Symbolic-Numeric Factorization of Linear Differential Operators

Alexandre Goyer

co-supervised by

Frédéric Chyzak and Marc Mezzarobba

SpecFun/PolSys seminar

December 6, 2020

The topic

Object of study:

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

with $a_i \in \mathbb{K}(z)$ and $\mathbb{K} \subset \mathbb{C}$ algebraically closed.

Formalism: y solution of $(E) \Leftrightarrow L \cdot y = 0$
with $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (differential operator)

The topic

Object of study:

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

with $a_i \in \mathbb{K}(z)$ and $\mathbb{K} \subset \mathbb{C}$ algebraically closed.

Formalism: y solution of $(E) \Leftrightarrow L \cdot y = 0$
with $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (differential operator)

Definition: *Factoring a differential operator* L means writing it as the composition $L = L_1L_2$ of two operators of smaller orders.

Example:

$$4z^3\partial^3 + 20z^2\partial^2 + 17z\partial + 1 = (2z^2\partial^2 + 5z\partial + 1)(2z\partial + 1)$$

Object of study:

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

with $a_i \in \mathbb{K}(z)$ and $\mathbb{K} \subset \mathbb{C}$ algebraically closed.

Formalism: y solution of $(E) \Leftrightarrow L \cdot y = 0$
with $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (differential operator)

Definition: *Factoring a differential operator* L means writing it as the composition $L = L_1 L_2$ of two operators of smaller orders.

Example:

$$4z^3\partial^3 + 20z^2\partial^2 + 17z\partial + 1 = (2z^2\partial^2 + 5z\partial + 1)(2z\partial + 1)$$

$$\boxed{\partial z = z\partial + 1}$$

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

Contents

I. Van der Hoeven's algorithm, forgetting round-off errors

$\nearrow \mathcal{F} := \mathbb{K}(z)$

polynomial $P \in \boldsymbol{k}[X]$	differential operator $L \in \mathcal{F}\langle\partial\rangle$
splitting field $\boldsymbol{K}$	Picard-Vessiot extension $\mathcal{E}$
$\mathrm{Gal}(\boldsymbol{K}/\boldsymbol{k}) = \left\{ \begin{matrix} \sigma \in \mathrm{Aut}(\boldsymbol{K}) \text{ such that} \\ \forall x \in \boldsymbol{k}, \sigma(x) = x \end{matrix} \right\}$	$\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F}) = \left\{ \begin{matrix} \sigma \in \mathrm{Aut}(\mathcal{E}) \text{ such that} \\ \forall f \in \mathcal{F}, \sigma(f) = f \\ \forall f \in \mathcal{E}, \sigma(f') = \sigma(f)' \end{matrix} \right\}$
Galois group	differential Galois group

$\mathrm{Ker}(L) := \{f \in \mathcal{E} \mid L \cdot f = 0\}$ vector space of dimension $n = \mathrm{ord}(L)$

Goal: linear left action of the group $\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F})$ on $\mathrm{Ker}(L)$.

Ref.: van der Put, Singer. *Galois theory of linear differential equations*, 2003

The differential Galois group

$\mathcal{F} := \mathbb{K}(z)$

polynomial $P \in \boldsymbol{k}[X]$	differential operator $L \in \mathcal{F}\langle\partial\rangle$
splitting field $\boldsymbol{K}$	Picard-Vessiot extension $\mathcal{E}$
$\mathrm{Gal}(\boldsymbol{K}/\boldsymbol{k}) = \left\{ \begin{smallmatrix} \sigma\in\mathrm{Aut}(\boldsymbol{K}) \text{ such that} \\ \forall x\in\boldsymbol{k}, \sigma(x)=x \end{smallmatrix} \right\}$	$\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F}) = \left\{ \begin{smallmatrix} \sigma\in\mathrm{Aut}(\mathcal{E}) \text{ such that} \\ \forall f\in\mathcal{F}, \sigma(f)=f \\ \forall f\in\mathcal{E}, \sigma(f')=\sigma(f)' \end{smallmatrix} \right\}$
Galois group	differential Galois group

$\mathrm{Ker}(L) := \{f \in \mathcal{E} \mid L \cdot f = 0\}$ vector space of dimension $n = \mathrm{ord}(L)$

Goal: linear left action of the group $\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F})$ on $\mathrm{Ker}(L)$.

