Liouvillian solutions of linear differential equations of order three and higher

Mark van Hoeij*& Jean-François Ragot†& Felix Ulmer‡& Jacques-Arthur Weil§

September 30, 1997

Abstract

In [SUl97], Singer and Ulmer gave an algorithm to compute Liouvillian ("closed-form") solutions of homogeneous linear differential equations. However, there were several efficiency problems that made computations not practical. In this paper we address these problems. We extend the algorithm in [HWe97] to compute semi-invariants and a theorem in [SUl97] in such a way that, by computing one semi-invariant that factors into linear forms, one gets *all* coefficients of the minimal polynomial of an algebraic solution of the Riccati equation, instead of only one coefficient. This way we no longer need to do large computations to obtain the remaining coefficients. These remaining coefficients come "for free" as a byproduct of our algorithm for computing semi-invariants. We specifically detail the algorithm in the cases of equations of order 3 (order 2 equations are handled by the Kovacic algorithm [Kov86, UWe96, Fak97]).
In the appendix, we present several methods to decide when a multivariate polynomial depending on parameters can admit linear factors, which is a keystone in the algorithm.

1 Introduction

In this paper k will denote a differential field whose field of constants $\mathcal{C}$ is algebraically closed of characteristic 0. For the computations, however (Section 2.2), we will consider more concretely the field $\mathbb{C}(x)$ with the usual derivation d/dx. We denote by $L = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ $(a_i \in k)$ a differential operator and by $L(y) = y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_0 y = 0$ the corresponding linear homogeneous differential equation.

*Florida State University , hoeij@math.fsu.edu
†Université de Limoges, ragot@cict.fr
‡Université de Rennes, ulmer@univ-rennes1.fr
§Université de Limoges, weil@unilim.fr

We refer to [Mag94, Sin97] for definitions of a *Picard-Vessiot extension* (PVE) of k, of the *differential Galois group* G and of *Liouvillian solutions* of $L(y) = 0$. A PVE K of k for L is a differential field extension $K = k < y_1, \dots, y_n >$, where $\{y_1, \dots, y_n\}$ a fundamental set of solutions, with no new constants in K. It is the equivalent of a splitting field for $L(y) = 0$. Under our assumptions a PVE exists and is unique up to differential automorphisms. We denote the solution space $\{y \in K | L(y) = 0\}$ of an operator L by $V(L)$. The dimension of $V(L)$ equals the order of L. The differential Galois group G of L, which is the group of differential automorphisms of K/k, is a linear algebraic group over $\mathcal{C}$. The group G acts faithfully on the vector space $V(L)$, and so G can be viewed as a subgroup of $GL(V(L))$. There is a Galois correspondence between algebraic subgroups of G and differential subfields of the PVE of $L(y) = 0$. The fixed field of G under this correspondence is k. A solution of $L(y) = 0$ in k is called a *rational solution*, a solution in an algebraic extension of k is called an *algebraic solution*, a solution whose logarithmic derivative is in k is called an *exponential solution* and a solution belonging to a field obtained by successive adjunctions of exponentials, exponentials of integrals and algebraic extensions is called a *Liouvillian solution*. If L has a Liouvillian solution then L also has a Liouvillian solution of the form $y = \exp(\int r)$ where $r \in \overline{k}$ is an algebraic function [Sin81].

Definition 1 *An element r of the PVE is called a* Riccati solution *of L if r is the logarithmic derivative $r = y'/y$ of some solution y of L. If r is an algebraic Riccati solution (a Riccati solution in $\overline{k}$) then the minimum polynomial of r over k is called a* Riccati polynomial *of L.*

Definition 2 *An element $I \in Sym^m(V(L))$ is called a* semi-invariant *of the differential Galois group G of L of degree m if there is a character χ of G of degree 1 such that $\forall g \in G$ the action of g on I is $g(I) = \chi(g)I$. I is called an* invariant *if χ is the trivial character, i.e. $\forall g \in G$, $g(I) = I$.*

We call a polynomial or semi-invariant *completely factorable* if it is a product of linear factors. It is known (see section 2 in [SUl97]) that an algebraic Riccati solution r of degree m over k corresponds to a completely factorable semi-invariant I of degree m of the differential Galois group G. In [SUl97] the Riccati polynomial of r is computed as follows:

1. Compute (bases of) the spaces of all semi-invariants of a given degree
2. For each such space, compute a linear combinations of the basis corresponding to a completely factorable semi-invariant I. If such a linear combination is found, then $L(y) = 0$ has an algebraic Riccati solution and the first coefficient of the associated Riccati polynomial is given by I.
3. In [SUl97] the factorization of I into linear forms is used to compute the remaining coefficients.

The goal of this paper is, if a Liouvillian solution exists, to compute an algebraic Riccati solution and its minimum polynomial over k in an efficient way.
First we extend the algorithm in [HWe97] for computing invariants to the case of semi-invariants. If a completely factorable semi-invariant is known and given in a certain form, then theorem 1 immediately gives us all coefficients of the Riccati polynomial. This central result avoids the third step above and makes the computation much more feasible in practice.
In the appendix we discuss methods for finding the linear combinations of the basis corresponding to a completely factorable semi-invariant I (second step). If the dimension of the vector space of semi-invariants for a character is high then it is a very costly step. This can be resolved by looking at semi-invariants (not always of minimal degree) which are guaranteed to be completely factorable. This is particularly interesting because of the third step above, i.e. the factorization, is no longer needed. The result is a Kovacic-like algorithm for order$(L) = 3$, given in section 4.

Acknowledgments: We thank Anne Bellido, Marius van der Put and Michael F. Singer for fruitful conversations during the makeup of this paper.
J.A.Weil specially thanks Marius van der Put and the NWO AIDA project for their material and immaterial support.
This research was partially supported by the European Cathode II working group and, for the third author, also by the Calife project (INTAS-RBFR 95-0412). Most computations were realized thanks to the French CNRS-GDR Medicis.

2 Semi-invariants of differential Galois groups

2.1 The formalism

The basis of our approach is the following useful formalism:

Proposition 1 *([HWe97], Proposition 2.5) Let K be the Picard-Vessiot extension and G the differential Galois group of L. Define the $\mathcal{C}$-algebra homomorphism*

$$\phi : Sym(V(L)) \to K[X_1, \ldots, X_n]$$

by (it suffices to define ϕ for homogeneous elements $\overline{y}$ of degree 1)

$$\phi(\overline{y}) = \sum_{i=1}^{n} X_i y^{(i-1)} \quad \text{for} \quad y \in V(L).$$

Here $\overline{y}$ is the element of $Sym^1(V(L)) \subset Sym(V(L))$ that corresponds to the solution $y \in V(L) \subset K$ of L. Then ϕ is an embedding (as $\mathcal{C}$-algebra and as G-module) of $Sym(V(L))$ in $K[X_1, \ldots, X_n]$, where the action of G on $X_1, \ldots, X_n$ is trivial.

Often the two vector spaces $V(L)$, which is a subset of K, and $Sym^1(V(L))$, which is a subset of $Sym(V(L))$, are identified. In this paper we can not do so because multiplication in K is not the same as multiplication in $Sym(V(L))$.
The following extension of Theorem 3 of [SUl97] illustrates the usefulness of the above formalism and is central to our approach.

