Computing the Lie Algebra of the Differential Galois Group of a Linear Differential System

Moulay Barkatou, Thomas Cluzeau,
Jacques-Arthur Weil
Univ. de Limoges, CNRS ; XLIM UMR 7252
123 av. Albert Thomas, 87 060 Limoges, France
forename.surname@unilim.fr

Lucia Di Vizio
Univ. de Versailles Saint-Quentin-En-Yvelines
Laboratoire de Mathématiques ; UMR 8100
45 av. des États-Unis, 78035 Versailles, France
divizio@math.cnrs.fr

ABSTRACT

We consider a linear differential system $[A] : \mathbf{y}' = A\,\mathbf{y}$ with coefficients in $\mathbb{C}(x)$. The differential Galois group G of $[A]$ is a linear algebraic group which measures the algebraic relations among solutions. Although there exist general algorithms to compute G, none of them is either practical or implemented. This paper proposes an algorithm to compute the Lie algebra $\mathfrak{g}$ of G when $[A]$ is absolutely irreducible. The algorithm is implemented in MAPLE.

Keywords

Computer algebra; Algorithms; Linear differential systems; Differential Galois theory; Lie algebras; Grothendieck-Katz p-curvature conjecture; Eigenrings; Reduced forms

1. INTRODUCTION

Consider a linear differential system $[A] : \mathbf{y}' = A\,\mathbf{y}$ with $A \in \mathbb{M}_n(\mathbb{C}(x))$ and $n > 1$. Its differential Galois group G measures everything that algebra can tell about the solutions, see [25]. For example, it measures solvability (with applications to integrability of dynamical systems, see references in [3, 1]), reducibility, transcendance properties for number theory, and so on. In theory, there exist general algorithms for computing differential Galois groups. Compoint and Singer gave such an algorithm in [12] in the case of reductive groups. Hrushovski gave a general algorithm in [19] which was recently clarified and improved by Feng in [16]. A symbolic-numeric algorithm is proposed by van der Hoeven in [24], based on the Schlesinger-Ramis density theorems. However, although these are wonderful decision procedures, none of them are either practical or implemented.

For a large class of problems, it is sufficient to compute the Lie algebra $\mathfrak{g}$ of G (which amounts to computing the connected component of the identity G°) instead of the differential Galois group G itself. See, for instance, Morales-Ramis-Simó integrability theory ([3]) or the work by Nguyen and van der Put in [22] where they study when a given differential system can be solved in terms of systems of lower order. The purpose of the present paper is to use a similar philosophy for computing $\mathfrak{g}$. Our starting point is the theory of Katz ([21]). Let $\mathcal{M}$ be the differential module associated with $[A]$. There is a theoretical identification (tannakian correspondence) between $\mathfrak{g}$ and a submodule $\mathcal{W}$ of $\mathrm{End}(\mathcal{M})$. Our main contribution is to make this identification algorithmic and provide an effective algorithm to compute $\mathfrak{g}$ when $\mathcal{M}$ is *absolutely irreducible*.

To achieve this, we proceed in four main steps. The first step (Section 3) consists in computing a maximal decomposition of $\mathrm{End}(\mathcal{M})$. Using eigenring techniques, this requires to compute rational solutions ([4]) of a structured system of dimension n^4. By exploiting the structure of the system, we reduce this problem to computing rational solutions of systems of lower dimensions which significantly improves the complexity of this step. In Section 4, to find a candidate for the submodule $\mathcal{W}$ (corresponding to $\mathfrak{g}$), we use a modular approach based on Grothendieck-Katz conjecture (see Conjecture 4.1). We choose a prime p, compute the p-curvature χ_p ([10]) and identify the smallest submodule of $\mathrm{End}(\mathcal{M})$ whose reduction modulo p contains χ_p. This provides a guess for $\mathcal{W}$ which is given by a basis $M_1, \ldots, M_d$ of matrices in $\mathbb{M}_n(\mathbb{C}(x))$. The next steps (Section 5) rely on the fact that $\mathfrak{g}$ can also be directly read off from a reduced form of $[A]$ (see Theorem 5.1). Using recent results from [2], we then prove that computing a reduction matrix amounts to computing a conjugation matrix between two semisimple Lie subalgebras of $\mathfrak{gl}_n(\mathbb{C}(x))$ respectively generated by the M_i and their evaluations $M_i(x_0)$ at some ordinary point x_0 of $[A]$. For the third step of our algorithm, we use a method for computing conjugation matrices based on results on semisimple Lie algebras ([20, 14]). In our last step, we find a reduction matrix among the conjugation matrices. If our guess for $\mathcal{W}$ is not correct, then the third and fourth steps may fail. In this case, we go back to the second step and restart with another prime.

The resulting algorithm is deterministic, assuming the veracity of the Grothendieck-Katz conjecture. We also give a less fancy algorithm which works independently of the Grothendieck-Katz conjecture. Note that a reduced form is obtained as a byproduct of our algorithm.

We have a prototype implementation of our algorithm in MAPLE. We have applied it to many examples and it turns out that the most costly step is the decomposition of $\mathrm{End}(\mathcal{M})$. This step has a polynomial complexity in n ([7]) compared to the exponential (several levels) complexity in n of the existing algorithms for computing G ([16]).

ISSAC '16, July 19-22, 2016, Waterloo, ON, Canada
© 2016 ACM. ISBN 978-1-4503-4380-0/16/07…$15.00
DOI: http://dx.doi.org/10.1145/2930889.2930932

Notations.

Throughout this paper, $k \triangleq \mathbb{C}(x)$ denotes the differential field of rational functions in the (complex) variable x with the derivation $' \triangleq \frac{d}{dx}$. For the actual calculations in our algorithms, $\mathbb{C}$ is replaced by a computable subfield of $\overline{\mathbb{Q}}$. If $u_1, \ldots, u_n$ are elements of some vector space E, we denote by $\mathbf{u}$ in bold the column vector $\mathbf{u} = (u_1 \, \ldots \, u_n)^T \in E^n$. For a square matrix $U \in \mathbb{M}_n(k)$ of size n with entries in k, we denote $U_{i\bullet}$ (resp. $U_{\bullet i}$) the ith row (resp. column) of U, and $\mathrm{Vect}(U) \triangleq (U_{1\bullet}, \ldots, U_{n\bullet})^T \in k^{n^2}$ is the vector obtained by stacking the vectors $U_{i\bullet}^T$ successively. Conversely, for a vector $\mathbf{v} \in k^{n^2}$, we note $\mathrm{Mat}(\mathbf{v})$ the matrix in $\mathbb{M}_n(k)$ obtained by the reverse operation. The *Kronecker product* $A \otimes B$ of $A \in \mathbb{M}_{n\times p}(k)$ and $B \in \mathbb{M}_{q\times r}(k)$ is the matrix defined by:

$$A \otimes B \triangleq \begin{pmatrix} a_{1,1}\, B & \ldots & a_{1,p}\, B \\ \vdots & \vdots & \vdots \\ a_{n,1}\, B & \ldots & a_{n,p}\, B \end{pmatrix} \in \mathbb{M}_{nq\times pr}(k).$$

If $A \in \mathbb{M}_n(k)$, we denote $[A]$ the linear differential system $[A]: \ \mathbf{y}' = A\,\mathbf{y}$, where $\mathbf{y}$ is a column vector of n unknown functions. A change of variables also called *gauge transformation* $\mathbf{y} = P\,\mathbf{z}$ with $P \in \mathrm{GL}_n(k)$ yields $\mathbf{z}' = P[A]\,\mathbf{z}$, where $P[A] \triangleq P^{-1}(A\,P - P')$. The linear differential systems $[A]$ and $[P[A]]$ are then said to be *(gauge) equivalent* over k.

Acknowledgements.

We warmly thank the referees for their suggestions which enhanced the clarity of this paper.

2. PRELIMINARIES

We recall here some definitions and facts concerning differential modules, linear differential systems, differential Galois groups and their Lie algebras. See, e.g., [25] for more details.

2.1 Differential modules and systems

A *differential module* $\mathcal{M}$ over k is a finite-dimensional k-vector space equipped with an additive map $\partial : \mathcal{M} \rightarrow \mathcal{M}$ satisfying $\partial(f\,m) = f'\,m + f\,\partial(m)$, for all $f \in k$ and for all $m \in \mathcal{M}$. A *differential submodule* of $\mathcal{M}$ is then a vector subspace of $\mathcal{M}$ which is stable under the action of ∂.

A differential module $\mathcal{M}$ is *irreducible* if it has no non-trivial submodules. Otherwise it is *reducible*. $\mathcal{M}$ is *absolutely irreducible* if $\overline{k} \otimes_k \mathcal{M}$ is irreducible. $\mathcal{M}$ is *decomposable* if there exist two non-trivial differential submodules $\mathcal{M}_1$ and $\mathcal{M}_2$ of $\mathcal{M}$ such that we have the direct sum decomposition $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2$. Otherwise $\mathcal{M}$ is *indecomposable*. $\mathcal{M}$ is *completely reducible* if it is a direct sum of *irreducible* modules.