Notation: $\mathrm{Gal}_{\mathrm{diff}}(L, h) :=$ the representation in $\mathrm{GL}_n(\mathbb{C})$ of this action with respect to a basis $h = (h_1, \ldots, h_n)$ of solutions of L.

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

Ref.: van der Put, Singer. *Galois theory of linear differential equations*, 2003

Lemma: Let G be a Zariski-dense subset of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$.
A subspace of $\mathbb{C}^n$ is invariant under the action of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ iff it is invariant under the action of G.

Proposition: There is an one-to-one correspondence.

$L = L_1 L_2$	$\longleftrightarrow$ $V = \mathrm{Ker}(L_2)$ $= \{f \in \mathcal{E} \mid L_2 \cdot f = 0\}$	subspaces V invariant under the action of the differential Galois group

Ref.: Magid. *Lectures on differential galois theory*, 1994
van der Put, Singer. *Galois theory of linear differential equations*, 2003

Factorization and differential Galois group

Lemma: Let G be a Zariski-dense subset of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$.
A subspace of $\mathbb{C}^n$ is invariant under the action of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ iff it is invariant under the action of G.

Proposition: There is an one-to-one correspondence.

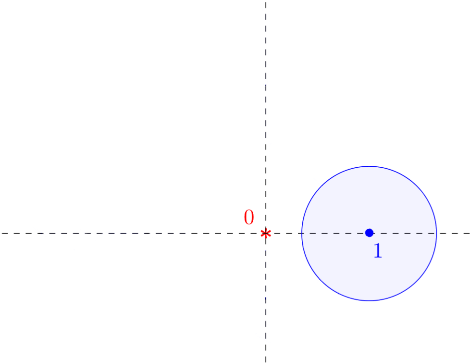
$L = L_1 L_2$	$\longleftrightarrow$ $V = \mathrm{Ker}(L_2)$ $= \{f \in \mathcal{E} \mid L_2 \cdot f = 0\}$	subspaces V invariant under the action of the differential Galois group

Corollary: Assume that $M_1, \ldots, M_r \in \mathrm{GL}_n(\mathbb{C})$ generate a Zariski-dense subgroup of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$. Then L admits a factorization iff there exists a subspace V invariant under the action of M_i.

Ref.: Magid. *Lectures on differential galois theory*, 1994
van der Put, Singer. *Galois theory of linear differential equations*, 2003

Example: $L = \partial^2 + \frac{1}{z}\partial$

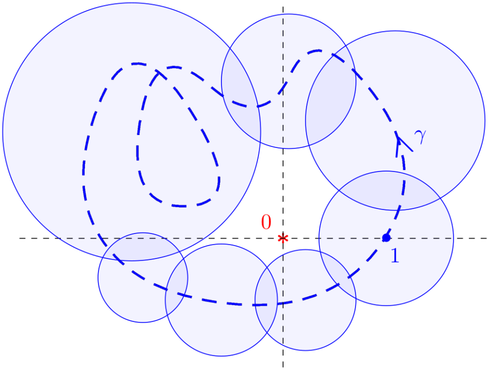
$h = (1, \log(z))$ basis of solutions of L