Theorem 1 *Let $L(y) = 0$ be a homogeneous linear differential equation over k. Let K be a Picard-Vessiot extension of k for L and G be its differential Galois group. Assume that G has a semi-invariant $I \in Sym^m(V(L))$ that is a product of linear factors and assume that the degree m of I is minimal with this property. Let $P(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ be its canonical image Let a be the coefficient of X_1^m in P. Then:*

1. $a \neq 0$
2. *Let $Q := \frac{1}{a}P(X, -1, 0, \ldots, 0)$. Then $Q \in k[X]$ and Q is a Riccati polynomial.*

Proof. The invariant I is completely factorable, so $I = \prod_{i=1}^m \overline{y}_i$ where $\overline{y}_i \in Sym^1(V(L)) \subset Sym(V(L))$ and $y_i \in V(L)$ are the corresponding solutions of $L(y) = 0$. Thus, as $P = \phi(I)$, we have

$$P = \prod_{i=1}^{m}(y_i X_1 + y_i' X_2 + \cdots + y_i^{(n-1)} X_n)$$

If $g \in G$ then $g(y_i) = c_i y_j$ (with $c_i \in \mathcal{C}$) for some j because of the uniqueness of factorization in $Sym(V(L))$ (which is isomorphic to a polynomial ring in n variables over $\mathcal{C}$). Hence G permutes the set $\{\frac{y_1'}{y_1}, \ldots, \frac{y_m'}{y_m}\}$. The action of G on this set is transitive because m is minimal. Note that $a = \prod y_i \neq 0$ because $P \neq 0$.

$$Q = \prod_{i=1}^{m} \frac{1}{y_i}(y_i \cdot X + y_i' \cdot (-1) + y_i'' \cdot 0 + \cdots + y_i^{(n-1)} \cdot 0) = \prod_{i=1}^{m}(X - \frac{y_i'}{y_i}).$$

Since G permutes the $\frac{y_i'}{y_i}$ it follows that Q is invariant under G and hence by the Galois correspondence $Q \in k[X]$. Q is irreducible because the action of G on the $\frac{y_i'}{y_i}$ is transitive. The Riccati solutions $\frac{y_i'}{y_i}$ are the roots of Q and hence they are algebraic functions with minimum polynomial Q. □

Remark: with notations as above, if m is not minimal, then it is easily seen that the polynomial Q is either irreducible or is a product of Riccati polynomials. Conversely, theorem 3 of [SUl97] (combined with our theorem) shows immediately that any Riccati polynomial is obtained that way. This is used (implicitly) in section 4.

The algorithm presented in [HWe97] computes the invariants I of G by computing their images $\phi(I)$. The reason for using ϕ in [HWe97] was to be able to compute invariants without having to compute symmetric powers $Sym^m(L)$. In the following this same approach is extended to the computation of semi-invariants. The above then shows that this approach does not only produce the semi-invariant whose logarithmic derivative is the first coefficient of the Riccati polynomial, but in fact gives all the coefficients. This makes this algorithm for computing (semi-) invariants very attractive for finding Liouvillian solutions. We now proceed with the computation of semi-invariants via the above formalism

Lemma 1 *The image of a semi-invariant under the embedding ϕ is an element of $a \cdot k[X_1, \ldots, X_n]$ where $a = \exp(\int y)$ for some $y \in k$.*

Proof. Let I be a semi-invariant of degree m, and $P = \phi(I)$. Because ϕ is a G-homomorphism, $g(P) = \chi(g) \cdot P$ for some character χ. Let $a \in K$ be one of non-zero coefficients of $P \in K[X_1, \ldots, X_n]$. Now $g(\frac{1}{a}P) = g(\frac{1}{a})\chi(g)P = \left(a\, g(\frac{1}{a})\, \chi(g)\right) \frac{1}{a}P$. The action of G on the X_i is trivial, so that the coefficients of $g(\frac{1}{a}P)$ are just the image of the corresponding coefficients under g. One of the coefficients of $\frac{1}{a}P$ equals 1 and since $g(1) = 1$ the corresponding coefficient of $g(\frac{1}{a}P)$ must also be 1. Hence $\forall g \in G$, $ag(\frac{1}{a})\chi(g) = 1$ and so $\frac{1}{a}P$ is, i.e. all its coefficients are, invariant under G. By the Galois correspondence

$$\frac{1}{a}P \in k[X_1, \ldots, X_n].$$

Furthermore $\forall g \in G$, $g(a) = \chi(g) \cdot a$ showing that a'/a is left invariant by G and thus $a'/a \in k$. $\square$

Definition 3 *For $t \in k$ the k-automorphism $\mathcal{S}_t^*$ of $k[\partial]$ is defined by $\mathcal{S}_t^*(\partial) = \partial + t$.*

Let $V(L) \subset K$, $a \in K$ and assume $t = a'/a \in k$. Then multiplication by a is a 1-1 map

$$\cdot a : V(L) \to V(\mathcal{S}_{-t}^*(L)).$$

It is a G-isomorphism if and only if $a \in k$. The map $\cdot a$ induces a map

$$Sym^m(V(L)) \to Sym^m(V(\mathcal{S}_{-t}^*(L))).$$

We would like to view this map as multiplication by a^m. This is problematic, however, because $Sym^m(V(L))$ is not a K-vector space but a $\mathcal{C}$-vector space; multiplication by a^m is not defined on $Sym^m(V(L))$. Instead we will examine which map $\cdot a$ induces on $\phi(Sym(V(L))) \subset K[X_1, \ldots, X_n]$. This induced map on $\phi(Sym(V(L)))$ is denoted by ϕ_a. A solution $y \in V(L)$ is mapped by $\cdot a$ to ay. Now $(ay)' = ay' + a'y = a(y' + ty)$ where $t = a'/a \in k$, and $(ay)^{(i)} = a(y^{(i)} + A(t, i, i-1)y^{(i-1)} + \cdots + A(t, i, 0)y)$ for some $A(t, i, j) \in k$. So ϕ_a acts on $(yX_1 + y'X_2 + \cdots + y^{(n-1)}X_n)$ as the following substitution:

$$(X_1, X_2, \ldots, X_n)^t \mapsto aA \cdot (X_1, X_2, \ldots, X_n)^t \tag{1}$$

where A is a lower triangular matrix, with 1's on the diagonal, and entries $A_{i,j} = A(t, i-1, j-1) \in k$ below the diagonal. Because all elements of $\phi(Sym^m(V(L)))$ are sums of products of expressions of the form $yX_1 + y'X_2 + \cdots + y^{(n-1)}X_n$, the substitution (1) describes ϕ_a. On the vector of all monomials in $X_1, \ldots, X_n$ of degree m, ϕ_a acts as $a^m M$ for some unipotent matrix M (computed from matrix A) with entries in k. If $S = b \cdot I$ is a semi-invariant of degree m (using the embedding ϕ we will identify semi-invariants with elements of $K[X_1, \ldots, X_n]$) where $b'/b \in k$ and $I \in k[X_1, \ldots, X_n]$ then $\phi_a(S)$ is a semi-invariant of the form $a^m b I'$ for some $I' \in k[X_1, \ldots, X_n]$. In particular, $\phi_a(S)$ is an invariant if and only if $a^m b \in k$.

Definition 4 *The equivalence relation $\sim_*$ on k is defined as follows: $t_1 \sim_* t_2$ when there exists $y \in k$ for which $t_1 - t_2 = y'/y$.*

Let L be a differential operator and K the Picard-Vessiot extension. Let $S \in \phi(Sym^m(V(L)) \subset K[X_1, \ldots, X_n]$ be a semi-invariant of degree m. So $S = a \cdot I \in K[X_1, \ldots, X_n]$ for some $a \in K$, $I \in k[X_1, \ldots, X_n]$. Let $t_1 = a'/a \in k$. Then $\phi_{\exp(\int -t/m)}(S)$ is an invariant of $\mathcal{S}^*_{t/m}(L)$ if and only if $t \sim_* t_1$.

2.2 Computation of semi-invariants

In this section we assume that $k = \mathbb{C}(x)$.
Algorithm Semi-invariants.
Input: a differential operator $L \in \mathbb{C}(x)[\partial]$ of order n, and an integer m.
Output: all semi-invariants of degree m.
Step 1. Compute a finite set $B \subset \mathbb{C}(x)/\sim_*$ such that for all semi-invariants aI of L, $a \in K$, $I \in \mathbb{C}(x)[X_1, \ldots, X_n]$ the equivalence class of $\frac{a'}{a}$ is an element of B.
Step 2. For each element of B take a representant $t \in \mathbb{C}(x)$ and compute the invariants of $\mathcal{S}^*_{t/m}(L)$. These correspond to semi-invariants of L.

Note that this algorithm resembles Beke's algorithm for computing exponential solutions $\exp(\int t)$ with $t \in \mathbb{C}(x)$. We give the same sketch of this algorithm as in section 4 in [Hoe97]:
Step 1. Compute a finite set $B \subset \mathbb{C}(x)/\sim_*$ such that for all exponential solutions a one has $(\frac{a'}{a} \bmod \sim_*) \in B$.
Step 2. For each element of B take a representant $t \in \mathbb{C}(x)$ and compute the rational solutions of $\mathcal{S}^*_t(L)$. Return the corresponding exponential solutions of L.