Remark 2.1. *Every differential module $\mathcal{M}$ can be written as $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2 \oplus \cdots \oplus \mathcal{M}_r$, where the $\mathcal{M}_i$'s are indecomposable differential submodules of $\mathcal{M}$. If we have another decomposition $\mathcal{M} = \mathcal{N}_1 \oplus \mathcal{N}_2 \oplus \cdots \oplus \mathcal{N}_s$, then $s = r$ and there is a permutation σ such that $\mathcal{M}_i \simeq \mathcal{N}_{\sigma(i)}$ (Krull-Schmidt theorem). In the sequel, such a decomposition is called a* maximal decomposition *of $\mathcal{M}$. If $\mathcal{M}$ is completely reducible, then in such a maximal decomposition, the differential submodules $\mathcal{M}_i$ are irreducible.*

Let $\mathcal{M}$ be a differential module of dimension n. Choosing a basis $e_1, \ldots, e_n$, $\mathcal{M}$ is associated with the linear differential system $[A]$, where $A = (a_{i,j})_{1\le i,j\le n} \in \mathbb{M}_n(k)$ is defined by the relations $\partial(e_i) \triangleq -\sum_{j=1}^{n} a_{j,i}\, e_j$, $i = 1, \ldots, n$. A change of basis $\overline{\mathbf{e}}^T = \mathbf{e}^T\, P$ with $P \in \mathrm{GL}_n(k)$ in $\mathcal{M}$, corresponds to a gauge transformation $\mathbf{y} = P\,\mathbf{z}$ in $[A]$. The fact that $\mathcal{M}$ is a reducible, decomposable or completely reducible differential module then corresponds to the fact that $[A]$ is equivalent to a linear differential system $[B]$ with $B = P[A]$ block triangular, block diagonal or block diagonal with irreducible diagonal blocks. A maximal decomposition corresponds to a block diagonal form with indecomposable diagonal blocks.

Let $\mathcal{M}$ be a differential module of dimension n over k. We fix a basis $e_1, \ldots, e_n$ of $\mathcal{M}$ and we denote by $[A]$ the associated linear differential system. The module $\mathcal{M}$ is called *trivial* when $[A]$ has a full space of rational solutions, i.e, if there exists a basis $\tilde{e}_1, \ldots, \tilde{e}_n$ such that $\partial(\tilde{e}_i) = 0$ for all i. The *dual of the differential module* $\mathcal{M}$ is the differential module $\mathcal{M}^\star$ of dimension n over k defined by $\mathcal{M}^\star \triangleq \mathrm{Hom}_k(\mathcal{M}, \mathbb{1}_k)$, where $\mathbb{1}_k$ is the trivial differential module of dimension 1 over k. The dual $\mathcal{M}^\star$ is endowed with the map $\partial^\star$ given by $(\partial^\star(\phi))(m) \triangleq -\phi(\partial(m)) + \partial_{\mathbb{1}_k}(\phi(m))$, for $\phi \in \mathcal{M}^\star$ and $m \in \mathcal{M}$. The linear differential system associated with $\mathcal{M}^\star$ with respect to the dual basis $e_1^\star, \ldots, e_n^\star$ defined by $e_i^\star(e_j) = 1$, if $i = j$ and 0 otherwise, is then $[-A^T]$.

Let $\mathcal{M}_1$ and $\mathcal{M}_2$ be two differential modules over k endowed respectively with the maps ∂_1 and ∂_2. The *tensor product* of $\mathcal{M}_1$ and $\mathcal{M}_2$ is the differential module $\mathcal{M}_1 \otimes_k \mathcal{M}_2$ endowed with the map ∂ defined by $\partial(m_1 \otimes m_2) \triangleq \partial_1(m_1) \otimes m_2 + m_1 \otimes \partial_2(m_2)$, for all $m_1 \in \mathcal{M}_1$ and for all $m_2 \in \mathcal{M}_2$.

Let us now consider the differential module $\mathcal{M} \otimes_k \mathcal{M}^\star$. With respect to the basis $e_i \otimes e_j^\star$, $i, j = 1, \ldots, n$, the elements of $\mathcal{M} \otimes_k \mathcal{M}^\star$ can be identified with matrices in $\mathbb{M}_n(k)$, namely, if $m = \mathbf{x}^T\,\mathbf{e} \in \mathcal{M}$ and $\phi = \mathbf{y}^T\,\mathbf{e}^\star \in \mathcal{M}^\star$, then $m \otimes \phi$ is identified with the Kronecker product $\mathbf{x}^T \otimes \mathbf{y}$. The matrix differential system associated with $\mathcal{M} \otimes_k \mathcal{M}^\star$ is then

$$F' = [A, F] \triangleq A\,F - F\,A. \qquad (1)$$

If A, B and C are three matrices of appropriate dimensions, then we have the relation $\mathrm{Vect}(A\,B\,C) = (A \otimes C^T)\,\mathrm{Vect}(B)$ so that (1) can be written as the linear differential system

$$\mathrm{Vect}(F)' = \Big(A \otimes I_n - I_n \otimes A^T\Big)\,\mathrm{Vect}(F). \qquad (2)$$

Finally, from [25, Ex. 2.38(3)], if $\mathcal{M}$ is an irreducible differential module, then $\mathcal{M} \otimes_k \mathcal{M}^\star$ is completely reducible so that all its submodules can be read off from a maximal decomposition as in remark 2.1.

2.2 Decomposition of differential modules

The problem of computing a decomposition of a differential module $\mathcal{M}$ has been studied in the literature of computer algebra: see [23, 5], [25, §4.2] and references therein.

Decomposing $\mathcal{M}$ (over k) is equivalent to finding a gauge transformation $P \in \mathrm{GL}_n(k)$ such that $P[A]$ is a block diagonal matrix and such a gauge transformation can be found by calculating the so-called *eigenring* $\mathcal{E}(A)$ of $[A]$ defined by $\mathcal{E}(A) \triangleq \{F \in \mathbb{M}_n(k) \mid F' = [A, F] = A\,F - F\,A\}$. In practice, computing $\mathcal{E}(A)$ reduces to computing the rational solutions of the matrix differential system (1) or equivalently of the linear differential system (2). The Maple package IntegrableConnections ([6]) based on Isolde ([8]) provides a procedure for computing the eigenring using the algorithm in [4] for computing rational solutions.

If $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$ is a decomposition of $\mathcal{M}$ into submodules $\mathcal{M}_i$ of dimension n_i, then $\mathcal{E}(A)$ contains an element similar to $\mathrm{diag}(\lambda_1 I_{n_1}, \ldots, \lambda_r I_{n_r})$, where $\lambda_i \in \mathbb{C}$. Given $F \in \mathcal{E}(A)$ and $T \in \mathrm{GL}_n(k)$ such that $T^{-1} F T = \mathrm{diag}(F_1, \ldots, F_r)$, for constant[1] matrices $F_1, \ldots, F_r$ having distinct eigenvalues in $\mathbb{C}$ (e.g., Jordan blocks of F), we have $T[A] = \mathrm{diag}(A_1, \ldots, A_r)$ for some matrices $A_i \in \mathbb{M}_{n_i}(k)$. Bases of the submodules $\mathcal{M}_i$ in the corresponding decomposition $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$ are given by the columns of the matrix T, namely, a basis of $\mathcal{M}_i$ is given by the columns $T_{\bullet j}$ of T for $j = (n_1 + \cdots + n_{i-1} + 1), \ldots, (n_1 + \cdots + n_{i-1} + n_i)$. Note finally that a *maximal* decomposition is in general obtained by taking a random element in the eigenring. We refer to [5] for more details.

2.3 Differential Galois group and Lie algebra

Let $\mathcal{M}$ be a differential module of dimension n over k. We fix a basis of $\mathcal{M}$ and we denote by $[A]$ the associated linear differential system.

There exists a differential field extension K of k called *Picard-Vessiot extension* for $\mathcal{M}$ (equivalently for $[A]$) which is such that K has the same constants as k (namely, the elements of $\mathbb{C}$), $[A]$ admits a *fundamental matrix of solutions* $U \in \mathrm{GL}_n(K)$ and K is the differential field generated over k by the entries of U (see [25, §1.3, Prop. 1.22]).

The *differential Galois group* G of $\mathcal{M}$ (equivalently of $[A]$), is the group $\mathrm{Aut}_\partial(K/k)$ of differential automorphisms of the k-algebra K, *i.e.*, for every $g \in G$ and every $f \in K$, we have $g(f') = g(f)'$ and, if $f \in k$, then $g(f) = f$. The *differential Galois correspondence* shows that we have $K^G = k$, where $K^G = \{f \in K \mid \forall g \in G,\ g(f) = f\}$.

The group G acts on vectors or matrices with entries in K componentwise. If $g \in G$ and $U \in \mathrm{GL}_n(K)$ is a fundamental matrix of solutions of $[A]$, then $g(U)$ is also a fundamental matrix of solutions of $[A]$ so that there exists $C_g \in \mathrm{GL}_n(\mathbb{C})$ such that $g(U) = U\, C_g$. Hence choosing a fundamental matrix of solutions yields a faithful representation of G in $\mathrm{GL}_n(\mathbb{C})$, *i.e.*, the map $\rho :\ G \to \mathrm{GL}_n(\mathbb{C}),\ g \mapsto C_g$, is an injective group homomorphism.