Ref. : Mitschi, Sauzin. *Divergent series, summability and resurgence I*, 2016

Example: $L = \partial^2 + \frac{1}{z}\partial$

$h = (1, \log(z))$ basis of solutions of L



Ref. : Mitschi, Sauzin. *Divergent series, summability and resurgence I*, 2016

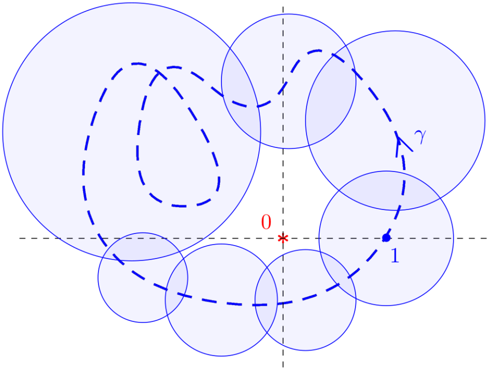
Monodromy

Example: $L = \partial^2 + \frac{1}{z}\partial$

$h = (1, \log(z))$ basis of solutions of L

$$h \xrightarrow{\gamma} g$$

$$g = (1, \log(z) + 2i\pi)$$



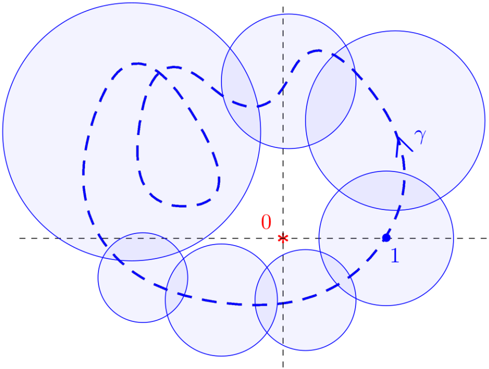
Ref. : Mitschi, Sauzin. *Divergent series, summability and resurgence I*, 2016

Example: $L = \partial^2 + \frac{1}{z}\partial$

$h = (1, \log(z))$ basis of solutions of L

$$h \xrightarrow{\gamma} g$$

$$g = (1, \log(z) + 2i\pi)$$



$$\begin{pmatrix} g_1(1) & g_2(1) \\ g_1'(1) & g_2'(1) \end{pmatrix} = \begin{pmatrix} h_1(1) & h_2(1) \\ h_1'(1) & h_2'(1) \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 2i\pi \\ 0 & 1 \end{pmatrix}}_{\substack{\text{monodromy around 0, based in 1,} \\ \text{with respect to the basis } (1, \log(z))}}$$

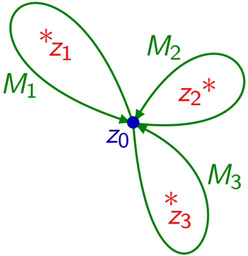
Ref. : Mitschi, Sauzin. *Divergent series, summability and resurgence I*, 2016

A density theorem

Theorem: [Schlesinger, 1895]

- L regular linear differential operator
- $z_1, \ldots, z_r$ singular points of L
- h basis of solutions analytic at $z_0 \in \mathbb{C} \backslash \{z_1, \ldots, z_r\}$
- M_i monodromy around z_i based in z_0 and w.r.t. h

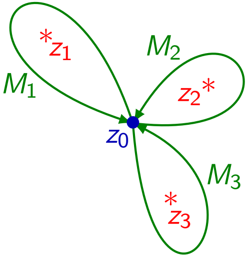
The subgroup of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ generated by $M_1, \ldots, M_r$ is Zariski-dense.



Theorem: [Schlesinger, 1895]

- L **regular** linear differential operator
- $z_1, \ldots, z_r$ singular points of L
- h basis of solutions analytic at $z_0 \in \mathbb{C} \setminus \{z_1, \ldots, z_r\}$
- M_i monodromy around z_i based in z_0 and w.r.t. h

The subgroup of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ generated by $M_1, \ldots, M_r$ is Zariski-dense.

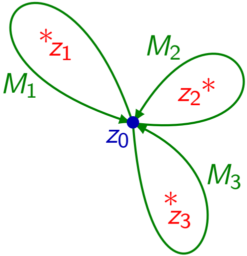


- How to check the regularity of L?
  $\rightarrow$ Fuchs' Criterion [Fuchs, 1866]
- What if L is not regular?
  $\rightarrow$ add exponential matrices and Stokes's matrices [Ramis, 1985]

Theorem: [Schlesinger, 1895]

- L **regular** linear differential operator
- $z_1, \dots, z_r$ singular points of L
- h basis of solutions analytic at $z_0 \in \mathbb{C} \setminus \{z_1, \dots, z_r\}$
- M_i monodromy around z_i based in z_0 and w.r.t. h

The subgroup of $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ generated by $M_1, \dots, M_r$ is Zariski-dense.



