homogeneous invariants of degree m of $\mathcal{G}(L)$. We thus first compute a basis $\{f_1(x), \ldots, f_l(x)\}$ of the rational solution space of $L^{\circledS m}(y) = 0$ (cf. [3,12]). To get an expression of a rational solution in terms of solutions of $L(y) = 0$ we proceed in the following way:

(i) Pick a regular point $c \in \mathbb{C}$ of both $L(y) = 0$ and $L^{\circledS m}(y)$ and compute the Taylor series expansion of the fundamental set of solutions $\{y_1, \ldots, y_n\}$ of $L(y) = 0$ with $y_i^{(j-1)}(c) = \delta_{ij}$.

(ii) Decompose each rational solution into a homogeneous polynomial of the solutions y_i of $L(y)=0$. We set

$$f_j(x)=\sum_{i_1+\ldots+i_n=m} h_{j,i_1,\ldots,i_n} y_1^{i_1} y_2^{i_2}\cdots y_n^{i_n}$$

and equate the first $\binom{n+m-1}{n-1}$ coefficients of the Taylor series expansions. The corresponding linear system must have a unique solution since ψ_m is isomorphism.
This will give a representation $P_j(y_1,\ldots,y_n)$ of each $f_j(x)$ as a homogeneous polynomial in solutions which will correspond to the invariant $P_j(Y_1,\ldots,Y_n)$ of $\mathcal{G}(L)$.

If we work with $L^{\circledS m}(y)=0$ when this operator has order less than the dimension of the symmetric product of the solution space, then the linear system described in 2. will not have a unique solution. It will have a solution that depends on dim(ker ψ_m) parameters and not all of these solutions lead to invariants. In Proposition 9 we show that despite this fact, we can sometimes use the information to show that the original equation has Liouvillian solutions. The next example gives the calculation for an equation where the symmetric power has order lower than the dimension of the symmetric product of the solution space.

Example 7 *Consider the equation $L(y)=0$ given in (5). The set of exponential solutions of $L^{\circledS 3}(y)=0$, which is of order 7 instead of 10, is the one dimensional rational solution space spanned by $f(x)=x^2(x-1)$. In order to* determine *the corresponding polynomial invariant, we pick a regular point $c=-1$ of $L(y)=0$ and $L^{\circledS 3}(y)=0$ and consider the following series expansion of the solutions y_1, y_2 and y_3 with $y_1(-1)=1, y_2(-1)=0, y_3(-1)=0,$ $y_1{}'(-1)=0, y_2{}'(-1)=1, y_3{}'(-1)=0$ and $y_1{}''(-1)=0, y_2{}''(-1)=0, y_3{}''(-1)=1$ and get:*

$$\begin{aligned}
y_1(x) &= 1-\frac{167}{1728}(x+1)^3-\frac{169}{2304}(x+1)^4-\frac{28523}{497664}(x+1)^5\\
&\quad -\frac{559201}{11943936}(x+1)^6+O\left((x+1)^7\right)\\
y_2(x) &= (x+1)-\frac{43}{432}(x+1)^3-\frac{167}{2304}(x+1)^4-\frac{6931}{124416}(x+1)^5\\
&\quad -\frac{67717}{1492992}(x+1)^6+O\left((x+1)^7\right)\\
y_3(x) &= \frac{1}{2}(x+1)^2-\frac{43}{1728}(x+1)^4-\frac{167}{6912}(x+1)^5-\frac{16057}{746496}(x+1)^6\\
&\quad +O\left((x+1)^7\right)
\end{aligned}$$

