Symbolic-Numeric Factorization of Linear Differential Operators

Frédéric Chyzak [1] **Alexandre Goyer** [1] Marc Mezzarobba [2]

[1]Inria Saclay – Île-de-France, France

[2]LIX, CNRS, Computer Science Laboratory of École Polytechnique, France

Functional Equations in LIMoges 2022, France

March 30, 2022

Factorization of differential operators

Object of study: linear differential operator

$$P = a_r\partial^r + a_{r-1}\partial^{r-1} + \cdots + a_1\partial + a_0 \in \mathbb{K}(x)\langle\partial\rangle$$

for a number field $\mathbb{K} \subset \mathbb{C}$, $a_i \in \mathbb{K}(x)$, $a_r \neq 0$, and $\partial = d/dx$

Commutation rule: $\partial x = x\partial + 1$ Leibniz: $(xf)' = xf' + f$

Goal

Find $L, R \in \overline{\mathbb{K}}(x)\langle\partial\rangle$ of order > 0 such that $P = LR$

Example:

$$x\partial^2 + (-4x^3 + 5x)\partial + 4x^2 - 5 = (\partial - 4x^2 + 5)(x\partial - 1)$$

History: around factorization algorithms

1894 Beke
hyperexponential solutions
+ exterior power method

1996 Singer
eigenring method

1997 van Hoeij
local-to-global method
➤ Maple DEtools package

2004 Cluzeau, van Hoeij
modular approach

2007 van der Hoeven
symbolic-numeric approach
➤ SageMath package (new)

2013 Johansson, Kauers, Mezzarobba
hyperexponential solutions by symbolic-numeric approach

2014 Llorente
Liouvillian solutions by symbolic-numeric approach

Improvements of Beke's algorithm

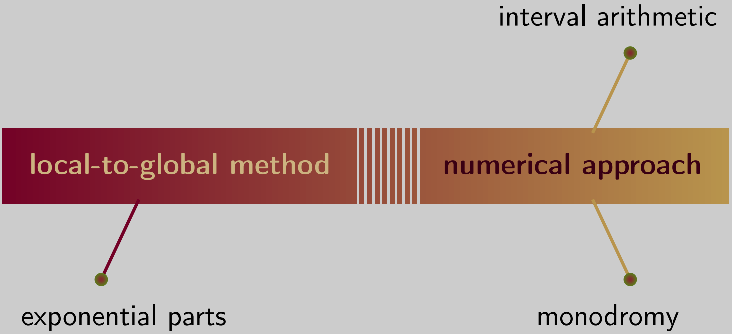
1989 Schwarz

1990 Grigor'ev
(complexity analysis)

1994 Bronstein

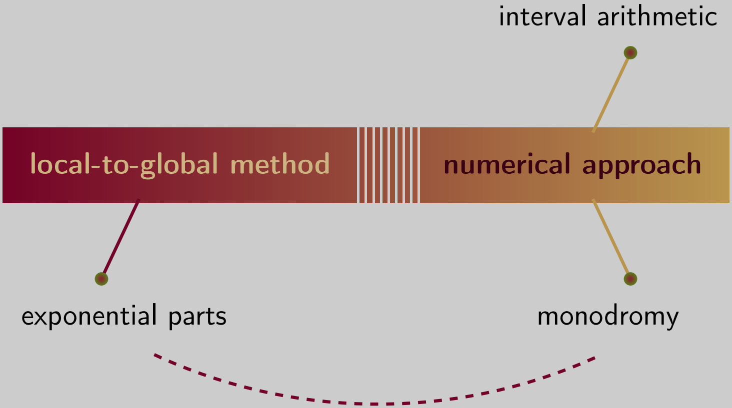
1996 Tsarev

local-to-global method | numerical approach


interval arithmetic
local-to-global method
numerical approach
exponential parts
monodromy

Hybrid Algorithm

[Chyzak, G., Mezzarobba, 2022]