Algorithm for factorization (simple version)

Conclusion of the previous considerations

L admits a factorization iff there exists a subspace of $\mathbb{K}^n$ which is invariant under the action of the monodromy matrices.

INPUT: a regular linear differential operator L
OUTPUT: a right-hand factor of L or `None`

1) Compute the monodromy matrices $\mathcal{M} = \{M_1, \ldots, M_r\}$ of L
2) Search for a nontrivial $\mathcal{M}$-invariant subspace:
   IF "no such subspace exists": return `None`
   ELSE: compute a basis B of such a subspace
3) Compute a right-hand factor L_2 from B
4) Return L_2

Algorithm for factorization (simple version)

Conclusion of the previous considerations

L admits a factorization iff there exists a subspace of $\mathbb{K}^n$ which is invariant under the action of the monodromy matrices.

INPUT: a regular linear differential operator L
OUTPUT: a right-hand factor of L or `None`

1) Compute the monodromy matrices $\mathcal{M} = \{M_1, \ldots, M_r\}$ of L
2) Search for a nontrivial $\mathcal{M}$-invariant subspace:
   IF "no such subspace exists": return `None`
   ELSE: compute a basis B of such a subspace
3) Compute a right-hand factor L_2 from B
4) Return L_2

$\mathrm{Vect}(B) = \mathrm{Ker}\,(L_2)$

Ensuring the irreducibility

Data: $\mathcal{M} = \{M_1, \dots, M_r\} \subset \mathrm{Mat}_n(\mathbb{C})$

Definition: Let $v \in \mathbb{C}^n$. We denote by $\mathrm{Inv}_{\mathcal{M}}(v)$ the smallest $\mathcal{M}$-invariant subspace containing v.

Lemma: There exists a nontrivial $\mathcal{M}$-invariant subspace V iff there exists a nonzero vector $v \in \mathbb{C}^n$ such that $\mathrm{Inv}_{\mathcal{M}}(v) \subsetneq \mathbb{C}^n$.

Proposition: [van der Hoeven, 2007]
Let $(v_1, \dots, v_n)$ be a basis of $\mathbb{C}^n$ such that:

- for each i, the coordinate projection $\mathbb{C}^n \to \mathbb{C}v_i$ can be written as a polynomial in the matrices of $\mathcal{M}$,
- for each i, $\mathrm{Inv}_{\mathcal{M}}(v_i) \subsetneq \mathbb{C}^n$.

Then there exists no nontrivial $\mathcal{M}$-invariant subspace.

Computation of invariant subspace by saturation

How to compute a basis B of $\mathrm{Inv}_{\mathcal{M}}(v)$?

Start with $B = (v)$.
Until saturation:

- add to B the vectors Mu for all $M \in \mathcal{M}$ and all $u \in B$
- reduce B

Reduce = keep only a linearly independent sequence of vectors

Example: (Gaussian elimination)

$$\begin{pmatrix} 22 & 3 & 36 & -11 \\ -8 & -1 & -13 & 4 \\ -18 & -3 & -30 & 9 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & -2 & -3 \end{pmatrix}$$

II. How to manage the round-off errors?

Manipulating numbers on a machine

Exact representations ($\rightarrow$ symbolic computation)

Rational numbers, algebraic numbers, effective numbers, ...

Approximated representations ($\rightarrow$ numerical computation)

Floating-point numbers, intervals, ...

Manipulating numbers on a machine

Exact representations ($\rightarrow$ symbolic computation)

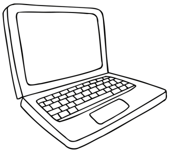
Rational numbers, algebraic numbers, effective numbers, ...