The group G viewed as a subgroup of $\mathrm{GL}_n(\mathbb{C})$ is a *linear algebraic group* (see [25, Thm 1.27]). Indeed, there exists a polynomial ideal $\mathcal{I} \subset \mathbb{C}[X_{1,1}, X_{1,2}, \ldots, X_{n,n}, \det^{-1}]$, where $\det^{-1}$ is the inverse of $\det((X_{i,j})_{1 \le i,j \le n})$, such that

$$G \cong \{M = (m_{i,j})_{1 \le i,j \le n} \in \mathrm{GL}_n(\mathbb{C}) \mid \forall P \in \mathcal{I},\ P(m_{i,j}) = 0\}.$$

Let $\mathfrak{g}$ denote the *Lie algebra of the differential Galois group* G, namely, the tangent space of G at the identity. The Lie algebra $\mathfrak{g}$ can be represented as a Lie subalgebra of the Lie algebra $\mathfrak{gl}_n(\mathbb{C})$ of $n \times n$ matrices with entries in $\mathbb{C}$ and endowed with the natural Lie bracket $[\cdot,\cdot]$ of matrices:

$$\mathfrak{g} \cong \{N \in \mathbb{M}_n(\mathbb{C}) \mid I_n + \epsilon\, N \in G(\mathbb{C}[\epsilon]) \text{ with } \epsilon \neq 0 \text{ and } \epsilon^2 = 0\},$$

where $G(\mathbb{C}[\epsilon])$ is the set of $\mathbb{C}[\epsilon]$-points of G, i.e., the set of matrices with entries in $\mathbb{C}[\epsilon]$ satisfying the equations of the polynomial ideal $\mathcal{I}$ defined above.

For $g \in G$ and $h \in \mathfrak{g}$, we have $g\,(\mathrm{id} + \epsilon\, h)\, g^{-1} = \mathrm{id} + \epsilon(g\, h\, g^{-1}) \in G(\mathbb{C}[\epsilon])$. Thus $g\, h\, g^{-1} \in \mathfrak{g}$ and G acts on $\mathfrak{g}$ via the *adjoint action*: $G \times \mathfrak{g} \to \mathfrak{g},\ (g, h) \mapsto g\, h\, g^{-1}$. In terms of matrices, the adjoint action Ad is given by $(M, N) \mapsto M\, N\, M^{-1}$.

Let V denote the $\mathbb{C}$-vector space of solutions of $[A]$ in K^n and $\mathrm{End}(V)$ the set of endomorphisms of V, *i.e.*, the set of linear maps from V to V. The set $\mathrm{End}(V)$ is naturally endowed with a Lie algebra structure denoted by $\mathfrak{gl}(V)$. As V is a finite-dimensional $\mathbb{C}$-vector space of dimension n, $\mathfrak{gl}(V)$ can be identified with $\mathfrak{gl}_n(\mathbb{C})$. Now, we have the following classical isomorphism of finite-dimensional k-vector spaces: $V \otimes V^\star \to \mathrm{End}(V),\ v \otimes \varphi \mapsto (w \in V \mapsto \varphi(w)\, v)$. Consequently *the Lie algebra $\mathfrak{g}$ can be viewed as a vector subspace of $V \otimes V^\star$ which is stable under the adjoint action Ad of G.*

With the previous notation, the *tannakian correspondence* ([25, Thm 2.33, Cor. 2.35]) provides a one-to-one correspondence between vector subspaces of V stable under the action of G and differential submodules of $\mathcal{M}$. More precisely, to a vector subspace W of V stable under the action of G corresponds the differential submodule $(K \otimes_{\mathbb{C}} W)^G$ of $\mathcal{M}$, [25, Rmk 2.34]. This correspondence is compatible with all constructions of linear algebra (see Definition 5.2 below) and the fact of taking subspaces or quotients, so that there is a one-to-one correspondence between vector subspaces of $V \otimes V^\star$ stable under the action of G and differential submodules of $\mathcal{M} \otimes \mathcal{M}^\star$. With the previous notation, this yields:

PROPOSITION 2.1. *The Lie algebra $\mathfrak{g}$, viewed as a G-module under the adjoint action of G on $\mathrm{End}(V)$, corresponds to the differential submodule $\mathfrak{g}^k \triangleq (K \otimes_{\mathbb{C}} \mathfrak{g})^G$ of $\mathcal{M} \otimes \mathcal{M}^\star$.*

We shall denote by $\mathfrak{g}^k$ this *k-Lie algebra* $(K \otimes_{\mathbb{C}} \mathfrak{g})^G$ included in $\mathfrak{gl}_n(k)$. Note that $\mathfrak{g}^k$ corresponds to the Lie algebra considered by Katz in [21, Conj. 9.2]. For expository reasons, we assume in this paper that $\mathcal{M}$ is an *absolutely irreducible* differential module (which can be effectively tested, see [13]). The case of a completely reducible module $\mathcal{M}$ is quite similar and will appear in a forthcoming paper.

REMARK 2.2. *The assumption that $\mathcal{M}$ is absolutely irreducible means that $\mathfrak{g}$ acts* irreducibly *on V. If we further assume, w.l.o.g. [12, Thm. 4.1], that $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C})$, then the Lie algebras $\mathfrak{g}$ and $\mathfrak{g}^k$ are* semisimple *([20, Prop. 19.1]).*

Thanks to Proposition 2.1, the k-Lie algebra $\mathfrak{g}^k$ can be investigated by studying differential submodules of $\mathcal{M} \otimes \mathcal{M}^\star$.

3. DECOMPOSITION OF $\mathcal{M} \otimes \mathcal{M}^\star$

In the sequel, $\mathcal{M}$ is an absolutely irreducible differential module of dimension $n > 1$ over k. We fix a basis of $\mathcal{M}$ and we denote by $[A]$ the associated linear differential system.

Our algorithm requires to compute a maximal decomposition of the differential module $\mathcal{M} \otimes \mathcal{M}^\star$ associated to the linear differential system $\mathbf{y}' = \left(A \otimes I_n - I_n \otimes A^T\right)\mathbf{y}$. If we denote $\mathcal{A} \triangleq A \otimes I_n - I_n \otimes A^T$, then such a decomposition can be obtained by computing the eigenring $\mathcal{E}(\mathcal{A})$ of $[\mathcal{A}]$, as shown in Subsection 2.2. However, starting from a differential module of dimension n, this method would then require to compute the rational solutions of a linear differential system of size n^4 so that the dependency on n in the arithmetic complexity estimate for computing rational solutions of such a linear differential system would roughly be in n^{20} (see [7, Cor. 1]). Consequently, to obtain a more practicable algorithm, we will take into account the specific form of the differential module $\mathcal{M} \otimes \mathcal{M}^\star$/the particular structure of the linear differential system $[A \otimes I_n - I_n \otimes A^T]$.

3.1 Adapting the general method

The algorithm in [4] for computing rational solutions of a linear differential system is divided into two steps: the first one consists in computing local datas (considering one by one each singularity of the system) in order to construct

[1] the eigenvalues of any element of $\mathcal{E}(A)$ are constants in $\mathbb{C}$.

a universal denominator for the rational solutions and the second one consists in computing polynomial solutions of an auxiliary linear differential system. Here, the linear differential system that we consider has a specific structure, namely, its matrix is given by $\overline{\mathcal{A}} \triangleq \mathcal{A} \otimes I_{n^2} - I_{n^2} \otimes \mathcal{A}^T$ with the previous notation $\mathcal{A} = A \otimes I_n - I_n \otimes A^T$. Consequently, the specific techniques developed in [9] for computing rational solutions of $[\mathcal{A}]$ can be adapted and reused here. This implies that all the local datas needed for computing rational solutions of $[\overline{\mathcal{A}}]$ can be deduced from the local datas needed for computing rational solutions of $[A]$. For instance, the local exponential parts of $[\mathcal{A}]$ (resp. of $[\overline{\mathcal{A}}]$) are the differences (resp. the differences of the differences) between the local exponential parts of $[A]$. The first step of the algorithm can thus be performed by considering only the matrix A of size n instead of $\overline{\mathcal{A}}$ of size n^4 which leads to a real gain. Note that the ideas in [9] to accelerate the second step of the algorithm can also be adapted to be used here.

3.2 Using structural decompositions

With the previous notation, we are interested in computing the rational solutions of the linear differential system $[\overline{\mathcal{A}}]$ which is associated with the differential module

$$\mathrm{End}(\mathrm{End}(\mathcal{M})) \triangleq (\mathcal{M} \otimes \mathcal{M}^\star) \otimes (\mathcal{M} \otimes \mathcal{M}^\star)^\star.$$

We shall now prove that the problem can be reduced to computing the rational solutions of linear differential systems of size smaller than n^4. To do that, we shall first use the isomorphism $(\mathcal{M} \otimes \mathcal{M}^\star)^\star \cong (\mathcal{M} \otimes \mathcal{M}^\star)$ which leads to

$$\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong (\mathcal{M} \otimes \mathcal{M}^\star) \otimes (\mathcal{M} \otimes \mathcal{M}^\star). \qquad (3)$$

Let us provide explicit matrix formulas for (3):

Lemma 3.1. *The matrix $\mathcal{A} = A \otimes I_n - I_n \otimes A^T$ satisfies*

$$-\mathcal{A}^T = \mathcal{J}\,\mathcal{A}\,\mathcal{J}, \qquad \mathcal{J} \triangleq \sum_{i=1}^{n}\sum_{j=1}^{n} E_{i,j}(n) \otimes E_{i,j}(n)^T,$$

where $E_{i,j}(n)$ denotes the elementary $n \times n$ matrix having 1 at position (i,j) and 0 elsewhere. In particular, the matrix $\mathcal{J}$ is orthogonal and further satisfies $\mathcal{J}^T = \mathcal{J}^{-1} = \mathcal{J}$.