Computation of set B in step 1 of algorithm semi-invariants:
In [HWe97] and [Hoe97] a generalization of the classical notion of exponents has been defined. A generalized exponent is an element of $\mathbb{C}[x^{-1/r}]$ for some integer r (called the ramification index). In the regular singular case the generalized exponents are the

exponents and the ramification index is 1 in this case. For $t \in \mathbb{C}(x)$ and $p \in \mathbb{P}^1(\mathbb{C})$ denote $EP_p(\partial - t) \in \mathbb{C}[x^{-1}]/\mathbb{Z}$ as the generalized exponent $e \in \mathbb{C}[x^{-1}]$ at the point p of $\partial - t$ modulo the integers. $EP_p(\partial - t)$ is the exponential part of $\partial - t$ at p. Now t modulo $\sim_*$ is determined by the $EP_p(\partial - t)$ for all p (see [Hoe97]).

Let $e \in \mathbb{C}[x^{-1}]$ be the generalized exponent of $\partial - t$ at the point p. Then e/m is the generalized exponent of $\partial - t/m$ at p. The generalized exponents of $\mathcal{S}^*_{t/m}(L)$ at p equal $-e/m$ plus the generalized exponents of L at p. So the generalized exponents of the monomials in lemma 4.1 in [HWe97] for $\mathcal{S}^*_{t/m}(L)$ are $-e$ plus the generalized exponents of the monomials for L. According to this lemma 4.1, at least one of those generalized exponents should be in $\frac{1}{r}\mathbb{Z}$ (where r is the ramification index at p) if $\mathcal{S}^*_{t/m}(L)$ has an invariant. This leaves only finitely many possibilities for e modulo $\mathbb{Z}$ and hence for $EP_p(\partial - t) = e + \mathbb{Z} \in \mathbb{C}[x^{-1}]/\mathbb{Z}$.

At regular points, there is only one possibility for $e + \mathbb{Z}$, namely $e + \mathbb{Z} = \mathbb{Z}$, because $r = 1$ and the generalized exponents are integers at regular points.

At a singular point p, we can compute all generalized exponents of L, and all generalized exponents of the monomials in the lemma (these are sums of m generalized exponents of L) and so we can compute a finite set of possible values of $EP_p(\partial - t)$. If $p_1, \ldots, p_l$ are the singularities, and we find N_i possible $EP_{p_i}(\partial - t)$ then we have $N = N_1 \cdot N_2 \cdots N_l$ possible combinations, so we find at most[1] N possible values of t modulo $\sim_*$. These t modulo $\sim_*$ are the elements of the set B in the algorithm.

A comment on step 2: Note that we need to compute invariants of many (the number of elements of B) operators. It can be faster first to apply the heuristic algorithm in [HWe97], and to apply the complete algorithm invariants in [HWe97] only for the cases when the heuristic does not prove that no invariants exist.

Another efficiency improvement can be obtained as follows: For computing the invariants of $\mathcal{S}^*_{t/m}(L)$ we need the generalized exponents of $\mathcal{S}^*_{t/m}(L)$ at all singularities. However, these can be easily computed from t and the generalized exponents of L. Furthermore we compute with formal solutions of $\mathcal{S}^*_{t/m}(L)$ at one singularity, but these can be computed from the formal solutions of L. This way we only need to compute generalized exponents and formal solutions of L, not of each $\mathcal{S}^*_{t/m}(L)$ for every $t \in B$.

Note that our algorithm for computing semi-invariants has the same drawback as Beke's algorithm for computing exponential solutions: If the singularities or the generalized exponents involve algebraic extensions over the coefficients field then the algorithm may need to compute in exponentially large algebraic extensions. For $m = 1$ it is in fact the same algorithm.

[1] not for any combination of exponential parts needs a corresponding t exist because there exists one relation between the exponential parts, called Fuchs' relation (lemma 9.2 in [Hoe97])

Sometimes, e.g. step [2.1] in section 4.1, we need to compute only those semi-invariants whose n-th power is rational (with $n \in \mathbb{N}$ given). The computation is then shorter: in step 2 of algorithm semi-invariants, we need only to consider those $t \in B$ for which $nt \sim_* 0$ (i.e. the generalized exponents of $\partial - t$ are in $\frac{1}{n}\mathbb{Z}$). This will be used in section 4.

2.3 Constructors of semi-invariants

In this part, we gather some results from [Wei95b] that will be used in section 4
Let X denote the transposed vector $(X_1, \ldots, X_n)^t$. Let D be the derivation on $K[X_1, \ldots, X_n]$ defined by $D(X) = -A^t X$ and D is the usual derivation on K. Then, $\phi(Sym(V(L))) = \{P \in K[X_1, \ldots, X_n] : D(P) = 0\}$ ([Wei95a])[2].
Let S be a semi-invariant of degree m, and $P = \phi(S)$ be its canonical image in $K[X_1, \ldots, X_n]$. In this setting, it is shown in [Wei95b] (proposition 50, section 6, page 57) that the Hessian of P (with respect to $X_1, \ldots, X_n$) is again, up to multiples, the canonical image of a semi-invariant (same results hold for the bordered Hessian and the Jacobian). Thus, once a semi-invariant is known, we can apply directly Hessians and related constructors on its canonical image (see [Wei95b] section 6.3 page 65 for a fairly detailed example). In view of theorem 1, this will allow us (in section 4) to construct Riccati polynomials of high degrees directly from invariants of small degree.

3 Computing Liouvillian solutions of equations of order n

Lemma 2 *If L is reducible and L has a Liouvillian solution then L has an irreducible right-hand factor $R \in \mathbb{C}(x)[\partial]$ for which R has a Liouvillian solution.*

Proof. The Liouvillian solutions of L form a subspace of $V(L)$ that is invariant under the differential Galois group. Hence there exists a right-hand factor R' having this subspace as solution space. Now take for R any irreducible right-hand factor of R'. □

From the fact that an operator M that has a Liouvillian solution must have a solution of the form $\exp(\int r)$ for some algebraic function $r \in \overline{\mathbb{C}(x)}$, i.e. M has a right-hand factor of order 1 in $\overline{\mathbb{C}(x)}[\partial]$, it follows by induction that if all solutions are Liouvillian then M is completely factorable in $\overline{\mathbb{C}(x)}[\partial]$ (i.e. M is a product of operators of order 1). Conversely, if M is completely factorable then all solutions are Liouvillian. Hence the operator R' in the lemma is the highest order right-hand factor of L that is completely factorable in $\overline{\mathbb{C}(x)}[\partial]$.

[2] In fact, this derivation turns $K[X_1, \ldots, X_n]$ to a differential module isomorphic to $Sym\,(\mathcal{D}/\mathcal{D}L)$.

1 Reducible case. If L is reducible and has a Liouvillian solution then according to the lemma there exists an irreducible right-hand factor that has a Liouvillian solution. Though there may be infinitely many different right-hand factors, there are only finitely many *types* (see [Tsa96, Sin95]) of irreducible right-hand factors. For each type we need to compute one right-hand factor and compute the Liouvillian solutions of that factor. This way we find a Liouvillian solution of L, if such solution exists.

2 Ireducible case case. In [SUl93b] and references therein, the authors give an upper bound for the lowest degree of (if it exists) a Riccati polynomial of L. So, by checking a finite number of degrees, one can decide if a Riccati polynomial exists. For each possible degree m, compute the semi-invariants of degree m and check (see appendix A) if there is a completely factorable semi-invariant. If so, return the corresponding Riccati polynomial.

In the algorithms the irreducible case is usually split into the imprimitive and the primitive case (containing only a finite list of possible groups); this is explained in [SUl93b]. Also, several ideas from section 4 below can be re-used when handling equations of higher order (e.g the fact that knowing in advance which groups to check for makes it very easy to check only a small number of degrees for the semi-invariants).