Local solutions at a nonsingular point

Definition: $\Sigma(P) := \bigcup_{i=0}^{r-1} \left\{ \text{poles of } \frac{a_i}{a_r} \right\} \subset \mathbb{P}^1(\mathbb{C})$ (singularities)

Cauchy-type theorem:

If $x_0 \in \mathbb{C} \backslash \Sigma(P)$ then there is a basis $(f_0, \ldots, f_{r-1})$ of solutions such that:

$$\forall 0 \leqslant i, j < r, \;\; f_i \in \mathbb{K}[[x - x_0]] \;\; \text{and} \;\; f_i^{(j)}(x_0) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}.$$

Throughout this talk

- $0 \notin \Sigma(P)$
- $\mathrm{Sol}(P) := \mathrm{Span}_{\mathbb{C}}(f_0, \ldots, f_{r-1})$ space of local solutions at 0
- Identification: $\mathrm{Sol}(P) \ni f \longleftrightarrow \mathrm{coord}(f) \in \mathbb{C}^r$

Differential Galois group

and

monodromy

Differential Galois group *e.g.* [Singer, van der Put, 2003]

$$E := \mathbb{C}(x)(f_0, \ldots, f_{r-1}, f_0', \ldots, f_{r-1}', \ldots, f_0^{(r-1)}, \ldots, f_{r-1}^{(r-1)})$$

Picard-Vessiot extension

$$\mathrm{Gal}_{\mathrm{diff}}(P) := \{\, \sigma \in \mathrm{Aut}\,(E/\mathbb{C}(x)) \mid \forall f \in E,\, \sigma(f') = \sigma(f)' \,\}$$

- left action of $\mathrm{Gal}_{\mathrm{diff}}(P)$ on $\mathrm{Sol}(P)$

Differential Galois group *e.g.* [Singer, van der Put, 2003]

$$E := \mathbb{C}(x)(f_0, \dots, f_{r-1}, f_0', \dots, f_{r-1}', \dots, f_0^{(r-1)}, \dots, f_{r-1}^{(r-1)})$$

Picard-Vessiot extension

$$\mathrm{Gal}_{\mathrm{diff}}(P) := \{\, \sigma \in \mathrm{Aut}\,(E/\mathbb{C}(x)) \mid \forall f \in E,\ \sigma(f') = \sigma(f)' \,\}$$

➤ left action of $\mathrm{Gal}_{\mathrm{diff}}(P)$ on $\mathrm{Sol}(P)$

Theorem: $\mathrm{Gal}_{\mathrm{diff}}(P)$ is a linear algebraic group.

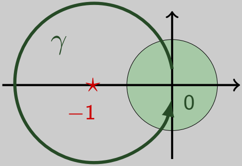
Faithful representation: $\psi : \sigma \mapsto M \in \mathbb{C}^{r \times r}$ such that

$$\forall f \in \mathrm{Sol}(P),\ \ \mathrm{coord}(\sigma(f)) = M \times \mathrm{coord}(f)$$

➤ left action of $\mathcal{G} := \psi\,(\mathrm{Gal}_{\mathrm{diff}}(P))$ on $\mathbb{C}^r$

Monodromy

e.g. [Mitschi, Sauzin, 2016]



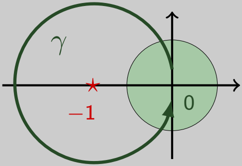
Example/Definition: $Q = (x+1)\partial^2 + \partial$ admits $f_0 := 1$, $f_1 := \log(1+x)$ as basis of solutions

$$af_0 + bf_1 \xrightarrow{\text{analytic continuation along } \gamma} (a + 2i\pi b)f_0 + bf_1$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \longrightarrow \begin{pmatrix} a + 2i\pi b \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 2i\pi \\ 0 & 1 \end{pmatrix}}_{\text{local monodromy matrix around } -1} \begin{pmatrix} a \\ b \end{pmatrix}$$