Proof. A result about the Kronecker product asserts that given two square matrices M and N of size n, we have $N \otimes M = \mathcal{J}\,(M \otimes N)\,\mathcal{J}$, where $\mathcal{J}$ is the matrix defined in Lemma 3.1 (see [17, §2.5]). Therefore, we get $-\mathcal{A}^T = I_n \otimes A - A^T \otimes I_n = \mathcal{J}\,(A \otimes I_n - I_n \otimes A^T)\,\mathcal{J} = \mathcal{J}\,\mathcal{A}\,\mathcal{J}$. □

Lemma 3.1 implies $\mathcal{J}[\mathcal{A}] = -\mathcal{A}^T$ so that the isomorphism $(\mathcal{M} \otimes \mathcal{M}^\star) \cong (\mathcal{M} \otimes \mathcal{M}^\star)^\star$ is explicitly given by:

$$\mathcal{M} \otimes \mathcal{M}^\star \to (\mathcal{M} \otimes \mathcal{M}^\star)^\star, \quad U \mapsto \mathrm{Mat}(\mathcal{J}\,\mathrm{Vect}(U)).$$

With the previous notation, a rational solution of the linear differential system associated with the differential module $(\mathcal{M} \otimes \mathcal{M}^\star) \otimes (\mathcal{M} \otimes \mathcal{M}^\star)$ is then sent to a rational solution of $[\overline{\mathcal{A}}]$ by multiplication by $I_{n^2} \otimes \mathcal{J}$.

For any differential module $\mathcal{N}$ of dimension n, we have the classical explicit isomorphism $\mathcal{N} \otimes \mathcal{N} \cong \mathrm{Sym}^2(\mathcal{N}) \oplus \Lambda^2(\mathcal{N})$, where $\mathrm{Sym}^2(\mathcal{N})$ (resp. $\Lambda^2(\mathcal{N})$) denotes the symmetric (resp. exterior) square of the differential module $\mathcal{N}$ which is of dimension $\frac{n\,(n+1)}{2}$ (resp. $\frac{n\,(n-1)}{2}$). From (3), we thus have:

$$\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathrm{Sym}^2(\mathcal{M} \otimes \mathcal{M}^\star) \oplus \Lambda^2(\mathcal{M} \otimes \mathcal{M}^\star). \qquad (4)$$

Now, due to its specific structure the differential module $\mathcal{M} \otimes \mathcal{M}^\star$ can always be decomposed which allows us to go further in the decomposition of the right-hand side of (4).

Lemma 3.2. *With the previous notation, the matrix defined by $\mathcal{T} \triangleq \mathrm{Vect}(I_n)^T \otimes \mathrm{Vect}(I_n) \in \mathbb{M}_{n^2}(\mathbb{C})$ belongs to the eigenring $\mathcal{E}(\mathcal{A})$ and provides the decomposition*

$$\mathcal{M} \otimes \mathcal{M}^\star = \mathbb{1}_k \oplus \mathcal{W}, \qquad (5)$$

where $\mathcal{W}$ is a submodule of $\mathcal{M} \otimes \mathcal{M}^\star$ of dimension $n^2 - 1$.

Proof. The fact that $\mathcal{T} \in \mathcal{E}(\mathcal{A})$ is straightforward since $\mathrm{Vect}(I_n)$ is a trivial rational solution of both $\mathbf{y}' = \mathcal{A}\,\mathbf{y}$ and $\mathbf{y}' = -\mathcal{A}^T\,\mathbf{y}$. The result then follows from the explanations in Subsection 2.2 because $\mathcal{T}$ is the block matrix $(E_{i,j}(n))_{1 \le i,j \le n}$ which admits two distinct eigenvalues, namely n of multiplicity 1 and 0 of multiplicity $n^2 - 1$. □

Theorem 3.1. *With the previous notation, we have:*

$$\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathbb{1}_k \oplus \mathcal{W} \oplus \mathrm{Sym}^2(\mathcal{W}) \oplus \mathcal{W} \oplus \Lambda^2(\mathcal{W}). \quad (6)$$

Proof. From Lemma 3.2 and the isomorphism (4), we obtain $\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathrm{Sym}^2(\mathbb{1}_k \oplus \mathcal{W}) \oplus \Lambda^2(\mathbb{1}_k \oplus \mathcal{W})$. If we denote e the basis element of $\mathbb{1}_k$ and e_i, $i = 1, \ldots, n^2 - 1$ a basis of $\mathcal{W}$, then a basis of $\mathrm{Sym}^2(\mathbb{1}_k \oplus \mathcal{W})$ is given by $e.e$, $e.e_i$, $i = 1, \ldots, n^2 - 1$ and $e_i.e_j$ for i, $j = 1, \ldots, n^2 - 1$ and $i \le j$. This basis yields the isomorphism $\mathrm{Sym}^2(\mathbb{1}_k \oplus \mathcal{W}) \cong \mathbb{1}_k \oplus \mathcal{W} \oplus \mathrm{Sym}^2(\mathcal{W})$. Moreover, a basis of $\Lambda^2(\mathbb{1}_k \oplus \mathcal{W})$ is given by $e \wedge e_i$, $i = 1, \ldots, n^2 - 1$ and $e_i \wedge e_j$ for i, $j = 1, \ldots, n^2 - 1$ and $i < j$ so that $\Lambda^2(\mathbb{1}_k \oplus \mathcal{W}) \cong \mathcal{W} \oplus \Lambda^2(\mathcal{W})$. The isomorphisms of k-vector spaces explicitly given above are isomorphisms of differential modules which ends the proof. □

Let us explain how to use decomposition (6) of Theorem 3.1 for computing effectively the rational solutions of $[\overline{\mathcal{A}}]$:

① Let $\mathbf{u} \in k^m$ with $m = \frac{(n^2-1)\,n^2}{2}$ be a rational solution of $\mathbf{u}' = \mathrm{sym}^2(W)\,\mathbf{u}$, where $[W]$ (resp. $[\mathrm{sym}^2(W)]$) is the differential system associated with $\mathcal{W}$ (resp. $\mathrm{Sym}^2(\mathcal{W})$);

② Construct the associated matrix U in $\mathrm{Sym}^2(\mathbb{1}_k \oplus \mathcal{W})$ (see the proof of Theorem 3.1) which can also be viewed as an element of $(\mathbb{1}_k \oplus \mathcal{W}) \otimes (\mathbb{1}_k \oplus \mathcal{W})$;

③ Computing $(P \otimes P)\mathrm{Vect}(U)$, where P denotes the gauge transformation yielding (5), we then obtain an element of $(\mathcal{M} \otimes \mathcal{M}^\star) \otimes (\mathcal{M} \otimes \mathcal{M}^\star)$;

④ Finally, using the isomorphism (3), we then get the rational solution $(P \otimes \mathcal{J}\,P)\,\mathrm{Vect}(U)$ of $[\overline{\mathcal{A}}]$.

Note that the matrix P appearing in the above process is formed by eigenvectors of the diagonalizable matrix $\mathcal{T}$ of Lemma 3.2 and can be given explicitly. A similar constructive process can be applied from a rational solution of the differential system $[\mathrm{ext}^2(W)]$ associated with $\Lambda^2(\mathcal{W})$.

Proposition 3.1. *With the previous notation, the eigenring $\mathcal{E}(\mathcal{A})$ can be computed from the rational solutions of two linear differential systems $[\mathrm{sym}^2(W)]$ and $[\mathrm{ext}^2(W)]$ of respective sizes $\frac{(n^2-1)\,n^2}{2}$ and $\frac{(n^2-1)\,(n^2-2)}{2}$.*

Proof. This is straightforward from Theorem 3.1 and the assumption that $\mathcal{M}$ is irreducible since a rational solution of $[W]$ would lead to a decomposition of $\mathcal{M}$. □

Note that, in practice, this has a real gain since already for $n = 3$, we have $\frac{(n^2-1)\,n^2}{2} = 36$ and $\frac{(n^2-1)\,(n^2-2)}{2} = 28$

compared to $n^4 = 81$. Moreover, one can speed up the computation of rational solutions since the systems under considerations are symmetric (resp. exterior) squares so that the techniques in [1, §5] can be applied to obtain the local datas by considering smaller systems.

We now provide another isomorphism as (6). We have $\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong (\mathcal{M} \otimes \mathcal{M}) \otimes (\mathcal{M} \otimes \mathcal{M})^\star$ which can be written as $\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathrm{End}(\mathcal{M} \otimes \mathcal{M})$ so that we obtain $\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathrm{End}(\mathrm{S}^2 \oplus \Lambda^2)$, where, for the purposes of notation, we denote $\mathrm{S}^2 \triangleq \mathrm{Sym}^2(\mathcal{M})$, $\Lambda^2 \triangleq \Lambda^2(\mathcal{M})$. We then get: $\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong \mathrm{End}(\mathrm{S}^2) \oplus \mathrm{End}(\Lambda^2) \oplus \mathrm{Hom}(\mathrm{S}^2, \Lambda^2) \oplus \mathrm{Hom}(\Lambda^2, \mathrm{S}^2)$. Finally, using the decompositions $\mathrm{End}(\mathrm{S}^2) = \mathbb{1}_k \oplus \mathcal{N}_{\mathrm{S}^2}$ and $\mathrm{End}(\Lambda^2) = \mathbb{1}_k \oplus \mathcal{N}_{\Lambda^2}$ for some differential modules $\mathcal{N}_{\mathrm{S}^2}$ and $\mathcal{N}_{\Lambda^2}$ of respective dimensions $\frac{n^2\,(n+1)^2}{4} - 1$ and $\frac{n^2\,(n-1)^2}{4} - 1$, we have proved:

Theorem 3.2. *The module* $\mathrm{End}(\mathrm{End}(\mathcal{M}))$ *decomposes as*

$$\mathrm{End}(\mathrm{End}(\mathcal{M})) \cong$$
$$\mathbb{1}_k \oplus \mathcal{N}_{\mathrm{S}^2} \oplus \mathbb{1}_k \oplus \mathcal{N}_{\Lambda^2} \oplus \mathrm{Hom}(\mathrm{S}^2, \Lambda^2) \oplus \mathrm{Hom}(\Lambda^2, \mathrm{S}^2). \quad (7)$$

The decomposition (7) can be used exactly as (6) for our purposes and we get:

Proposition 3.2. *With the previous notation, the eigenring* $\mathcal{E}(\mathcal{A})$ *can be computed from the rational solutions of four linear differential systems of respective sizes* $\frac{n^2\,(n+1)^2}{4} - 1$, $\frac{n^2\,(n-1)^2}{4} - 1$, $\frac{n^2\,(n^2-1)}{4}$, *and* $\frac{n^2\,(n^2-1)}{4}$.