Examples: $e = \sum_{n=0}^{+\infty} \frac{1}{n!}$, $\pi = 4\sum_{n=0}^{+\infty} \frac{(-1)^n}{2n+1}$, $\log(2) = \sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n}$, $f(z_1)$ where f satisfies a linear ODE and initial conditions at z_0.

Approximated representations ($\rightarrow$ numerical computation)

Floating-point numbers, intervals, ...

What do I mean by “symbolic-numeric algorithm”?



INPUT: exact data

computation with **approximated** numbers

OUTPUT: rigorous mathematical statement

How is it possible to achieve such a result?

1) bounding round-off errors + mathematical argument

   Example: computation of $\frac{1}{2i\pi} \oint \frac{f'(z)}{f(z)} dz$ (residue theorem)

2) guessing + checking the result

   Example: see next slide

Let $L = L_1 L_2$ be a nontrivial factorization.
Write $L_2 = a_s\partial^s + \cdots + a_1\partial + a_0$ with $a_i \in \overline{\mathbb{Q}}(z)$.

VdH's algorithm computes approximations $\tilde{a}_i \in {\mathbb{C}^{\approx_\epsilon}}_{\le T}[[z]]$ of the a_i with an arbitrary precision.

GUESSING: $\tilde{a}_i \to$ candidate for a_i

- Hermite-Padé approximants: ${\mathbb{C}^{\approx}}_{\le}[[z]] \to \mathbb{C}^{\approx}(z)$
- LLL algorithm: $\mathbb{C}^{\approx}(z) \to \overline{\mathbb{Q}}(z)$

CHECKING: $L_2 = a_s\partial^s + \cdots + a_1\partial + a_0$ divides L?

- Right Euclidean division in $\overline{\mathbb{Q}}(z)\langle\partial\rangle$

What if that fails? Restart with $\epsilon = \epsilon^2$ and $T = 2T$.

Algorithm for factorization (with approximations)

INPUT: a regular linear differential operator $L \in \mathbb{K}(z)\langle\partial\rangle$
OUTPUT: a right-hand factor of L or `None`

1) Compute approximations $\tilde{\mathcal{M}} = \{\tilde{M}_1, \ldots, \tilde{M}_r\}$ of the monodromy matrices of L
2) Search for a nontrivial approximate $\tilde{\mathcal{M}}$-invariant subspace:
   IF "no such subspace exists": **?????**
   ELSE: compute a basis $\tilde{B}$ of such a subspace
3) Compute an approximate right-hand factor $\tilde{L_2}$ from $\tilde{B}$
4) Guess a candidate right-hand factor $L_2 \in \mathbb{K}(z)\langle\partial\rangle$ from $\tilde{L_2}$
5) Check L_2:
   IF "L_2 divides L": return L_2
   ELSE: restart with higher precision

Interval arithmetic [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 $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R} \text{ s.t. } 3.1415 \leq x^2 \leq 3.1416\}$.

Interval arithmetic [Moore, 1962]

Implementing basic operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}, \dots$ 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 $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R} \text{ s.t. } 3.1415 \leq x^2 \leq 3.1416\}$.

Difficulties

- Overestimation
- Testing the nullity

Interval arithmetic [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 $\sqrt{\boldsymbol{\pi}} \supset \{x \in \mathbb{R} \text{ s.t. } 3.1415 \leq x^2 \leq 3.1416\}$.

Difficulties

- Overestimation
- Testing the nullity

Extensions

- Complex numbers
- Vectors, matrices

Definition:

A sequence of interval vectors $(\boldsymbol{v_1}, \ldots, \boldsymbol{v_s})$ is *linearly independent* if: $\forall v_1 \in \boldsymbol{v_1}, \ldots, \forall v_s \in \boldsymbol{v_s}$, $(v_1, \ldots, v_s)$ is linearly independant.

