Factorisation symbolique-numérique d'opérateurs différentiels

Alexandre GOYER

Co-encadrement : Frédéric Chyzak (Inria Saclay – Île-de-France)
Marc Mezzarobba (CNRS, Sorbonne Université)

28 septembre 2020

Objet d'étude :

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

avec $a_i \in \mathbb{K}(z)$ où $\mathbb{K} \subset \mathbb{C}$ algébriquement clos

Présentation du sujet

Objet d'étude :

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

avec $a_i \in \mathbb{K}(z)$ où $\mathbb{K} \subset \mathbb{C}$ algébriquement clos

Formalisme : y solution de $(E) \Leftrightarrow L \cdot y = 0$
avec $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (opérateur différentiel)

Objet d'étude :

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

avec $a_i \in \mathbb{K}(z)$ où $\mathbb{K} \subset \mathbb{C}$ algébriquement clos

Formalisme : y solution de $(E) \Leftrightarrow L \cdot y = 0$
avec $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (opérateur différentiel)

Définition : *Factoriser un opérateur différentiel L*, c'est l'écrire comme la composée $L = L_1L_2$ de deux opérateurs d'ordres plus petits.

Exemple :

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

Objet d'étude :

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

avec $a_i \in \mathbb{K}(z)$ où $\mathbb{K} \subset \mathbb{C}$ algébriquement clos

Formalisme : y solution de $(E) \Leftrightarrow L \cdot y = 0$
avec $L = a_n\partial^n + \cdots + a_1\partial + a_0 \in \mathbb{K}(z)\langle\partial\rangle$ (opérateur différentiel)

Définition : *Factoriser un opérateur différentiel* L, c'est l'écrire comme la composée $L = L_1L_2$ de deux opérateurs d'ordres plus petits.

Exemple :

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

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

Factoriser un opérateur différentiel linéaire

- **1894** : Algorithme de Beke (facteur droit d'ordre 1)
- **1996** : Singer (« algorithme de Berlekamp » adapté)
- **1997** : van Hoeij (algorithme de type « local $\to$ global »)
- **2004** : Cluzeau, van Hoeij (algorithme modulaire)
- $\boxed{\textbf{2007} : \text{van der Hoeven (algorithme symbolique-numérique)}}$

Améliorations de l'algorithme de Beke

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

Analyse de la complexité (bornes sur les coefficients) :

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

Le groupe de Galois différentiel

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

polynôme $P \in \boldsymbol{k}[X]$	opérateur différentiel $L \in \mathcal{F}\langle\partial\rangle$
$\boldsymbol{K}$ corps de décomposition	$\mathcal{E}$ extension de Picard-Vessiot
$\mathrm{Gal}(\boldsymbol{K}/\boldsymbol{k}) = \left\{ \begin{array}{c} \sigma\in\mathrm{Aut}(\boldsymbol{K}) \text{ tels que} \\ \forall x\in\boldsymbol{k}, \sigma(x)=x \end{array} \right\}$	$\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F}) = \left\{ \begin{array}{c} \sigma\in\mathrm{Aut}(\mathcal{E}) \text{ tels que} \\ \forall f\in\mathcal{F}, \sigma(f)=f \\ \forall f\in\mathcal{E}, \sigma(f')=\sigma(f)' \end{array} \right\}$
groupe de Galois	groupe de Galois différentiel

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

Le groupe de Galois différentiel

polynôme $P \in \boldsymbol{k}[X]$	opérateur différentiel $L \in \mathcal{F}\langle\partial\rangle$ $\mathcal{F} := \mathbb{K}(z)$
$\boldsymbol{K}$ corps de décomposition	$\mathcal{E}$ extension de Picard-Vessiot
$\mathrm{Gal}(\boldsymbol{K}/\boldsymbol{k}) = \left\{ \begin{matrix} \sigma \in \mathrm{Aut}(\boldsymbol{K}) \text{ tels que} \\ \forall x \in \boldsymbol{k}, \sigma(x) = x \end{matrix} \right\}$	$\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F}) = \left\{ \begin{matrix} \sigma \in \mathrm{Aut}(\mathcal{E}) \text{ tels que} \\ \forall f \in \mathcal{F}, \sigma(f) = f \\ \forall f \in \mathcal{E}, \sigma(f') = \sigma(f)' \end{matrix} \right\}$
groupe de Galois	groupe de Galois différentiel

$\mathrm{Ker}(L) := \{f \in \mathcal{E} \mid L \cdot f = 0\}$ $\mathbb{K}$-e.v. de dimension $n = \mathrm{ord}(L)$
Fait : action linéaire (à gauche) de $\mathrm{Gal}_{\mathrm{diff}}(\mathcal{E}/\mathcal{F})$ sur $\mathrm{Ker}(L)$.