Note that for $n = 3$, we would then have to compute the rational solutions of four linear differential systems of respective size 35, 8, 18 and 18. The systems corresponding to (7) have specific structures so that existing techniques (e.g., adapting the ones developed in [9, 1]) can be used here to speed up the computation.

4. CANDIDATE FOR THE LIE ALGEBRA

Let $\mathcal{M}$ be an absolutely irreducible differential module. From Proposition 2.1, the representation of the Lie algebra $\mathfrak{g}$ in $\mathrm{End}(V)$ corresponds to the submodule $\mathfrak{g}^k$ of $\mathcal{M} \otimes \mathcal{M}^\star$. Section 3 provides a maximal decomposition of the completely reducible module $\mathcal{M} \otimes \mathcal{M}^\star$ which yields all its submodules. We now develop a modular method for identifying $\mathfrak{g}^k$ as a submodule of $\mathcal{M} \otimes \mathcal{M}^\star$.

The approach that we propose relies on the reduction modulo a prime number p of the linear differential system $[A]$ or equivalently of the differential module $\mathcal{M}$. Here, the constant field $\mathbb{C}$ of k is replaced by a computable subfield of $\overline{\mathbb{Q}}$. For almost all primes p, the coefficients of the matrix $A \in \mathbb{M}_n(k)$ can be reduced modulo p and we obtain a matrix $A_p \in \mathbb{M}_n(\mathbb{F}_q(x))$, for $q = p^r$, corresponding to a linear differential system $[A_p]$ over the differential field $\mathbb{F}_q(x) = \oplus_{i=0}^{p-1} \mathbb{F}_q(x^p)\, x^i$ of characteristic p. As in characteristic zero, a differential module $\mathcal{M}_p$ over $\mathbb{F}_q(x)$ endowed with an action ∂ is associated with $[A_p]$. We refer to [25, §13] and references therein or [21] for details on differential modules and differential systems in characteristic p. A central object for the study of differential modules/systems in characteristic p is the so-called *p-curvature* defined as the operator $\chi_p \triangleq \partial^p$ acting on $\mathcal{M}_p$ or equivalently $\chi_p \triangleq \left(\frac{d}{dx} - A_p\right)^p$. In terms of matrices, the p-curvature χ_p corresponds to the p-th iterate of the sequence of matrices $(\chi_i)_{i \geq 1}$ defined by $\chi_1 = A_p$ and, for $i > 1$, $\chi_{i+1} = \frac{d}{dx}\chi_i - A_p\,\chi_i$, so that it can be effectively computed (see [21, 11] or [25, §13]). For a fast algorithm and complexity analyses, we refer to the recent work [10].

The following *Grothendieck-Katz p-curvature conjecture* ([21, Conj. 9.2 & 10.1]) links the reductions modulo p of the Lie algebra $\mathfrak{g}^k$ and the p-curvature of the reduction modulo p of the differential system/module.

Conjecture 4.1. *The* k*-Lie algebra* $\mathfrak{g}^k$ *is the smallest (algebraic) Lie subalgebra of* $\mathfrak{gl}_n(k)$ *whose reduction modulo* p *contains the* p*-curvature for almost all* p.

One inclusion of the conjecture, namely, the fact that the reduction modulo p of $\mathfrak{g}^k$ contains the p-curvature for all but finitely many primes p, has been proved (see [21, Prop. 9.3]). We refer to [21] for more details.

Let $\mathcal{M} \otimes \mathcal{M}^\star = \bigoplus_{i=1}^r \mathcal{W}_i$ be a maximal decomposition given by a gauge transformation $T \in \mathrm{GL}_{n^2}(k)$ (see Subsection 2.2) so that the $\mathrm{Mat}(T_{\bullet j})$'s provide bases of the submodules $\mathcal{W}_i$. We can then obtain a guess $\mathfrak{g}^s$ for the k-Lie algebra $\mathfrak{g}^k$ by using the following procedure:

ModularSelection

① Choose a prime number p such that A can be reduced modulo p and $\det(T)$ does not vanish modulo p. Reducing the maximal decomposition $\bigoplus_{i=1}^r \mathcal{W}_i$ modulo p we get a decomposition $\bigoplus_{i=1}^r \mathcal{W}_{i,p}$ which is given by the reduction T_p of T modulo p;

② Compute the p-curvature χ_p of $[A_p]$;

③ Compute $T_p^{-1}\,\mathrm{Vect}(\chi_p)$ and let $\mathcal{S}$ be the set containing the indices of its non-zero entries which correspond to the columns of T_p involved in the writing of $\mathrm{Vect}(\chi_p)$;

④ Return the Lie algebra generated by the $\mathrm{Mat}(T_{\bullet j})$'s for $j \in \mathcal{S}$, which form then a basis of the submodule of the maximal decomposition $\bigoplus_{i=1}^r \mathcal{W}_i$ whose reduction modulo p contains χ_p.

This method yields a submodule $\mathfrak{g}^s$ of $\mathcal{M} \otimes \mathcal{M}^\star$ which according to the above Grothendieck-Katz conjecture 4.1 can be used as a guess for the k-Lie algebra $\mathfrak{g}^k$. However, ModularSelection may select either a bigger or a smaller submodule of $\mathcal{M} \otimes \mathcal{M}^\star$ than $\mathfrak{g}^k$ (see explanations in Section 6). The next section will use the notion of *reduced form* to check whether or not our guess is correct. In practice, we can (and will) perform the above (fast) modular guessing for several prime numbers in order to refine our guess.

5. VALIDATION OF THE CANDIDATE

In this section, we check whether the guessed Lie algebra $\mathfrak{g}^s$ is the desired k-Lie algebra $\mathfrak{g}^k$ from Proposition 2.1.

5.1 Reduced Form and conjugation problem

Let $\mathcal{M}$ be a differential module and $[A]$, $A \in \mathbb{M}_n(k)$, an associated linear differential system. We denote by V the $\mathbb{C}$-vector space of solutions of $\mathcal{M}$ in a Picard-Vessiot extension K of k, G the differential Galois group of $\mathcal{M}$, and $\mathfrak{g}$ the Lie algebra of G. Let $N_1, \ldots, N_d \in \mathbb{M}_n(\mathbb{C})$ denote a basis of $\mathfrak{g}$.

One can associate another Lie algebra to $[A]$ by considering a *Wei-Norman decomposition* [2] of the matrix A, namely, $A = \sum_{i=1}^m \alpha_i\, A_i$ where $\alpha_1, \ldots, \alpha_m$ is a basis of the $\mathbb{C}$-vector space generated by the entries of A, and $A_i \in \mathbb{M}_n(\mathbb{C})$. We then define $\mathrm{Lie}(A)$ as the smallest algebraic Lie algebra containing the matrices A_i. The Lie algebra $\mathfrak{g}$ is always contained in $\mathrm{Lie}(A)$, [25, Prop. 1.31], hence $\mathfrak{g} \subset \mathrm{Lie}(P[A])$ for any matrix $P \in \mathrm{GL}_n(\overline{k})$. The *reduced form* corresponds to the case where we have $\mathrm{Lie}(A) = \mathfrak{g}$.

Definition 5.1. *Let $[A]$ with $A \in \mathbb{M}_n(k)$ be a linear differential system. A matrix $B \in \mathbb{M}_n(\overline{k})$ is a* reduced form *of $[A]$ if $B \in \overline{k} \otimes \mathfrak{g}$ and there exists $P \in \mathrm{GL}_n(\overline{k})$ such that $B = P[A]$.*

The linear differential system $[A]$ is thus in reduced form iff there exist $f_1, \dots, f_d$ in $\overline{k}$ such that $A = f_1 N_1 + \cdots + f_d N_d$. The following result due to Kolchin and Kovacic proves the existence of a reduced form: see [25, Prop. 1.31 & Cor. 1.32] and [2, Prop. 3 & Cor. 4].

Theorem 5.1. *Let $[A]$ with $A \in \mathbb{M}_n(k)$ be a linear differential system. There exists a matrix $P \in \mathrm{GL}_n(\overline{k})$ such that $[P[A]]$ is in reduced form.*

A matrix P as in Theorem 5.1 is called a *reduction matrix* for $[A]$. We shall now recall a useful result of [2] concerning invariants and reduced forms.

