Computer Algebra Algorithms for Linear Ordinary Differential and Difference equations

Manuel Bronstein

Abstract. Galois theory has now produced algorithms for solving linear ordinary differential and difference equations in closed form. In addition, recent algorithmic advances have made those algorithms effective and implementable in computer algebra systems. After introducing the relevant parts of the theory, we describe the latest algorithms for solving such equations.

1. Introduction

Linear ordinary differential equations are equations (resp. systems) of the form

$$\sum_{i=0}^{n} a_i(x) \frac{d^i y(x)}{dx^i} = 0 \quad \left(\text{resp. } \frac{dY(x)}{dx} = A(x)Y(x)\right),$$

while linear ordinary difference equations are equations (resp. systems) of the form

$$\sum_{i=0}^{n} a_i(x) y(x+i) = 0 \quad (\text{resp. } Y(x+1) = A(x)Y(x)),$$

where in both cases the unknown(s) and the coefficients are functions of the continuous or discrete variable x. Similarities between those equations have been noticed and used for a long time, to the point that algebraic algorithms based on the underlying linear operators allow large common parts of differential or difference equations solvers to be described, and indeed programmed, in the same algebraic setting (see e.g. [1, 8]). With the recent discovery of a difference Galois theory [30] with effective algorithms [10], both problems of deciding whether differential or difference equations have closed–form solutions are now solved. Furthermore, a recent reformulation of differential Galois theory [22] allows both cases to presented using the same algebraic framework, and its interpretation using invariants [12, 13, 29] has led for the first time to effective implementations in computer algebra systems. After describing the common algebraic setting (below) and outlining the Galois theory required (section 2), we describe the computation of invariants of differential equations (section 3) and of Liouvillian solutions of difference equations (section 4). All fields in this paper are commutative, rings are not necessarily commutative, and all rings and fields have characteristic 0.

We briefly outline the common algebraic setting for differential and difference equations. This formalism will be used in the rest of this paper when describing constructions common to both cases. A *σ–differential ring (resp. field)* is a triple (R, σ, δ) where R is a ring (resp. field), σ is an automorphism of R and δ is an additive map of R satisfying the modified Leibniz rule $\delta(ab) = (\sigma a)(\delta b) + (\delta a)b$ for all $a, b \in R$. The set

$$\mathrm{Const}_{\sigma,\delta}(R) = \{a \in R \text{ such that } \sigma a = a \text{ and } \delta a = 0\}$$

is a ring (resp. field), which is called the *constant subring (resp. subfield)* of R. Given a left R–module M, a map $\theta : M \to M$ is called *pseudo–linear* if it is additive and if $\theta(am) = (\sigma a)\theta m + (\delta a)m$ for any $a \in R$ and $m \in M$. The set of all the pseudo-linear maps of M is denoted $\mathrm{End}_{R,\sigma,\delta}(M)$. A *$\sigma$–differential extension of* (R, σ, δ) is a σ–differential ring (S, σ', δ') such that $R \subseteq S$, $\sigma' = \sigma$ on R and $\delta' = \delta$ on R. When R is commutative, $\mathrm{End}_{R,\sigma,\delta}(R) = \{\gamma\sigma + \delta \text{ for } \gamma \in R\}$ [5], which means that any $\theta \in \mathrm{End}_{R,\sigma,\delta}(R)$ has a unique extension to any commutative σ–differential extension (S, σ', δ') of R, namely $\theta' = \gamma\sigma' + \delta'$ where $\gamma \in R$ is such that $\theta = \gamma\sigma + \delta$. Given a σ–differential ring (R, σ, δ), the *univariate skew–polynomial ring* over R, denoted $(R[X]; \sigma, \delta)$, is the ring of univariate polynomials with the usual addition, but with the multiplication given by $Xa - \sigma(a)X = \delta a$ for any $a \in R$. This ring was introduced by Ore [19] who studied in particular its factorization properties. A key property that we use in this paper is that when R is a field, it has both left and right Euclidean divisions, which implies the existence of left and right greatest common divisors and least common multiples (see [8] for additional properties and algorithms). When σ is the identity on R, (R, δ) is a differential ring and $(R[X]; 1_R, \delta)$ is the ring of linear ordinary differential operators with coefficients in R. When $\delta r = 0$ for every $r \in R$, (R, σ) is a difference ring and $(R[X]; \sigma, 0_R)$ is the ring of linear ordinary difference operators with coefficients in R.

2. Galois groups and Liouvillian Solutions

We summarize in this section the basic definitions and results that allow us to describe and justify the algorithms of the next sections. See [10, 22, 30] for proofs and a complete treatment of this subject.

Definition 2.1 ([22, 30]). *Let (k, σ, δ) be a σ–differential field, $\theta \in End_{k,\sigma,\delta}(k)$ and $A \in GL_n(k)$. A* Picard–Vessiot ring *over k for the equation $\theta Y = AY$ is a commutative σ–differential extension ring R of k satisfying:*

(i) *The only ideals of R closed under σ and δ are* (0) *and* (1)*.*
(ii) *$\exists U \in GL_n(R)$ such that $\theta U = AU$.*
(iii) *R is generated as a ring by k, the coefficients of U and $1/\det(U)$.*

*For any σ–differential extension ring S of k, the σ–*differential Galois group *of S over k is the group of automorphisms of S over k that commute with σ and δ.*

While the above definition is stated in terms of systems of equations, it applies to scalar equations as well: we associate to the scalar equation $Ly = 0$ where $L = \theta^n + \sum_{i=0}^{n-1} a_i \theta^i$, the companion system $\theta Y = A_L Y$ where

$$A_L = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ -a_0 & -a_1 & \dots & -a_{n-1} \end{pmatrix}$$

The map $y \to (y, \theta y, \dots, \theta^{n-1} y)^T$ is an isomorphism between the solution spaces of $Ly = 0$ and $\theta Y = A_L Y$, so we define the Picard–Vessiot ring and Galois group for L to be the ones of the associated companion system.

If $(k, 1_k, \delta)$ is a differential field with an algebraically closed constant field C, then for any $A \in GL_n(k)$, there exist a Picard–Vessiot ring R, for $\delta Y = AY$, and it is unique up to differential isomorphism [22]. Furthermore, R is an integral domain, whose field of fractions K is called the *Picard–Vessiot field* for the equation $\delta Y = AY$, and $\mathrm{Const}_\delta(K) = \mathrm{Const}_\delta(R) = C$ [22]. In that case, the σ–differential Galois group of R over k is called the *differential Galois group* of $\delta Y = AY$ over k, and it coincides with the group of field–automorphisms of K over k that commute with the derivation.