4 Computing Liouvillian solutions of equations of order 3

The general algorithm can be improved in several ways. First of all, the computation of semi-invariants can often be avoided. For example in the case that L is irreducible of order 2, we know from [UWe96] that it is sufficient to compute only invariants, which are easier to compute than semi-invariants.

The factorization of a semi-invariant (cf. appendix A) becomes a problematic step if the number of parameters is not small. For second order equations this problem does not occur because any invariant will factor into linear forms. For third order equations we will use section 2.3 to find invariants that are guaranteed to factor, so that appendix A can be avoided in most cases.

Furthermore we can reduce the size and number of different degrees m that need to be checked by studying the possible Galois groups.

In this section, we develop along these guidelines a Kovacic-like algorithm for computing Liouvillian solutions of linear differential equations of order 3. For the possible Galois groups, we follow the notations from [SUl93a, SUl93b].

4.1 The algorithm

Let $L = \partial^3 + a_2\partial^2 + a_1\partial + a_0$ where the $a_i \in \mathbb{C}(x)$. If there exists an $f \in k$ such that $f'/f = a_2$, then $G \subset SL_3$; if not, then we may first apply $\mathcal{S}^*_{-a_2/3}$ on L so that $a_2 = 0$. Hence, we may assume in all that follows that the Galois group is unimodular, i.e $G \subset SL_3$.
Remark: the sentence "there are s invariants of degree m" should be read as "the vector space of invariants of degree m has dimension s".

1 Reducible case.

[1.1] If L can be written as $L_1 \cdot (\partial - r)$ for some $r \in \mathbb{C}(x)$ then let $a = \exp(\int r)$ and compute a basis y_1, y_2 of solutions of L_1. Return $a, a\int (y_1/a), a\int (y_2/a)$.

[1.2] If L allows only a factorization $L = L_1L_2$, where L_2 has order 2. Then apply the Kovacic algorithm on L_2. If a basis of Liouvillian solutions is found, then (assume that L is monic) L can be factored as $(\partial - r)(\partial - a)(\partial - b)$ for some algebraic functions a and b and rational function r. Let $z_1 = \exp(\int a - b)$ and $z_2 = \int \exp(\int r - a)$. Then $y_1 = \exp(\int b)$, $y_2 = y_1 \int z_1$ and $y_3 = y_1 \int z_1 z_2$ is a basis of Liouvillian solutions of L.

2 Imprimitive case: Do one of the following steps, [2.1] or [2.2]:

[2.1] Compute all semi-invariants of degree 3 whose square is invariant (see the remark at the end of section 2.2). Decide if one of these semi-invariants has a linear factor (use Appendix A if there is a semi-invariant linearly depending on parameters[3]). Return the corresponding Riccati polynomial Q (see theorem 1).

[2.2] Compute invariants of degree 6 and decide which of those is a square (see Appendix A4). The corresponding square roots are all semi-invariants of degree three whose square is invariant. Now proceed as in [2.1].

3 Compute the invariants of degree 2. If there is one (there can not be more) compute the invariants of degree 6:

[3.1] Either there is ONE invariant of degree 6; then $G \simeq PSL_2$ and there is no Liouvillian solution.

[3.2] Or there are TWO invariants of degree 6; then $G \simeq A_5$. Return either the unique Riccati polynomial of degree 6 (the corresponding completely factorable invariant must be found in a space of dimension 2) or the unique Riccati polynomial of degree 15 corresponding to the unique invariant of degree 15.

4 Compute invariants of degree 4. If there is one (there can not be more), then $G \simeq G_{168}$. Return the Riccati polynomial of degree 21 corresponding to the unique invariant of degree 21.

[3] i.e. a vector space of semi-invariants corresponding to the same character.

5 Compute invariants of degree 6.

[5.1] If there are no such invariants, then

[5.1.1] If there is one invariant of degree 9 (there can not be more), then $G \simeq H_{216}^{SL_3}$. Return the corresponding Riccati polynomial of degree 9..

[5.1.2] Else, the group is SL_3 and there are no Liouvillian solutions.

[5.2] If there is ONE invariant of degree 6, then

[5.2.1] If the invariant is a cube (Appendix A4), then $G \simeq PSL_2 \times C_3$ and there are no Liouvillian solutions

[5.2.2] If there is one invariant of degree 9 (there can not be more), then $G \simeq H_{72}^{SL_3}$. Return the corresponding Riccati polynomial of degree 9.

[5.2.3] If there is an invariant[4] of degree 12 which is the cube of a semi-invariant S (Appendix A4), then $G \simeq G_{168} \times C_3$. Return the Riccati polynomial of degree 21 corresponding to the unique invariant of degree 21.

[5.2.4] Else $G \simeq A_6^{SL_3}$. Return the Riccati polynomial of degree 45 corresponding to the unique invariant of degree 45.

[5.3] If there are TWO invariants of degree 6, then

[5.3.1] If there is one invariant of degree 9 (there can not be more), then $G \simeq F_{36}^{SL_3}$; Return the corresponding Riccati polynomial of degree 9.

[5.3.2] Else, $G \simeq A_5 \times C_3$. Return either the unique Riccati polynomial of degree 6 (the corresponding completely factorable invariant must be found in a space of dimension 2) or the Riccati polynomial of degree 15 corresponding to the unique invariant of degree 15.

4.2 Practical remarks on the algorithm

We note that, in practice, some cases from the algorithm can be fastly excluded by the necessary conditions from [SUl94] and/or the heuristic from section 4.1 in [HWe97]. For example, if the equation is not Fuchsian, then there are Liouvillian solutions if and only if step 1 or step 2 succeeds.

One consequence of the above algorithm is that we can decide whether an irreducible third order equation has Liouvillian solutions by using only invariants of degrees 2,4,6,9.

Another remark concerns the rationality problem: The algorithm we use for computing invariants, unlike for semi-invariants, does not introduce algebraic extensions in its

[4]Alternatively, at this step, one could directly search for a (unique) semi-invariant of degree 4 whose cube is rational. Or, to avoid factorisation, one could compute the dimension of the space of invariants of degree 18 (dimension 2 for $G_{168} \times C_3$ and dimension 3 for $A_6^{SL_3}$).

output $\phi(I)$. The only case of an irreducible operator L of order 3 where we compute a Riccati polynomial that may require an extension of the constant field is the imprimitive case (there may be an extension of degree at most 4, see [HvP94, Ulm94]), because this is the only case where semi-invariants and appendix A need to be used.

Choosing step [2.2] instead of [2.1] to handle the imprimitive case has several extra advantages. For example, in step 3 and 5, we need not recompute the invariants of degree 6 (note, however, that one can not safely perform step 3 before step 2). Also, if the dimension of the space of invariants of degree 6 is bigger than 2, then we know automatically that the group is imprimitive (this follows from the properties of the primitive subgroups of $SL_3(\mathbb{C})$). Furthermore we do not need to compute semi-invariants (such computations could involve large algebraic extensions) this way.

4.3 Correctness of the algorithm

The fact that the successions of tests proposed in the algorithms yield the correct groups follow from the decomposition of the symmetrisations of the characters (cf. [SUl93a]) for all primitive subgroups of SL_3. To prove that the corresponding degrees of algebraic Riccati solutions are correct, we proceed by inspection of all imprimitive and finite primitive subgroups of SL_3.

4.3.1 Imprimitive groups

Assume that G is irreducible. If there is a semi-invariant of degree 3, then the group is either imprimitive or $F_{36}^{SL_3}$ (cf. [SUl93a], Table 2 and Proposition 3.6). In both case there is a Liouvillian solution. If the group is $F_{36}^{SL_3}$, then there is no semi-invariant of degree 3 corresponding to a character of order 2 (i.e. whose square is an invariant). Thus, if there is a semi-invariant of degree 3 corresponding to a character of order 2 (i.e. whose square is rational) then the group must be imprimitive. An imprimitive group of degree 3 is monomial, i.e. there exists a basis $\{y_1, y_2, y_3\}$ such that an element of G has only one non zero entry in row and column. Since $G \subset SL(3, \mathbb{C})$, we have $\forall g \in G$, $g(y_1y_2y_3) = \pm y_1y_2y_3$ (cf. [SUl93a], Proposition 3.6). There are at least one and at most 4 Riccati polynomials of degree 3 in this case (cf. [HvP94, Ulm94]).

