Symbolic-Numeric Factorization of Linear Differential Operators

Alexandre Goyer [1,2]

co-supervised by

Frédéric Chyzak[1] and Marc Mezzarobba[2]

(1) INRIA Saclay – Île-de-France
(2) Laboratoire d'Informatique de l'École polytechnique

De rerum natura meeting

June 3, 2021

Object of study. Let $a_i \in \overline{\mathbb{Q}}(z)$.

$$(E) : a_n(z)f^{(n)}(z) + \cdots + a_1(z)f'(z) + a_0(z)f(z) = 0$$

Formalism. f solution of $(E) \Leftrightarrow L \cdot f = 0$ where

$$L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \overline{\mathbb{Q}}(z)\langle\partial\rangle$$

is a so-called *linear differential operator*.

Object of study. Let $a_i \in \overline{\mathbb{Q}}(z)$.

$$(E) : a_n(z)f^{(n)}(z) + \cdots + a_1(z)f'(z) + a_0(z)f(z) = 0$$

Formalism. f solution of $(E) \Leftrightarrow L \cdot f = 0$ where

$$L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \overline{\mathbb{Q}}(z)\langle\partial\rangle$$

is a so-called *linear differential operator*.

Leibniz rule: $(zf)' = zf' + f \quad \rightarrow \quad \boxed{\partial z = z\partial + 1}$

Example. $L = z\partial^2 + (-4z^3 + 5z)\partial + 4z^2 - 5$
and an example of factorization:

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

Factoring a linear differential operator

- **1894**: Beke (right-hand factor of order 1)
- **1996**: Singer (adaptation of Berlekamp's algorithm)
- **1997**: van Hoeij (algorithm of the type "local $\rightarrow$ global")
- **2004**: Cluzeau, van Hoeij (modular algorithm)
- **2007**: van der Hoeven (symbolic-numeric algorithm)

Improvements of Beke's algorithm

- **1989**: Schwarz
- **1990**: Grigor'ev
- **1994**: Bronstein
- **1996**: Tsarev

Complexity analysis (bounds on coefficients):

- **1990**: Grigor'ev
- **2020**: Bostan, Rivoal, Salvy

Let $\mathcal{F}$ denote $\overline{\mathbb{Q}}(z)$ and consider a differential operator $L \in \mathcal{F}\langle\partial\rangle$. Write $L = q\,(a_n\partial^n + \cdots + a_1\partial + a_0)$ with $q \in \overline{\mathbb{Q}}(z)$ such that the $a_i \in \overline{\mathbb{Q}}[z]$ are coprime.

Definition. A point $z_0 \in \mathbb{C}$ is an ordinary point of L if $a_n(z_0) \neq 0$. Otherwise, it is a singular point (or a singularity) of L.

Fix an ordinary point z_0 of L.

Proposition. For each $1 \leq i \leq n$, there is a unique power series $h_i = \sum_{j=0}^{+\infty} h_{i,j}(z - z_0)^j$ such that:

- h_i est solution of L in a neighborhood of z_0,
- $h_i^{(j)}(z_0) = \delta_{i,j+1}$ for $0 \leq j < n$.

Remark. The basis $(h_1, \ldots, h_n)$ gives an canonical identification of the solution space $\mathrm{Sol}(L) := \mathrm{Span}_{\overline{\mathbb{Q}}}(h_1, \ldots, h_n)$ with $\overline{\mathbb{Q}}^n$.

approximation $\rightarrow$ guessing $\rightarrow$ post-certification

Factorization of a reducible polynomial $P \in \mathbb{Q}[X]$ [Lenstra, 1984]

1: compute an approximation $\tilde{x}$ of a solution $x \in \mathbb{C}$ (Newton's method)

2: guess the minimal polynomial $m_x \in \mathbb{Q}[X]$ from $\tilde{x}$ (LLL algorithm)

3: check that m_x divides P (Euclidean division)

Factorization of a reducible operator $L \in \mathcal{F}\langle\partial\rangle$ where $\mathcal{F} = \overline{\mathbb{Q}}(z)$

1: compute an approximation $\tilde{y}$ of a solution $y \in \overline{\mathbb{Q}}[[z - z_0]]$
(differential equation $\leftrightarrow$ recurrence relation on coefficients)

2: guess the minimal operator $m_y \in \overline{\mathbb{Q}}[z]\langle\partial\rangle$ from $\tilde{y}$
(Hermite–Padé approximants)

3: check that m_y divides L in $\overline{\mathbb{Q}}(z)\langle\partial\rangle$ (right-Euclidean division) approximation → guessing → post-certification