Algorithm for factorization (with interval arithmetic)

INPUT: a regular linear differential operator $L \in \mathbb{K}(z)\langle\partial\rangle$
OUTPUT: a right-hand factor of L or `None`

1) Compute interval matrices $\mathcal{M} = \{\boldsymbol{M_1}, \ldots, \boldsymbol{M_r}\}$ of the monodromy matrices of L
2) Search for a nontrivial $\mathcal{M}$-invariant interval subspace:
   IF "no such subspace exists": return `None`
   ELSE: compute a basis $\boldsymbol{B}$ of such a subspace
3) Compute an approximate right-hand factor $\tilde{L_2}$ from $\tilde{B} \in \boldsymbol{B}$
4) Guess a candidate right-hand factor $L_2 \in \mathbb{K}(z)\langle\partial\rangle$ from $\tilde{L_2}$
5) Check L_2:
   IF "L_2 divides L": return L_2
   ELSE: restart with higher precision

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 pivots $\leq$ rank of the exact matrix

Theorem: Let $\boldsymbol{M}$ be an interval matrix and write $\boldsymbol{R}$ for the result of interval Gaussian elimination (previous slide).
For any $M \in \boldsymbol{M}$, there exists an $P \in \mathrm{GL}_n(\mathbb{C})$ such that $PM \in \boldsymbol{R}$.

Sketch of proof. Let $M \in \boldsymbol{M}$.

$\boldsymbol{M}$		M
Elementary operations driven by the interval coefficients	$\longrightarrow$	Same operations (P representing the sequence of operations)
$\boldsymbol{R}$		$R = PM$

The compliance with the IA principle ensures that $\boldsymbol{R} \ni R$.

Correction for interval invariant subspaces by saturation

Theorem:

- $\boldsymbol{\mathcal{M}} = \{\boldsymbol{M_1}, \ldots, \boldsymbol{M_r}\}$ a list of interval matrices
- $\boldsymbol{v}$ an interval vector
- $\boldsymbol{B} = (\boldsymbol{b_1}, \ldots, \boldsymbol{b_s})$ the basis of the invariant subspace computed in interval arithmetic

Then, for any $\mathcal{M} \in \boldsymbol{\mathcal{M}}$ (*i.e.* $M_i \in \boldsymbol{M_i}$ for each i) and any $v \in \boldsymbol{v}$:

- for each i, $\boldsymbol{b_i}$ contains a vector which belongs to $\mathrm{Inv}_{\mathcal{M}}(v)$
- in particular, if $\boldsymbol{B}$ contains n vectors, then $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$.

Correction for interval invariant subspaces by saturation

Theorem:

- $\boldsymbol{\mathcal{M}} = \{\boldsymbol{M_1}, \ldots, \boldsymbol{M_r}\}$ a list of interval matrices
- $\boldsymbol{v}$ an interval vector
- $\boldsymbol{B} = (\boldsymbol{b_1}, \ldots, \boldsymbol{b_s})$ the basis of the invariant subspace computed in interval arithmetic

Then, for any $\mathcal{M} \in \boldsymbol{\mathcal{M}}$ (*i.e.* $M_i \in \boldsymbol{M_i}$ for each i) and any $v \in \boldsymbol{v}$:

- for each i, $\boldsymbol{b_i}$ contains a vector which belongs to $\mathrm{Inv}_{\mathcal{M}}(v)$
- in particular, if $\boldsymbol{B}$ contains n vectors, then $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$.

Theorem: Given $\mathcal{M}$ and v such that $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$, there exist tight enough $\boldsymbol{\mathcal{M}} \ni \mathcal{M}$ and $\boldsymbol{v} \ni v$ such that $\boldsymbol{B}$ (computed as above) contains n vectors.

(Under reasonable assumptions on the implementation of interval arithmetic)

Ensuring the irreducibility with IA

Denote by $(e_i)_i$ the canonical basis, $(\pi_i)_i$ the coordinate projections.

Context:

- $\mathcal{M} = \{M_1, \dots, M_r\}$ s.t. $\nexists$ nontrivial $\mathcal{M}$-invariant subspace
- $\boldsymbol{\mathcal{M}}$ list of interval matrices corresponding to $\mathcal{M}$
- $\boldsymbol{\pi_i} \ni \pi_i$ computed from $\boldsymbol{\mathcal{M}}$ ($\exists P_i$ s.t. $P_i(\mathcal{M}) \in \boldsymbol{\pi_i}$)

Show that: $\forall v \neq 0$, $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$.