On note $\mathrm{Gal}_{\mathrm{diff}}(L, h) \subset \mathrm{Mat}_n(\mathbb{K})$ la représentation matricielle de cette action relativement à une base $h = (h_1, \dots, h_n)$ de solutions.

Théorème : $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ est un groupe algébrique linéaire.

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

Factorisation et groupe de Galois différentiel

Lemme : Soit G une partie Zariski-dense de $\mathrm{Gal}_{\mathrm{diff}}(L, h)$. Alors, un sous-espace de $\mathbb{K}^n$ est invariant sous l'action de $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ ssi il est invariant sous l'action de G.

Proposition : On a la correspondance bijective suivante.

$$L = L_1 L_2 \xleftrightarrow[\substack{V=\mathrm{Ker}(L_2)\\ =\{f\in\mathcal{E} \mid L_2\cdot f=0\}}]{} \text{sous-espace } V \text{ invariant sous l'action du groupe de Galois différentiel}$$

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

Factorisation et groupe de Galois différentiel

Lemme : Soit G une partie Zariski-dense de $\mathrm{Gal}_{\mathrm{diff}}(L, h)$. Alors, un sous-espace de $\mathbb{K}^n$ est invariant sous l'action de $\mathrm{Gal}_{\mathrm{diff}}(L, h)$ ssi il est invariant sous l'action de G.

Proposition : On a la correspondance bijective suivante.

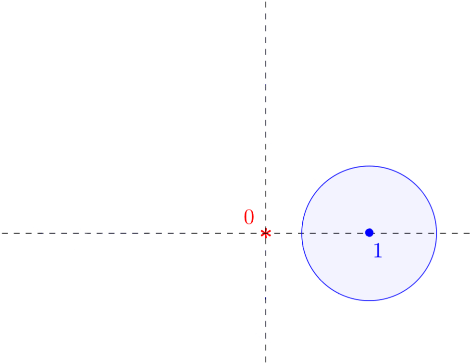
$$L = L_1 L_2 \quad \xleftrightarrow[\substack{V = \mathrm{Ker}(L_2) \\ = \{f \in \mathcal{E} \mid L_2 \cdot f = 0\}}]{} \quad \begin{array}{c}\text{sous-espace } V \text{ invariant} \\ \text{sous l'action du groupe} \\ \text{de Galois différentiel}\end{array}$$

Corollaire : Si $M_1, \ldots, M_r \in \mathrm{GL}_n(\mathbb{K})$ engendrent un sous-groupe Zariski-dense de $\mathrm{Gal}_{\mathrm{diff}}(L, h)$, alors L admet une factorisation ssi il existe un sous-espace V invariant sous l'action des M_i.

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

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

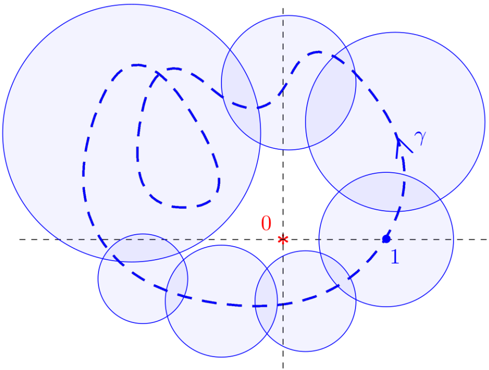
$h = (1, \log(z))$ base de solutions de L



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

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

$h = (1, \log(z))$ base de solutions de L



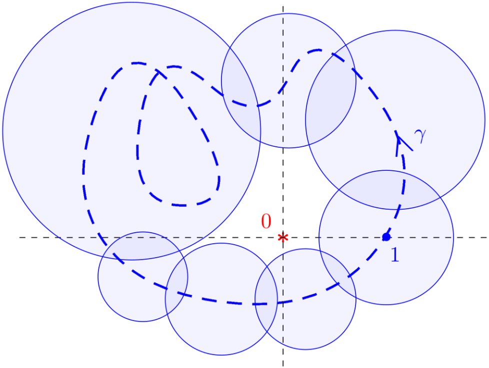
Réf. : Mitschi, Sauzin. *Divergent series, summability and resurgence I*, 2016