If $(k, \sigma, 0_k)$ is a difference field with an algebraically closed constant field C, then for any $A \in GL_n(k)$, there exist a Picard–Vessiot ring R, for $\sigma Y = AY$, it is unique up to difference isomorphism and $\mathrm{Const}_\sigma(R) = C$ [30]. In that case, the σ–differential Galois group of R over k is called the *difference Galois group* of $\sigma Y = AY$ over k.

In both of the above cases, the σ–differential Galois group G has a natural structure of a linear algebraic group over C, *i.e.* it is an algebraic subgroup of $GL_n(C)$. Furthermore, the Picard–Vessiot extension R is normal over k, *i.e.* for any $t \in R \setminus k$, there is an element g of the group such that $g(t) \neq t$ [22, 30]. Since G is an algebraic group, it is the disjoint union of finitely many connected components in the Zariski topology. The component containing the identity will be denoted G^0.

A major success of differential and difference Galois theory has been the discovery of effective group–theoretic criteria for the existence of closed–form solutions to linear ordinary differential and difference equations. Before presenting those criteria, we need to formalize the notions of closed–form solutions that they use, starting with the differential case: let $(k, 1_k, \delta)$ be a differential field and K a differential extension of k. We say that K is *Liouvillian over* k if there are $t_1, \dots, t_m \in K^*$ such that $K = k(t_1, \dots, t_m)$ and for each i, either t_i is algebraic over $K(t_1, \dots, t_{i-1})$, or $\delta t_i \in K(t_1, \dots, t_{i-1})$ or $\delta(t_i)/t_i \in K(t_1, \dots, t_{i-1})$. We say that a differential equation with coefficients in k has a *Liouvillian solution* if it has a nonzero solution in a Liouvillian extension of k. The main criterion for the differential case is then:

Theorem 2.2 ([17]). *Let $L \in k[D; 1_k, \delta]$ be a linear ordinary differential operator with coefficients in a differential field k whose constant subfield is algebraically closed, and G be the differential Galois group of L over k.*

(i) *All the solutions of $Ly = 0$ are Liouvillian over k if and only if G^0 is a solvable group.*

(ii) *$Ly = 0$ has a Liouvillian solution over k if and only if it has a solution y such that y'/y is algebraic over k.*

Even though theorem 2.2 relates the existence of Liouvillian solutions to the existence of a solution of a very special form, it does not yield an algorithm because it gives no bound on the degree of y'/y as an algebraic function. Singer produced such a bound for n arbitrary as well as an algorithm for determining the coefficients of the minimal polynomial of y'/y over k.

Theorem 2.3 ([25]). *There exists a function $F : \mathbb{N} \to \mathbb{N}$ such that $Ly = 0$ has a Liouvillian solution over k if and only if it has a solution y such that y'/y is algebraic over k and $[k(y'/y) : k] \le F(n)$.*

The function $F(n)$ is defined by $F(0) = 1$ and $F(n) = \max(f(n), n!F(n-1))$ where $f(n)$ is such that every finite subgroup of $GL_n(\mathbb{C})$ has a normal Abelian subgroup of index at most $f(n)$. Jordan's Theorem [15] implies the existence of such a function and there are explicit formulas. This general upper bound can be improved in many cases, in particular for specific values of n [28, 31, 32].

A criterion also exists for a restricted class of difference equations [10], namely when $k = C(x)$ for some algebraically closed constant field C, and σ is the automorphism of k over C that maps x to $x+1$. In that case, Picard–Vessiot rings over k can be viewed as subrings of the commutative ring $\mathcal{S}$ of germs of sequences defined as $\mathcal{S} = C^{\mathbb{N}}/J$ where J is the ideal of sequences having finitely many nonzero terms. The map $\sigma(a_0, a_1, a_2, \dots) = (a_1, a_2, \dots)$ is a well-defined automorphism of $\mathcal{S}$ and k can be embedded in $\mathcal{S}$ by the difference embedding that maps $f \in k$ to the sequence $a_n = 0$ if n is a pole of f, $f(n)$ otherwise. A sequence $a \in \mathcal{S}$ is called *hypergeometric* if $\sigma a = fa$ for some $f \in k$. For a sequence $a = (a_n)_{n \ge 0}$ in $\mathcal{S}$, and $m > 0$, define the m^{th} *spread of* a to be the sequence $a^{\vec{m}}$ given by

$$\left(a^{\vec{m}}\right)_n = \begin{cases} a_{n/m} & \text{if } n \equiv 0 \pmod{m} \\ 0 & \text{if } n \not\equiv 0 \pmod{m} \end{cases} . \tag{1}$$

The *interlacing* of m sequences $a^{(1)}, \dots, a^{(m)}$ is the sequence

$$\biguplus_{j=1}^{m} a^{(j)} = \sum_{j=1}^{m} \sigma^{1-j}\left({a^{(j)}}^{\vec{m}}\right) = (a_0^{(1)}, \dots, a_0^{(m)}, a_1^{(1)}, \dots)$$

Finally, the ring $\mathcal{L}$ of the *Liouvillian sequences* is the smallest difference subring of $\mathcal{S}$ containing k such that

1. $a \in k, b \in \mathcal{S}, \sigma b = ab \implies b \in \mathcal{L}$.
2. $a \in \mathcal{L}, b \in \mathcal{S}, \sigma b = b + a \implies b \in \mathcal{L}$.
3. $a \in \mathcal{L} \implies \forall i, m$ such that $0 \le i < m, \sigma^{-i}(a^{\vec{m}}) \in \mathcal{L}$.

