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

Journées Nationales de Calcul Formel

March 1, 2021

Linear differential operators

Object of study. Assume that $a_i \in \mathcal{F} := \mathbb{K}(z)$ with $\mathbb{K} \subset \mathbb{C}$.

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

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

$$L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathcal{F}\langle\partial\rangle$$

is a *linear differential operator*.

Linear differential operators

Object of study. Assume that $a_i \in \mathcal{F} := \mathbb{K}(z)$ with $\mathbb{K} \subset \mathbb{C}$.

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

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

$$L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathcal{F}\langle\partial\rangle$$

is a *linear differential operator*.

Commutation rule. $\partial z = z\partial + 1$ (Leibniz: $(zf)' = zf' + f$)

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 $\to$ global")

Improvements of Beke's algorithm

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

- **2004**: Cluzeau, van Hoeij (modular algorithm)
- **2007**: van der Hoeven (symbolic-numeric algorithm)

Complexity analysis (bounds on coefficients):

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

Symbolic-numeric algorithms

Factorization of a 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: prove that m_x divides P (Euclidean division)

Factorization of an operator $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}[z]\langle\partial\rangle$

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

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

3: prove that m_y divides L (Right-Euclidean division)

Symbolic-numeric algorithms

Factorization of a 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: prove that m_x divides P (Euclidean division)

Factorization of an operator $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}[z]\langle\partial\rangle$

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

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

3: prove that m_y divides L (Right-Euclidean division)

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

Differential Galois group [Singer, van der Put, 2003]

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

linear left action of $\mathrm{Gal}_{\mathrm{diff}}(L)$
on $\mathrm{Ker}(L) := \{f \in \mathcal{E} \mid L \cdot f = 0\}$

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

Differential Galois group

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

linear left action of $\mathrm{Gal}_{\mathrm{diff}}(L)$
on $\mathrm{Ker}(L) := \{f \in \mathcal{E} \mid L \cdot f = 0\}$

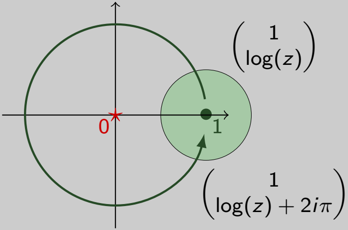
Theorem. $\mathrm{Gal}_{\mathrm{diff}}(L)$ is a linear algebraic group.

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

$L = L_1 L_2$ ⟷ subspaces V invariant under the action of the differential Galois group, via $V = \mathrm{Ker}(L_2)$

Monodromy

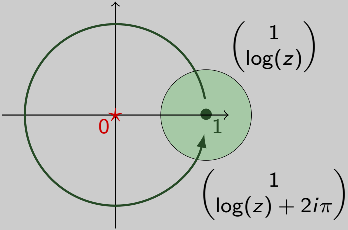
Example: $L = z\partial^2 + \partial$



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

monodromy of L around the singularity 0

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



$$\underbrace{\begin{pmatrix} 1 & 0 \\ 2i\pi & 1 \end{pmatrix}} \begin{pmatrix} 1 \\ \log(z) \end{pmatrix} = \begin{pmatrix} 1 \\ \log(z) + 2i\pi \end{pmatrix}$$

monodromy of L around the singularity 0

Theorem. [Schlesinger, 1885]
Let $L \in \mathcal{F}\langle\partial\rangle$ be a operator. If L is regular 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 regularity of L?
  $\rightarrow$ Fuchs' Criterion [Fuchs, 1866]

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

Symbolic-numeric factorization [van der Hoeven, 2007]

Under regularity assumption:

$L = L_1 L_2$ ⟷ subspaces V invariant under the action of the the monodromy matrices

$V = \mathrm{Ker}(L_2)$

Algorithm Right_Factor(L)

INPUT: a regular operator $L \in \mathcal{F}\langle\partial\rangle$

OUTPUT: a non-trivial right factor $\in \mathcal{F}\langle\partial\rangle$ of L **or** `Irreducible`

```
loop
    compute M = {M_1, ..., M_r} the monodromy matrices by
    approximations with rigorous error bounds
    V = Invariant_Subspace(M)
    if V is Fail then increase precision
    else
        if V is None then return Irreducible
        else
            guess a candidate operator L_2 from V
            if L_2 divides L then return L_2
            else increase precision and order of truncature
```

Algorithm Orbit($\mathcal{M}, E$)

INPUT: a list $\mathcal{M} = \{M_1, \ldots, M_r\} \subset \mathrm{Mat}_n(\mathbb{C})$ **and** $E \subset \mathbb{C}^n$
OUTPUT: the orbit of E under the action of $\mathbb{C}[M_1, \ldots, M_r]$

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` **or** `Fail`

1: take at random an $M \in \mathbb{C}[M_1, \ldots, M_r]$
2: **for** each generalized eigenspace E of M **do** */* computation of E can* `Fail` **/*
3: **if** Orbit($\mathcal{M}, E$) $\neq \mathbb{C}^n$ **then** return Orbit($\mathcal{M}, E$)
4: **if** all the generalized eigenspaces of M are 1-dimensional **then** return `None`
5: **else**
6: take E a generalized eigenspace of M of dimension > 1
7: select $v \in E$ such that Orbit($\mathcal{M}, \{v\}$) $\neq \mathbb{C}^n$ */* can* `Fail` *(details hidden) */*
8: return Orbit($\mathcal{M}, \{v\}$)

Runtime comparison

Operator	Order	van Hoeij (Maple)	my implementation of van der Hoeven (SageMath)	
			total	monodromy
L of demo	5	206s	9.34s	6.19s
fcc3 (*)	3	0.15s	0.28s	0.26s
fcc4 (*)	4	0.76s	0.96s	0.94s
fcc5 (*)	6	57.7s	3.94s	3.90s
fcc6 (*)	8	>4h	37.5s	37.4s
$P[1, 0, 0, \text{'xy'}]$ (**)	3	0.16s	0.53s	0.47s
$P[19, 0, 0, \text{'xy'}]$ (**)	4	4.58s	2.73s	2.36s
$(z^2\partial + 3)((z-3)\partial + 4z^5)$	2	>4h	110.9s	110.8s

(*) http://koutschan.de/data/fcc1/ (Probabilist walks)

(**) https://specfun.inria.fr/chyzak/ssw/ (Combinatorial walks)

Thank you for listening!

Summary

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

Remaining work and perspectives

- more efficient computation of monodromy matrices
- numerically-stable computation of Hermite-Padé approximants
- study the theoretical complexity
- Non-regular case
- algebraic/exponential/liouvillian solutions
- Differential Galois group or its Lie algebra