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

$h = (1, \log(z))$ base de solutions de L

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

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



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

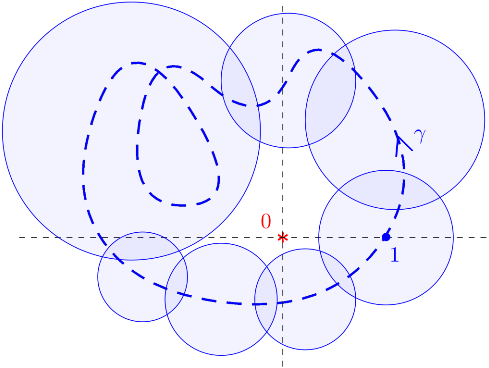
Monodromie

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

$h = (1, \log(z))$ base de solutions de L

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

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



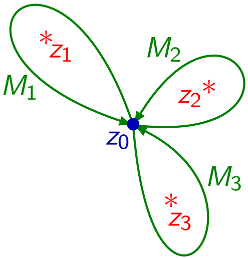
$$\begin{pmatrix} g_1(1) & g_2(1) \\ g_1'(1) & g_2'(1) \end{pmatrix} = \begin{pmatrix} h_1(1) & h_2(1) \\ h_1'(1) & h_2'(1) \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 2i\pi \\ 0 & 1 \end{pmatrix}}_{\substack{\text{matrice de monodromie correspondant à un} \\ \text{tour autour de 0 et basé en 1} \\ \text{relativement à la base } (1, \log(z))}}$$

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

Théorème : [Schlesinger, 1895]

- $L \in \mathbb{K}(z)\langle\partial\rangle$ un opérateur régulier
- $z_1, \ldots, z_r$ points singuliers de L
- h base de solutions analytiques en $z_0 \in \mathbb{C} \setminus \{z_1, \ldots, z_r\}$
- M_i = « monodromie autour de z_i basé en z_0 relativement à h »

Le sous-groupe engendré par $M_1, \ldots, M_r$ est Zariski-dense dans $\mathrm{Gal}_{\mathrm{diff}}(L, h)$.

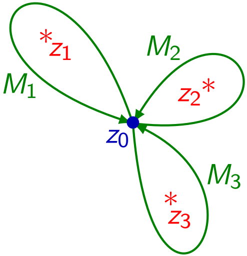


Théorème de densité

Théorème : [Schlesinger, 1895]

- $L \in \mathbb{K}(z)\langle\partial\rangle$ un opérateur **régulier**
- $z_1, \ldots, z_r$ points singuliers de L
- h base de solutions analytiques en $z_0 \in \mathbb{C}\backslash\{z_1, \ldots, z_r\}$
- $M_i =$ « monodromie autour de z_i basé en z_0 relativement à h »

Le sous-groupe engendré par $M_1, \ldots, M_r$ est Zariski-dense dans $\mathrm{Gal}_{\mathrm{diff}}(L, h)$.

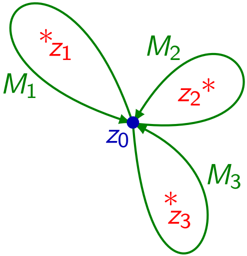


- Vérifier la régularité ?
  $\rightarrow$ Critère de Fuchs

Théorème : [Schlesinger, 1895]

- $L \in \mathbb{K}(z)\langle\partial\rangle$ un opérateur régulier
- $z_1, \ldots, z_r$ points singuliers de L
- h base de solutions analytiques en $z_0 \in \mathbb{C} \backslash \{z_1, \ldots, z_r\}$
- M_i = « monodromie autour de z_i basé en z_0 relativement à h »

Le sous-groupe engendré par $M_1, \ldots, M_r$ est Zariski-dense dans $\mathrm{Gal}_{\mathrm{diff}}(L, h)$.



- Vérifier la régularité ?
  $\rightarrow$ Critère de Fuchs
- Et si l'opérateur n'est pas régulier ?
  $\rightarrow$ Ajouter matrices exponentielles et matrices de Stokes (théorème dû à Ramis, 1985)

Algorithme de van der Hoeven

L'opérateur admet une factorisation ssi il existe un sous-espace invariant sous l'action des matrices de monodromie.

1) Calculer les matrices de monodromie
2) Chercher un sous-espace invariant sous l'action de ces matrices
3) En déduire un facteur droit

Algorithme de van der Hoeven

L'opérateur admet une factorisation ssi il existe un sous-espace invariant sous l'action des matrices de monodromie.

1) Calculer les matrices de monodromie **de manière approchée**
2) Chercher un sous-espace invariant sous l'action de ces matrices
3) En déduire un facteur droit **candidat**
4) Vérification et retour au point 1 avec une meilleure précision en cas d'échec

Algorithme de van der Hoeven

L'opérateur admet une factorisation ssi il existe un sous-espace invariant sous l'action des matrices de monodromie.