Factorization of a reducible **polynomial** $P \in \mathbb{Q}[X]$ [Lenstra, 1984]

1: compute an approximation $\tilde{x}$ of a solution $x \in \mathbb{C}$ (Newton's method)

2: guess the minimal polynomial $m_x \in \mathbb{Q}[X]$ from $\tilde{x}$ (LLL algorithm)

3: check that m_x divides P (Euclidean division)

Factorization of a reducible **operator** $L \in \mathcal{F}\langle\partial\rangle$ where $\mathcal{F} = \overline{\mathbb{Q}}(z)$

1: compute an approximation $\tilde{y}$ of a solution $y \in \overline{\mathbb{Q}}[[z - z_0]]$
(differential equation ↔ recurrence relation on coefficients)

if y is not well-chosen then $m_y = L$ ☹

2: guess the minimal operator $m_y \in \overline{\mathbb{Q}}[z]\langle\partial\rangle$ from $\tilde{y}$
(Hermite–Padé approximants)

3: check that m_y divides L in $\overline{\mathbb{Q}}(z)\langle\partial\rangle$ (right-Euclidean division)

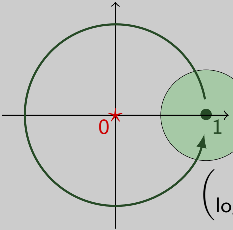
polynomial $P \in \mathbb{Q}[X]$	operator $L \in \mathcal{F}\langle\partial\rangle$
degree d	order n
d roots $x_1, \dots, x_d \in \overline{\mathbb{Q}}$ counted with multiplicity	n linearly independent solutions $y_1, \dots, y_n \in \overline{\mathbb{Q}}[[z - z_0]]$
splitting field $\mathbb{L} = \mathbb{Q}(x_i)$	Picard–Vessiot extension $\mathcal{E} = \mathcal{F}(y_i)$
$\mathrm{Gal}(P) := \mathrm{Aut}\,(\mathbb{L}/\mathbb{Q})$	$\mathrm{Gal_{diff}}(L) := \left\{ \begin{matrix} \sigma \in \mathrm{Aut}(\mathcal{E}/\mathcal{F}) \\ \text{s.t. } \sigma \circ \partial = \partial \circ \sigma \end{matrix} \right\}$

linear left action of $\mathrm{Gal_{diff}}(L)$
on $\mathrm{Sol}(L) = \{f \in \mathcal{E} \mid L \cdot f = 0\}$

Proposition. There is a one-to-one correspondance:

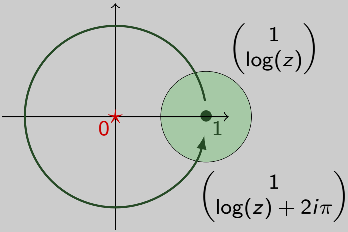
$$L = L_1 L_2 \quad \xleftrightarrow[V = \mathrm{Ker}(L_2)]{} \quad \text{subspace } V \text{ invariant under the action of the differential Galois group}$$

Example: $L = z\partial^2 + \partial$



$$\underbrace{\begin{pmatrix} 1 & 0 \\ 2i\pi & 1 \end{pmatrix}}_{\text{monodromy of } L \text{ around the singularity } 0} \begin{pmatrix} 1 \\ \log(z) \end{pmatrix} = \begin{pmatrix} 1 \\ \log(z) + 2i\pi \end{pmatrix}$$

Example: $L = z\partial^2 + \partial$



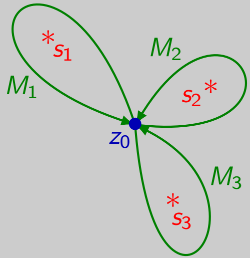
$$\underbrace{\begin{pmatrix} 1 & 0 \\ 2i\pi & 1 \end{pmatrix}}_{\text{monodromy of } L \text{ around the singularity } 0} \begin{pmatrix} 1 \\ \log(z) \end{pmatrix} = \begin{pmatrix} 1 \\ \log(z) + 2i\pi \end{pmatrix}$$

Theorem. [Schlesinger, 1885]
Let $L \in \mathcal{F}\langle\partial\rangle$ be an operator.
If L is *Fuchsian* then $\mathrm{Gal}_{\mathrm{diff}}(L)$ is the Zariski-closure of the group generated by the monodromy matrices of L (with a fixed base-point).