Monodromy

Example/Definition: $Q = (x+1)\partial^2 + \partial$ admits $f_0 := 1$, $f_1 := \log(1+x)$ as basis of solutions



$$af_0 + bf_1 \xrightarrow{\text{analytic continuation along } \gamma} (a + 2i\pi b)f_0 + bf_1$$

$$\begin{pmatrix} a \\ b \end{pmatrix} \longrightarrow \begin{pmatrix} a + 2i\pi b \\ b \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 2i\pi \\ 0 & 1 \end{pmatrix}}_{\text{local monodromy matrix around } -1} \begin{pmatrix} a \\ b \end{pmatrix}$$

$\mathbb{C}^{r\times r} \supset \mathcal{M} :=$ group generated by all the local monodromy matrices of P

Remark: rigorous arbitrary-precision computation of monodromy matrices available in the SageMath package `ore_algebra` [Mezzarobba, 2016]

Theorem [Schlesinger, 1885]
If P is Fuchsian then $\mathcal{G} = \overline{\mathcal{M}}$ (for the Zariski topology).

Fuchs' criterion, 1866: The operator P is Fuchsian if and only if the fraction $\frac{a_i}{a_r}$ has no pole in $\mathbb{P}^1(\mathbb{C})$ of order $< i - r$, for each $0 \leqslant i < r$.

Theorem [Ramis, 1995] $\mathcal{G} = \overline{\mathcal{M} + \text{the exponential torus} + \text{the Stokes matrices}}$

Theorem [Schlesinger, 1885]
If P is Fuchsian then $\mathcal{G} = \overline{\mathcal{M}}$ (for the Zariski topology).

Fuchs' criterion, 1866: The operator P is Fuchsian if and only if the fraction $\frac{a_i}{a_r}$ has no pole in $\mathbb{P}^1(\mathbb{C})$ of order $< i - r$, for each $0 \leqslant i < r$.

Theorem [Ramis, 1995] $\mathcal{G} = \overline{\mathcal{M} + \text{the exponential torus} + \text{the Stokes matrices}}$

Remark: If P is Fuchsian then, for $\sigma \in \Sigma(P)$, there is a basis of solutions of the form

$$f(x) = (x-\sigma)^\alpha \sum_{j=0}^{d} s_j(x-\sigma) \log(x-\sigma)^j \quad \text{where} \begin{cases} \alpha \in \overline{\mathbb{K}}, \\ d \in \mathbb{Z}_{\geqslant 0}, \\ s_0, \ldots, s_d \in \overline{\mathbb{K}}[[x]]. \end{cases}$$

Moreover $(x-\sigma)^\alpha = e^{\alpha \log(x-\sigma)} \longrightarrow \boldsymbol{e^{2i\pi\alpha}}(x-\sigma)^\alpha$ after ↻.

Therefore: $\underbrace{\text{exponential parts}}_{:= \alpha + \mathbb{Z}}$ ⇔ eigenvalues of the local monodromy matrix

$:= \alpha + \mathbb{Z}$, see [van Hoeij, 1996]

$$\boxed{\mathcal{A} := \mathbb{C}[\mathcal{M}]} \subset \mathbb{C}^{r\times r} \quad \text{(group algebra)}$$

Proposition: There is a one-to-one correspondence:

right-hand factor R of P $\xleftrightarrow[V \simeq \mathrm{Sol}(R)]{}$ $\mathcal{A}$-submodule V of $\mathbb{C}^r$

Strategy for finding a right-hand factor [van der Hoeven, 2007]

1. Loop over precision until success:
2. Compute approximations of the local monodromy matrices
3. Search for an approximate nontrivial proper $\mathcal{A}$-submodule V
4. If no such V exists then
5. Exploit error bounds to ensure the irreducibility
6. Else guess a symbolic $R \in \overline{\mathbb{K}}(x)\langle\partial\rangle$ from V and check it

Norton's criterion

or: how to adapt the local-to-global method to the module framework?