1) Calculer les matrices de monodromie **de manière approchée**
2) Chercher un sous-espace invariant sous l'action de ces matrices
3) En déduire un facteur droit **candidat**
4) Vérification et retour au point 1 avec une meilleure précision en cas d'échec

Comment assurer que l'opérateur est irréductible, le cas échéant ?

Calculer un sous-espace invariant

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

Définition : Soit $v \in \mathbb{K}^n$. On note $\mathrm{Inv}_{\mathcal{M}}(v)$ le plus petit sous-espace qui contient v et invariant sous $\mathcal{M}$.

Lemme : il existe un sous-espace V non trivial invariant sous $\mathcal{M}$ ssi il existe un vecteur $v \in \mathbb{K}^n$ non nul tel que $\mathrm{Inv}_{\mathcal{M}}(v) \subsetneq \mathbb{K}^n$.

Calculer un sous-espace invariant

Donnée : $\mathcal{M} = \{M_1, \ldots, M_r\} \subset \mathrm{Mat}_n(\mathbb{K})$

Définition : Soit $v \in \mathbb{K}^n$. On note $\mathrm{Inv}_{\mathcal{M}}(v)$ le plus petit sous-espace qui contient v et invariant sous $\mathcal{M}$.

Lemme : il existe un sous-espace V non trivial invariant sous $\mathcal{M}$ ssi il existe un vecteur $v \in \mathbb{K}^n$ non nul tel que $\mathrm{Inv}_{\mathcal{M}}(v) \subsetneq \mathbb{K}^n$.

Définition : Une décomposition $\mathbb{K}^n = E_1 \oplus \cdots \oplus E_k$ est un *$\mathcal{M}$-découpage* si les projections $\pi_i : \mathbb{K}^n \to E_i$ s'écrivent comme des polynômes en les matrices de $\mathcal{M}$.

Proposition : si on dispose d'un $\mathcal{M}$-découpage de la forme $\mathbb{K}^n = \mathbb{K}v_1 \oplus \cdots \oplus \mathbb{K}v_n$, alors :

- soit $\mathrm{Inv}_{\mathcal{M}}(v_i) \subsetneq \mathbb{K}^n$ pour un certain i,
- soit il n'existe pas de sous-espace invariant sous $\mathcal{M}$.

```
def Inv (M, v) :
   E = [v]
   old_dim, dim = 0, 1
   while old_dim < dim :
      E = E + [mat*u for u in E for mat in M]
      reduce(E)
      old_dim, dim = dim, card(E)
   return E
```

Exemple : réduction de 3 vecteurs dans $\mathbb{K}^4$ (vus en lignes) :

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

Arithmétique d'intervalles

Principe : remplacer les nombres par des intervalles, et s'assurer, à chaque étape de calcul, que l'intervalle contient la valeur exacte.
Exemple : si $\pi \in [3.14 \pm 0.01]$ et $e \in [2.71 \pm 0.01]$, alors $\pi + e \in [5.85 \pm 0.02]$

Arithmétique d'intervalles

Principe : remplacer les nombres par des intervalles, et s'assurer, à chaque étape de calcul, que l'intervalle contient la valeur exacte.
Exemple : si $\pi \in [3.14 \pm 0.01]$ et $e \in [2.71 \pm 0.01]$, alors $\pi + e \in [5.85 \pm 0.02]$

$\rightarrow$ extension aux nombres complexes

Arithmétique d'intervalles

Principe : remplacer les nombres par des intervalles, et s'assurer, à chaque étape de calcul, que l'intervalle contient la valeur exacte.
Exemple : si $\pi \in [3.14 \pm 0.01]$ et $e \in [2.71 \pm 0.01]$, alors $\pi + e \in [5.85 \pm 0.02]$

$\rightarrow$ extension aux nombres complexes, aux matrices

Arithmétique d'intervalles

Principe : remplacer les nombres par des intervalles, et s'assurer, à chaque étape de calcul, que l'intervalle contient la valeur exacte.
Exemple : si $\pi \in [3.14 \pm 0.01]$ et $e \in [2.71 \pm 0.01]$, alors $\pi + e \in [5.85 \pm 0.02]$

$\rightarrow$ extension aux nombres complexes, aux matrices

Notations :
Si o est un objet exact, on note $\boldsymbol{o}$ une approximation de o.