Replacing $f(x)$, $y_1(x)$, $y_2(x)$ and $y_3(x)$ by their Taylor series in $x=-1$ in

$$f(x) = \sum_{i_1+i_2+i_3=3} h_{i_1,i_2,i_3} y_1^{i_1} y_2^{i_2} y_3^{i_3}$$

we get an inhomogeneous linear system whose solution space is of dimension 3, due to the kernel of $\psi_3 : \mathcal{S}^3(V) \mapsto V_3$. We get an expression for $f(x)$ depending on 3 parameters α, β, γ:

$$4y_1^3 - 12y_1^2y_2 + \left(\frac{59717}{16641} - \frac{20736}{1849}\gamma - \frac{144}{43}\alpha\right) y_1^2 y_3 + \left(-\frac{5561}{1032} - \frac{144}{43}\beta\right) y_1y_2y_3$$
$$\left(\frac{372949}{33282} + \frac{10368}{1849}\gamma + \frac{72}{43}\alpha\right) y_1 y_2^2 + \alpha y_1 y_3^2 + \left(-\frac{5171}{1548} + \frac{72}{43}\beta\right) y_2^3 +$$
$$\left(\frac{225373}{111456} + \frac{72}{43}\gamma\right) y_2^2 y_3 + \beta y_2 y_3^2 + \gamma y_3^3$$

4.3 Finding an invariant that factors into linear forms

The set of forms of degree m which factor into linear forms is a closed algebraic subvariety in $\mathcal{S}^m(\mathbb{C}^n)$ whose defining equations, the *Brill equations*, can be derived ([4], p. 127 and p. 140). In order to find those invariants that factor into linear forms, we consider a linear combination of a basis of the invariants of degree m $\sum_{j=1}^r \lambda_j P_j(Y_1, \ldots, Y_n)$, plug the coefficients into the Brill equations and solve for $\lambda_1, \ldots, \lambda_r$ by computing a Gröbner basis.
When one restricts oneself to irreducible third order equations, one computes the *Brill equations* for certain forms (resp. squares of forms) that factor into linear forms. Theorem 5 (working with increasing m) implies that there will always be, up to multiples, a finite set of possible forms if $ker(\psi_m)$ is trivial. The fact that the solution set is finite makes the computation of the Gröbner basis easier.
In the following example we give the *Brill equations* for forms of degree three in three variables and apply them to the situation of Example 7.

Example 8 *A form*

$$Y_3^3 + (a_0Y_1 + a_1Y_2)Y_3^2 + (b_0Y_1^2 + b_1Y_1Y_2 + b_2Y_2^2)Y_3$$
$$+(c_0Y_1^3 + c_1Y_1^2Y_2 + c_2Y_1Y_2^2 + c_3Y_2^3)$$

factors into linear forms over $\mathbb{C}$ if and only if ([2], p. 181)

$$0 = (1/3)a_0P + 3b_2c_0 - a_1^2c_0 + c_1(a_0a_1 - b_1) + b_0c_2$$
$$0 = (1/3)a_1P + 3b_0c_3 - a_0^2c_3 + c_2(a_0a_1 - b_1) + b_2c_1$$
$$0 = -(1/3)b_0P - a_0b_2c_0 + a_1b_1c_0 - a_1b_0c_1 - 3c_0c_2 + c_1^2$$
$$0 = -(1/3)b_1P + a_1b_2c_0 - a_0b_2c_1 - a_1b_0c_2 + a_0b_0c_3 - 9c_0c_3 + c_1c_2$$

$$0 = -(1/3)b_2P - a_1b_0c_3 + a_0b_1c_3 - a_0b_2c_2 - 3c_1c_3 + c_2^2$$

where

$$P = a_0^2b_2 + a_1^2b_0 - 4b_0b_2 - b_1(a_0a_1 - b_1) - a_1c_1 - a_0c_2$$

Consider the forms:

$$\begin{aligned}
F_1 &= 4y_1^3 - 12y_1^2y_2 + \frac{59717}{16641}y_1^2y_3 + \frac{372949}{33282}y_1y_2^2 - \frac{5561}{1032}y_1y_2y_3 - \frac{5171}{1548}y_2^3 \\
&\quad + \frac{225373}{111456}y_2^2y_3 \\
F_2 &= -\frac{20736}{1849}y_1^2y_3 + \frac{10368}{1849}y_1y_2^2 + \frac{72}{43}y_2^2y_3 + y_3^3 \\
F_3 &= -\frac{144}{43}y_1^2y_3 + \frac{72}{43}y_1y_2^2 + y_1y_3^2, \qquad F_4 = -\frac{144}{43}y_1y_2y_3 + \frac{72}{43}y_2^3 + y_2y_3^2
\end{aligned}$$