Definition 5.2. *A* (tensor) construction $\mathrm{Const}(V)$ *on the G-module V is a vector space obtained from V by finite iterations of tensor products $\otimes$, direct sums $\oplus$, taking the dual $\star$, symmetric powers Sym^m, and exterior powers Λ^r. To a constructor* Const *corresponds naturally a "Lie algebra" constructor $\mathfrak{Const}$. An* invariant of $[A]$ *is a rational solution of a linear differential system $[\mathfrak{Const}(A)]$.*

Let $P \in \mathrm{GL}_n(k_0)$ with $k \subseteq k_0 \subset \overline{k}$. A change of variables $\mathbf{y} = P\,\mathbf{z}$ in $[A]$ induces an action on the elements of constructions. If $\mathbf{f}$ is an invariant of $\mathcal{M}$ given as a rational solution of $[\mathfrak{Const}(A)]$, then we say that P *sends* $\mathbf{f}$ *to* $\mathbf{g}$ if $\mathbf{f} = \mathrm{Const}(P)\,\mathbf{g}$ ($\mathbf{g}$ is then a rational solution of $[\mathfrak{Const}(P[A])]$). Theorems 1 and 2 of [2] show that when a system is in reduced form, all its invariants have *constant* coefficients in $\mathbb{C}$ and we have:

Lemma 5.1 ([2], Thm. 3). *Let $[A]$ with $A \in \mathbb{M}_n(k)$ be a linear differential system. For any ordinary point $x_0 \in \mathbb{C}$ of $[A]$, there exists a reduction matrix $P \in \mathrm{GL}_n(\overline{k})$ for $[A]$ that sends every invariant $\mathbf{f}$ of $[A]$ to its evaluation at x_0, namely $\mathrm{Const}(P)\,\mathbf{f} = \mathbf{f}(x_0)$.*

In Section 4, we found a candidate $\mathfrak{g}^s$ for the Lie algebra $\mathfrak{g}^k$ as a submodule of $\mathcal{M} \otimes \mathcal{M}^\star$. Let $F \in \mathbb{M}_{n^2}(k)$ denote the element of $\mathcal{E}(\mathcal{A})$ from which we obtained this maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$; let $T \in \mathrm{GL}_{n^2}(k)$ denote the gauge transformation which provides the maximal decomposition, namely, $T^{-1}\,F\,T = J$ is the Jordan form of F. Note that $J \in \mathbb{M}_{n^2}(\mathbb{C})$ and T is formed by generalized eigenvectors of F so that it can be chosen as a polynomial matrix.

Following the terminology in [18], we introduce the notion of *conjugated Lie algebras.*

Definition 5.3. *Two Lie subalgebras $\mathfrak{g}_1$ and $\mathfrak{g}_2$ of $\mathfrak{gl}_n(\overline{k})$ are said to be* conjugated (over $\overline{k}$) *if there exists $P \in \mathrm{GL}_n(\overline{k})$ such that $\mathfrak{g}_2 = P^{-1}\,\mathfrak{g}_1\,P$. Such a matrix P is then a* conjugation matrix *between $\mathfrak{g}_1$ and $\mathfrak{g}_2$.*

Theorem 5.2. *Let $M_i \triangleq \mathrm{Mat}(T_{\bullet i})$, $i = 1, \dots, d$, be a basis of the Lie algebra $\mathfrak{g}^s$ and let x_0 be an ordinary point of $[A]$ such that $\det(T(x_0)) \neq 0$. Let $\mathfrak{g}^t$ denote the Lie subalgebra of $\mathfrak{gl}_n(\mathbb{C})$ with basis $M_1(x_0), \dots, M_d(x_0)$. If $\mathfrak{g}^s = \mathfrak{g}^k$, then there exists a gauge transformation $P \in \mathrm{GL}_n(\overline{k})$ that is a conjugation matrix between $\mathfrak{g}^s$ and $\mathfrak{g}^t$ and for which $\mathrm{Lie}(P[A]) = \mathfrak{g}^t$.*

Proof. The matrix $F \in \mathcal{E}(\mathcal{A})$ is an invariant of $[A]$ so that Lemma 5.1 implies that there exists a reduction matrix P that sends F to its evaluation $F(x_0)$. Now we have $T(x_0)^{-1}\,F(x_0)\,T(x_0) = J$ so that if we perform the change of variables defined by P in $\mathcal{M}$, a new basis of $\mathfrak{g}^s$ will be given by the $M_i(x_0) \triangleq \mathrm{Mat}(T(x_0)_{\bullet i})$. On the other hand, M_i belongs to the construction $\mathcal{M} \otimes \mathcal{M}^\star$ so that after a change of variables given by P, M_i is transformed to $P^{-1}\,M_i\,P$. Consequently, P is a conjugation matrix between $\mathfrak{g}^s$ and $\mathfrak{g}^t$. □

If $\mathfrak{g}^s = \mathfrak{g}^k$, Theorem 5.2 suggests to find a reduction matrix among conjugation matrices between the "target" Lie algebra $\mathfrak{g}^t$ with basis $M_i(x_0)$ and the "source" Lie algebra $\mathfrak{g}^s$ with basis M_i. Conversely, if we find a conjugation matrix P between $\mathfrak{g}^s$ and $\mathfrak{g}^t$ such that $\mathrm{Lie}(P[A]) = \mathfrak{g}^t$, then $\mathfrak{g} \subseteq \mathfrak{g}^t$ so that $\mathfrak{g}^k \subseteq \mathfrak{g}^s$.

5.2 Step 1: computing conjugation matrices

Let $\mathcal{M}$ be an absolutely irreducible module and recall that if we assume, w.l.o.g., that $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C})$, then $\mathfrak{g}^t$ and $\mathfrak{g}^s$ are semisimple Lie algebras (otherwise, the guess $\mathfrak{g}^s$ is wrong). See Remark 2.2.

Definition 5.4. *Let $\mathfrak{g}$ be a semisimple Lie algebra of dimension d and rank r. Let $\mathfrak{h}$ be a Cartan subalgebra of $\mathfrak{g}$, Φ a root system associated with $\mathfrak{h}$ and $\Delta = \{\alpha_1, \dots, \alpha_r\}$ a simple system of Φ. Then a* set of canonical generators *of $\mathfrak{g}$ is a set of $3\,r$ non-zero matrices $H_1, \dots, H_r$, $X_1, \dots, X_r$, $Y_1, \dots, Y_r$ such that, for $i = 1, \dots, r$, $H_i \in \mathfrak{h}$, $X_i \in L_{\alpha_i}$, the root space associated with α_i and $Y_i \in L_{-\alpha_i}$ and which satisfies, for all $i, j \in \{1, \dots, r\}$, the relations*

$$\left\{ \begin{array}{l} [H_i, H_j] = 0, \quad [X_i, Y_j] = \delta_{i,j}\,H_i, \\ [H_i, X_j] = c_{j,i}\,X_j, \quad [H_i, Y_j] = -c_{j,i}\,Y_j, \quad c_{i,i} = 2. \end{array} \right. \tag{8}$$

where $\delta_{i,j} = 1$ if $i = j$ and 0 otherwise.
The matrix $C = (c_{i,j})_{1 \le i,j \le r}$ is called a Cartan matrix *of $\mathfrak{g}$.*

The sets of canonical generators (and their completion into *Chevalley bases*) are central objects in the study of semisimple Lie algebras. We refer to [20] and [14] for more details. Moreover algorithms for computing sets of canonical generators and Chevalley bases are given in [14].

Conjugation matrices between $\mathfrak{g}^t$ and $\mathfrak{g}^s$ can be computed using the following[2] procedure:

ConjugationMatrices (between $\mathfrak{g}^s$ and $\mathfrak{g}^t$)

① Compute canonical generators $\{H_i^t, X_i^t, Y_i^t\}_{i=1,\dots,r}$ of $\mathfrak{g}^t$;

② Compute generators $\tilde{H}_i^s$ of a split Cartan subalgebra $\mathfrak{h}^s$ of $\mathfrak{g}^s$ such that we have $\chi(\tilde{H}_i^s) = \chi(H_i^t)$, $i = 1, \dots, r$, where $\chi(M)$ denotes the characteristic polynomial of a matrix M. This can be done by taking an ansatz $\tilde{H}_i^s = \sum_{j=1}^{d} a_{i,j}\,M_j$ in $\mathfrak{g}^s$ and solving the algebraic equations in the $a_{i,j}$'s provided by the relation $\chi(\tilde{H}_i^s) = \chi(H_i^t)$;

③ From $\mathfrak{h}^s$ generated by the $\tilde{H}_i^s$, compute a set of canonical generators $\{H_i^s, X_i^s, Y_i^s\}_{i=1,\dots,r}$ of $\mathfrak{g}^s$ having the same Cartan matrix as $\{H_i^t, X_i^t, Y_i^t\}_{i=1,\dots,r}$;

④ Compute the matrices $P \in \mathrm{GL}_n(\overline{k})$ such that for $i = 1, \dots, r$, $P\,X_i^t = X_i^s\,P$ and $P\,Y_i^t = Y_i^s\,P$. This amounts

[2] This is probably known but we have not found a reference.

to solving a linear system of $2\,r\,n^2$ equations for the n^2 unknown entries of P in $\overline{k}$.