Finding a submodule

Assume that P admits a nontrivial factorization $P = LR$.

$\tilde{\mathcal{A}} := T^{-1}\mathcal{A}T$ where $T :=$ transition matrix from $(f_0, \ldots, f_{r-1})$ to a basis adapted to a decomposition $\mathrm{Sol}(P) = \mathrm{Sol}(R) \oplus S$.

Remark: Any $M \in \tilde{\mathcal{A}}$ has a block-triangular form $\left(\begin{array}{c|c} M_R & * \\ \hline 0 & M_L \end{array}\right)$.

If there is $M \in \tilde{\mathcal{A}}$ with a simple eigenvalue λ,
let $v \in \mathbb{C}^{r\times 1}$, $w \in \mathbb{C}^{1\times r}$ be such that $Mv = \lambda v$, $wM = \lambda w$, then

$$\begin{array}{rcl} \textbf{either } \lambda \text{ is an eigenvalue of } M_R & \Rightarrow & \tilde{\mathcal{A}}v \subsetneq \mathbb{C}^{r\times 1}, \\ \textbf{or } \lambda \text{ is an eigenvalue of } M_L & \Rightarrow & w\tilde{\mathcal{A}} \subsetneq \mathbb{C}^{1\times r}. \end{array}$$

Finding a submodule

Assume that P admits a nontrivial factorization $P = LR$.

$\tilde{\mathcal{A}} := T^{-1}\mathcal{A}T$ where $T :=$ transition matrix from $(f_0, \dots, f_{r-1})$ to a basis adapted to a decomposition $\mathrm{Sol}(P) = \mathrm{Sol}(R) \oplus S$.

Remark: Any $M \in \tilde{\mathcal{A}}$ has a block-triangular form $\left(\begin{array}{c|c} M_R & * \\ \hline 0 & M_L \end{array}\right)$.

If there is $M \in \tilde{\mathcal{A}}$ with a simple eigenvalue λ,
let $v \in \mathbb{C}^{r\times 1}$, $w \in \mathbb{C}^{1\times r}$ be such that $Mv = \lambda v$, $wM = \lambda w$, then

$$\begin{array}{rcl} \textbf{either } \lambda \text{ is an eigenvalue of } M_R & \Rightarrow & \tilde{\mathcal{A}}v \subsetneq \mathbb{C}^{r\times 1}, \\ \textbf{or } \lambda \text{ is an eigenvalue of } M_L & \Rightarrow & w\tilde{\mathcal{A}} \subsetneq \mathbb{C}^{1\times r}. \end{array}$$

Remark: in the local-to-global method:

e is an exponential part of multiplicity 1 of P $\Rightarrow$ either e is an exponential part of R or e is an exponential part of L

Theorem: Given $M \in \mathcal{A}$, a simple eigenvalue λ, and nonzero $v \in \mathbb{C}^{r\times 1}$, $w \in \mathbb{C}^{1\times r}$ satisfying $Mv = \lambda v$, $wM = \lambda w$, the following statements are equivalent:

(1) the left $\mathcal{A}$-module $\mathbb{C}^{r\times 1}$ is irreducible,

(2) $\mathcal{A}v = \mathbb{C}^{r\times 1}$ and $w\mathcal{A} = \mathbb{C}^{1\times r}$,

(3) the right $\mathcal{A}$-module $\mathbb{C}^{1\times r}$ is irreducible.

Note: right action of $\mathcal{A}$ on $\mathbb{C}^{1\times r} \longleftrightarrow$ monodromy action on $\mathrm{Sol}(P^*)$
$P^* :=$ image of P by the anti-endomorphism of $\mathbb{K}(x)\langle\partial\rangle$ mapping ∂ to $-\partial$ (so that $(LR)^* = R^*L^*$)

Interval arithmetic

or: how to certify independence?