4.3.2 A_5

Lemma 3 *If $G \simeq A_5$, then there is exactly one Riccati polynomial of degree 6 and exactly one of degree 15.*
The Riccati polynomial of degree 6 can be obtained by applying complete factorization on the 2-dimensional space of invariants of degree 6.
The canonical image of the invariant of degree 15 is obtained the following way: compute the images P_2 and P_6 of the invariants of degrees 2 and 6. Let P_{10} be their bordered

Hessian, and P_{15} be the Jacobian of these three[5].

Proof. That there exists a Riccati polynomial of degree 6 is proven in [SUl93b]. Its uniqueness follows from the fact that there are 6 conjugated non-Abelian subgroups of index 6 having each one common eigenvector. So we turn to degree 15.
There are 5 conjugated subgroups of order 4 in A_5 which are all Abelian of exponent 2. Using the matrix representation of A_5 given in [SUl93b], we get that one such group, say H, is generated by the matrices $\{E_2E_1E_2E_3E_2E_1, E_3E_1\}$ which have

$$[\frac{9}{46}+\frac{1}{23}\alpha^3+\frac{3}{46}\alpha^2-\frac{27}{46}\alpha, 1, -\frac{27}{46}\alpha+\frac{1}{23}\alpha^3+\frac{3}{46}\alpha^2+\frac{55}{46}]$$

as a common eigenvector, where $\alpha^4+2\alpha^3-7\alpha^2-8\alpha+31=0$ and

$$\begin{aligned}\sqrt{5} &= -\frac{2}{23}\alpha^3-\frac{3}{23}\alpha^2+\frac{27}{23}\alpha+\frac{14}{23}\\ \xi=\sqrt[5]{1} &= \frac{2}{23}\alpha^3+\frac{3}{23}\alpha^2-\frac{4}{23}\alpha-\frac{14}{23}\end{aligned}$$

In order to find the corresponding semi-invariant that factors into linear forms, we look at a set

$$\mathcal{S}=\{id, E_1^{-1}, E_2^{-1}, E_3^{-1}, E_2^{-1}E_1^{-1}, E_1^{-1}E_2^{-1}, E_2^{-1}E_3^{-1}, E_1^{-1}E_2^{-1}E_1^{-1}, E_3^{-1}E_2^{-1}E_1^{-1},$$
$$E_1^{-2}E_2^{-1}, E_2^{-1}E_1^{-1}E_2^{-1}, E_1^{-1}E_2^{-1}E_3^{-1}, E_1^{-2}E_2^{-1}E_1^{-1}, E_3^{-1}E_1^{-1}E_2^{-1}E_1^{-1}, E_1^{-1}E_3^{-1}E_2^{-1}E_1^{-1}\}$$

of left coset representatives of H in A_5. The resulting polynomial

$$\prod_{g\in\mathcal{S}}\left(g\left(\left(\frac{9}{46}+\frac{1}{23}\alpha^3+\frac{3}{46}\alpha^2-\frac{27}{46}\alpha\right)y_1+y_2+\left(-\frac{27}{46}\alpha+\frac{1}{23}\alpha^3+\frac{3}{46}\alpha^2+\frac{55}{46}\right)y_3\right)\right)$$

which by construction factors into linear forms over the complex numbers, is a semi-invariant and thus an invariant[6] of the simple group A_5. The length of the orbit of the logarithmic derivative of the eigenvector, i.e. the degree of its minimal polynomial, divides $15=[A_5:H]$. From [SUl93b] we know that this degree must be ≥ 6, so the degree must be 15 and that the associated polynomial must be the minimal polynomial of the logarithmic derivative of a solution which is algebraic of degree 15. Note that there is, up to multiple, a unique invariant of degree 15 which thus must factor into linear forms.
The statement on the construction of the invariant of degree 15 from the invariants of degree 2 and 6 follows from the uniqueness and from a simple direct computation on classical invariants ([MBD38] paragraph 125 pp 253–255). □

---

[5]Note that P_{15} is unique and does not depend on the choice of P_6.

[6]This invariant does not correspond to the invariants given in [SUl93b] where another basis of the solution space has been chosen in order to express the invariants

4.3.3 G_{168}

Lemma 4 *If $G \simeq G_{168}$, then there is a unique Riccati polynomial of degree 21. Its canonical image P_{21} is obtained the following way. Let P_4 be the image of the invariant of degree 4, let P_6 be its Hessian, and let P_{14} be the bordered Hessian of P_4 and P_6; then P_{21} is obtained from the Jacobian of P_4, P_6, P_{14}.*

Proof. From [SUl93b] we get that there exists a Riccati polynomial of degree 21. Since the group is simple, any semi-invariant must be an invariant. There is a unique trivial summand in the decomposition of the character of the 21-th symmetric power of the faithful irreducible unimodular 3-dimensional characters, we get that the semi-invariant must correspond to the, up to multiple, unique invariant of degree 21 and thus factor into linear forms. The corresponding group H and the coset representatives are given in [SUl93b].
The statement on P_{21} follows from the uniqueness and from direct computation on classical invariants ([MBD38] paragraph 125 pp 253–255). □

4.3.4 $H_{216}^{SL_3}$

From [SUl93b] we get that there exists Riccati polynomial of degree 9. Since there is no non-trivial character of degree 1 and a unique trivial summand in the decomposition of the character of the 9-th symmetric power of the faithful irreducible unimodular 3-dimensional characters, we get that the semi-invariant must correspond to the, up to multiple, unique invariant of degree 9 which thus must factor into linear forms. The corresponding group H and the coset representatives are given in [SUl93b].

4.3.5 $H_{72}^{SL_3}$

From [SUl93b] we get that there exists Riccati polynomial of degree 9. Since there is no non-trivial character of degree 1 and a unique trivial summand in the decomposition of the character of the 9-th symmetric power of the faithful irreducible unimodular 3-dimensional characters, we get that the semi-invariant must correspond to the, up to multiple, unique invariant of degree 9 which thus must factor into linear forms. The corresponding group H and the coset representatives are given in [SUl93b].

4.3.6 $G_{168} \times C_3$

The, up to multiple, unique invariant of degree 21 of G_{168} which by the above factors into linear forms is, since its order is divisible by 3, also an invariant of C_3 and thus an, up to multiple, unique invariant of $G_{168} \times C_3$ which factors into linear forms. Since 21 is the minimal degree of a Riccati polynomial in this case (cf. [SUl93b]), it must correspond to a Riccati polynomial. This Riccati polynomial can be constructed from the semi-invariant of degree 4 (whose cube is rational) as in section 4.3.3.

4.3.7 $A_6^{SL_3}$

Lemma 5 *If $G \simeq A_6^{SL_3}$, then there is exactly one Riccati polynomial of degree 45, and it is obtained from an invariant.*
The corresponding Riccati polynomial is obtained the following way: let P_6 be the invariant of degree 6, let P_{12} be the Hessian of P_6, and let P_{30} be the bordered Hessian of P_6 and P_{12}. Then P_{45} is obtained from the Jacobian of P_6, P_{12}, P_{30}.