- How to check the Fuchsianity of L?
  $\rightarrow$ Fuchs' Criterion [Fuchs, 1866]

- What if L is not Fuchsian?
  $\rightarrow$ add exponential matrices and Stokes's matrices [Ramis, 1985]

If L is Fuchsian:
$L = L_1 L_2 \longleftrightarrow$ subspace V invariant under the action of the the monodromy matrices



$L \in \overline{\mathbb{Q}}(z)\langle\partial\rangle$ with singularities $s_1, \ldots, s_r$

↓

monodromy matrices $M_1, \ldots, M_r \in \mathrm{Mat}_n(\mathbb{C})$

→ a non-trivial subspace $V \subset \mathrm{Sol}(L)$ invariant under the action of the M_i's

↓

$L_2 \in \overline{\mathbb{Q}}(z)\langle\partial\rangle$ a minimal annihilator of a non-zero $f \in V$

↓

$L = L_1 L_2$

→ no non-trivial subspace of $\mathrm{Sol}(L)$ is invariant under the action of the M_i's

↓

L is irreducible

Let $\mathcal{M} = \{M_1, \ldots, M_r\} \subset \mathrm{Mat}_n(\mathbb{C})$ be a finite list of matrices.

- $\mathcal{A} := \mathbb{C}[\mathcal{M}]$, the algebra of non-commutative polynomials in the M_i's
- $\mathrm{Orb}_{\mathcal{M}}(v) := \{Mv\,;\ M \in \mathcal{A}\}$, the orbit of v under the action of $\mathcal{M}$

Algorithm `Orbit`$(\mathcal{M}, v)$

Input: a list $\mathcal{M} = \{M_1, \ldots, M_r\} \subset \mathrm{Mat}_n(\mathbb{C})$ *and* $v \in \mathbb{C}^n$
Output: the orbit of v under the action of the M_i's

Proposition. There is a non-trivial $\mathcal{M}$-invariant subspace $V \subset \mathbb{C}^n$ iff there is a non-zero vector $v \in \mathbb{C}^n$ such that $\mathrm{Orb}_{\mathcal{M}}(v) \subsetneq \mathbb{C}^n$.

Proposition [van der Hoeven, 2007]. Let $(v_1, ..., v_n)$ be a basis of $\mathbb{C}^n$ such that the projection maps onto the $\mathbb{C}v_i$'s belong to $\mathcal{A}$. Then there is a non-trivial $\mathcal{M}$-invariant subspace $V \subset \mathbb{C}^n$ iff there is an index i such that $\mathrm{Orb}_{\mathcal{M}}(v_i) \subsetneq \mathbb{C}^n$.

Remark. Let $M \in \mathcal{A}$. Denote by $\lambda_1, \ldots, \lambda_k$ the eigenvalues, with multiplicities $m_1, \ldots, m_k$, of M. For each j, the projection map onto the generalized eigenspace $E_j := \mathrm{Ker}\left((M - \lambda_j I_n)^{m_j}\right)$ is polynomial in M (therefore it belongs to $\mathcal{A}$).

Lemma 1. Assume that there is no non-trivial $\mathcal{M}$-invariant subspace. Then there is an $M \in \mathcal{A}$ with exactly n eigenvalues.

Lemma 2. Consider $N_1, \ldots, N_s \in \mathrm{Mat}_n(\mathbb{C})$ and take a random linear combination $N \in \mathrm{Span}_{\mathbb{C}}(N_1, \ldots, N_s)$.
With probability 1, the number of eigenvalues of N is maximal.

Algorithm `Invariant_Subspace`($\mathcal{M}$)

Input: a list $\mathcal{M} = \{M_1, \ldots, M_r\} \subset \mathrm{Mat}_n(\mathbb{C})$

Output: a non-trivial $\mathcal{M}$-invariant subspace *or* `None`

take a random $M \in \mathcal{A} := \mathbb{C}[\mathcal{M}]$
for each 1-dimensional generalized eigenspace E of M *do*
    if $\mathrm{Orbit}(\mathcal{M}, E) \neq \mathbb{C}^n$ *then*
        return $\mathrm{Orbit}(\mathcal{M}, E)$
if all the generalized eigenspaces of M are 1-dimensional *then*
    return `None`
else
    take a generalized eigenspace E of M of dimension > 1
    select $v \in E$ such that $\mathrm{Orbit}(\mathcal{M}, v) \neq \mathbb{C}^n$ *(/* (details hidden) */)*
    return $\mathrm{Orbit}(\mathcal{M}, v)$

Implementation of operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}$, ... on intervals in such a way that the following invariant is respected.

