Computing the Lie algebra of the differential Galois group of a linear differential system

M. A. Barkatou

University of Limoges ; CNRS ; XLIM (France)

In collaboration with Thomas Cluzeau, J.-A. Weil and L. Di Vizio (CNRS, UVSQ)

Colloque SMM(e, r) de mathématiques,
22-24 Septembre 2016,Kénitra, Maroc

Motivation

$\diamond$ $k = \mathbb{C}(z)$ (for actual computations $\mathbb{C}$ is replaced by a computable subfield of $\overline{\mathbb{Q}}$), $A \in \mathbb{M}_n(k)$, $\mathbf{y}$ vector of unknown functions, $' = \frac{d}{dz}$

Linear differential system $[A] : \mathbf{y}' = A\,\mathbf{y}$

$\diamond$ Important object for studying $[A]$: its differential Galois group G

$\rightarrow$ G measures everything that algebra can see about the solutions

$\diamond$ Direct problem in diff. Galois theory: given $[A]$, compute G

- Several theoretical algorithms: *Compoint-Singer'99*, *Hrushovski'02* and *Feng'15*, *van der Put-Singer'03*, *van der Hoeven'07*
- None of them are either practical or implemented

Objective

Philosophy of our work (see also *Nguyen-van der Put'10*)

$\rightarrow$ For a large class of problems, computing the Lie algebra $\mathfrak{g}$ of the linear algebraic group G is enough

$\diamond$ For the computation of $\mathfrak{g}$, not much is known (*Aparicio's PhD thesis'10*, *Aparicio-Compoint-Weil'13*)

Goal of my talk

Provide a full algorithm for computing the Lie algebra $\mathfrak{g}$ of G in the case of an absolutely irreducible system

- Completely reducible case quite similar (only small modif.)
- Reducible case studied recently in a work of *Dreyfus-Weil*

General idea of our algorithm

◇ Let $\mathcal{M}$ be the differential module associated with system $[A]$.

◇ Tannakian correspondence : $\mathfrak{g}$ can be viewed as a submodule $\mathcal{W}$ of $\mathrm{End}(\mathcal{M}) \cong \mathcal{M} \otimes_k \mathcal{M}^\star$.

◇ We proceed in four main steps :

1. Determine the submodules of $\mathrm{End}(\mathcal{M})$.
2. Find a candidate for the submodule $\mathcal{W}$ (modular approach based on Grothendieck-Katz conjecture):
   - Choose a prime p, compute the p-curvature χ_p, and identify the smallest submodule whose reduction modulo p contains χ_p.
   - This provides a guess for $\mathcal{W}$ given by a basis $M_1, \ldots, M_d$ of matrices in $\mathfrak{gl}_n(\mathbb{C}(z))$.
3. Remark that $\mathfrak{g}$ can also be directly read off from a reduced form of $[A]$: Computing a reduction matrix amounts to computing a conjugation matrix between two semisimple Lie subalgebras of $\mathfrak{gl}_n(\mathbb{C}(z))$ respectively generated by the M_i and their evaluations $M_i(z_0)$ at some ordinary point z_0 of $[A]$.
4. Find a reduction matrix among the conjugation matrices.

◇ If our guess for $\mathcal{W}$ is not correct, then restart with another prime.

I

Differential systems/modules/Galois group and Lie algebra

Differential Fields

A *differential field* (K, δ) is a field K with a map (*derivation*) $\delta : \mathrm{K} \to \mathrm{K}$, satisfying
$\delta(a+b) = \delta(a) + \delta(b), \quad \delta(ab) = \delta(a)b + a\delta(b)$ for all $a, b \in \mathrm{K}$.
Notation: $\delta(a) = a'$

The *field of constants* of K:

$$\mathcal{C}_{\mathrm{K}} = \{a \in \mathrm{K} | a' = 0\}$$

Examples:

- $(\mathbb{C}(z), \delta = \frac{d}{dz}) =$ field of rational functions
- $(\mathbb{C}(z, e^z), \delta = \frac{d}{dz})$
- $\mathbb{C}[[z]] =$ ring of formal power series

  $(\mathbb{C}((z)), \frac{d}{dz}) =$ quotient field of $\mathbb{C}[[z]] = \mathbb{C}[[z]][\frac{1}{z}]$
- $(\mathcal{M}(\Omega), \frac{d}{dz}) =$ field of fncs merom on Ω open, connected $\subset \mathbb{C}$