We note that there is also a Riccati polynomial of degree 36 ([SUl93b]) but we know of no simple formula to obtain it; furthermore, the space of invariants of degree 36 for $A_6^{SL_3}$ has dimension 5 so selecting the completely factorable invariant would be a very hard task.
Proof. There are 3 types of non conjugated subgroups of order 24 in $A_6^{SL_3}$. Only one type consisting of 45 conjugated non Abelian subgroups of order 24 is 1-reducible (The elements have exactly one common eigenvector). Using the matrix representation of $A_6^{SL_3}$ given in [SUl93b], we get that one such group, say H, is generated by the matrices $\{E_4E_1E_2E_3E_1E_2E_1^-1E_4, (E_4E_1^-1)^2, E_3E_2E_4E_3, E_3E_4E_3\}$ which have

$$[-\frac{24}{23} - \frac{3}{46}\alpha^3 + \frac{7}{46}\alpha^2 - \frac{29}{46}\alpha, \frac{5}{23}\alpha - \frac{5}{46}\alpha^3 + \frac{2}{23}\alpha^2 - \frac{11}{46}, 1]$$

as a common eigenvector (here we use the same notation as for A_5).
In order to find the corresponding semi-invariant that factors into linear forms, we look at a set $\mathcal{S}$ of left coset representatives of H in $A_6^{SL_3}$ (containing 45 elements). Since the group is perfect and has no non-trivial character of degree 1, the semi-invariant must be an invariant. There is, up to multiple, only one invariant of degree 45 for this group which thus must factor into linear forms by the above. The length of the orbit of the logarithmic derivative of the eigenvector divides $45 = [A_6^{SL_3} : H]$. From [SUl93b] we get that this degree must be ≥ 36 and thus that the degree must be 45 and that the associated polynomial must be a Riccati polynomial of degree 45. The statement on P_{45} follows from the uniqueness and from direct computation on classical invariants ([MBD38] paragraph 125 pp 253–255). □

4.3.8 $F_{36}^{SL_3}$

There are 9 conjugated subgroups of order 12 in $F_{36}^{SL_3}$ which are all Abelian. Using the matrix representation of $F_{36}^{SL_3}$ given in [SUl93b], we get that one such group, say H, is generated by the matrices $\{V\,T\,S\,T\,V, S\,T\,S^{-1}\,T^{-1}, T\,S\,V\,S^{-1}\}$ which have $[-\epsilon^3, 0, 1]$ (with $\epsilon^6 + \epsilon^3 + 1 = 0$, cf. [SUl93b]) as a common eigenvector. In order to find the corresponding semi-invariant that factors into linear forms, we look at a set $\mathcal{S} = \{id, S^{-1}, T^{-1}, S^{-2}, T^{-1}S^{-1}, T^{-2}, T^{-1}S^{-2}, T^{-2}S^{-1}, T^{-2}S^{-2}\}$ of left coset representatives of H in $F_{36}^{SL_3}$. The resulting polynomial

$$\prod_{g\in\mathcal{S}} \left(g(-e^3y_1 + y_3)\right) = -y_3^3y_2^6 + y_1^3y_2^6 - y_1^6y_2^3 + y_3^6y_2^3 - y_3^6y_1^3 + y_1^6y_3^3$$

which by construction factors into linear forms over the complex numbers, is in fact an invariant[7] of $F_{36}^{SL_3}$ (check using the generators). The length of the orbit of the logarithmic derivative of the eigenvector, i.e. the degree of its minimal polynomial, divides $9 = [F_{36}^{SL_3} : H]$. From [SUl93b] we know that this degree must be ≥ 6, so the degree must be 9 and the associated minimal polynomial must be an irreducible Riccati polynomial of degree 9.

4.3.9 $A_5^{SL_3} \times C_3$

The, up to multiple, unique invariant of degree 15 of A_5 which by the above factors into linear forms is, since its order is divisible by 3, also an invariant of C_3 and thus an, up to multiple, unique invariant of $A_5 \times C_3$ which factors into linear forms. Since 6 is the minimal degree of a Riccati polynomial in this case (cf. [SUl93b]), it must correspond to a Riccati polynomial.

4.3.10 Example

$$L = \partial^3 + \frac{21\,(x^2 - x + 1)}{25\,x^2\,(x^2 - 2\,x + 1)}\partial - \frac{21\,(5\,x - 2 - 3\,x^2 + 2\,x^3)}{50\,x^3\,(x^3 - 3\,x^2 + 3\,x - 1)}$$

The operator is irreducible. There is a two-dimensional space of invariants of degree 6. None of them is a square so we proceed to step 3. There is one invariant of degree 2, so we know that $G/Z(G) \simeq A_5^{SL_3}$.
The invariants of degree 6 (variables $\overline{y}_i$, parameters a_1, a_2) are:

$$\begin{aligned}&(2560\,a_1 - 30\,a_2)\,{\overline{y}_1}^3\,{\overline{y}_2}^3 + 6\,\overline{y}_3\,{\overline{y}_1}^5\,a_1\\&\quad + (-1024\,a_1 + 30\,a_2)\,{\overline{y}_3}^6 - 393216\,\overline{y}_3\,{\overline{y}_2}^5\,a_1\\&\quad + (15360\,a_1 - 90\,a_2)\,\overline{y}_1\,\overline{y}_2\,\overline{y}_3^4 + 90\,{\overline{y}_3}^2\,{\overline{y}_2}^2\,{\overline{y}_1}^2\,a_2\end{aligned}$$

Using a complete factorization approach, we find that for $256a_1 = 3a_2$ we have the following factor (up to conjugation):

$$\overline{y}_1 - \alpha^2\overline{y}_2 + \alpha\overline{y}_3, \qquad \text{where} \;\; \alpha^5 - 256 = 0$$

and the remaining factor is simply $\overline{y}_1$.
The coefficients of the corresponding canonical image are:

$$\Big[-4608\,x^4\,(x-1)^4,\; -3072\,(-1 + 2\,x)\,x^3\,(x-1)^3,\\ \quad - 1536/5\,x^2\,\Big(7\,x^2 - 7\,x - 3\Big)\,(x-1)^2,$$

[7] Note that if the result would be a semi invariant, one could find the corresponding one dimensional character using this construction.

$$
\begin{aligned}
&-\frac{1536}{25}\,x^2\left(133\,x^2-133\,x+33\right)(x-1)^2,\\
&-\frac{2304}{125}\,x\,(x-1)\,(-1+2\,x)\left(77\,x^2-77\,x-34\right),\ -\frac{110592}{625}\\
&+\frac{1204224}{625}\,x^3-\frac{602112}{625}\,x^4-\frac{562176}{625}\,x-\frac{39936}{625}\,x^2,\\
&-\frac{13824}{125}\,x\,(x-1)\,(7\,x-4)\,(-1+2\,x)\,(7\,x-3),\ \frac{262656}{625}\\
&+\frac{4666368}{625}\,x^3-\frac{2333184}{625}\,x^4-\frac{479232}{625}\,x-\frac{1853952}{625}\,x^2,\\
&-\frac{3072\,(-1+2\,x)\,(637\,x^4-1274\,x^3+25\,x^2+612\,x+126)}{3125\,x\,(x-1)},\ \ldots\Big]
\end{aligned}
$$

From this, we read the coefficients of the minimum polynomial of an algebraic solution of the corresponding Riccati equation using theorem 1. We use rows that correspond to the monomials $X_1^l X_2^{6-l}$, $l=0,1,\ldots,6$. The way we numbered the monomials $X_1^{l_1}X_2^{l_2}X_3^{6-l_1-l_2}$, this corresponds to rows 1, 2, 4, 7, 11, 16, 22. We obtain:

$$
\begin{aligned}
X^6 &- 4\,\frac{(-1+2\,x)\,X^5}{x\,(x-1)}+\frac{(133\,x^2-133\,x+33)\,X^4}{5\,x^2\,(x-1)^2}\\
&-\frac{12\,(7\,x-4)\,(-1+2\,x)\,(7\,x-3)\,X^3}{25\,x^3\,(x-1)^3}\\
&+\frac{(351-11662\,x^3+5831\,x^4-2862\,x+8693\,x^2)\,X^2}{125\,x^4\,(x-1)^4}\\
&-\frac{4\,(-1+2\,x)\,(9604\,x^4-19208\,x^3+14275\,x^2-4671\,x+567)\,X}{3125\,x^5\,(x-1)^5}\\
&+\frac{(16807\,x^4-33614\,x^3+24907\,x^2-8100\,x+972)\,(-1+2\,x)^2}{12500\,x^6\,(x-1)^6}
\end{aligned}
$$