Ensuring the irreducibility with IA

Denote by $(e_i)_i$ the canonical basis, $(\pi_i)_i$ the coordinate projections.

Context:

- $\mathcal{M} = \{M_1, \ldots, M_r\}$ s.t. $\nexists$ nontrivial $\mathcal{M}$-invariant subspace
- $\boldsymbol{\mathcal{M}}$ list of interval matrices corresponding to $\mathcal{M}$
- $\boldsymbol{\pi_i} \ni \pi_i$ computed from $\boldsymbol{\mathcal{M}}$ ($\exists P_i$ s.t. $P_i(\mathcal{M}) \in \boldsymbol{\pi_i}$)

Show that: $\forall v \neq 0$, $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$.
Legitimate assumptions: $||v||_\infty = 1$ and $\pi_i(v) = e_i$ for a certain i.

① $v \xrightarrow{\mathcal{M}} e_i^{\approx}$ ② $e_i^{\approx} \xrightarrow{\mathcal{M}}$ any vector of $\mathbb{C}^n$

Ensuring the irreducibility with IA

Denote by $(e_i)_i$ the canonical basis, $(\pi_i)_i$ the coordinate projections.

Context:

- $\mathcal{M} = \{M_1, \dots, M_r\}$ s.t. $\nexists$ nontrivial $\mathcal{M}$-invariant subspace
- $\boldsymbol{\mathcal{M}}$ list of interval matrices corresponding to $\mathcal{M}$
- $\boldsymbol{\pi_i} \ni \pi_i$ computed from $\boldsymbol{\mathcal{M}}$ ($\exists P_i$ s.t. $P_i(\boldsymbol{\mathcal{M}}) \in \boldsymbol{\pi_i}$)

Show that: $\forall v \neq 0$, $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{C}^n$.
Legitimate assumptions: $||v||_\infty = 1$ and $\pi_i(v) = e_i$ for a certain i.

① $v \xrightarrow{\mathcal{M}} e_i^{\approx}$ ② $e_i^{\approx} \xrightarrow{\mathcal{M}}$ any vector of $\mathbb{C}^n$

① $||P_i(\mathcal{M})v - e_i||_\infty \leq |||P_i(\mathcal{M}) - \pi_i|||_\infty ||v||_\infty \leq \epsilon$
where ϵ is a computed bound for $\max_{M \in \boldsymbol{\pi_i}} |||M - \pi_i|||_\infty$.
② Computation of invariant subspace by saturation from the input data $\boldsymbol{\mathcal{M}}$ and $\boldsymbol{e_i} \supset \mathrm{Ball}_{||.||_\infty}(e_i, \epsilon)$.

Invariant_subspace algorithm

Definition: An $\mathcal{M}$-*splitting* is a decomposition $\mathbb{K}^n = E_1 \oplus \cdots \oplus E_k$ for which the projections $\mathbb{K}^n \to E_i$ can be written as polynomials in $\mathcal{M}$.

Definition: A square matrix N is *monopotent* if $\mathrm{Card}(\mathrm{Sp}(N)) = 1$.

① refine $\mathcal{M}$-splitting w.r.t. $\mathcal{M}$

② for each line $\mathbb{K}v$: $\mathrm{Inv}_{\mathcal{M}}\, v$?

  if only lines: return `None`

③ for a E non-line: compute $K = \bigcap_{M \in \mathcal{M}} \vec{\mathrm{ev}}(M_E)$

$K = 0$ ④

compute $N \in \mathcal{A}$ non mono on E

$\mathcal{M} = \mathcal{M} \cup \{N\} \to$ ①

$K \neq 0$ ⑤

for a $v \in K \backslash \{0\}$: $\mathrm{Inv}_{\mathcal{M}}\, v$?

compute $N \in \mathcal{A} \mid N_E v \notin \mathbb{K}v$

$\mathcal{M} = \mathcal{M} \cup \{N\} \to$ ①