We say that a difference equation with coefficients in k has a *Liouvillian solution* if it has a nonzero solution in $\mathcal{L}$. The main criterion for the difference case is then:

Theorem 2.4 ([10]). *Let $L \in k[E;\sigma,0_k]$ be a linear ordinary differential operator with coefficients in the difference field $k = C(x)$, where C is algebraically closed and σ is the automorphism of k over C mapping x to $x+1$. Let G be the difference Galois group of L over k.*

(i) *All the solutions of $Ly = 0$ are Liouvillian if and only if G is a solvable group.*

(ii) *$Ly = 0$ has a Liouvillian solution if and only if it has a solution y such that y is the interlacing of m hypergeometric sequences where $1 \le m \le n$.*

3. Invariants and Differential Equations

Let W be a vector space over a field F and $G \subseteq GL(W)$ be a group of automorphisms of W. We say that $w \in W$ is an *invariant of* G if $g(w) = w$ for every $g \in G$. The set of all the invariants of G in W is denoted W^G and is a subspace of W. We say that w is a *semi–invariant of* G if for every $g \in G$, there exists $f_g \in F$ such that $g(w) = f_g w$. Invariants and semi–invariants of differential Galois groups play an important role in algorithms for solving differential equations. For the rest of this section, let k be a differential field with algebraically closed constant field C, L be a linear ordinary differential operator of order $n > 0$ with coefficients in k, K be its Picard–Vessiot extension, $V \subset K$ be the solution space of $Ly = 0$, G be its Galois group and G^0 be its connected component of the identity. The (faithful) action of G on V is extended to the symmetric algebra $S(V)$ via

$$g\left(\sum_{e=(e_1,\dots,e_{m_e})} c_e v_{e_1} \otimes \cdots \otimes v_{e_{m_e}}\right) = \sum_e c_e g(v_{e_1}) \otimes \cdots \otimes g(v_{e_{m_e}}) \qquad (2)$$

for any $c_e \in C$ and $v_i \in S^1(V) = V$. Note that $S(V) = \bigoplus_{m\ge 0} S^m(V)$ is a graded C-algebra, and that the action of G given by (2) preserves the grading, so in particular $S(V)^G = \bigoplus_{m\ge 0} S^m(V)^G$ and we can restrict our attention to *homogeneous* invariants and semi–invariants in $S^m(V)$. Define the *degree* of a nonzero $w \in S(V)$ to be the smallest $d \ge 0$ such that $w \in \bigoplus_{m=0}^{d} S^m(V)$. We say that $w \in S(V)$ *factors into linear forms* if $w = w_1 \otimes \cdots \otimes w_m$ for some $w_1, \dots, w_m \in V$. Liouvillian solutions of $Ly = 0$ and semi-invariants of G are related by the following result, in which $F(n)$ is as in theorem 2.3.

Theorem 3.1 ([29]). *$Ly = 0$ has a Liouvillian solution over k if and only if G has a semi-invariant $I \in S(V)$ of degree at most $F(n)$ and which factors into linear forms.*

It turns out that looking for semi-invariants can be reduced to looking for invariants of the same degree of transformed operators [12]. In addition, “semi–invariant” can be replaced by “invariant” in the above theorem for a large class of equations[1] (see the discussion at the end of this section for details), so we consider only the problem of searching for invariants in $S^d(V)^G$ where d ranges over a given subset of $\{1,\dots,F(n)\}$. The basic idea to is to map them via G-morphisms to G-modules where their images can be computed. Singer and Ulmer [29] used the C-algebra evaluation homomorphism $\psi : S(V) \to K$ given by

$$\psi\left(\sum_{e=(e_1,\dots,e_{m_e})} c_e v_{e_1} \otimes \cdots \otimes v_{e_{m_e}}\right) = \sum_e c_e v_{e_1} \dots v_{e_{m_e}}$$

for any $c_e \in C$ and $v_i \in S^1(V) = V \subset K$. It is easily checked that ψ commutes with the actions of G on $S(V)$ and K, hence that $\psi(S(V)^G) \subseteq K^G$. Since Picard–Vessiot extensions are normal, $K^G = k$, so $I \in S(V)^G \implies \psi(I) \in k$. Define the d^{th} *symmetric power* of L, denoted $L^{\circledS d}$, to be a differential operator of minimal order whose solution space is $\psi(S^d(V))$. Symmetric powers can be computed from L using only linear algebra over k [7]. Then $I \in S^d(V)^G \implies \psi(I) \in k$ and $L^{\circledS d}(\psi(I)) = 0$. If in addition $L^{\circledS d}$ has order $\dim_C(S^d(V)) = \binom{n+d-1}{n-1}$, then ψ_d (the restriction of ψ to $S^d(V)$) must be injective, so in that case

$$I \in S^d(V)^G \setminus \{0\} \iff \psi(I) \in k^* \text{ and } L^{\circledS d}(\psi(I)) = 0\,.$$

Such solutions in k^* can be computed for a large class of fields [4, 6, 26], and a basis $(f_1,\dots,f_r)$ for them implies that $I_1,\dots,I_r$ is a basis for $S^d(V)^G$ where $I_j = \psi_d^{-1}(f_j)$. Inverting ψ_d is possible whenever k is a finitely generated differential extension of $\mathbb{Q}$: Seidenberg's Embedding Theorem [23, 24] states that any such field is isomorphic to a differential field of meromorphic functions on an open region of $\mathbb{C}$. This means that given any finite subset S of k, there exists infinitely many $x_0 \in \mathbb{C}$ such that the elements of S can be seen as analytic functions at x_0, and hence evaluated at $x = x_0$. We now say that $x_0 \in \mathbb{C}$ is an *ordinary point* of $L = \sum_{i=0}^n a_i D^i$ if each a_i is analytic in an open neighborhood of x_0 (including x_0) and if $a_n(x_0) \neq 0$. Since meromorphic functions have isolated singularities, it follows from the Embedding Theorem that L has infinitely many ordinary points. To compute $I = \psi_d^{-1}(f)$ for $f \in k$, pick an ordinary point $c \in \mathbb{C}$ of L and compute a basis $(y_1,\dots,y_n)$ of the formal Taylor series solutions of $Ly = 0$ around c. Writing I as a homogeneous polynomial of degree d in $Y_1,\dots,Y_n$ with undetermined constant coefficients and equating the first $\binom{n+d-1}{n-1}$ coefficients of $I(y_1,\dots,y_n)$ with those of the Taylor series of f yields a nonsingular linear algebraic system for the coefficients of I, whose solution yields I. If $L^{\circledS d}$ has order strictly smaller than $\binom{n+d-1}{n-1}$, then ψ_d is not injective and one needs to perform a generic change of variable to ensure that ψ_d will be injective for the transformed operator [29]. Alternatively, one can use the above series method to compute $\ker \psi_d$, since its dimension is known.

The above method is particularly well adapted for second-order operators, because $L^{\circledS d}$ is straightforward to compute via a simple iteration in that case [7].

[1] At the cost of increasing the degree bound.