Implementing basic operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}$, ... on intervals:

Motto

The interval contains the exact value.

Example: Let $\boldsymbol{\pi} := [3.1415, 3.1416]$ be an interval representing π.
We require that $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R}$ such that $3.1415 \leqslant x^2 \leqslant 3.1416\}$.

Interval arithmetic

e.g. [Moore, 1962]

Implementing basic operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}$, $\ldots$ on intervals:

Motto

The interval contains the exact value.

Example: Let $\boldsymbol{\pi} := [3.1415, 3.1416]$ be an interval representing π.
We require that $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R} \text{ such that } 3.1415 \leqslant x^2 \leqslant 3.1416\}$.

Difficulties

- Overestimation
- Testing the nullity

Implementing basic operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}$, $\ldots$ on intervals:

Motto

The interval contains the exact value.

Example: Let $\boldsymbol{\pi} := [3.1415, 3.1416]$ be an interval representing π.
We require that $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R} \text{ such that } 3.1415 \leqslant x^2 \leqslant 3.1416\}$.

Difficulties

- Overestimation
- Testing the nullity

Extensions

- Complex numbers
- Vectors, matrices

Interval Gaussian elimination

$$\begin{pmatrix} [3.14, 3.15] & [3.33, 3.34] & [1.72, 1.73] \\ [2.41, 2.42] & [3.55, 3.56] & [2.14, 2.15] \\ [-0.7, -0.69] & [1.27, 1.28] & [5, 5.01] \end{pmatrix}$$

Interval Gaussian elimination

Operation: $r_1 \leftarrow r_1 / c_{11}$

$$\begin{pmatrix} \mathbf{1} & [1.05, 1.07] & [0.54, 0.56] \\ [2.41, 2.42] & [3.55, 3.56] & [2.14, 2.15] \\ [-0.7, -0.69] & [1.27, 1.28] & [5, 5.01] \end{pmatrix}$$

Interval Gaussian elimination

Operations: $r_2 \leftarrow r_2 - c_{21} r_1$ and $r_3 \leftarrow r_3 - c_{31} r_1$

$$\begin{pmatrix} \mathbf{1} & [1.05, 1.07] & [0.54, 0.56] \\ \mathbf{0} & [0.96, 1.03] & [0.78, 0.85] \\ \mathbf{0} & [1.99, 2.04] & [1.64, 1.68] \end{pmatrix}$$

Interval Gaussian elimination

Operations: $r_2 \leftrightarrow r_3$ then $r_2 \leftarrow r_2/c_{22}$ and $r_3 \leftarrow r_3 - c_{32} r_2$

$$\begin{pmatrix} \mathbf{1} & [1.05, 1.07] & [0.54, 0.56] \\ \mathbf{0} & \mathbf{1} & [0.8, 0.85] \\ \mathbf{0} & \mathbf{0} & [-0.1, 0.09] \end{pmatrix}$$

Interval Gaussian elimination

$$\begin{pmatrix} \mathbf{1} & [1.05, 1.07] & [0.54, 0.56] \\ \mathbf{0} & \mathbf{1} & [0.8, 0.85] \\ \mathbf{0} & \mathbf{0} & [-0.1, 0.09] \end{pmatrix}$$

number of "interval pivots" $\leqslant$ rank of the exact matrix

Correction of interval Gaussian elimination

Notation: $\mathbb{C}_\bullet := \{\mathcal{B}(c,\epsilon)\,;\, c \in \mathbb{C}, \epsilon \in \mathbb{R}_{\geqslant 0}\}$ the set of balls

Proposition 1:
Given $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p \in \mathbb{C}_\bullet^r$, we can compute $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_t \in \mathbb{C}_\bullet^r$ such that:
for all $v_1 \in \boldsymbol{v}_1, \ldots v_p \in \boldsymbol{v}_p$, there are $u_1 \in \boldsymbol{u}_1, \ldots, u_t \in \boldsymbol{u}_t$ satisfying:

- $(u_1, \ldots, u_t)$ is linearly independent,
- $\mathrm{Span}_{\mathbb{C}}(u_1, \ldots, u_t) \subset \mathrm{Span}_{\mathbb{C}}(v_1, \ldots, v_p)$.