Linear Differential Equations over $(\mathrm{K}, ')$

Three equivalent forms:

- a scalarlinear differential equation of order n:

$$D(y) = a_n y^{(n)} + \ldots + a_1 y' + a_0 y = 0, \ a_j \in \mathrm{K}$$

- a differential system of dimension n:

$$\mathbf{y}' = A\mathbf{y}, \ A \in M_n(\mathrm{K})$$

- a differential module of dimension n:

an n dim. K-vector space V with an additive map $\partial : V \to V$ satisfying

$$\partial(\alpha v) = \alpha' v + \alpha \partial(v)$$

for all $\alpha \in \mathrm{K}, v \in V$.

Equivalent Systems

Consider a system $[A] \quad \mathbf{y}' = A\mathbf{y},\ A \in M_n(\mathrm{K})$.

Gauge transformation: $\mathbf{y} = T\mathbf{z},\ T \in \mathrm{G}L_n(\mathrm{K})$, leads to

$$[B] \quad \mathbf{z}' = B\mathbf{z},$$

$$B = T[A] := T^{-1}AT - T^{-1}T'.$$

Systems $[A]$ and $[B]$ are called equivalent (over K).

If $T \in \mathrm{G}L_n(L)$ for some differential field extension L of K then $[A]$ and $[B]$ are called equivalent over L.

Differential module $\leftrightarrow$ Differential system

$\diamond$ Via a choice of basis, a differential module $\mathcal{M}$ is associated with a linear differential system $[A]$ and *vice versa*

$\rightarrow$ If we choose a basis $e_1, \ldots, e_n$ of $(\mathcal{M}, \partial)$ then ∂ is determined by

$$\partial(e_i) \triangleq -\sum_{j=1}^{n} a_{j,i}\, e_j \quad hbox for\ i = 1, \ldots, n.$$

The associated linear differential system $[A]$, is given by the matrix $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathbb{M}_n(k)$

$\diamond$ A change of basis $\mathbf{f}^T = \mathbf{e}^T\, P$ with $P \in \mathrm{GL}_n(\mathrm{K})$ in $\mathcal{M}$, corresponds to a gauge transformation $\mathbf{y} = P\,\mathbf{z}$ in $[A]$, leading to equivalent system $[B]$ with

$$B := P[A] \triangleq P^{-1}\, A\, P - P^{-1} P'$$

Solutions

Consider a differential system of dimension n with coefficients in K:

$$[A]: \quad \mathbf{y}' = A\mathbf{y}, \quad A \in M_n(\mathrm{K})$$

. • We should describe the class of functions in which the solutions are to be found:

• A (rational) solution: a vector $\mathbf{y} \in \mathrm{K}^n$ such that $\mathbf{y}' = A\mathbf{y}$.

• The set $\mathcal{S}_{\mathrm{K}} = \{\mathbf{y} \in \mathrm{K}^n \mid \mathbf{y}' = A\mathbf{y}\}$ is a vector-space of dim $\leq n$ over the field of constants.

• In general, $\dim \mathcal{S}_{\mathrm{K}} < n$. However, there always exists a differential field extension $\mathrm{K} \subset L$ such that over L the solution space has dimension n.

• Fundamental solution matrix of $[A]$: an n by n invertible matrix U (with entries in some extension L of K) satisfying $U' = AU$.

Differential modules

$\diamond$ A differential module $\mathcal{M}$ over k is a finite dimensional vector space over k equipped with an additive map $\partial : \mathcal{M} \to \mathcal{M}$ s.t. $\forall\, f \in k, \forall\, m \in \mathcal{M},\ \partial(f\, m) = f'\, m + f\, \partial(m)$

A differential submodule of $\mathcal{M}$ is then a sub-vector space of $\mathcal{M}$ which is stable under the action of ∂

$\diamond$ A differential module $\mathcal{M}$ is

- irreducible if it has no non-trivial differential submodule
- absolutely irreducible if $\overline{k} \otimes_k \mathcal{M}$ is irreducible
- decomposable if $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2$
- completely reducible if it is a direct sum of *irreducible* modules

$\diamond$ We have $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2 \oplus \cdots \oplus \mathcal{M}_r$, with $\mathcal{M}_i$ indecomposable (& *Krull-Schmidt* thm). It is called a maximal decomposition of $\mathcal{M}$ (Rk: if $\mathcal{M}$ is completely reducible, then the $\mathcal{M}_i$ are irreducible)