Furthermore, its order is always $d+1$ so ψ_d is always injective. Finally, any homogeneous polynomial in $C[Y_1, Y_2]$ factors into linear forms, implying that any homogeneous invariant factors into linear forms. The bound $F(2)$ can be improved and an optimal result for $n = 2$, which holds for arbitrary coefficients fields, even when the constant field is not algebraically closed, is that $Ly = 0$ has a Liouvillian solution if and only if G has either a semi-invariant of degree 1 or a homogeneous invariant of degree $d \in \{2, 4, 6, 8, 12\}$ [33].

Example 3.2. *Consider the equation $x^2 y''(x) - (36x^6 e^{4x^3} + 9x^6 + 2)y(x) = 0$, whose operator $L = x^2 D^2 - 36x^6 t^4 - 9x^6 - 2$ has coefficients in $k = \mathbb{Q}(x, t)$ with $\delta x = 1$ and $\delta t = 3x^2 t$. Its symmetric square is*

$$L^{ⓢ 2} = x^3 D^3 - 4x(36x^6 t^4 + 9x^6 + 2)D - 8(1 + 3x^3)(36x^6 t^4 + 3x^3 - 1)\,,$$

whose solution space in k is generated by $f = x^{-2} t^{-2}$. A basis of local solutions of the equation around $x = 1$ is

$$y_1 = 1 + \left(18e^4 + \frac{11}{2}\right)(x-1)^2 + \dots\,,$$

$$y_2 = (x-1) + \left(6e^4 + \frac{11}{6}\right)(x-1)^3 + \dots\,,$$

and equating the first 3 terms of $c_{11} y_1^2 + c_{12} y_1 y_2 + c_{22} y_2^2$ with the first 3 terms of $f = e^{-2} - 8e^{-2}(x-1) + 27e^{-2}(x-1)^2 + \dots$ yields $c_{11} = e^{-2}, c_{12} = -8e^{-2}$ and $c_{22} = 16e^{-2} - 36e^2$. It follows that

$$I = e^{-2}(Y_1^2 - 8Y_1 Y_2 + (16 - 36e^4)Y_2^2) = e^{-2}(Y_1 + (6e^2 - 4)Y_2)(Y_1 - (6e^2 + 4)Y_2)$$

is an invariant of the Galois group of L that factors into linear forms.

For equations of higher order, the above method suffers from the cost of computing $L^{ⓢ d}$ as well as from the occasionally required generic transformation. To avoid those problems, van Hoeij and Weil used a different C-algebra homomorphism [13]. For any commutative ring R, write $N_d = \binom{n+d-1}{n-1}$ and define $\sigma_d : R^n \to R^{N_d}$ by $\sigma_d((r_1, \dots, r_n)^T) = (r_1^d, r_1^{d-1} r_2, r_1^{d-1} r_3, \dots, r_n^d)^T$ where the N_d homogeneous monomials of degree d in $r_1, \dots, r_n$ are ordered lexicographically with $r_1 < r_2 < \dots < r_d$. Let $R = F[Y_1, \dots, Y_n]$ be a polynomial ring over a field F and $Y = (Y_1, \dots, Y_n)^T \in R^n$. For any $M \in GL_n(F)$, the entries of MY are linear forms in the Y_i's, which implies that the entries of $\sigma_d(MY)$ are homogeneous of degree d. Since $\sigma_d(Y)$ is a basis for the homogeneous polynomials of degree d, this defines a matrix $\mathrm{Sym}^d(M)$ given by $\sigma_d(MY) = \mathrm{Sym}^d(M)\sigma_d(Y)$. The map $\mathrm{Sym}^d : GL_n(F) \to GL_{N_d}(F)$ is then a group-homomorphism. When F is the the constant field C of k, Sym^d describes the extension (2) of the action of the Galois group G from V to $S^d(V)$ as it makes the following diagram commute:

$$\begin{tikzcd}
 & GL(S^d(V)) \\
G \arrow[ur] \arrow[dr] & \\
 & GL(V) \arrow[uu, "\mathrm{Sym}^d"']
\end{tikzcd}$$

Let now $T \in GL_n(\mathbb{Q})$ be the upper triangular matrix given by $T_{ij} = 1$ for $i \le j$ and $\Delta_d \in GL_{N_d}(\mathbb{Q})$ be the diagonal matrix whose diagonal is the first row of $\mathrm{Sym}^d(T)$. One can check that the diagonal element of Δ_d corresponding to the monomial $Y_1^{e_1} \dots Y_n^{e_n}$ is $d!/\prod_{i=1}^n e_i!$. Let $\mathcal{Y} = (y_1, \dots, y_n)$ be a basis for V and $W \in GL_n(K)$ be the corresponding Wronskian matrix. Using the notation v^e for the e-fold tensor $v \otimes \dots \otimes v$ of $S(V)$, let $\mathcal{Y}_d$ be the basis $(y_1^d, y_1^{d-1} \otimes y_2, y_1^{d-1} \otimes y_3, \dots, y_n^d)$ of $S^d(V)$ where the symmetric tensors are ordered lexicographically with $y_1 < y_2 < \dots < y_d$. The *injective* morphism used by van Hoeij and Weil is then $\lambda_d : S^d(V) \to K^{N_d}$ given by $\lambda_d(w) = \mathrm{Sym}^d(W)\Delta_d^{-1}\overline{w}$ where $\overline{w} \in C^{N_d}$ is the vector of coefficients of w with respect to $\mathcal{Y}_d$. If G acts pointwise on the coordinates in K^{N_d} then they prove in [13] that λ_d commutes with the actions of G on $S^d(V)$ and K^{N_d}, hence that $\lambda_d\big(S^d(V)^G\big) \subseteq {K^{N_d}}^G$. As earlier, the normality of the Picard–Vessiot extension implies that ${K^{N_d}}^G = k^{N_d}$, hence that $I \in S^d(V)^G \implies \lambda_d(I) \in k^{N_d}$. They then define the d^{th} *symmetric power system* of L to be the differential system $Z' = S^d(L)Z$ where $S^d(L)$ is the $N_d \times N_d$ matrix with entries in k given by $\sigma_d(\mathcal{Y}^T)' = S^d(L)\sigma_d(\mathcal{Y}^T)$. The entries of $S^d(L)$ can be easily computed from the coefficients of L [13] and they prove that the solution space of $Z' = S^d(L)Z$ is generated by the columns of $\mathrm{Sym}^d(W)$, which implies that the solution space is exactly $\lambda_d(S^d(V))$. Therefore,

$$I \in S^d(V)^G \setminus \{0\} \iff \lambda_d(I) \in k^{N_d} \setminus \{0\} \text{ and } \lambda_d(I)' = S^d(L)\lambda_d(I)\,. \tag{3}$$