In order to find which of the forms $F_1 + \lambda_2F_2 + \lambda_3F_3 + \lambda_4F_4$ factors into linear forms we plug the coefficients (polynomials in $\lambda_2, \lambda_3, \lambda_4$) into the above Brill equations and get a polynomial system in the variables $\lambda_2, \lambda_3, \lambda_4$. This system has 15 solutions which are the 15 values of $\lambda_2, \lambda_3, \lambda_4$ for which the form $F_1 + \lambda_2F_2 + \lambda_3F_3 + \lambda_4F_4$ factors into linear forms. One solution of the system is

$$\lambda_2 = \frac{2699}{186624},\ \lambda_3 = \frac{47}{144},\ \lambda_4 = -\frac{523}{1728} \tag{6}$$

which correspond to the form:

$$\begin{aligned}
F &= 4y_1^3 - 12y_1^2y_2 + \frac{7}{3}y_1^2y_3 + \frac{71}{6}y_1y_2^2 - \frac{35}{8}y_1y_2y_3 + \frac{47}{144}y_1y_3^2 \\
&\quad - \frac{277}{72}y_2^3 + \frac{221}{108}y_2^2y_3 - \frac{523}{1728}y_2y_3^2 + \frac{2699}{186624}y_3^3
\end{aligned}$$

which is irreducible over $\mathbb{Q}$ but factors over $\mathbb{C}$.

The Brill equations do not provide a factorization, but only determine a polynomial system for the parameter values for which a linear combination of forms factor into linear forms. One then needs to effectively compute an *absolute factorization* of the forms. For the above form F, the *AFactor* algorithm of MAPLE computes the following factorization [5] of F:

$$4\left(y_1+\left(-\frac{5684}{8595}+\frac{122\alpha}{955}-\frac{72\alpha^2}{955}\right)y_2+\left(-\frac{2842}{8595}-\frac{833\alpha}{1910}-\frac{36\alpha^2}{955}\right)y_3\right)$$

$$\left(y_1+\left(-\frac{5684}{8595}+\frac{122\beta}{955}-\frac{72\beta^2}{955}\right)y_2+\left(-\frac{2842}{8595}-\frac{833\beta}{1910}-\frac{36\beta^2}{955}\right)y_3\right)$$

$$\left(y_1+\left(-\frac{10259}{8595}-\frac{122\alpha}{955}-\frac{122\beta}{955}-\frac{72\left(-\frac{25}{6}-\alpha-\beta\right)^2}{955}\right)y_2\right.$$

$$\left.+\left(\frac{51107}{34380}+\frac{833\alpha}{1910}+\frac{833\beta}{1910}-\frac{36\left(-\frac{25}{6}-\alpha-\beta\right)^2}{955}\right)y_3\right)$$

Where α is a root of $Q_1(z)=93312z^3+388800z^2+510624z+216161$ and β is a root of $Q_2(z)=36z^2+(36\alpha+150)z+150\alpha+36\alpha^2+197$

To compute a linear differential equation whose m^{th} symmetric power has maximal order, in general gives a new operator with very complicated coefficients and it may be very expensive to compute rational or exponential solutions of the symmetric power of this new equation. The following proposition allows us to occasionally avoid such a transformation and use the original equation even when the symmetric power is not of maximal order.