Differential module $\leftrightarrow$ Differential system

$\diamond$ Via a choice of basis, a differential module $\mathcal{M}$ is associated with a linear differential system $[A]$ and *vice versa*

$\diamond$ Change of basis in $\mathcal{M} \leftrightarrow$ gauge transfo. $P \in \mathrm{GL}_n(k)$ in $[A]$ leading to equivalent system $[P[A]]$ with $P[A] \triangleq P^{-1}(AP - P')$

$\rightarrow \mathcal{M}$ decomposable: $\exists P,\ P[A] = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ block diagonal

$\diamond\ \mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r \leftrightarrow \exists P,\ P[A] = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}$

Maximal dec. $\leftrightarrow [A_i]$ indec. (Rk: irred. if $\mathcal{M}$ is completely red.)

The differential module $\mathcal{M} \otimes_k \mathcal{M}^\star$

$\diamond$ $\mathcal{M}$ differential module, $[A]$ associated differential system

$\diamond$ Its dual $\mathcal{M}^\star \triangleq \mathrm{Hom}_k(\mathcal{M}, \mathbb{1}_k)$ is associated with $[-A^T]$

$\diamond$ Consider $\mathcal{M} \otimes_k \mathcal{M}^\star$: elements viewed in $\mathbb{M}_n(k)$

$\rightarrow$ $\mathcal{M} \otimes_k \mathcal{M}^\star$ is associated with the matrix differential system

$$F' = [A, F] \triangleq A\,F - F\,A$$

Using the classical Kronecker product of matrices:

$$F' = [A, F] \Longleftrightarrow \mathrm{Vect}(F)' = \left(A \otimes I_n - I_n \otimes A^T\right) \mathrm{Vect}(F),$$

with $\mathrm{Vect}(F) = (F_{1\bullet} \ \ldots \ F_{n\bullet})^T \in k^{n^2}$ and $F_{i\bullet}$ the i-th row of F

$\diamond$ $\mathcal{M}$ completely reducible $\Rightarrow$ $\mathcal{M} \otimes_k \mathcal{M}^\star$ is completely reducible

The differential Galois group

$\diamond$ $\mathcal{M}$ differential module associated with a differential system $[A]$

$\diamond$ K Picard-Vessiot extension for $\mathcal{M}$: diff. field ext. of k

$\rightarrow$ $[A]$ admits a fundamental matrix of solutions $U \in \mathrm{GL}_n(K)$

$\diamond$ The differential Galois group G of $\mathcal{M}$ is the group $\mathrm{Aut}_\partial(K/k)$ of differential k-algebra automorphisms of K:
$\forall g \in G,\ \forall f \in K, \quad g(f') = g(f)', \quad f \in k \Rightarrow g(f) = f$

$\diamond$ G viewed as a subgroup of $\mathrm{GL}_n(\mathbb{C})$ is a linear algebraic group:

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 $\det((X_{i,j})_{i,j})$, such that

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

The Lie algebra $\mathfrak{g}$ of G

$\diamond$ The Lie algebra $\mathfrak{g}$ of G is the tangent space of G at the point $\mathrm{id} \in G$: $\mathfrak{g}$ can be represented as a Lie sub-algebra of $\mathfrak{gl}_n(\mathbb{C})$

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

where $G(\mathbb{C}[\epsilon])$ set of $\mathbb{C}[\epsilon]$-points of G

$\diamond$ Adjoint action of G on $\mathfrak{g}$: $G \times \mathfrak{g} \to \mathfrak{g},\ (g, h) \mapsto g\, h\, g^{-1}$

$\diamond$ $V \triangleq \mathbb{C}$-vector space of solutions of $[A]$ in K^n, $\mathrm{End}(V)$ endowed with a Lie algebra structure $\mathfrak{gl}(V)$ identified with $\mathfrak{gl}_n(\mathbb{C})$
$\Rightarrow$ We have a representation of $\mathfrak{g}$ in $\mathrm{End}(V)$

$\diamond$ Using $\mathrm{End}(V) \cong V \otimes V^\star$, $\mathfrak{g}$ can then be viewed as a sub-vector space of $V \otimes V^\star$ stable under the adjoint action of G

Tannakian correspondence and characterization of $\mathfrak{g}$

$\diamond$ Tannakian correspondence: 1-1 correspondence (compatible with all constructions of linear algebra) between sub-vector spaces of V stable under the action of G and differential submodules of $\mathcal{M}$