Their algorithm, which is applicable when k is the rational function field $C(x)$ with derivation d/dx proceeds as follows: compute first from the Newton polygons of L at all its poles denominators of the entries of a solution in $C(x)^{N_d}$ of $Z' = S^d(L)Z$ as well as bounds on the degrees of the corresponding numerators. Compute then a local fundamental solution matrix $\widehat{W}$ of $Ly = 0$ around some point $x_0 \in \mathbb{P}^1(\overline{C})$. Let $\overline{I}$ be a vector of N_d indeterminates, then $F = \mathrm{Sym}^d(\widehat{W})\Delta_d^{-1}\overline{I}$ is a local formal solution of $Z' = S^d(L)Z$ around x_0. Multiply each row by its corresponding denominator and reduce the remaining series modulo x^{n_i+1} where n_i is the corresponding degree bound. This yields a vector Z of rational functions in x where the indeterminates of $\overline{I}$ appear linearly. Equating Z' with $S^d(L)Z$ yields a linear algebraic system of the form $M\overline{I} = 0$ whose kernel is isomorphic to $S^d(V)^G$ ([13] contains several heuristics to reduce the number of unknowns, down to the dimension of $S^d(V)^G$ in many cases).

Their algorithm is quite effective for operators of order 3 or more when the coefficient field is of the form $(C(x), d/dx)$. Furthermore, once they find an invariant (or semi–invariant) I that factors linearly, the entries of $\lambda_d(I)$ can be used to produce a polynomial $P \in C[x,u]$ such that $P(x,u) = 0 \implies Le^{\int u dx} = 0$ [12].

In the case of more general coefficient fields, even though $\widehat{W}$ can still be computed, it is not known how to convert Taylor series to elements of k, so the above method is not applicable. However, we can invert λ_d without knowing a fundamental solution matrix, so we can still use the symmetric power system to compute invariants:

Theorem 3.3. *Suppose that k is a finitely generated differential extension of $\mathbb{Q}$ and let $F \in k^{N_d}$ be a nonzero solution of $Z' = S^d(L)Z$. Then, for any $M \in GL_n(\mathbb{C})$ and any ordinary point x_0 of L, $\Delta_d Sym^d(M)F(x_0)$ is the coefficient vector of an invariant of G with respect to a basis that depends on M. In particular $\Delta_d F(x_0)$ is an invariant of G with respect to the basis $(y_1, \dots, y_n)$ satisfying $y_j^{(i-1)}(x_0) = \delta_{ij}$.*

Proof. By the classical existence and uniqueness theorems [14], there exists for each $1 \le j \le n$ a unique solution y_j of $Ly = 0$, analytic at x_0 and satisfying $y_j^{(i-1)}(x_0) = M_{ij}^{-1}$ for $1 \le i \le n$. Let W be the Wronskian matrix of $y_1, \dots, y_n$. Since $W(x_0) = M^{-1}$ is invertible, W is invertible so it is a fundamental matrix for L. Since the solution space of $Z' = S^d(L)Z$ is $\lambda_d(S^d(V))$, it follows from (3) that $F = \lambda_d(I)$ for some invariant $I \in S^d(V)^G$. Writing $\overline{I}$ for the coefficients of I, we have $F = \mathrm{Sym}^d(W)\Delta_d^{-1}\overline{I}$. Since the entries of W are analytic at x_0, the entries of $\mathrm{Sym}^d(W)$ are also analytic at x_0, so evaluating at x_0 yields

$$F(x_0) = \mathrm{Sym}^d(W)(x_0)\Delta_d^{-1}\overline{I} = \mathrm{Sym}^d(W(x_0))\Delta_d^{-1}\overline{I} = \mathrm{Sym}^d(M)^{-1}\Delta_d^{-1}\overline{I}$$

which implies that $\overline{I} = \Delta_d \mathrm{Sym}^d(M)F(x_0)$. The last sentence of the theorem follows from taking M to be the identity matrix in the proof. □

Using cyclic vectors [9], we can compute the solutions in k^{N_d} of symmetric power systems for a large class of fields [4, 6, 26]. Theorem 3.3 then implies that $\Delta_d F(x_0)$ is an invariant of G for any solution, and this yields an alternative to the algorithm of Singer & Ulmer that does not require ψ_d to be injective. Prototypes implementations of those algorithms exist both in the Maple system and the Bernina[2] server.

Example 3.4. *Consider the same equation as in Example 3.2. Its second symmetric power system is*

$$Z' = \begin{pmatrix} 0 & 2 & 0 \\ 36x^4e^{4x^3} + 9x^4 + 2x^{-2} & 0 & 1 \\ 0 & 72x^4e^{4x^3} + 18x^4 + 4x^{-2} & 0 \end{pmatrix} Z$$

[2] http://www.inria.fr/cafe/Manuel.Bronstein/sumit/bernina.html

whose solution space in k^3 is generated by

$$F = (x^{-2}t^{-2}, -(1+3x^3)x^{-3}t^{-2}, (1+6x^3+9x^6-36x^6t^4)x^{-4}t^{-2})^T\,. \qquad (4)$$

We have $\Delta_3 F(1) = (e^{-2}, -8e^{-2}, 16e^{-2}-36e^2)^T$, so we get the same invariant as in Example 3.2.

Once an invariant that factors linearly has been found, a Liouvillian solution of the equation can be computed: using $\sigma_d((Z_1,\ldots,Z_n)^T)$ as a basis of the ring $k[Z_1,\ldots,Z_n]_d$ of homogeneous polynomials of degree d with coefficients in k, we can identify k^{N_d} with $k[Z_1,\ldots,Z_n]_d$. Under this identification, Theorem 2.1 of [12] implies that if $F \in k^{N_d}$ is a nonzero solution of $Z' = S^d(L)Z$, then $Q = (\Delta_d F)(U, -1, 0, \ldots, 0) \in k[U]$ has degree d and is such that $Q(u) = 0$ implies that $L(e^{\int u}) = 0$. Such a polynomial can also be computed from a semi–invariant that factors into linear forms [12].