Proposition 9 *Let k be as above and let $L(y)=0$ be a linear differential equation with coefficients in k. Let $\{y_1,\ldots,y_n\}$ be a fundamental set of solutions of $L(y)=0$ in the associated PVE and let W_m be the space of homogeneous polynomials of degree m in variables $Y_1,\ldots,Y_n$. Assume that the set $\mathcal{S}$ of polynomials $P(Y_1,\ldots,Y_n)$ in W_m such that*

(i) *$P(Y_1,\ldots,Y_n)$ factors into linear factors, and*

(ii) $$\frac{(P(y_1,\ldots,y_n))'}{P(y_1,\ldots,y_n)}\in k$$

is a finite union of one dimensional subspaces of W_m. Then $L(y)=0$ has a liouvillian solution.

Proof. The assumptions imply that there exist $P_1,\ldots,P_t\in\mathcal{S}$ such that any element of $\mathcal{S}$ is a constant multiple of some P_i. Let K be the associated PVE

[5] The explicit form of the factorization obtained by *AFactor* depends on the name of the variables used to represent the form.

and let $\mathcal{G}(L)$ be the Galois group. For $P \in \mathcal{S}$, and $\sigma \in \mathcal{G}(L)$, the polynomial $P(\sigma(Y_1), \ldots, \sigma(Y_n))$ again factors into linear factors and

$$\frac{(P(\sigma(y_1), \ldots, \sigma(y_n)))'}{P(\sigma(y_1), \ldots, \sigma(y_n))} \in k$$

Therefore $P(\sigma(Y_1), \ldots, \sigma(Y_n)) = c_\sigma P_i(Y_1, \ldots, Y_n)$ for some $c_\sigma \in \mathcal{C}$ and some i. In particular, the element σ will map each linear factor of $P(Y_1, \ldots, Y_n)$ to a linear factor of one of the P_i. This implies that the orbit of such a linear factor $l(Y_1, \ldots, Y_n)$ under the action of $\mathcal{G}(L)$ is contained in the set of constant multiples of a finite set of linear polynomials. Therefore the orbit of $(l(y_1, \ldots, y_n))'/(l(y_1, \ldots, y_n))$ is finite and so $l(y_1, \ldots, y_n)$ is a solution of $L(y) = 0$ whose logarithmic derivative is algebraic. □

The finite (up to multiples) set of forms in the Proposition may not be an invariant, but the product of the forms belonging to the same $\mathcal{G}(L)$-orbit will be a semi-invariant that factors into linear forms [6]. It is thus sufficient to consider products of the forms belonging to the set.

Example 10 *Consider the equation $L(y) = 0$ given in (5). From Example 8 we get that there are, up to mutiples, 15 forms in the set $\mathcal{S}$. Thus $L(y) = 0$ has a Liouvillian solution. In this case $\mathcal{S}$ consists of one $\mathcal{G}(L)$-orbit of length 1 and seven $\mathcal{G}(L)$-orbits of length 2.*

4.4 Computing the remaining coefficients of the minimal polymial

Using the factorization of the (semi-)invariant one gets Taylor series expansions of arbitrary precision of the factors using the same initial conditions for $k \subseteq \mathbb{C}(x)$ than those used to compute the invariant. One can use these expansions of the factors to compute the coefficients of the minimal polynomial of an algebraic logarithmic derivative corresponding to the form.
Let

$$\begin{aligned} P(u) &= \prod_{i=1}^{m} \left(u - \frac{\delta(z_i)}{z_i} \right) && (7) \\ &= u^m - \frac{\delta\left(\prod_{i=1}^{m} z_i\right)}{\prod_{i=1}^{m} z_i} u^{m-1} + \ldots + (-1)^m \prod_{i=1}^{m} \frac{\delta(z_i)}{z_i} && (8) \\ &= u^m + b_{m-1}(x) u^{m-1} + \ldots + b_0(x) && (9) \end{aligned}$$

[6] An orbit of length > 1 is the result of an imprimitive permutation representation of $\mathcal{G}(L)$ on the linear forms in the factors of that orbit.