Arithmétique d'intervalles

Principe : remplacer les nombres par des intervalles, et s'assurer, à chaque étape de calcul, que l'intervalle contient la valeur exacte.
Exemple : si $\pi \in [3.14 \pm 0.01]$ et $e \in [2.71 \pm 0.01]$, alors $\pi + e \in [5.85 \pm 0.02]$

$\rightarrow$ extension aux nombres complexes, aux matrices

Notations :
Si o est un objet exact, on note $\boldsymbol{o}$ une approximation de o.
Si f est une fonction qui s'applique à o, on note $\boldsymbol{f}$ une approximation de f, c'est-à-dire une fonction qui s'applique à $\boldsymbol{o}$ vérifiant $\boldsymbol{f}(\boldsymbol{o}) \supset \{f(o)\,;\, o \in \boldsymbol{o}\}$.

Exemple : en notant $\boldsymbol{\pi} = [3.14 \pm 0.01]$, $\boldsymbol{e} = [2.71 \pm 0.01]$, on a $\boldsymbol{\pi} + \boldsymbol{e} \supset [5.85 \pm 0.02]$.

Cas simple : si $f(o) \in \mathbb{Z}$ et $\boldsymbol{f}(\boldsymbol{o}) \cap \mathbb{Z} = \{a\}$, alors $f(o) = a$.
Par exemple, théorème des résidus : calcul du nombre de zéros.

Cas simple : si $f(o) \in \mathbb{Z}$ et $\boldsymbol{f}(\boldsymbol{o}) \cap \mathbb{Z} = \{a\}$, alors $f(o) = a$.
Par exemple, théorème des résidus : calcul du nombre de zéros.

Ici, les coefficients de L_2 sont dans $\overline{\mathbb{Q}}(z)$.
$\rightarrow$ ok si on a assez de décimales $\left(\substack{\text{algorithme LLL +}\\ \text{approximants de Padé-Hermite}}\right)$

Identités exactes et « test à zéro »

Cas simple : si $f(o) \in \mathbb{Z}$ et $\boldsymbol{f}(\boldsymbol{o}) \cap \mathbb{Z} = \{a\}$, alors $f(o) = a$.
Par exemple, théorème des résidus : calcul du nombre de zéros.

Ici, les coefficients de L_2 sont dans $\overline{\mathbb{Q}}(z)$.
$\rightarrow$ ok si on a assez de décimales $\left(\substack{\text{algorithme LLL +} \\ \text{approximants de Padé-Hermite}}\right)$

Problème : « test à zéro »
Situation : $\lambda \in \mathbb{R}$ approximé par $\boldsymbol{\lambda}$ tel que $0 \in \boldsymbol{\lambda}$.
Comment gérer un test « `if λ = 0 :` » ?

Cas simple : si $f(o) \in \mathbb{Z}$ et $\boldsymbol{f}(\boldsymbol{o}) \cap \mathbb{Z} = \{a\}$, alors $f(o) = a$.
Par exemple, théorème des résidus : calcul du nombre de zéros.

Ici, les coefficients de L_2 sont dans $\overline{\mathbb{Q}}(z)$.
$\rightarrow$ ok si on a assez de décimales $\left(\begin{array}{c}\text{algorithme LLL +}\\ \text{approximants de Padé-Hermite}\end{array}\right)$

Problème : « test à zéro »
Situation : $\lambda \in \mathbb{R}$ approximé par $\boldsymbol{\lambda}$ tel que $0 \in \boldsymbol{\lambda}$.
Comment gérer un test « `if λ = 0 :` » ?

Remarque : si $\lambda \neq 0$ alors $0 \notin \boldsymbol{\lambda}$ si la précision est assez grande.

Cas simple : si $f(o) \in \mathbb{Z}$ et $\boldsymbol{f}(\boldsymbol{o}) \cap \mathbb{Z} = \{a\}$, alors $f(o) = a$.
Par exemple, théorème des résidus : calcul du nombre de zéros.

Ici, les coefficients de L_2 sont dans $\overline{\mathbb{Q}}(z)$.
$\rightarrow$ ok si on a assez de décimales $\left(\begin{array}{c}\text{algorithme LLL +}\\ \text{approximants de Padé-Hermite}\end{array}\right)$

Problème : « test à zéro »
Situation : $\lambda \in \mathbb{R}$ approximé par $\boldsymbol{\lambda}$ tel que $0 \in \boldsymbol{\lambda}$.
Comment gérer un test « `if λ = 0 :` » ?

Remarque : si $\lambda \neq 0$ alors $0 \notin \boldsymbol{\lambda}$ si la précision est assez grande.

Proposition de solution :
$\rightarrow$ interpréter une approximation contenant 0 comme un 0 exact.