Example 3.5. *Consider the same equation as in Examples 3.2 and 3.4. From the solution (4) of its second symmetric power system, we get*

$$Q = (\Delta_3 F)(U,-1) = x^{-4}t^{-2}\big(x^2U^2 + (2x+6x^4)U + (1+6x^3+9x^6-36x^6t^4)\big)$$

whose roots are $u = -(1+3x^3 \pm 6x^3t^2)/x$. It follows that a basis of the solution space of $Ly = 0$ is $x^{-1}e^{-x^3 \pm e^{2x^3}}$.

We conclude this section with a discussion of when it is sufficient to look for invariants rather than semi–invariants. The results in the rest of this section are all from M. Singer (personal communications). Lemma 3.6 was independently discovered by D. Boucher and appears as a non-integrability criterion in [3].

Lemma 3.6. *If G is reductive, then every connected solvable normal subgroup of G is diagonalizable.*

Proof. Every group is diagonal for $n = 1$, so suppose that $n > 1$ and that the lemma holds for $1 \le m < n$, and let H be a connected solvable normal subgroup of G. H is triangularizable by the Lie–Kolchin Theorem [16, 18], so it has a semi–invariant $v \in V$. Let $g \in G$ and $h \in H$ be arbitrary. Since H is normal in G, $hg = gh'$ for some $h' \in H$. Then, $h(g(v)) = g(h'(v)) = g(c_{h'}v) = c_{h'}g(v)$ where $c_{h'} \in C$. This implies that $g(v)$ is a semi–invariant of H for every $g \in G$. Let $(g_1(v), \ldots, g_m(v))$ be a basis for V', the C-span of Gv. If $m = n$, then H is diagonal with respect to that basis. Otherwise, since G is reductive, $V = V' \oplus W$ where $GW \subseteq W$. Let $(w_1, \ldots, w_{n-m})$ be a basis of W. Relative to the basis $(g_1(v), \ldots, g_m(v), w_1, \ldots, w_{n-m})$ of V, every $g \in G$ has the block–diagonal form

$$g = \begin{pmatrix} A_g & \\ & B_g \end{pmatrix}$$

where $A_g \in GL_m(C)$ and $B_g \in GL_{n-m}(C)$. The map $g \to B_g$ is a rational morphism from G into $GL_{n-m}(C)$. It is continuous in the Zariski topology [16, Lemma 4.3], so the image of H is connected and solvable. By our induction hypothesis, there is a basis $(b_1, \ldots, b_{n-m})$ of W which diagonalizes the image of H. H is then diagonal with respect to the basis $(g_1(v), \ldots, g_m(v), b_1, \ldots, b_{n-m})$. □

Lemma 3.7. *If G has a diagonalizable unimodular normal subgroup of finite index, then G has an invariant $I \in S(V)$ that factors into linear forms.*

Proof. Let H be a diagonalizable unimodular normal subgroup of G of finite index, $(y_1, \ldots, y_n)$ be a basis of V that diagonalizes H and $z = y_1 \otimes \cdots \otimes y_n$. Then, for each $h \in H$, $h(z) = h(y_1) \otimes \cdots \otimes h(y_n) = \det(h) z = z$ since H is unimodular. Let $g_1 H, \ldots, g_m H$ be the distinct cosets of H in G. Any $g \in G$ can be written as $g = g_j h$ for some $h \in H$, which implies that $g(z) = g_j(h(z)) = g_j(z)$. Therefore, $Gz \subseteq \{g_1(z), \ldots, g_m(z)\}$ is finite, so $Gz = \{f_1(z), \ldots, f_s(z)\}$ where $s \leq m$ and each f_j is in G. Then $I = f_1(z) \otimes \cdots \otimes f_s(z)$ factors into linear forms and since each $g \in G$ acts as a permutation on Gz, $g(I) = I$ so I is an invariant of G. □

Since G^0 is always a connected normal subgroup of G of finite index, combining theorem 2.2 with lemmas 3.6 and 3.7 we get:

Theorem 3.8. *If G is reductive, G^0 is unimodular and all the solutions of $Ly = 0$ are Liouvillian over k, then G has an invariant that factors into linear forms.*

Remark that $L = \operatorname{llcm}(D - x^2, D^2 + x^2 D - 1)$ has a reductive unimodular Galois group, as well as the Liouvillian solution $e^{\int x^2 dx}$, but no invariant, so the above theorem does not hold when some solutions are Liouvillian and some not. However, having one Liouvillian solution is equivalent to all solutions being Liouvillian in the case of irreducible equations, so a consequence of theorem 3.8 is that an irreducible equation with a unimodular G^0 has a Liouvillian solution if and only if G has an invariant that factors into linear forms. If we can find rational and exponential solutions over k, then we can factor operators over k into irreducibles [8, 11, 27], which ensures that we only solve operators with irreducible Galois groups. In addition, the transformation $z = y e^{\int a_{n-1}/n a_n}$ where $L = a_n D^n + a_{n-1} D^{n-1} + \cdots + a_0$ transforms $Ly = 0$ into $\bar{L} z = 0$ where $\bar{L}$ has order n and a unimodular Galois group, which remains irreducible if L was irreducible. In addition to factoring, it is thus sufficient to look for homogeneous invariants of prescribed degrees in order to check for Liouvillian solutions (although it may be preferable in some cases to look for semi-invariants of lower degrees).

4. Difference Equations

We describe in this section the algorithm of [10] for computing all the Liouvillian solutions of ordinary linear difference equations with polynomial coefficients. Based on theorem 2.4, this algorithm looks for solutions of $Ly = 0$ that are interlacings of m hypergeometric sequences for $1 \leq m \leq n$.

Definition 4.1. *Let F be a field, $F[t;\sigma,\delta]$ be a skew–polynomial ring over F and $p \in F[t;\sigma,\delta] \setminus \{0\}$. For any $m > 0$, the* least m-sparse left multiple of p *is a monic $p^{\overleftarrow{m}} \in F[t;\sigma,\delta]$ of minimal degree such that $p^{\overleftarrow{m}} = qp$ for some $q \in F[t;\sigma,\delta]$ and such that only powers of t^m appear in $p^{\overleftarrow{m}}$.*

Such multiples can be computed by linear algebra over F: let θ be the image of t^m in $V = F[t;\sigma,\delta]/F[t;\sigma,\delta]p$, which is a vector space of dimension $n = \deg(p)$ over F, and N be the largest integer such that $\theta^0, \theta^1, \dots, \theta^{N-1}$ are linearly independent over F (note that $1 \le N \le n$). Then $\theta^N = \sum_{i=0}^{N-1} c_i \theta^i$ for some $c_0, \dots, c_{N-1} \in F$ and $p^{\overleftarrow{m}} = t^{Nm} - \sum_{i=0}^{N-1} c_i t^{im}$ is the desired multiple.