Motto

The interval contains the exact value.

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

Difficulties

- Overestimation
- Testing nullity

Extensions

- Complex numbers
- Vectors, matrices

Interval version of the algorithm for computing an invariant subspace

rigorous output

Algorithm `Invariant_Subspace`($\mathcal{M}$)

Input: a list $\mathcal{M} = \{\boldsymbol{M}_1, \ldots, \boldsymbol{M}_r\} \subset \mathrm{Mat}_n(\boldsymbol{C})$

Output: a non-trivial $\mathcal{M}$-invariant subspace *or* `None` *or* `Fail`

1: take a random $\boldsymbol{M} \in \mathcal{A} := \boldsymbol{C}[\mathcal{M}]$

2: *for* each 1-dimensional generalized eigenspace $\boldsymbol{E}$ of $\boldsymbol{M}$ *do* /* *can* `Fail` */

3: *if* $\mathrm{Orbit}(\mathcal{M}, \boldsymbol{E}) \neq \boldsymbol{C}^n$ *then*

4: return $\mathrm{Orbit}(\mathcal{M}, \boldsymbol{E})$

5: *if* all the generalized eigenspaces of $\boldsymbol{M}$ are 1-dimensional *then*

6: return `None`

7: *else*

8: take a generalized eigenspace $\boldsymbol{E}$ of $\boldsymbol{M}$ of dimension > 1

9: select $\boldsymbol{v} \in \boldsymbol{E}$ such that $\mathrm{Orbit}(\mathcal{M}, \boldsymbol{v}) \neq \boldsymbol{C}^n$ /* *can* `Fail` (details hidden) */

10: return $\mathrm{Orbit}(\mathcal{M}, \boldsymbol{v})$

Symbolic-numeric factorization [van der Hoeven, 2007]

Algorithm `Right_`∂`Factor`(L)

Input: a Fuchsian operator $L \in \overline{\mathbb{Q}}(z)\langle\partial\rangle$
Output: a non-trivial right factor $\in \overline{\mathbb{Q}}(z)\langle\partial\rangle$ of L *or* `Irreducible`

loop
    compute $\boldsymbol{\mathcal{M}} = \{\boldsymbol{M}_1, \ldots, \boldsymbol{M}_r\}$ the monodromy matrices by approximations with rigorous error bounds
    $\boldsymbol{V}$ = `Invariant_Subspace`$(\boldsymbol{\mathcal{M}})$
    if $\boldsymbol{V}$ is `Fail` *then*
        increase precision
    else-if $\boldsymbol{V}$ is `None` *then*
        return `Irreducible`
    else
        guess a candidate operator L_2 from $\boldsymbol{V}$
        if L_2 divides L *then*
            return L_2
        else
            increase precision and order of truncation

In SageMath system, source available at
https://github.com/a-goyer/diffop_factorization.

Main functions

- `InvSub` (interval version, with rigorous `None`)
- `right_dfactor`, `dfactor`
- and the structure `ComplexOptimisticField`

The code takes advantage of:

- `ore_algebra` package, in particular the subpackage `analytic` for arbitrary-precision monodromy computation (https://github.com/mkauers/ore_algebra)
- Arb library (https://arblib.org/)
- some Sage functions (the method `.minimal_approximant_basis` of polynomial matrices for Hermite–Padé approximation, . . .)

operator	order	DEtools (*)	diffop_factorization
fcc3 (**)	3	0.182s	0.148s
fcc4 (**)	4	0.630s	1.32s
fcc5 (**)	6	61.9s	**12.9s**
fcc6 (**)	8	>10h	**432s**
lclm(fcc3, fcc4)	7	66.6s	98.0s
fcc4 × fcc3	7	**1.88s**	31.5s
fcc3 × fcc4	7	**4.59s**	24.8s
fcc4^2	8	122.s	108.s
random4 × fcc3	7	**2.04s**	169.s
random4 × random3	7	**2.40s**	404.s
$(z^2\partial + 3)((z-3)\partial + 4z^5)$	2	>10h	**1.96s**

(*) command DFactor of the Maple package DEtools (author: van Hoeij)
(**) http://koutschan.de/data/fcc1/ (probabilistic walks)

Thank you for listening!

Summary

- an implementation of van der Hoeven's algorithm for factorization of operators is now available! ☺
- confirmation that symbolic-numeric approach can compete with purely symbolic approach!
- detailed proofs of correction of the irreducible case

Remaining work and outlook

- study the theoretical complexity
- non-Fuchsian case
- algebraic/exponential/liouvillian solutions