Algorithme de van der Hoeven

1) Calculer les matrices de monodromie de manière approchée
2) Chercher un sous-espace invariant sous l'action de ces matrices
3) En déduire un facteur droit candidat
4) Vérification et retour au point 1 avec une meilleure précision en cas d'échec

Algorithme de van der Hoeven

1) Calculer les matrices de monodromie de manière approchée
2) Chercher un sous-espace invariant sous l'action de ces matrices
3) En déduire un facteur droit candidat
4) Vérification et retour au point 1 avec une meilleure précision en cas d'échec

Dans le cas où l'opérateur admet une factorisation $\rightarrow$ OK
mais que se passe-t-il si l'opérateur est irréductible ?

Quid de `reduce(`$\mathbf{E}$`)` lorsque $\mathbf{E} = [\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}]$?

$$
\begin{aligned}
& \text{nombre de vecteurs linéairement indépendants} \\
= \quad & \text{nombre de pivots utilisés dans l'algorithme de Gauss} \\
= \quad & \text{nombre de colonnes non nulles } \text{\small (dans les sous-matrices considérées)}
\end{aligned}
$$

Calcul approché de $\mathrm{Inv}_{\mathcal{M}}(\boldsymbol{v})$

Quid de `reduce(`$\mathbf{E}$`)` lorsque $\mathbf{E}$ `=` `[`$\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}$`]` ?

$$
\begin{aligned}
& \text{nombre de vecteurs linéairement indépendants} \\
= \; & \text{nombre de pivots utilisés dans l'algorithme de Gauss} \\
= \; & \text{nombre de colonnes non nulles} \text{ (dans les sous-matrices considérées)}
\end{aligned}
$$

Conséquence : en interprétant à tort une colonne $\boldsymbol{C}$ comme la colonne nulle, on ne fait que **sous-estimer** le rang de $\mathrm{Vect}(\mathbf{E})$.

Calcul approché de $\mathrm{Inv}_{\mathcal{M}}(v)$

Quid de `reduce(E)` lorsque $\mathbf{E} = [\boldsymbol{v_1}, \ldots, \boldsymbol{v_k}]$?

$$\begin{array}{rl} & \text{nombre de vecteurs linéairement indépendants} \\ = & \text{nombre de pivots utilisés dans l'algorithme de Gauss} \\ = & \text{nombre de colonnes non nulles (dans les sous-matrices considérées)} \end{array}$$

Conséquence : en interprétant à tort une colonne $\boldsymbol{C}$ comme la colonne nulle, on ne fait que **sous-estimer** le rang de $\mathrm{Vect}(\mathbf{E})$.

Conclusion :
$\mathbf{Inv}_{\boldsymbol{\mathcal{M}}}(\boldsymbol{v})$ renvoie n vecteurs $\boldsymbol{v_1}, \ldots, \boldsymbol{v_n}$
$\Rightarrow \mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{K}^n$ pour la liste $\mathcal{M}$ les matrices de monodromie exactes (théoriques) et pour n'importe quel vecteur $v \in \boldsymbol{v}$.

Assurer l'irréductibilité à partir d'approximations

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \text{ et } \pi_i = \begin{pmatrix} 0 & & & & \\ & \ddots & & (0) & \\ & & 1 & & \\ & (0) & & \ddots & \\ & & & & 0 \end{pmatrix}$$

Situation :

- $\mathbb{K}^n = \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_n$
- projections $\boldsymbol{\pi_i}$ calculées à partir de $\boldsymbol{\mathcal{M}}$
  (il existe p_i tel que $p_i(M_1, \ldots, M_r) \in \boldsymbol{\pi_i}$)
- $\mathbf{Inv}_{\mathcal{M}}(\boldsymbol{e_i})$ renvoie n vecteurs

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \text{ et } \pi_i = \begin{pmatrix} 0 & & & \\ & \ddots & & (0) \\ & & 1 & \\ & (0) & & \ddots & \\ & & & & 0 \end{pmatrix}$$

Situation :

- $\mathbb{K}^n = \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_n$
- projections $\boldsymbol{\pi_i}$ calculées à partir de $\boldsymbol{\mathcal{M}}$
  (il existe p_i tel que $p_i(M_1, \ldots, M_r) \in \boldsymbol{\pi_i}$)
- $\mathbf{Inv}_{\boldsymbol{\mathcal{M}}}(\boldsymbol{e_i})$ renvoie n vecteurs

Soit $v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ non nul. Justifions que $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{K}^n$.