Proposition 5.1. ConjugationMatrices *computes the conjugation matrices between the semisimple Lie algebras $\mathfrak{g}^t$ and $\mathfrak{g}^s$. If $\mathfrak{g}^t$ is (or contains) a representation of $\mathfrak{g}$ in $\mathfrak{gl}_n(\mathbb{C})$, e.g., if we have made the correct guess for $\mathfrak{g}^s$, then all the conjugation matrices found are of the form $P = c\,\tilde{P}$, with $\tilde{P} \in \mathrm{GL}_n(\overline{k})$ given and c an arbitrary element of $\overline{k}$.*

Proof. The correctness of ConjugationMatrices follows essentially from material in the book of W. de Graaf [14], in particular, Cor. 5.11.5 (see also [20]). The split Cartan subalgebra $\mathfrak{h}^s$ in Step ② exists because we know that $\mathfrak{g}^t$ and $\mathfrak{g}^s$ are conjugated (see Theorem 5.2). In Step ②, the matrices H_i^t (resp. $\tilde{H}_i^s$) are simultaneously diagonalizable ([20, Cor. 15.3, p.80]) so that there exists $P \in \mathrm{GL}_n(\overline{k})$ such that $P\,H_i^t = \tilde{H}_i^s\,P$, for $i = 1, \ldots, r$. The feasability of Step ③ is ensured by the fact that we know from Theorem 5.2 that the Lie algebras $\mathfrak{g}^t$ and $\mathfrak{g}^s$ are conjugated and a conjugation matrix sends a set of canonical generators of $\mathfrak{g}^t$ to a set of canonical generators of $\mathfrak{g}^s$ having the same Cartan matrix. In Step ④, the conjugation of the H_i^t and H_i^s is automatic because of the second relation of (8).
If P and $\tilde{P}$ are two conjugation matrices in Step ④, then $P\,\tilde{P}^{-1} \in \mathrm{GL}_n(\overline{k})$ commutes with all matrices in $\mathfrak{g}^t \otimes \overline{k}$ which contains $\mathfrak{g} \otimes \overline{k}$. As $\mathfrak{g}$ acts irreducibly on V (Remark 2.2), the only such matrices are scalar multiples of the identity (Schur's lemma) so $P = c\,\tilde{P}$ with $c \in \overline{k}$. □

In the procedure CheckGuess below, we say that "ConjugationMatrices fails" if the set of the matrices P computed in Step ④ is not of the form $P = c\,\tilde{P}$ given in Proposition 5.1. This implies that our guess $\mathfrak{g}^s$ was not correct.

5.3 Step 2: computing a reduction matrix

In the previous subsection, we found the conjugation matrices between the Lie algebras $\mathfrak{g}^t$ and $\mathfrak{g}^s$. If our guess $\mathfrak{g}^s$ equals $\mathfrak{g}^k$, then we know that among these conjugation matrices there exists a gauge transformation P such that $\mathrm{Lie}(P[A]) = \mathfrak{g}^t$. The last step then consists in finding this P which, if it succeeds, will partially validate our choice for the Lie algebra $\mathfrak{g}^s$ (i.e., $\mathfrak{g}^s = \mathfrak{g}^k$ or $\mathfrak{g}^k \subset \mathfrak{g}^s$). Let $P = c\,\tilde{P}$ be as in Proposition 5.1 and let $(N_i^t)_{i=1,\ldots,d}$ be a Chevalley basis of $\mathfrak{g}^t$. See [14] for an algorithm to complete our set of canonical generators of $\mathfrak{g}^t$ into a Chevalley basis. If $\mathrm{Lie}(P[A]) = \mathfrak{g}^t$, then there exist $c \in \overline{k}$ and $f_i \in \overline{k}$ such that $P[A] = \sum_{i=1}^d f_i\,N_i^t$. The latter relation then yields

$$\tilde{P}^{-1}\,A\,\tilde{P} - \frac{c'}{c}\,I_n - \tilde{P}^{-1}\,\tilde{P}' = \sum_{i=1}^{d} f_i\,N_i^t. \tag{9}$$

Taking the trace Tr(.) of the matrices in (9) we obtain

$$\mathrm{Tr}(A) - n\,\frac{c'}{c} - \frac{\det(\tilde{P})'}{\det(\tilde{P})} = \sum_{i=1}^{d} f_i\,\mathrm{Tr}(N_i^t).$$

As we can assume, w.l.o.g., that $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C})$ (see Remark 2.2), we have $\mathrm{Tr}(N_i^t) = 0$ and $\mathrm{Tr}(A) = w'/w$, for some $w \in k$, so that we get $c = \left(w/\det(\tilde{P})\right)^{1/n}$. The following procedure checks if there exists a gauge transformation $P = c\,\tilde{P}$ such that $\mathrm{Lie}(P[A]) = \mathfrak{g}^t$:

```
PartialReductionMatrix
① Let $c = \left(w/\det(\tilde{P})\right)^{1/n}$ and set $P = c\,\tilde{P}$;
② Check if there exist $f_1, \ldots, f_d$ in $\overline{k}$ such that $P[A] = \sum_{i=1}^d f_i\,N_i^t$. If it succeeds, Return $P$, Else Return "Fail".
```

6. ALGORITHM AND IMPLEMENTATION

6.1 Full algorithm

Let $A \in \mathbb{M}_n(k)$ be such that $[A]$ is an absolutely irreducible linear differential system. Let G be its differential Galois group and $\mathfrak{g}$ be the Lie algebra of G. We first design an algorithm which, given a submodule $\mathfrak{g}^s$ of $\mathcal{M} \otimes \mathcal{M}^\star$, returns "Yes" when $\mathfrak{g}^s = \mathfrak{g}^k$ (or $\mathfrak{g}^s \supset \mathfrak{g}^k$) and "Fail" if $\mathfrak{g}^k \not\subseteq \mathfrak{g}^s$.

```
CheckGuess
① Given a basis $M_1, \ldots, M_d$ of $\mathfrak{g}^s$, pick an ordinary point
  $x_0$ and let $\mathfrak{g}^t$ be generated by $M_1(x_0), \ldots, M_d(x_0)$;
② Apply ConjugationMatrices to $\mathfrak{g}^s$ and $\mathfrak{g}^t$.
  If it fails, Return "Fail";
③ Complete the set of canonical generators of $\mathfrak{g}^t$ into a
  Chevalley basis $(N_i^t)_{i=1,\ldots,d}$ of $\mathfrak{g}^t$;
④ Apply PartialReductionMatrix.
  If it fails, Return "Fail"; Else Return "Yes".
```

Correctness of CheckGuess follows from Theorem 5.2 and Proposition 5.1: if it returns "Yes" then $\mathfrak{g}^k \subset \mathfrak{g}^s$; it surely returns "Yes" when $\mathfrak{g}^s = \mathfrak{g}^k$. This provides a first algorithm for computing $\mathfrak{g}$. Apply CheckGuess to each (isomorphism class of) submodule of $\mathcal{M} \otimes \mathcal{M}^\star$: $\mathfrak{g}^k$ is the only one for which CheckGuess replies "Yes" while it replies "Fail" to each of its proper submodules.
We now give our (better) full algorithm[3] for computing $\mathfrak{g}$.

```
Algorithm 1 (Computing the Lie Algebra $\mathfrak{g}$).
① Compute a maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$.
  Let $\mathcal{G} := \{0\}$.
② Apply ModularSelection to get a guess for $\mathfrak{g}^s$.
  Let $\mathcal{G} := \mathcal{G} + \mathfrak{g}^s$.
③ Apply CheckGuess to $\mathcal{G}$. If it fails, pick next prime p,
  go to Step ②. Repeat until CheckGuess replies "Yes".
④ Apply CheckGuess to all (finitely many isomorphism
  classes of) proper submodules of $\mathcal{G}$.
  If the answer is "Fail" for all of them, then $\mathfrak{g}^k = \mathcal{G}$.
  Otherwise, $\mathfrak{g}^k$ is the smallest submodule for which the
  answer is "Yes".
```

In Step ②, Algorithm 1 applies calculations modulo a prime number p to make a guess $\mathfrak{g}^s$ for the Lie algebra $\mathfrak{g}^k$ based on the Grothendieck-Katz conjecture 4.1. This guess may, for some primes, pick a $\mathfrak{g}^s$ which is "too small" (e.g., the p-curvature may be accidentally zero); this is a "Fail" case of Step ③. If we choose *successive* primes, the Grothendieck-Katz conjecture 4.1 implies that, after a finite number of primes, the sum $\mathcal{G}$ of guessed modules will contain $\mathfrak{g}^k$.
For a finite number of primes, the guess in Step ② may pick a "bigger" $\mathfrak{g}^s$, i.e. $\mathfrak{g}^s \supsetneq \mathfrak{g}^k$ and this will not be tested by CheckGuess, hence the necessity of Step ④. This situation may also occur when we have two isomorphic $L \oplus L$ in the maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$: ModularSelec-

[3] Note that we get a reduced form of $[A]$ as a byproduct.

TION may select the sum when only one summand appears in the true $\mathfrak{g}^k$, hence Step ④.

REMARK 6.1. *In Algorithm 1, Step ② is cheap. It often fastens calculations to apply Step ② to several p and deduce from this a "reasonable" guess before applying the next step.*

Note that each step of Algorithm 1 can be performed in an arithmetic complexity which is polynomial in n except (maybe) in Step 2 of the procedure CONJUGATIONMATRICES where we need to solve algebraic systems. This makes a significant difference compared to the exponential (several levels) complexity obtained in [16] for the computation of the differential Galois group G.