$\rightarrow$ The representation of $\mathfrak{g}$ in $\mathrm{End}(V)$ corresponds to the differential submodule $\mathfrak{g}^s \triangleq (K \otimes_{\mathbb{C}} \mathfrak{g})^G$ of $\mathcal{M} \otimes_k \mathcal{M}^\star$

(Rk: $\mathfrak{g}^s$ is the Lie algebra considered by *Katz* in his works)

$\rightarrow$ $\mathfrak{g}^s$ (and thus $\mathfrak{g}$) can be investigated by studying differential submodules of $\mathcal{M} \otimes_k \mathcal{M}^\star$ which can all be obtained from a maximal decomposition if $\mathcal{M}$ is completely reducible

Sketch of our algorithm

1. Compute a maximal decomposition of $\mathcal{M} \otimes_k \mathcal{M}^\star$
   (tools: *eigenring techniques* & use specific *structure*)
2. Find a candidate for $\mathfrak{g}^s$
   (tools: *modular approach based on Grothendieck-Katz p-curvature conjecture*)
3. Validation of the candidate
   (tools: *reduced form & conjugation between Lie algebras*)

$\diamond$ In the following, we assume $\mathcal{M}/\ [A]$ absolutely irreducible (it can be checked: *Compoint-Weil'04*) and w.l.o.g. $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C})$

Rk: Completely reducible case quite similar (only small modif.)

II

Maximal decomposition of $\mathcal{M} \otimes_k \mathcal{M}^\star$

Maximal decomposition: general method

Problem: given [A], find $P \in \mathrm{GL}_n(k)$ s.t. $P[A]$ block diagonal

$\diamond$ Already studied in computer algebra: *Singer'96, Barkatou'07*

$\rightarrow$ Compute the eigenring (rational solutions - *Barkatou'99*)

$$\mathcal{E}(A) \triangleq \{F \in \mathbb{M}_n(k) \mid F' = [A, F] = A\,F - F\,A\}$$

$\diamond$ If $F \in \mathcal{E}(A)$, $P^{-1}\,F\,P = \mathrm{diag}(F_1, \ldots, F_r)$ (F_i constant matrices with distinct eigenvalues), then $P[A] = \mathrm{diag}(A_1, \ldots, A_r)$

$\diamond$ This corresponds to $\mathcal{M} = \mathcal{M}_1 \oplus \cdots \oplus \mathcal{M}_r$, where the bases of the submodules $\mathcal{M}_i$ are given by the columns of P

$\diamond$ Maximal dec. given by a random element of $\mathcal{E}(A)$ (*Barkatou'07*)

Maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$: specific methods (1)

$\diamond$ We could apply the previous method to $\mathcal{A} \triangleq A \otimes I_n - I_n \otimes A^T$

$\rightarrow$ Computing $\mathcal{E}(\mathcal{A})$: rational solutions of $\mathcal{A} \otimes I_{n^2} - I_{n^2} \otimes \mathcal{A}^T$ of size n^4! *Barkatou-Cluzeau-ElBacha-Weil'12* $\rightarrow O(n^{20})$ arithm. op.

$\rightarrow$ We should take into account the specific form of $\mathcal{A}$

$\diamond$ **Problem**: compute rational solutions of $\overline{\mathcal{A}} \triangleq \mathcal{A} \otimes I_{n^2} - I_{n^2} \otimes \mathcal{A}^T$

$\diamond$ First approach: algorithm in *Barkatou'99* proceeds in two steps:

1. Local data at each singularity $\rightarrow$ universal denominator
2. Polynomial solutions of an auxiliary system

Adapt ideas of *Barkatou-Pfluegel'98* $\Rightarrow$ local datas needed for rational solutions of $\overline{\mathcal{A}}$ (size n^4) can be computed from A (size n)

(Rk: the second step can also be accelerated)

Maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$: specific methods (2)

◇ Second approach: use structural decompositions

$[\overline{\mathcal{A}}]$ associated with $\mathrm{End}(\mathrm{End}(\mathcal{M})) \triangleq (\mathcal{M} \otimes \mathcal{M}^\star) \otimes (\mathcal{M} \otimes \mathcal{M}^\star)^\star$

$\rightarrow$ Decompose $\mathrm{End}(\mathrm{End}(\mathcal{M}))$ and rational sol. of smaller systems

Theorem 1 (*BCdVW'16*): we have $\mathcal{M} \otimes \mathcal{M}^\star = \mathbb{1}_k \oplus \mathcal{W}$ and the explicit iso.