Let now $L = \sum_{i=0}^{n} a_i E^i$ be a linear ordinary difference operator with coefficients in (k,σ) where $k = C(x)$ and $\sigma x = x + 1$. Let $L^{\overleftarrow{m}} = E^{Nm} + \sum_{i=0}^{N-1} b_i E^{im}$ be its least m-sparse left multiple and for $1 \le j \le m$ let

$$L_j^{\overleftarrow{m}} = E^N + \sum_{i=0}^{N-1} \left(\tau_m \sigma^{j-1} b_i\right) E^i$$

where $\tau_m : C(x) \to C(x)$ is the automorphism over C mapping x to mx.

Theorem 4.2. [10] *For any $a^{(1)}, \dots, a^{(m)} \in \mathcal{S}$,*

$$L(\biguplus_{j=1}^{m} a^{(j)}) = 0 \implies L_j^{\overleftarrow{m}}\left(a^{(j)}\right) = 0 \text{ for } 1 \le j \le m\,.$$

Proof. Let $a = \biguplus_{j=1}^{m} a^{(j)}$. Since $La = 0$ and $L^{\overleftarrow{m}}$ is a left-multiple of L, $L^{\overleftarrow{m}} a = 0$, so $a_{s+Nm} + \sum_{i=0}^{N-1} b_i(s) a_{s+im} = 0$ for all $s \ge 0$. For $1 \le j \le m$ and any $t \ge 0$, applying that equality to $s = tm + j - 1$ and remarking that $a_{s+im} = a_{(t+i)m+j-1} = a^{(j)}_{t+i}$, we obtain $a^{(j)}_{t+N} + \sum_{i=0}^{N-1} b_i(tm + j - 1) a^{(j)}_{t+i} = 0$ for all $t \ge 0$. □

We therefore need to look for all the hypergeometric solutions of $L_j^{\overleftarrow{m}}$ for $1 \le j \le m$. We can use the algorithm `Hyper` [20, 21], which, given a linear ordinary difference operator R with coefficients in $C(x)$ returns $\gamma_1, \dots, \gamma_t \in C(x)^*$ and finitely many polynomials $p_{rs} \in C[x] \setminus \{0\}$ such that the hypergeometric solutions of $Ry = 0$ are exactly all the sequences satisfying

$$\frac{\sigma y}{y} = \gamma_r \frac{\sum_s c_{rs} \sigma p_{rs}}{\sum_s c_{rs} p_{rs}} \tag{5}$$

for some r, where the c_{rs}'s are arbitrary constants. Let now $1 \le j \le m$ be given and let $\mathcal{H}_j$ be $\{0\}$ if $L_j^{\overleftarrow{m}}$ has no nonzero hypergeometric solution, the finite set of all the $\gamma_r \sigma(p_{rs})/p_{rs}$ for all the γ_r and p_{rs} returned by `Hyper` on $L_j^{\overleftarrow{m}}$ otherwise. For each $h \in \mathcal{H}_j$, let z_h be 0 if $h = 0$, a nonzero hypergeometric solution of $\sigma y = hy$ otherwise. Then, (1) implies that $\sigma^m(z_h^{\overrightarrow{m}}) = h^{\overrightarrow{m}} z_h^{\overrightarrow{m}}$, hence that $(E^m - \tau_m^{-1} h) z_h^{\overrightarrow{m}} = 0$, which implies in turn that $(E^m - \sigma^{1-j} \tau_m^{-1} h) \sigma^{1-j}(z_h^{\overrightarrow{m}}) = 0$. Let now $a^{(j)}$ be any hypergeometric solution of $L_j^{\overleftarrow{m}} y = 0$. It follows from (5) that $a^{(j)} = \sum_{h \in \mathcal{H}_j} c_h z_h$ for some constants $c_h \in C$, hence, by linearity of all the operations involved, that $\biguplus_{j=1}^m a^{(j)} = \sum_{j=1}^m \sum_{h \in \mathcal{H}_j} c_h \sigma^{1-j}(z_h^{\overrightarrow{m}})$. Therefore, $L^{\overrightarrow{m}}(\biguplus_{j=1}^m a^{(j)}) = 0$ where

$$L^{\overrightarrow{m}} = \operatorname{llcm}_{\substack{1 \le j \le m \\ h \in \mathcal{H}_j}} \left(E^m - \sigma^{1-j} \tau_m^{-1} h\right).$$

Since $L^{\overrightarrow{m}}$ annihilates all the interlacings of hypergeometric solutions of $L_1^{\overleftarrow{m}}, \dots, L_m^{\overleftarrow{m}}$, theorems 2.4 and 4.2 imply that $Ly = 0$ has a Liouvillian solution if and only if $\operatorname{gcrd}(L, L^{\overrightarrow{m}})$ is nontrivial for some $1 \le m \le n$. The Hendriks–Singer algorithm proceeds as follows: if $\operatorname{gcrd}(L, L^{\overrightarrow{m}})$ has degree 0 for all $1 \le m \le n$, then $Ly = 0$ has no Liouvillian solution. Otherwise, let $m \ge 1$ be the smallest integer such that $R = \operatorname{gcrd}(L, L^{\overrightarrow{m}})$ is nontrivial. Then, $L^{\overrightarrow{m}} = QR$ for some operator Q of degree $q \ge 0$. Since $\{\biguplus_{j=1}^m z_{h_j}, (h_1, \dots, h_m) \in \mathcal{H}_1 \times \cdots \times \mathcal{H}_m\}$ generates the solution space of $L^{\overrightarrow{m}}$, a basis $(y^{(1)}, \dots, y^{(t)})$ of that space can be extracted from that set. If $q = 0$, then $(y^{(1)}, \dots, y^{(t)})$ is a basis of the solution space of R. Otherwise, let $g^{(i)} = Ry^{(i)}$ for $1 \le i \le t$, $N \ge 0$ be an integer such $L^{\overrightarrow{m}}, Q$ and R have no singularities at $x = N + s$ for any integer $s \ge 0$, and M be the $(q+1) \times t$ matrix given by $M_{ij} = g_{N+i-1}^{(j)}$ for $1 \le i \le q+1$ and $1 \le j \le t$. Since $Qg^{(i)} = 0$ for each i and $\deg(Q) = q$, the map $(c_1, \dots, c_t)^T \to \sum_{i=1}^t c_i y^{(i)}$ is an isomorphism between the kernel of M and the solution space of R, so we obtain a basis of the solution space of R composed of interlacings of hypergeometric sequences, and those are Liouvillian solutions of $Ly = 0$. Writing $L = \tilde{L}R$ and applying the algorithm recursively to $\tilde{L}$ eventually yields a basis of all the Liouvillian solutions of $Ly = 0$.