On peut supposer que $||v||_\infty = 1$ et que $c_i = 1$ pour un certain i.

$$||p_i(M_1, \ldots, M_r)v - e_i||_\infty \leq |||p_i(M_1, \ldots, M_r) - \pi_i|||_\infty ||v||_\infty$$

$$e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \text{ et } \pi_i = \begin{pmatrix} 0 & & & \\ & \ddots & & (0) \\ & & 1 & \\ & (0) & & \ddots \\ & & & & 0 \end{pmatrix}$$

Situation :

- $\mathbb{K}^n = \mathbb{K}e_1 \oplus \cdots \oplus \mathbb{K}e_n$
- projections $\boldsymbol{\pi_i}$ calculées à partir de $\boldsymbol{\mathcal{M}}$ (il existe p_i tel que $p_i(M_1, \ldots, M_r) \in \boldsymbol{\pi_i}$)
- $\mathbf{Inv}_{\boldsymbol{\mathcal{M}}}(\boldsymbol{e_i})$ renvoie n vecteurs

---

Soit $v = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ non nul. Justifions que $\mathrm{Inv}_{\mathcal{M}}(v) = \mathbb{K}^n$.

On peut supposer que $||v||_\infty = 1$ et que $c_i = 1$ pour un certain i.

$$||p_i(M_1, \ldots, M_r)v - e_i||_\infty \leq |||p_i(M_1, \ldots, M_r) - \pi_i|||_\infty ||v||_\infty$$

En calculant $\epsilon > 0$ tel que pour tout i, $\max_{M \in \boldsymbol{\pi_i}} |||M - \pi_i|||_\infty \leq \epsilon$, il suffit que $\boldsymbol{e_i} \supset \mathrm{Boule}_{||\cdot||_\infty}(e_i, \epsilon)$.

ANNEXES

Les diapositives suivantes sont prévues pour répondre à d'éventuelles questions.

Raffiner un $\mathcal{M}$-découpage

Soit $N \in \mathrm{Mat}_n(\mathbb{K})$.

Définition : Un $\mathcal{M}$-découpage est *N-adapté* si pour tout i, l'application $P_i N P_i$ vue dans $L(E_i)$ n'a qu'une valeur propre.

Définition : *Raffiner un $\mathcal{M}$-découpage* $E_1 \oplus \cdots \oplus E_k$ selon N, c'est calculer un nouveau $\mathcal{M}$-découpage $F_1 \oplus \cdots \oplus F_p$ tel que :

- la nouvelle décomposition est plus fine,
- le $\mathcal{M}$-découpage $\mathbb{K}^n = F_1 \oplus \cdots \oplus F_p$ est N-adapté.

Idée de l'algorithme : On part du $\mathcal{M}$-découpage trivial $\mathbb{K}^n = \mathbb{K}^n$ et on raffine ce découpage jusqu'à :

- soit trouver un vecteur $v \in \mathbb{K}^n$ non nul tel que $\mathrm{Inv}_{\mathcal{M}}(v) \subsetneq \mathbb{K}^n$,
- soit arriver à un $\mathcal{M}$-découpage composé que de droites.

L'algorithme de calcul de sous-espace invariant

`Invariant_subspace(`$\mathcal{M}$`)`

(1) calculer $\mathbb{K}^n = E_1 \oplus \cdots \oplus E_k$ un $\mathcal{M}$-découpage N-adapté pour toute matrice $N \in \mathcal{M}$

(2) pour chaque droite $E_i = \mathbb{K}v$: $\mathrm{Inv}_{\mathcal{M}}\, v$?

s'il n'y a que des droites : retourner `None`

(3) pour un E_i de dimension > 1 : calculer $K = \bigcap_{M \in \mathcal{M}} \vec{\mathrm{ev}}(P_i M P_i)$

$K = 0$ (4)	(5) $K \neq 0$
calculer $N \in \mathcal{A}$ telle que $\mathrm{card}\,(\mathrm{Sp}\,(P_i N P_i)) > 1$ $\mathcal{M} = \mathcal{M} \cup \{N\} \to (1)$	pour un $v \in K \backslash \{0\}$: $\mathrm{Inv}_{\mathcal{M}}\, v$? calculer $N \in \mathcal{A} \mid P_i N P_i v \notin \mathbb{K}v$ $\mathcal{M} = \mathcal{M} \cup \{N\} \to (1)$

Yaakov Levitzki (1904-1956)

Soit $\mathcal{S}$ un semi-groupe de matrices nilpotentes de $\mathrm{Mat}_n(\mathbb{K})$. Alors, les matrices de $\mathcal{S}$ sont co-trigonalisables.