Correction of interval Gaussian elimination

Notation: $\mathbb{C}_\bullet := \{\mathcal{B}(c,\epsilon)\,;\, c \in \mathbb{C}, \epsilon \in \mathbb{R}_{\geqslant 0}\}$ the set of balls

Proposition 1:
Given $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p \in \mathbb{C}_\bullet^r$, we can compute $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_t \in \mathbb{C}_\bullet^r$ such that:
for all $v_1 \in \boldsymbol{v}_1, \ldots v_p \in \boldsymbol{v}_p$, there are $u_1 \in \boldsymbol{u}_1, \ldots, u_t \in \boldsymbol{u}_t$ satisfying:

- $(u_1, \ldots, u_t)$ is linearly independent,
- $\mathrm{Span}_{\mathbb{C}}(u_1, \ldots, u_t) \subset \mathrm{Span}_{\mathbb{C}}(v_1, \ldots, v_p)$.

Proposition 2: Let $v_1, \ldots, v_p \in \mathbb{C}^r$ be fixed.
If $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_p \in \mathbb{C}_\bullet^r$ are such that $v_1 \in \boldsymbol{v}_1, \ldots v_p \in \boldsymbol{v}_p$ then:

"the $\boldsymbol{v}_i$ are precise enough" $\Rightarrow$ "the inclusion $\subset$ is an equality".

Correction of orbit computation

Corollary 1:
Given $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{C}_\bullet^{r \times r}$, $\boldsymbol{v} \in \mathbb{C}_\bullet^r$, we can compute $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_d \in \mathbb{C}_\bullet^r$ such that:
for all $M_1 \in \boldsymbol{M}_1, \ldots, M_k \in \boldsymbol{M}_k$, $v \in \boldsymbol{v}$, there are $w_1 \in \boldsymbol{w}_1, \ldots, w_d \in \boldsymbol{w}_d$ satisfying:

- $(w_1, \ldots, w_d)$ is linearly independent,
- $\mathrm{Span}_{\mathbb{C}}(w_1, \ldots, w_d) \subset \underbrace{\mathbb{C}[M_1, \ldots, M_k]v}_{\text{orbit of } v \text{ under the action of the } M_i}$.

Correction of orbit computation

Corollary 1:
Given $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{C}_\bullet^{r\times r}$, $\boldsymbol{v} \in \mathbb{C}_\bullet^r$, we can compute $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_d \in \mathbb{C}_\bullet^r$ such that:
for all $M_1 \in \boldsymbol{M}_1, \ldots, M_k \in \boldsymbol{M}_k$, $v \in \boldsymbol{v}$, there are $w_1 \in \boldsymbol{w}_1, \ldots, w_d \in \boldsymbol{w}_d$ satisfying:

- $(w_1, \ldots, w_d)$ is linearly independent,
- $\mathrm{Span}_{\mathbb{C}}(w_1, \ldots, w_d) \subset \underbrace{\mathbb{C}[M_1, \ldots, M_k]v}_{\text{orbit of } v \text{ under the action of the } M_i}$.

Corollary 2: Let $M_1, \ldots, M_k \in \mathbb{C}^{r\times r}$ and $v \in \mathbb{C}^r$ be fixed.
If $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{C}_\bullet^{r\times r}$, $\boldsymbol{v} \in \mathbb{C}_\bullet^r$ are such that $M_1 \in \boldsymbol{M}_1, \ldots, M_k \in \boldsymbol{M}_k$, $v \in \boldsymbol{v}$ then:

"the $\boldsymbol{M}_i$ and $\boldsymbol{v}$ are precise enough" $\Rightarrow$ "the inclusion $\subset$ is an equality".