be the minimal polynomial of an algebraic logarithmic derivative of a solution of $L(y) = 0$. Let

$$F(Y_1, \ldots, Y_n) = \prod_{j=1}^{m} \left(\sum_{i=1}^{n} a_{i,j} Y_i \right)$$

be a semi-invariant form of degree m that factors into linear forms and assume that we have obtained the factors. Let $z_j = \sum_{i=1}^{n} a_{i,j} y_i$, where the y_i form a fundamental set of solutions whose Taylor series can be determined to arbitrary precision. Assume that we have a bound N on the degrees of the numerators and of the denominators of the coefficients $b_i(x)$ of P (such a bound can be determined, c.f., [9,10] and [5] for related bounds). We write

$$b_r(x) = \frac{\sum_{t=0}^{N} c_{r,t} x^t}{\sum_{s=0}^{N} d_{r,s} x^s}$$

with the $c_{i,j}, d_{i,j}$ indeterminates. Equations 8 and 9 let us conclude that we can calculate the Taylor expansion $T_r(x)$ of each b_r in terms of the Taylor expansions of the z_i and so can calculate these to arbitrary order. Comparing powers of x in the equation

$$\sum_{t=0}^{N} c_{r,t} x^t = T_r(x) \sum_{s=0}^{N} d_{r,s} x^s$$

yields an infinite system of linear equations for the $c_{i,j}, d_{i,j}$. The first $2N$ of these equations will determine b_r. To see this, note that if p_1/q_1 and p_2/q_2 are rational functions whose numerators and denominators have degrees bounded by N and whose Taylor series agree up to order $2N$, then $p_1/q_1 - p_2/q_2 = (p_1q_2 - p_2q_1)/q_1q_2$ has a Taylor series T beginning with terms of order $2N+1$ or higher. Since $p_1q_2 - p_2q_1 = T(q_1q_2)$ we must have $p_1q_2 - p_2q_1 = 0$. This is, of course, a very inefficient way to find these solutions. Alternate methods for a related problem are discussed in [5] and we would expect these methods to yield more efficient algorithms in this situation as well.

Example 11 *Consider the equation $L(y) = 0$ given in (5) which, by Example 10, has liouvillian solutions. In order to compute a liouvillian solutions we, a priori, need to consider products of the 15 forms corresponding to the values found in Example 8. In fact, as we will see, the values (6) immediately yield an invariant (i.e., a $\mathcal{G}(L)$-orbit of length 1). We will try to compute a minimal polynomial $P(u) = b_3(x)u^3 + b_2(x)u^2 + b_1(x)u + b_0(x)$ ($b_i(x) \in \mathbb{C}[x]$) corresponding to this form, i.e. where $b_2(x)/b_3(x)$ is the logarithmic derivative of $f(x) = x^2(x-1)$.*
In order to bound the degrees of the $b_i(x)$ we use the method given in [1],

pp. 93–95 for the fuchsian case (cf. [9]). The exponents of $L(y)$ at 0 are $3/2, 1, 1/2$, at 1 they are $4/3, 1, 2/3$ and at ∞ they are $-2/3, -1, -4/3$. We must have $deg(b_3) \leq m(l+k)$ where $m = 3$ is the degree of $P(u)$, $k = 2$ is the number singular points $c_i \neq \infty$ of $L(y) = 0$ and l is the number of zeros of $b_3(x)$ which are not singular points of $L(y) = 0$. One has that

$$l \leq -mr - \left(\sum_{j=1}^{k} \left(\sum_{i=1}^{3} \alpha_{j,i} \right) \right)$$

where the $\alpha_{j,i}$ are possibly repeated exponents at the singular points $c_i \neq \infty$ and r is the smallest exponent at ∞. Thus $l \leq 0.5$ which gives $deg(b_3) \leq 6$. According to [1] we get $deg(b_i) \leq 6 + i$ for $i \in \{2, 1, 0\}$.
We now take Taylor series of the solutions y_i in Example 7 up to order 17 and compute the series ld_1, ld_2 and ld_3 of the logarithmic derivatives of the factors of F given in Section 4.3. For $i \in \{2, 1, 0\}$ the elementary symmetric functions $(-1)^i \sigma_i(ld_1, ld_2, ld_3)$ must correspond to the coefficients b_{3-i}/b_3. We get the following polynomial $P(u)$:

$$u^3 - \frac{2(2x-1)}{(x-1)x}u^2 + \frac{64x^2 - 63x + 15}{12(x-1)^2x^2}u - \frac{512x^3 - 745x^2 + 351x - 54}{216(x-1)^3x^3}$$