A prototype implementation of the above algorithm is in the Shasta[3] server. While the above algorithm is complete, remark that it really needs to compute the hypergeometric solutions of the $L_j^{\overleftarrow{m}}$'s over the algebraic closure of the constant field C. A rational alternative based on eigenring computations is developed [2], that alternative computes only in the constant field C of the equation to solve, even if it is not algebraically closed.

Acknowledgements

I would like to thank R. Bomboy, M. Singer, F. Ulmer and J.-A. Weil for their many useful comments and remarks during the preparation of this paper, as well as Prof. W. Decker for inviting me to present this survey at 3ecm.

[3] `http://www.inria.fr/cafe/Manuel.Bronstein/sumit/shasta.html`

References

[1] S.A. Abramov, M. Bronstein, and M. Petkovšek. On polynomial solutions of linear operator equations. In *Proceedings of ISSAC'95*, pages 290–296. ACM Press, 1995.

[2] R. Bomboy. *Solutions Liouvilliennes des équations aux différences finies linéaires.* Thèse de mathématiques, Université de Nice, 2001.

[3] D. Boucher. *Sur les équations différentielles paramétrées : une application aux systèmes hamiltoniens.* Thèse de mathématiques, Université de Limoges, 2000.

[4] M. Bronstein. On solutions of linear ordinary differential equations in their coefficient field. *J. Symbolic Computation*, 13(4):413–440, April 1992.

[5] M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. *Journal of Symbolic Computation*, 29(6):841–877, June 2000.

[6] M. Bronstein and A. Fredet. Solving linear ordinary differential equations over $C(x, e^{\int f(x)dx})$. In S. Dooley, editor, *Proceedings of ISSAC'99*, pages 173–179. ACM Press, 1999.

[7] M. Bronstein, T. Mulders, and J.-A. Weil. On symmetric powers of differential operators. In *Proceedings of ISSAC'97*, pages 156–163. ACM Press, 1997.

[8] M. Bronstein and M. Petkovšek. An introduction to pseudo–linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.

[9] F.T. Cope. Formal solutions of irregular linear differential equations ii. *American Journal of Mathematics*, 58:130–140, 1936.

[10] P.A. Hendriks and M.F. Singer. Solving difference equations in finite terms. *J. Symbolic Computation*, 27(3):239–260, March 1999.

[11] M. van Hoeij. Factorization of differential operators with rational functions coefficients. *J. Symbolic Computation*, 24(5):537–562, November 1997.

[12] M. Van Hoeij, J.-F. Ragot, F. Ulmer, and J.-A. Weil. Liouvillian solutions of linear differential equations of order three and higher. *J. Symbolic Computation*, 28(4 and 5):589–610, October/November 1999.

[13] M. van Hoeij and J.-A. Weil. An algorithm for computing invariants of differential galois groups. *Journal of Pure and Applied Algebra*, 117 & 118:353–379, 1997.

[14] E.L. Ince. *Ordinary Differential Equations.* Dover Publications Inc., 1956.

[15] C. Jordan. Mémoire sur les équations différentielles linéaires à intégrale algébrique. *Journal für Mathematik*, 84:89–215, 1878.

[16] Irving Kaplansky. *An introduction to differential algebra.* Hermann, Paris, 1957.

[17] E.R. Kolchin. Algebraic matrix groups and the Picard–Vessiot theory of homogeneous linear ordinary differential equations. *Annals of Mathematics*, 49:1–42, 1948.

[18] E.R. Kolchin. *Differential algebra and algebraic groups.* Academic Press, New York and London, 1973.

[19] O. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34:480–508, 1933.

[20] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *J. Symbolic Computation*, 14(2 and 3):243–264, August&September 1992.

[21] M. Petkovšek, H.S. Wilf, and D. Zeilberger. $A = B$. A.K. Peters, Wellesley, 1996.

[22] M. van der Put. Galois theory of differential equations, algebraic groups and Lie algebras. *J. Symbolic Computation*, 28(4 and 5):441–472, October/November 1999.

[23] A. Seidenberg. Abstract differential algebra and the analytic case. *Proceedings of the American Mathematical Society*, 9:159–164, 1958.

[24] A. Seidenberg. Abstract differential algebra and the analytic case II. *Proceedings of the American Mathematical Society*, 23:689–691, 1969.

[25] M.F. Singer. Liouvillian solutions of n^{th} order homogeneous linear differential equations. *American Journal of Mathematics*, 103:661–682, 1981.

[26] M.F. Singer. Liouvillian solution of linear differential equations with Liouvillian coefficients. *J. Symbolic Computation*, 11(3):251–274, March 1991.

[27] M.F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Applicable Algebra in Engineering, Communication and Computing*, 7:77–104, 1996.

[28] M.F. Singer and F. Ulmer. Liouvillian and algebraic solutions of second and third order linear differential equations. *J. Symbolic Computation*, 16(1):37–74, July 1993.

[29] M.F. Singer and F. Ulmer. Linear differential equations and products of linear forms. *Journal of Pure and Applied Algebra*, 117 & 118:549–563, 1997.

[30] M.F. Singer and M. van der Put. *Galois Theory of Difference Equations*. LNM 1666. Springer, 1997.

[31] F. Ulmer. On Liouvillian solutions of linear differential equations. *Applicable Algebra in Engineering, Communication and Computing*, 2:171–193, 1992.

[32] F. Ulmer. Irreducible linear differential equations of prime order. *J. Symbolic Computation*, 18(4):385–401, October 1994.

[33] F. Ulmer and J.-A. Weil. Note on Kovacic's algorithm. *J. Symbolic Computation*, 22(2):179–200, August 1996.

INRIA,
2004 route des Lucioles - B.P. 93
F-06902 Sophia Antipolis Cedex, France
E-mail address: `Manuel.Bronstein@sophia.inria.fr`