Démonstration : On raisonne par induction sur n. Si $n = 1$ ou $\mathcal{S} \subset 0$, il n'y a rien à faire. On suppose donc $n > 1$ et $\mathcal{S} \neq \varnothing, 0$. Admettons que l'on ait un s.e.v. $0 \subsetneq V \subsetneq \mathbb{K}^n$ tel que $\mathcal{S}V \neq \mathbb{K}^n$. On peut supposer que $\mathcal{S}V \subset V$ quitte à remplacer V par $\mathcal{S}V$. Notons W un supplémentaire de V dans $\mathbb{K}^n$. Dans une base adaptée à $V \oplus W$, chaque $M \in \mathcal{S}$ s'écrit par blocs $\left(\begin{array}{c|c} M_1 & M_3 \\ \hline 0 & M_2 \end{array}\right)$. Les ensembles $\mathcal{S}_1 = \{M_1 \;:\; M \in \mathcal{S}\}$ et $\mathcal{S}_2 = \{M_2 \;:\; M \in \mathcal{S}\}$ sont des semi-groupes de matrices nilpotentes de tailles $< n$, on peut donc leur appliquer l'hypothèse d'induction.

Yaakov Levitzki (1904-1956)

Soit $\mathcal{S}$ un semi-groupe de matrices nilpotentes de $\mathrm{Mat}_n(\mathbb{K})$. Alors, les matrices de $\mathcal{S}$ sont co-trigonalisables.

Démonstration : *(suite)* On suppose $n > 1$ et $\mathcal{S} \neq \varnothing, 0$. Montrons qu'il existe un s.e.v. $0 \subsetneq V \subsetneq \mathbb{K}^n$ tel que $\mathcal{S}V \neq \mathbb{K}^n$.

On choisit $M \neq 0$ telle que $V := \operatorname{Im} M$ soit de dimension minimale. Montrons que $\mathcal{S}V \subset \operatorname{Ker} M$. Soient $N \in \mathcal{S}$ et $v \in V$.

Notons f l'a.l.c.a. à MN et montrons que $f(v) = 0$. Supposons le contraire. Alors $0 \subsetneq \operatorname{Im} f \subset V$ donc $V = \operatorname{Im} f$ par minimalité. On en déduit $v \in \operatorname{Im} f$ puis $0 \subsetneq \operatorname{Im} f^2 \subset V$. Encore par minimalité, $V = \operatorname{Im} f^2 = f(V)$. Ainsi, f induit un isomorphisme sur V, donc f admet une valeur propre non nulle, contradiction. $\square$

Complication fortuite

Le raffinage NE conserve PAS le caractère adapté d'un découpage.

Contre-exemple : On se place dans $\mathbb{K}^3 =: E = F \oplus G$ avec $F := \mathrm{Vect}_{\mathbb{K}}(u, v)$ et $G := \mathrm{Vect}_{\mathbb{K}}(w)$ où $u = (1, 0, 0)$, $v = (0, 1, 1)$ et $w = (0, 0, 1)$ et on considère la matrice

$$M := \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} .$$

En notant $P \in \mathrm{Mat}_3(\mathbb{K})$ la projection sur F parallèlement à G, on a M monopotente mais PMP (vu dans $\mathcal{L}(\mathbb{K}^2)$) non monopotente. En effet, $Mu = 0$ et $Mv = 2u + v - w$ donc

$$\mathrm{Mat}_{\mathcal{B}=(u,v)}(\text{"}PMP\text{"}) = \begin{pmatrix} 0 & 2 \\ 0 & 1 \end{pmatrix} .$$

Procédure de raffinage

Soient $\mathbb{K}^n = E_1 \oplus \cdots \oplus E_k$ un $\mathcal{M}$-découpage, et $N \in \mathcal{A}$.
Expliquons comment raffiner le $\mathcal{M}$-découpage selon N.

Soit $1 \leq i \leq k$. On note $f_i : E_i \to E_i$ l'a.l.c.a. à $P_i N P_i$.
Notons $\chi = \prod_{j=1}^{s}(X - \lambda_j)^{m_{\lambda_j}}$ le polynôme caractéristique de f_i.
Notons $C_{\lambda_j} := \operatorname{Ker}(f_i - \lambda_j)^{m_{\lambda_j}}$ le s.e.v. caractéristique associé à λ_j.
On a $E_i = C_{\lambda_1} \oplus \cdots \oplus C_{\lambda_s}$ où les projections $\in \mathbb{K}[f_i]$ (dans $\mathcal{L}(E_i)$).
En réunissant les décompositions ainsi obtenues pour chaque i, on obtient une décomposition plus fine $\mathbb{K}^n = F_1 \oplus \cdots \oplus F_p$.

Cette décomposition est un $\mathcal{M}$-découpage : en effet, les projections sur les F_j appartiennent à $\mathcal{A}$ car sont les composées d'une projection P_i sur E_i et d'une projection qui est un polynôme en $P_i N P_i$.
Ce $\mathcal{M}$-découpage est par construction N-adapté.