Whose zeros are all logarithmic derivatives of solutions of $L(y) = 0$.

If we know that the form that factors into linear forms is an invariant of $\mathcal{G}(L)$ (e.g. if $ker(\psi_m)$ is trivial), then the above method will always give a unique polynomial $P(u)$ whose zeros are all logarithmic derivatives of solutions. If the invariant is not the product of semi-invariants of lower degree, then $P(u)$ will be irreducible.

Acknowledgement

We would like to thank Bernd Sturmfels for pointing us to the Brill equations.

References

[1] A. Boulanger, Contribution à l'étude des équation différentielles linéaires homogènes intégrable algébriquement, *J. École Polytechnique série 2* **4** (1898) 1–122.

[2] A. Brill, Ueber die Zerfällung einer Ternärform in Linearfactoren, *Math. Ann.* **50** (1898) 157–182.

[3] M. Bronstein, Solutions of linear differential equations in their coefficient field, *J. Symb. Comp.* **13** (1992) 413–439.

[4] I.M. Gelfand, M.M. Kapranov and A.V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, (Boston: Birkhäuser 1994).

[5] M. van Hoeij, Factorization of Differential Operators with Rational Coefficients, *preprint, Department of Mathematics, University of Nijmegen* (1995).

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

[7] M.F. Marotte, Équations différentielles linéaires et la théorie des groupes, *Annales Fac. de Toulouse* **12** (1898).

[8] S. Lang, *Algebra, Second Edition*, (Addison Wesley, New York, 1984).

[9] M.F. Singer, Algebraic solutions of n-th order linear differential equations, *Proceedings of the 1979 Queens Conference on Number Theory*, (Queens Papers in Pure and Applied Mathematics **54** 1980).

[10] M.F. Singer, Liouvillian Solutions of n^{th} Order Linear Differential Equations, *Am. J. Math.* **103** (1981) 661–682.

[11] M.F. Singer, An outline of differential Galois theory, in: E. Tournier, ed., *Computer Algebra and Differential Equations* (Academic Press, New York, 1990).

[12] M.F. Singer, Liouvillian solutions of linear differential equations with liouvillian coefficients, *J. Symb. Comp.* **11** (1991) 251–273.

[13] M.F. Singer, Testing reducibility of linear differential operators: a group theoretic perspective, *Appl. Alg. in Eng. Comm. and Comp.* **7** (1996) 77–104.

[14] M.F. Singer and F. Ulmer, Galois groups of second and third order linear differential equations, *J. Symb. Comp.* **16** (1993) 1–36.

[15] M.F. Singer and F. Ulmer, Liouvillian and algebraic solutions of second and third order linear differential equations, *J. Symb. Comp.* **16** (1993) 37–73.

[16] M.F. Singer and F. Ulmer, Necessary Conditions for Liouvillian Solutions of (Third Order) Linear Differential Equations, *Appl. Alg. in Eng. Comm. and Comp.* **6** (1995) 1–22.

[17] F. Ulmer, On Liouvillian solutions of differential equations, *Appl. Alg. in Eng. Comm. and Comp.* **2** (1992) 171–193.

[18] F. Ulmer, Linear differential equations of prime order, *J. Symb. Comp.* **18** (1994) 385–401.

[19] F. Ulmer and J.A. Weil, Note on Kovacic's algorithm, (Preprint Université de Rennes 1, 1995), *to appear in J. Symb. Comp.*