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

Theorem 2 (*BCdVW'16*): we have the explicit iso.

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

$\rightarrow$ Rational solutions of systems of smaller size still having specific structures (Sym^2, Λ^2, Hom) that can be used for rational solutions (*Aparicio-Barkatou-Simon-Weil'11, Barkatou-Pfluegel'98*)

III

Candidate for $\mathfrak{g}^s$

Candidate for $\mathfrak{g}^s$: reduction modulo p

Problem: In the max. dec. $\mathcal{M} \otimes_k \mathcal{M}^\star = \bigoplus_{i=1}^r \mathcal{W}_i$, find $\mathfrak{g}^s$

$\rightarrow$ Idea: use a modular approach to find a candidate for $\mathfrak{g}^s$

$\diamond$ Crucial object for studying diff. systems $[A_p]$ / modules $(\mathcal{M}_p, \partial)$ in characteristic $p > 0$: the p-curvature $\chi_p \triangleq \partial^p$ acting on $\mathcal{M}_p$

$\diamond$ In terms of matrices: χ_p is given by the pth iterate of the sequence $\chi_1 = A_p$ and, for $i > 1$, $\chi_{i+1} = \chi_i' - A_p \chi_i$

$\rightarrow$ Algorithms: *Katz'82*, *van der Put'95-96*, *Cluzeau'03* and recently *Bostan-Caruso-Schost'15* for a fast algorithm

Grothendieck-Katz p-curvature conjecture: The Lie algebra $\mathfrak{g}^s$ is the smallest (algebraic) Lie sub-algebra of $\mathfrak{gl}_n(k)$ whose reduction modulo p contains the p-curvature χ_p for almost all p.

Candidate for $\mathfrak{g}^s$: algorithm ModularSelection

$\diamond$ $\mathcal{M} \otimes_k \mathcal{M}^\star = \bigoplus_{i=1}^r \mathcal{W}_i$ given by gauge transfo. $T \in \mathrm{GL}_{n^2}(k)$
(the columns $T_{\bullet j}$ of T provide bases of the submodules $\mathcal{W}_i$)

1. Choose a prime $p \to \bigoplus_{i=1}^r \mathcal{W}_{i,p}$ given by $T_p = T \mod p$;
2. Compute the p-curvature χ_p of $[A_p]$;
3. Compute $V = T_p^{-1} \mathrm{Vect}(\chi_p)$;
4. From the non-zero entries of V, deduce a basis of the submodule of $\bigoplus_{i=1}^r \mathcal{W}_i$ whose reduction mod p contains χ_p.

$\diamond$ From G-K conjecture, the submodule found can be used as a reasonable guess for $\mathfrak{g}^s$

$\diamond$ Remark: this may select a bigger or smaller submodule

$\to$ we need to check whether our guess is correct or not

IV

Validation of the candidate

Reduced form of a linear differential system

Definition: $[A]$ in reduced form if $A \in \overline{k} \otimes \mathfrak{g}$.

$\rightarrow$ $\mathfrak{g}$ viewed as a $\mathbb{C}$-vector space generated by $N_1, \ldots, N_d \in \mathbb{M}_n(\mathbb{C})$

$\rightarrow$ reduced form iff $\exists f_1, \ldots, f_d \in \overline{k}$ s.t. $A = f_1 N_1 + \cdots + f_d N_d$

Theorem (*Kolchin-Kovacic*): There exists a *reduction matrix* $P \in \mathrm{GL}_n(\overline{k})$ such that $[P[A]]$ is in reduced form.

$\diamond$ Reduced forms $\Rightarrow$ invariants (rational sol. of *constructions*) have constant coefficients in $\mathbb{C}$: *Aparicio-Compoint-Weil'13*

Theorem (*Aparicio-Compoint-Weil'13*): For all ordinary point $z_0 \in \mathbb{C}$ 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 z_0.

A Lie algebra conjugation problem

Definition: Two Lie sub-algebras $\mathfrak{g}_1$, $\mathfrak{g}_2 \subset \mathfrak{gl}_n(k)$ are conjugated if there exists a conjugation matrix $P \in \mathrm{GL}_n(\overline{k})$ s.t. $\mathfrak{g}_2 = P^{-1}\,\mathfrak{g}_1\,P$.