6.2 Implementation and example

We have a prototype implementation of Algorithm 1 in MAPLE. We use the package INTEGRABLECONNECTIONS ([6]) based on ISOLDE ([8]) for computing the maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$ and the package LIEALGEBRAS for computing a set of canonical generators (and a Chevalley basis) of $\mathfrak{g}^t$. The other steps are based on linear algebra calculations and solving linear and algebraic systems. We have applied our implementation to many examples up to $n = 7$. It turns out that in practice the most costly step is the decomposition of $\mathrm{End}(\mathcal{M})$. For lack of space, we only give a small example here.

EXAMPLE 6.1. *We consider the absolutely irreducible differential module $\mathcal{M}$ associated via a choice of basis with $[A]$ given by:*

$$A := \begin{bmatrix} \frac{x-1}{x} & x & -1 \\ -x^3+1 & 0 & -1 \\ \frac{x-1}{x}+x^2 & x+1 & -1 \end{bmatrix}.$$

The Lie algebra $\mathrm{Lie}(A)$ *of the matrix A is of dimension 9. Computing a maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$, we find that $\mathcal{M} \otimes \mathcal{M}^\star = \mathbb{1}_k \oplus \mathcal{W}_1 \oplus \mathcal{W}_2$ where $\mathcal{W}_1$ (resp. $\mathcal{W}_2$) is of dimension 3 (resp. 5). Computing the p-curvature of $[A]$ for a random prime p, we find that a candidate for the Lie algebra $\mathfrak{g}^s$ is the irreducible differential submodule $\mathcal{W}_1$ of $\mathcal{M} \otimes \mathcal{M}^\star$ which admits the basis M_1, M_2, M_3 given by:*

$$\begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ -x^2-1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -x^2 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ -x^2-1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

The point $x_0 = 1$ is an ordinary point for $[A]$ and a set of canonical generators H^t, X^t, Y^t for the Lie algebra $\mathfrak{g}^t$ generated by $M_1(x_0), M_2(x_0), M_3(x_0)$ is given by:

$$\begin{bmatrix} 2i & 0 & -2i \\ 0 & 0 & 0 \\ 4i & 0 & -2i \end{bmatrix}, \begin{bmatrix} 0 & -i & 0 \\ 1+i & 0 & -1 \\ 0 & 1-i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i & 0 \\ -1+i & 0 & 1 \\ 0 & -1-i & 0 \end{bmatrix}.$$

Computing an "aligned" set of canonical generators H^s, X^s, Y^s for $\mathfrak{g}^s$, we find:

$$\begin{bmatrix} \frac{-2i}{x} & 0 & \frac{2i}{x} \\ 0 & 0 & 0 \\ \frac{-2i\left(x^2+1\right)}{x} & 0 & \frac{2i}{x} \end{bmatrix}, \begin{bmatrix} 0 & \frac{i}{x} & 0 \\ -ix+1 & 0 & -1 \\ 0 & \frac{i+x}{x} & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{i}{x} & 0 \\ -ix-1 & 0 & 1 \\ 0 & \frac{i-x}{x} & 0 \end{bmatrix}.$$

The conjugation matrices $P \in \mathrm{GL}_n(k)$ such that we have simultaneously $X^t P = P X^s$ and $Y^t P = P Y^s$ are then given by the matrices $P = c\,\tilde{P}$, where $c \in \overline{k}$ and

$$\tilde{P} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ x+1 & 0 & -x \end{bmatrix}.$$

Next, we find $c = a/x$ for an arbitrary constant $a \in \mathbb{C}^*$ so that $P = (a/x)\,\tilde{P}$ and $f_1,\ f_2,\ f_3 \in \overline{k}$ given by

$$\left\{ f_1 = \frac{i}{2x},\ f_2 = -\frac{i}{2}\left(x^2+i\right),\ f_3 = \frac{i}{2}\left(-x^2+i\right) \right\},$$

satisfy $P[A] = f_1\,H^t + f_2\,X^t + f_3\,Y^t$.

We can then conclude that the Lie algebra $\mathfrak{g}$ viewed as a Lie subalgebra of $\mathfrak{gl}_3(\mathbb{C})$ admits the basis H^t, X^t, Y^t and $R = P[A]$ is in reduced form where:

$$P = \begin{bmatrix} \frac{a}{x} & 0 & 0 \\ 0 & -a & 0 \\ \frac{(x+1)\,a}{x} & 0 & -a \end{bmatrix}, \quad R = \begin{bmatrix} -x & -x^2 & x \\ x^2+1 & 0 & -1 \\ -2x & -x^2+1 & x \end{bmatrix}.$$

7. CONCLUSION

We have provided an algorithm for computing the Lie algebra of the differential Galois group of an absolutely irreducible differential system. The case of a completely reducible system is not handled here only for lack of space but can be tackled by a slightly modified algorithm. It will appear in a future paper. Finally, the case of a reducible system is treated in the forthcoming paper [15].

8. REFERENCES

[1] A. Aparicio Monforte, M. A. Barkatou, S. Simon, and J.-A. Weil. Formal first integrals along solutions of differential systems I. In *ISSAC'11*, pages 19–26. ACM Press, 2011.

[2] A. Aparicio Monforte, E. Compoint, and J.-A. Weil. A characterization of reduced forms of linear differential systems. *Journal of Pure and Applied Algebra*, 217(8):1504–1516, 2013.

[3] A. Aparicio-Monforte, T. Dreyfus, and J.-A. Weil. Liouville integrability: an effective Morales–Ramis–Simó theorem. *J. Symbolic Comput.*, 74:537 – 560, 2016.

[4] M. A. Barkatou. On rational solutions of systems of linear differential equations. *J. Symbolic Comput.*, 28:547–567, 1999.

[5] M. A. Barkatou. Factoring systems of linear functional equations using eigenrings. *Latest Advances in Symbolic Algorithms, Proc. of the Waterloo Workshop, Ontario, Canada (10-12/04/06)*, I. Kotsireas and E. Zima (Eds.), World Scientific:22–42, 2007.

[6] M. A. Barkatou, T. Cluzeau, C. El Bacha, and J.-A. Weil. INTEGRABLECONNECTIONS, http://www.unilim.fr/pages_perso/thomas.cluzeau/PDS.html.

[7] M. A. Barkatou, T. Cluzeau, C. El Bacha, and J.-A. Weil. Computing closed-form solutions of integrable connections. In *ISSAC'12*, pages 43–50. ACM, 2012.

[8] M. A. Barkatou and E. Pfluegel. ISOLDE (Integration of Systems of Ordinary Linear Differential Equations) project, http://isolde.sourceforge.net/.

[9] M. A. Barkatou and E. Pfluegel. On the equivalence problem of linear differential systems and its application for factoring completely reducible systems. In *ISSAC'98*, pages 268–275. ACM Press, 1998.

[10] A. Bostan, X. Caruso, and É. Schost. A fast algorithm for computing the p-curvature. In *ISSAC'15*, pages 69–76. ACM Press, 2015.

[11] T. Cluzeau. Factorization of differential systems in characteristic p. In *ISSAC'03*, pages 58–65. ACM Press, 2003.

[12] E. Compoint and M. F. Singer. Computing Galois groups of completely reducible differential equations. *J. Symbolic Comput.*, 28(4-5):473–494, 1999.

[13] E. Compoint and J.-A. Weil. Absolute reducibility of differential operators and Galois groups. *J. Algebra*, 275(1):77–105, 2004.

[14] W. de Graaf. Lie Algebras: Theory and Algorithms. volume 56 of *North-Holland Mathematical Library*. Elsevier, 2000.

[15] T. Dreyfus and J.-A. Weil. Computing the Lie algebra of the differential Galois group: the reducible case. Preprint, February 2016.

[16] R. Feng. Hrushovski's algorithm for computing the Galois group of a linear differential equation. *Advances in Applied Mathematics*, 65:1 – 37, 2015.

[17] M. A. Graham. *Kronecker Products and Matrix Calculus with Applications*. E. Horwood Series in Math. and its Appl. Wiley & Sons, 1981.

[18] J. A. Grochow. Matrix Lie algebra isomorphism. In *IEEE Conference on Computational Complexity (CCC12)*, pages 203–213, 2012.

[19] E. Hrushovski. Computing the Galois group of a linear differential equation. In *Differential Galois theory (Bedlewo, 2001)*, volume 58 of *Banach Center Publ.*, pages 97–138. Polish Acad. Sci., Warsaw, 2002.

[20] J. E. Humphreys. *Introduction to Lie Algebras and Representation Theory*, volume 9 of *Graduate Texts in Mathematics*. Springer-Verlag, 1972.

[21] N. M. Katz. A conjecture in the arithmetic theory of differential equations. *Bull. Soc. Math. France*, 110(2):203–239, 1982.

[22] K. A. Nguyen and M. van der Put. Solving linear differential equations. *Journal of Pure Appl. Math.*, Q. 6, no. 1, Special Issue: In honor of John Tate. Part 2:173–208, 2010.

[23] M. F. Singer. Testing reducibility of linear differential operators: a group theoretic perspective. *Appl. Alg. in Engrg. Comm. Comput.*, 7(2):77–104, 1996.

[24] J. van der Hoeven. Around the numeric-symbolic computation of differential Galois groups. *J. Symbolic Comput.*, 42(1-2):236–264, 2007.

[25] M. van der Put and M. F. Singer. *Galois theory of linear differential equations*, volume 328 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 2003.