Alternatively, we can avoid the factoring by using sections 2.3 and 4.3.2 to construct directly the (unique) Riccati polynomial of degree 15 via bordered hessian and Jacobian applied on the invariants of degree 2 and 6. The result is the following irreducible Riccati polynomial:

$$
\begin{aligned}
X^{15} &- 6\,\frac{(7\,x^4-14\,x^3-4\,x^2+11\,x-3)}{x\,(x-1)\,(-2+x)\,(-1+2\,x)\,(x+1)}X^{14}\\
&+\frac{21\,(49\,x^4-98\,x^3-20\,x^2+69\,x-18)}{5\,x^2\,(x+1)\,(-2+x)\,(x-1)^2}X^{13}\\
&-\frac{13\,(9604\,x^6-28812\,x^5+19119\,x^4+9782\,x^3-15741\,x^2+6048\,x-756)}{50\,x^3\,(-2+x)\,(-1+2\,x)\,(x+1)\,(x-1)^3}X^{12}\\
&+\frac{13\,(50421\,x^6-151263\,x^5+107203\,x^4+37699\,x^3-71843\,x^2+27783\,x-3402)}{125\,x^4\,(x+1)\,(-2+x)\,(x-1)^4}X^{11}+\ldots
\end{aligned}
$$

Appendix A: Deciding when a homogeneous polynomials admits linear factors

If A is a ring, we denote by $A[X_1, \ldots, X_n]_m$ the space of homogeneous polynomials of total degree m in the variables X_i. Let $P \in \mathbb{C}[t_1, \ldots, t_s][X_1, \ldots, X_n]_m$ be homogeneous of degree m in the variables X_i. In this appendix, we show how to compute potential values of the parameters t_i such that P (then viewed as a homogeneous polynomial in $\mathbb{C}[X_1, \ldots, X_n]$) admits a linear factor. The subproblem relevant in this paper is the following: Let $P = \sum t_i P_i$ where $P_i \in \mathbb{C}[X_1, \ldots, X_n]_m$. Decide for which values of the t_i the polynomial P admits a linear factor.
This problem is part of the general problem of absolute factorization of polynomials. For the latter, the reader may consult [Rag97] where several methods and abundant references are proposed.

A1: Brill's equations

Completely factorable polynomials of degree m form a Zariski closed set. The defining equations, the Brill equations, are homogeneous equations of degree m that can be computed (c.f. [GKZ94, Bri98]). This can be used (c.f. [SUl97]) to select the completely factorable semi-invariants.

A2: Complete factorization of non-parametrized polynomials

If there are no parameters in P, then many methods exist ([Hoh95, KFF88] and [Rag97] for another method and references). We outline below a method that seems, from our experience, to be the most interesting. The tools and results are similar to the ones that are used in the three papers mentionned above.
Let C be a perfect field (usually C is $\mathbb{Q}$ or a finite extension of $\mathbb{Q}$).

Definition 5 Let P be a polynomial of $C[X_1, \ldots, X_n]_m$ of degree $d > 0$ in X_1. A $n-1$-uplet $(a_2, \ldots, a_n)$ of C^{n-1} is called a *non critical value* for P in X_1 if the polynomial $P(T, a_2, \ldots, a_n)$ is square-free and of degree d. This implies in particular that all roots of $P(T, a_2, \ldots, a_n)$ are simple.

Remark : The existence of such a non-critical value for P implies that P is square-free.
From now on, let $\underline{Z}$ denote the multi-variable $X_3, \ldots, X_n$.

Lemma 6 *Let P be a homogeneous square-free polynomial of $C[X_1, X_2, \underline{Z}]_m$, of degree $d > 0$ in X_1. Assume that P is of degree m in X_2, and let $(1, 0, \ldots, 0)$ be a non critical value for P in X_1. Denote by $p(T)$ the polynomial $P(T, 1, \underline{0})$ and let α be a root of $p(T)$. Then $P(X_1 + \alpha X_2, X_2, \underline{Z})$ is of degree $m - 1$ in X_2.*

*Proof.*Let $\bar{P}(X_1, X_2) = P(X_1, X_2, \underline{0})$. It is a homogeneous polynomial of $C[X_1, X_2]$. Write

$$\bar{P} = X_2^{m-d} \sum_{i=0}^{d} b_i\, X_1^i\, X_2^{d-i}\,;$$

It factors in $\overline{C}[X_1, X_2]$ as

$$b\, X_2^{m-d} \prod_{i=1}^{d} (X_1 - \alpha_i\, X_2)$$

where the α_i, with i from 1 to d, are the roots of $p(T)$. Hence

$$\bar{P}(X_1 + \alpha\, X_2, X_2) = b\, X_2^{m-d} \prod_{i=1}^{d} (X_1 + (\alpha - \alpha_i)\, X_2)\ .$$

The roots of $p(T)$ are simple, so $\alpha - \alpha_i = 0$ for one unique i, which proves that $\bar{P}(X_1 + \alpha\, X_2, X_2)$ is of degree $m-1$ in X_2. It is also true for $P(X_1 + \alpha\, X_2, X_2, \underline{Z})$, since $\bar{P}(X_1 + \alpha\, X_2, X_2)$ is its evaluation in $\underline{Z} = \underline{0}$. □

Proposition 2 *Let notations and assumptions be as above, and let* $\tilde{P}_T(X_1, X_2, \underline{Z}) = P(X_1 + T\, X_2, X_2, \underline{Z})$*; then* P *admits a linear factor in* $\overline{C}[X_1, X_2, \underline{Z}]$ *if and only if there exists* α *root of* p *such that* $\dfrac{\partial^{m-1} \tilde{P}_\alpha}{\partial\, X_2^{m-1}}$ *is a linear factor of* $\tilde{P}_\alpha$ *in* $C(\alpha)[X_1, \underline{Z}]$.

Proof. Let $L = X_1 + a\, X_2 + \sum_{i=3}^{n} c_i\, X_i$ be a linear factor of P and let C' be the field of its coefficients. Denote by r the degree of C' over C.
The polynomial L is absolutely irreducible and by theorem 1.2.2 of [Rag97], $F = Norm_{C'/C}(L)$ is an irreducible polynomial of $C[X_1, X_2, \underline{Z}]$. It is clearly of degree r, and it is a factor of P. The polynomial $F(T, 1, 0, \ldots, 0)$ is a factor of $p(T)$, it is hence square-free.
On the other hand, $F(T, 1, 0, \ldots, 0) = Norm_{C'/C}(L(T, 1, 0, \ldots, 0)) = Norm_{C'/C}(T + a)$, and by lemma 1.2.1 of [Rag97] (or theorem 2.1 of [Tra76] extended to perfect fields), $Norm_{C'/C}(T + a)$ is a power of an irreducible polynomial of $C[T]$.
This implies that $F(T, 1, 0, \ldots, 0)$ is an irreducible polynomial of degree r. Let $\alpha = -a$; then α is of degree r and $C' = C(\alpha)$.
Hence,

$$L = X_1 - \alpha\, X_2 + \sum_{i=3}^{n} c_i(\alpha)\, X_i$$

where the c_i's are polynomials with coefficients in C.
Let $P = L \cdot Q$, then $\tilde{P}_\alpha = \tilde{L}_\alpha \cdot \tilde{Q}_\alpha = (X_1 + \sum_{i=3}^{n} c_i(\alpha)\, X_i) \cdot \tilde{Q}_\alpha$. Now $\tilde{P}_\alpha$, and then $\tilde{Q}_\alpha$, are of degree $m-1$ in X_2 (lemma 6) and so

$$\frac{\partial^{m-1} \tilde{P}_\alpha}{\partial\, X_2^{m-1}} = c(\alpha) \cdot \left(X_1 + \sum_{i=3}^{n} c_i(\alpha)\, X_i \right)\ .$$

Conversely, if $X_1 + \sum_{i=3}^n c_i(\alpha)\, X_i$ is a factor of $\tilde{P}_\alpha$ then $X_1 - \alpha\, X_2 + \sum_{i=3}^n c_i(\alpha)\, X_i$ is a factor of P. $\square$

This suggests the following fast algorithm to check whether a given square-free polynomial has linear factors (and compute them as a byproduct).
After maybe a linear change of variables[8] we may assume that P satisfies the hypotheses of proposition 2. Form P_α and L_α as in proposition 2. Then the corresponding L is a factor of P iff L_α divides all coefficients of powers of X_2 in P_α; the latter conditions are easily stated via resultants or even Euclidean divisions and, together with the relation $p(\alpha) = 0$, they yield a system of polynomial equations for α: our polynomial P has a linear factor if and only if the latter system is consistent.