Theorem (*BCdVW'16*):

- M_i $(i = 1, \ldots, d)$ basis of candidate Lie algebra $\mathfrak{g}^s$,
- z_0 ordinary point of $[A]$,
- $\mathfrak{g}^t$ Lie sub-algebra of $\mathfrak{gl}_n(\mathbb{C})$ with basis $M_i(z_0)$ $(i = 1, \ldots, d)$.

If our choice for $\mathfrak{g}^s$ is correct, then there exists a reduction matrix $P \in \mathrm{GL}_n(\overline{k})$ for $[A]$ that is a conjugation matrix between the Lie algebra $\mathfrak{g}^s$ and $\mathfrak{g}^t$.

$\rightarrow$ A reduction matrix can be found among the conjugation matrices between $\mathfrak{g}^t$ and $\mathfrak{g}^s$

Semi-simple Lie algebras

$\diamond$ $\mathcal{M}$ absolutely irreducible and $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C})$

$\Rightarrow \mathfrak{g}^t$ and $\mathfrak{g}^s$ semi-simple Lie algebras

$\diamond$ Central objects in the study of a semi-simple Lie algebra $\mathfrak{g}$: set of canonical generators (and Chevalley bases)

$\rightarrow$ Matrices $H_1, \ldots, H_r, X_1, \ldots, X_r, Y_1, \ldots, Y_r$ which satisfies:

$[H_i, H_j] = 0$, $[X_i, Y_j] = \delta_{i,j} H_i$, $[H_i, X_j] = c_{j,i} X_j$, $[H_i, Y_j] = -c_{j,i} Y_j$

- This is associated with a root space decomposition of $\mathfrak{g}$
- $H_1, \ldots, H_r$ are generators of a Cartan sub-algebra of $\mathfrak{g}$
- $C = (c_{i,j})_{1 \leq i,j \leq r}$ is a Cartan matrix of $\mathfrak{g}$ ($c_{i,i} = 2$)

$\rightarrow$ Algorithms for computing set of canonical generators and Chevalley bases: *deGraaf'00*

ConjugationMatrices

Input: $\{M_i\}_i$ basis of $\mathfrak{g}^s$, $\{M_i(z_0)\}$ basis of $\mathfrak{g}^t$
Ouput: Conjugation matrices P between $\mathfrak{g}^t$ and $\mathfrak{g}^s$

1. Compute a set of canonical generators $\{H_i^t, X_i^t, Y_i^t\}$ of $\mathfrak{g}^t$;
2. Compute generators $\tilde{H}_i^s$ of a *split* Cartan sub-algebra $\mathfrak{h}^s$ of $\mathfrak{g}^s$ s.t. $\chi(\tilde{H}_i^s) = \chi(H_i^t)$ (ansatz $\rightarrow$ solving algebraic equations)
3. Compute a set of canonical generators $\{H_i^s, X_i^s, Y_i^s\}$ of $\mathfrak{g}^s$ having the same Cartan matrix as $\{H_i^t, X_i^t, Y_i^t\}$;
4. Compute the matrices $P \in \mathrm{GL}_n(\overline{k})$ such that $\forall i$, $P\,X_i^t = X_i^s\,P$ and $P\,Y_i^t = Y_i^s\,P$ (linear system).

Theorem (*BCdVW'16*): If our choice for $\mathfrak{g}^s$ is correct, then output of the form $P = c\,\tilde{P}$, with $\tilde{P} \in \mathrm{GL}_n(\overline{k})$, c arbitrary element of $\overline{k}$

ReductionMatrix

◇ Let $P = c\,\tilde{P}$ and $(N_i^t)_{i=1,\ldots,d}$ be a Chevalley basis of $\mathfrak{g}^t$

◇ $\exists f_i \in \overline{k}$ such that $P[A] = \sum_{i=1}^{d} f_i\, N_i^t$ implies:

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

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

1. $\mathfrak{g} \subseteq \mathfrak{sl}_n(\mathbb{C}) \Rightarrow \mathrm{Tr}(N_i^t) = 0$ and $\mathrm{Tr}(A) = \frac{w'}{w}$, $w \in k$

$$\Rightarrow c = \left(\frac{w}{\det(\tilde{P})}\right)^{1/n}$$

2. Set $P = c\,\tilde{P}$ and check if $\exists f_i \in \overline{k}$ s.t. $P[A] = \sum_{i=1}^{d} f_i\, N_i^t$

IV

Full algorithm and example

Full algorithm and remarks

1. Compute a maximal decomposition of $\mathcal{M} \otimes \mathcal{M}^\star$;
2. Apply ModularSelection to get a candidate for $\mathfrak{g}^s$;
3. Apply ConjugationMatrices;

   If it fails, go back to Step 2 and choose another prime p
4. Compute a Chevalley basis $(N_i^t)_i$ of $\mathfrak{g}^t$;
5. Apply ReductionMatrix.