Correction of orbit computation

Corollary 1:
Given $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{C}_\bullet^{r \times r}$, $\boldsymbol{v} \in \mathbb{C}_\bullet^r$, we can compute $\boldsymbol{w}_1, \ldots, \boldsymbol{w}_d \in \mathbb{C}_\bullet^r$ such that:
for all $M_1 \in \boldsymbol{M}_1, \ldots, M_k \in \boldsymbol{M}_k$, $v \in \boldsymbol{v}$, there are $w_1 \in \boldsymbol{w}_1, \ldots, w_d \in \boldsymbol{w}_d$ satisfying:

- $(w_1, \ldots, w_d)$ is linearly independent,
- $\mathrm{Span}_{\mathbb{C}}(w_1, \ldots, w_d) \subset \underbrace{\mathbb{C}[M_1, \ldots, M_k]v}_{\text{orbit of } v \text{ under the action of the } M_i}$.

Corollary 2: Let $M_1, \ldots, M_k \in \mathbb{C}^{r \times r}$ and $v \in \mathbb{C}^r$ be fixed.
If $\boldsymbol{M}_1, \ldots, \boldsymbol{M}_k \in \mathbb{C}_\bullet^{r \times r}$, $\boldsymbol{v} \in \mathbb{C}_\bullet^r$ are such that $M_1 \in \boldsymbol{M}_1, \ldots, M_k \in \boldsymbol{M}_k$, $v \in \boldsymbol{v}$ then:

"the $\boldsymbol{M}_i$ and $\boldsymbol{v}$ are precise enough" $\Rightarrow$ "the inclusion $\subset$ is an equality".

In particular, if $d = r$ then we can certify that the orbit is equal to $\mathbb{C}^r$.

Hybrid algorithm
for
factoring differential operators

Reconstructing a right-hand factor from a seed vector v

Proposition: $\mathcal{A}v \simeq \mathrm{Sol}(P_f)$ where $P_f :=$ minimal annihilator of f

Hermite–Padé approximants

Given $f, f', \dots, f^{(r-1)} \in \overline{\mathbb{K}}[[x]]$, find $p_0, \dots, p_{r-1} \in \overline{\mathbb{K}}[x]$ of degree $\leqslant d$ such that $\sum_{i=0}^{r-1} p_i f^{(i)} = o(x^\sigma)$. ($\sigma < r(d+1) \Rightarrow$ nonzero solutions)

- if we find a candidate right-hand factor (using LLL algorithm to guess coefficients in $\overline{\mathbb{K}}$), we can check it by Euclidean division in $\overline{\mathbb{K}}(x)\langle\partial\rangle$.

Reconstructing a right-hand factor from a seed vector v

Proposition: $\mathcal{A}v \simeq \mathrm{Sol}(P_f)$ where $P_f :=$ minimal annihilator of f

Hermite–Padé approximants

Given $f, f', \ldots, f^{(r-1)} \in \overline{\mathbb{K}}[[x]]$, find $p_0, \ldots, p_{r-1} \in \overline{\mathbb{K}}[x]$ of degree $\leqslant d$ such that $\sum_{i=0}^{r-1} p_i f^{(i)} = o(x^\sigma)$. $(\sigma < r(d+1) \Rightarrow$ nonzero solutions$)$

- if we find a candidate right-hand factor (using LLL algorithm to guess coefficients in $\overline{\mathbb{K}}$), we can check it by Euclidean division in $\overline{\mathbb{K}}(x)\langle\partial\rangle$.
- irreducible case? Two approaches:
  - **either** orbit computation to certify that $\mathcal{A}v = \mathbb{C}^{r\times 1}$
    price: a complete set of generators of $\mathcal{A}$ is *a priori* needed
  - **or** Hermite–Padé approximants to certify that $\mathrm{order}(P_f) = r$
    price: computations at a large order of truncation
    ($\sigma > rB$ where B is a degree bound for right-hand factors)
    [Bostan, Rivoal, Salvy, 2019]