A3: Complete factorization of parametrized polynomials

The above method can be adapted to polynomials depending on parameters, although the conditions that P be square-free and that $(1, 0, \ldots, 0)$ be non-critical may induce some nuisance (non-linear branchings); if one avoids the branching, then the algorithm is incomplete but yields an interesting heuristic.
The following straightforward method can also be used, without any restrictions on the parameters. Write $L = X_1 + \sum_{i=2}^n c_i X_i$. We want conditions for L to be a factor of P. Let $R := \text{resultant}(P, L, X_1) = P(-\sum_{i=2}^n c_i X_i)$ (note that $R = P(-\sum_{i=2}^n c_n X^n, X_2, \ldots, X_n))$. Of course, there is a linear factor if and only if R is the zero polynomial. The coefficients of R depend on the t_i and the c_i; equating all these to zero yields a polynomial system that we solve with any available method (see e.g [CLO92] for an introduction to these).
In our specific problem, the system is linear in the t_i and non-linear in the c_i so we can also apply the methods of [Sit92] for solving it.
Surprisingly, this simple method is quite satisfactory in practice and can be faster than (our implementation of) the Brill equations. We may interpret this experimental fact as follows. Using the Brill equations is like solving the system that we would obtain by first eliminating the c_i; however, here, it may be that another solving strategy is better (e.g because of the linearity in the t_i) so it could compensate for the fact of adding the extra variables c_i.

A4: Deciding when a polynomial is an k-th power

Let P be of the form $P = \sum t_i P_i$ where the $P_i \in \mathbb{C}[X_1, \ldots, X_n]$ are homogeneous of degree m. After a linear transformation we may assume that the degree of P in X_1 equals m.
Assume that $P = Q^k$. Let L be the coefficient of X_1^m. We need to distinguish two cases:

[8] The condition on a change of variables to be such that P satisfies the hypothesis of proposition 2 are easily seen to form a Zariski closed set so "almost any" change of variables will do.

After substituting values in $\mathbb{C}$ for the t_i either L vanishes or L remains non-zero. First we compute under the assumption that L vanishes. So we have a linear relation $L = 0$ between the parameters t_i (P is linear in the t_i). We use this relation to eliminate one of the t_i and then apply recursion.
Afterwards we may assume that L does not vanish. Because P is homogeneous in the t_i we may then assume that $L = 1$. We use this relation to eliminate one of the t_i. Then P is a monic polynomial in X_1 with coefficients in $\mathbb{C}[t_1, \ldots, t_s, X_2, \ldots, X_n]$, and the degree of Q in X_1 is $d = m/k$. Write $Q = \sum_{i=0}^{d} q_i X_1^i$ where $q_d = 1$. Taking the coefficient of X_1^{m-1} on both sides of the equation $P = Q^k$ (the coefficient on the right-hand side is kq_{d-1}) we find $q_{d-1} \in \mathbb{C}[t_1, \ldots, t_s, X_2, \ldots, X_n]$. Repeating this for the next coefficients $X_1^{m-2}, X_1^{m-3}, \ldots, X_1^{m-d}$ we determine $q_{d-2}, q_{d-3}, \ldots, q_0 \in \mathbb{C}[t_1, \ldots, t_s, X_2, \ldots, X_n]$. Then we can compute $P - Q^k$ and equate all coefficients with respect to $X_1, \ldots, X_n$ to 0. This gives a set of polynomial equations in the parameters t_i. Solving it gives the values of t_i for which P is a k-th power.

References

[Bri98] Brill, A. *Ueber die Zerfällung einer Ternärform in Linearfactoren*, Math. Ann. **50**, p. 157-182, (1898).

[CLO92] Cox D., Little J., O'Shea D. (1992) *Ideals, varieties, and Algorithms* Undergraduate Texts in Math, Springer

[Fak97] Fakler W. (1997) *On second order homogeneous linear differential equations with Liouvillian solutions* Proceedings of the "4-th Rhine Workshop on Computer Algebra". To appear in: Theoretical Computer Science.

[GKZ94] Gelfan'd I.M, Kapranov M.M, Zelevinski A.V (1994) *Discriminants, Resultants, and Multidimensional Determinants* Birkhaüser.

[HvP94] Hendriks P. & Van der Put M. (1995) *Galois action on solutions of a differential equation*, J. Symb. Comp. **19** (1995), pp. 559-576.

[Hoe97] van Hoeij M. (1997) *Factorization of Differential Operators with Rational Functions Coefficients*, J. Symb. Comp.

[HWe97] van Hoeij M, Weil J.A (1997) *An algorithm for computing invariants of differential Galois groups*, J. Pure and Applied Alg., **117 & 118**, (1997) pp. 353-379

[Hoh95] Hohl J.-C (1995) *Massively parallel search for linear factors in polynomials with many variables*, ICM preprint .

[KFF88] Kobayashi H, Fujise T, Furukawa A (1988) *Solving systems of algebraic equations by a general elimination method*, J. Symb. Comp, Vol **5**, pp 303-320.

[Kov86] Kovacic J (1986) *An algorithm for solving second order linear homogeneous differential equations* J. Symb. Comp **2** pp 3-43.

[Lan92] Lang S (1992) *Algebra* Third edition, Addison-Wesley.

[Mag94] Magid A (1994), *Lectures on Differential Galois Theory, University Lecture Series* of the American Mathematical Society.

[MBD38] Miller G.A, Blichfeldt H.F, Dickson L.E (1938) *Theory and Applications of Finite Groups.* New York: G. G. Stechert and Co.

[Rag97] Ragot J. F. (1997) *Sur la factorisation absolue des polynômes*, PhD dissertation, Université de Limoges (to appear, 1997).

[Sin81] Singer M .F. (1981) *Liouvillian Solutions of n^{th} Order Linear Differential Equations* Am. J. Math. **103**, pp. 661–682.

[Sin95] Singer M .F. (1995) *Testing reducibility of linear differential operators: a group theoretic perspective* Applicable Algebra in Engineering, Communication and Computing, **7**, p. 77-104, (1996).

[Sin97] Singer, M. F. (1997). *Direct and inverse problems in differential Galois theory.* To appear in: Collected Works of Ellis R. Kolchin .

[SUl93a] Singer M. F. & Ulmer F. (1993) *Galois groups for second and third order linear differential equations* J.Symb.Comp **16** No. 1, pp 1-36.

[SUl93b] Singer M. F. & Ulmer F. (1993) *Liouvillian and algebraic solutions of second and third order linear differential equations* J.Symb.Comp **16** No. 1, pp 37-73.

[SUl94] Singer M.F & Ulmer F (1995) *Necessary conditions for Liouvillian solutions of (third order) linear differential equations* J. of Appl. Alg. in Eng. Comm. and Comp. vol **6** No. 1, pp 1-22.

[SUl97] Singer M. F & Ulmer F *Linear differential equations and products of linear forms.* J. Pure and Applied Alg., **117 & 118**, (1997) pp. 549-564.

[Sit92] Sit W (1992) *An algorithm for solving parametric linear systems*, J. Symb. Comp. vol **13**, No 4, pp 353-413.

[Tra76] Trager B.M (1976) *Algebraic Factoring and Rational Function Integration.* Proceedings of the 1976 ACM Symposium on Symbolic and algebraic Computation.

[Tsa96] Tsarev S.P (1996), *An Algorithm for Complete Enumeration of All Factorizations of a Linear Ordinary Differential Operator*, ISSAC'96 Proceedings.

[Ulm94] Ulmer F (1994), *Irreducible linear differential equations of prime order* J. Symb. Comp. vol **18** No 4 , pp 385-401

[UWe96] Ulmer F. & Weil J. A. (1996) *Note on Kovacic's algorithm* J.Symb.Comp. vol 22 n° 2, pp 179-200

[Wei95a] Weil J.A *First integrals and Darboux polynomials of homogeneous linear differential systems*, Proceedings of AAECC 11 (Ed. M. Giusti & T. Mora), Lect. Notes in Comp. Sci. 948, Springer, 1995.

[Wei95b] Weil J.A *Constantes et polynômes de Darboux en algèbre différentielle : application aux systèmes différentiels linéaires*, PhD dissertation, École Polytechnique, 1995.