   If it fails, go back to Step 2 and choose another prime p,

   Else Return $(N_i^t)_i$.

◇ Remarks on the successive choices of p:

- There may exist an infinite number of "bad" primes: good strategy for choosing prime numbers $\rightsquigarrow$ deterministic algo.
- If $\mathcal{W}_1$, $\mathcal{W}_2$ are proved not correct: try $\mathcal{W}_1 + \mathcal{W}_2$ before new p
- If candidate decomposable: check each proper submodule

Remarks on complexity / Implementation

$\diamond$ Arithmetic complexity polynomial in n except algebraic systems solved in ConjugationMatrices

$\rightarrow$ Significant diff. compared to the exponential (several levels) complexity obtained in *Feng'15* for computing the Galois group

$\diamond$ We have a prototype Maple implementation

$\rightarrow$ We manage to apply it to many examples up to order $n = 7$

$\rightarrow$ In practice, the most costly step is the dec. of $\mathcal{M} \otimes \mathcal{M}^\star$

Example (1)

◇ Consider the linear differential system given by $\mathbf{y}' = A\,\mathbf{y}$ with

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

◇ $\mathcal{M} \otimes \mathcal{M}^\star = \mathbb{1}_k \oplus \mathcal{W}_1 \oplus \mathcal{W}_2$, with $\mathcal{W}_1$, $\mathcal{W}_2$ of resp. dim. 3 and 5

◇ p-curvature $\rightarrow$ candidate for $\mathfrak{g}^s$ is $\mathcal{W}_1$ irred with basis

$$M_1 = \begin{bmatrix} -1 & 0 & 1 \\ 0 & 0 & 0 \\ -x^2-1 & 0 & 1 \end{bmatrix}, M_2 = \begin{bmatrix} 0 & 1 & 0 \\ -x^2 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, M_3 = \begin{bmatrix} 0 & 1 & 0 \\ -x^2-1 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}.$$

Example (2)

◇ $x_0 = 1$ ordinary point for $[A]$: set of canonical gen. of $\mathfrak{g}^t$:

$$H^t = \begin{bmatrix} 2\,i & 0 & -2\,i \\ 0 & 0 & 0 \\ 4\,i & 0 & -2\,i \end{bmatrix}, X^t = \begin{bmatrix} 0 & -i & 0 \\ 1+i & 0 & -1 \\ 0 & 1-i & 0 \end{bmatrix}, Y^t = \begin{bmatrix} 0 & -i & 0 \\ -1+i & 0 & 1 \\ 0 & -1-i & 0 \end{bmatrix}.$$

◇ Computing an "aligned" set of canonical gen. of $\mathfrak{g}^s$, we get:

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

◇ Conjugation matrices P s.t. $X^t\,P = P\,X^s$ and $Y^t\,P = P\,Y^s$:

$$P = c\,\tilde{P}, \qquad c \in \overline{k}, \qquad \tilde{P} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & -x & 0 \\ x+1 & 0 & -x \end{bmatrix}.$$

Example (3)

$\diamond$ We then get $c = a/x$, $a \in \mathbb{C}^*$ and solving the linear system obtained from $P[A] = f_1\, H^t + f_2\, X^t + f_3\, Y^t$ with $P = c\,\tilde{P}$ yields

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

$\rightarrow$ Reduction matrix P and reduced form R given by:

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

$\rightarrow$ The Lie algebra $\mathfrak{g}$ viewed as a Lie sub-algebra of $\mathfrak{gl}_3(\mathbb{C})$ admits the basis H^t, X^t, Y^t

Summary

◇ We provide a full algorithm for computing the Lie algebra $\mathfrak{g}$ of G in the case of an absolutely irreducible system[1]

- Completely reducible case quite similar (only small modif.)
- Reducible case studied recently in a work of *Dreyfus-Weil*

→ All the cases are then handled

◇ We have a prototype Maple implementation (which needs to be improved)

Thank you for your attention!

[1] Note that we get a reduced form as a byproduct