Algorithm RightFactor(P) [Chyzak, G., Mezzarobba, 2022]

Input: $P \in \mathbb{K}(x)\langle\partial\rangle$ of order r
Output: `'Irreducible'` or a nontrivial proper right-hand factor of P

1. Initialize the working precision p and the order of truncation σ
2. While a complete set of generators of $\mathcal{A}$ has not been computed:
   - 2.a. Compute a new local monodromy matrix
   - 2.b. Choose randomly a combination M of the computed generators
   - 2.c. Try Norton's criterion or another method depending on the spectrum of M
   - 2.d. If the previous step succeeds then return the result
3. Increase p and σ, and go back to line 2

Lemma [Eberly, 1991]
The set $\{M \in \mathcal{A}$ without simple eigenvalue$\}$ is an algebraic subset of $\mathcal{A}$.

Note: Local-to-global method $\simeq$ 1st iteration of While loop

Experiments

operator	order, degree in x	classic (♒)	new (♋)	
rand (♏)	4, 20	6.4s	9.6s	local-to-global method applies
	6, 30	980s (!)	370s	
rand×rand (♏) (different factors)	4, 20	11s	1.9s	
	6, 30	220s	22s	
rand (♏)	4, 20	1400s	25s	local-to-global method does not apply
	6, 30	2900s (!)	270s	
rand×rand (♏) (different factors)	4, 20	1700s	8.4s	
	6, 30	14000s (!)(!!)	98s	
fcc5 (♈)	6, 17	62s	2.0s	combinatorial examples
fcc6 (♈)	8, 43	>36000s	30s	

(♒) command `DFactor(_,‘one step‘)` of the Maple package `DEtools`

(♋) command `rfactor(_)` of my branch of `ore_algebra` SageMath package, at `https://github.com/a-goyer/ore_algebra/tree/facto` under the GNU GPL

(♏) random irreducible operators, created following [Ince, 1926]

(♈) irreducible operators at `http://koutschan.de/data/fcc1/` (probabilistic walks)

(!) Warning message: “factorization of ... may be incomplete” (!!) Factorization is incomplete

Overview

Contributions

- Incremental hybrid algorithm + implementation in progress
- Link between local-to-global approach and Norton's criterion
- Package for symbolic-numeric factorization + validation

Remaining work

- Further timing comparisons between the different approaches
- Complexity analysis
- Extension to non-regular case
- Further possible applications?
  - Exponential/Liouvillian solutions
  - Decide whether there is a basis of algebraic solutions
  - The differential Galois group or its Lie algebra
  - Absolute factorization

Alin Bostan, Tanguy Rivoal, and Bruno Salvy.
Explicit degree bounds for right factors of linear differential operators.
Bulletin of the London Mathematical Society, 2019.

J. Della Dora and E. Tournier.
Formal solutions of differential equations in the neighborhood of singular points (regular and irregular).
In *Proceedings of the fourth ACM Symposium on Symbolic and Algebraic Computation*, pages 25–29, 1981.

Derek F. Holt and Sarah Rees.
Testing modules for irreducibility.
Journal of the Australian Mathematical Society, 57(1):1–16, 1994.

Edward Lindsay Ince.
Ordinary Differential Equations.
Dover Publications, New York, 1926.

Claude Mitschi and David Sauzin.
Divergent Series, Summability and Resurgence II. Monodromy and Resurgence.
Springer, 2016.

Joris van der Hoeven.
Around the numeric-symbolic computation of differential Galois groups.
Journal of Symbolic Computation, pages 236–264, 2007.

Marius van der Put and Michael F. Singer.
Galois Theory of Linear Differential Equations.
Springer-Verlag Berlin Heidelberg, 2003.

Mark van Hoeij.
Factorization of Linear Differential Operators.
PhD thesis, Catholic University of Nijmegen, 1996.