orithmes modulaires pour les équation différentielles linéaires

Thomas CLUZEAU

thèse sous la direction de M. A. Barkatou & J.-A. Weil)

Laboratoire STIX, École Polytechnique

thomas.cluzeau@stix.polytechnique.fr

http ://www.unilim.fr/pages_perso/thomas.cluzeau/

INRIA-Projet **ALGO**

Lundi 20 octobre 2003

Plan de l'exposé

torisation de systèmes différentiels linéaires en caractéristiq

néralisation : factorisation de systèmes d'équations aux dériv
elles (D-finis) en caractéristique p.

n algorithme modulaire pour le calcul de solutions expone
s.

I.
Factorisation de systèmes différentiels linéaires en caractéristique p.

Plan de la partie I

et motivation.

tèmes différentiels à coefficients dans $\overline{\mathbb{F}}_p(x)$.

torisation en caractéristique p.

Les deux principaux objets.
Décomposition maximale.
Le cas indécomposable.

ctif :

donné $Y' = AY =: [A]$ avec $A \in \mathcal{M}_n(\overline{\mathbb{F}}_p(x))$, trouver (si po
un système équivalent $[B]$ avec B triangulaire ou diagona
locs.

èmes équivalents :

$B]$ si $\exists\, P$ tel que $B = P^{-1}(AP - P') =: P[A]$.

èmes réductible/décomposable :

st réductible (resp. décomposable) si $\exists\, [B] \sim [A]$ avec
$\begin{pmatrix} B_1 & B_3 \\ 0 & B_2 \end{pmatrix}$ (resp. $B = \begin{pmatrix} B_1 & 0 \\ 0 & B_2 \end{pmatrix} = \mathrm{diag}(B_1, B_2)$).

Factorisation en caractéristique zéro

rithme de Beke : Beke *1894*, Tsarev *'94*, Bronstein *'94*,

le puis globale : van Hoeij *'97*, Pflügel *'98*,

node de l'eigenring : Singer *'96*, Barkatou-Pflügel *'98-'00*

orisation lorsque $A \in \mathcal{M}_n(\overline{\mathbb{F}}_p(x))$ = premier pas d'une approc
ulaire comme dans le cas polynomial.

$\overline{\mathbb{F}}_p(x)$ muni de la dérivation $' := \frac{d}{dx}$
$= AY$ avec $A \in \mathcal{M}_n(K)$.

s des constantes $\mathcal{C} := \overline{\mathbb{F}}_p(x^p)$.

$\bigoplus_{i=0}^{p-1} \mathcal{C}x^i \rightsquigarrow$ différent de la caractéristique zéro.

ateur différentiel $\Delta_A := \frac{d}{dx} - A$ agissant sur K^n.

ervation importante :
st un opérateur $\mathcal{C}$-linéaire de $\mathcal{C}^{np}$ dans $\mathcal{C}^{np}$.

État de l'art

rie algèbrique des équations différentielles en caractéristiq
atz *'70*, Honda *'81*, Chudnovsky *'85*, van der Put *'95*.
t central = p-courbure.

orisation d'opérateurs différentiels : van der Put *'95*, *'97*.
sée sur la forme de Jordan de la p-courbure.

orisation de polynômes de Ore : Giesbrecht-Zhang *'03*.
sée sur des éléments particuliers de l'eigenring.

Contributions

mes manipulés directement,

natives rationnelles à l'algorithme de van der Put,

mentation (en Maple), disponible à :
://www.unilim.fr/pages_perso/thomas.cluzeau/

paraisons de stratégies et analyse de complexité.

Objet 1 : Eigenring

$$\mathcal{E}(A) := \{P \in \mathcal{M}_n(K) \mid P' = AP - PA\}.$$

l $\leftrightarrow$ calculer les solutions rationnelles
mplexité en $\mathcal{O}(n^6 \max(a,p)^2 p)$ où $\deg(A) \leq a$.

ions rationnelles de $[A]$ $\leftrightarrow$ système linéaire de dimension np
mplexité en $\mathcal{O}(n^3 \max(a,p)^2 p)$ où $\deg(A) \leq a$.

général : un élément non trivial de $\mathcal{E}(A) \rightsquigarrow$ factorisation.
(A) et $P^{-1}TP = \mathrm{diag}(T_1, T_2) \Rightarrow P[A] = \mathrm{diag}([A^{[1]}], [A^{[2]}])$.

Objet 2 : p-courbure

urbure := l'opérateur K-linéaire $\Delta_A^p = (\frac{d}{dx} - A)^p$ sur K^n.

l (Katz) :

$$A_0 = I \text{ et } \forall\, i \geq 0, A_{i+1} = A_i' - AA_i.$$

mplexité en $\mathcal{O}(n^\omega a \log(a) p^2)$ (si produit de matrices en $\mathcal{O}(n^\omega$

e de Jordan de $A_p \rightsquigarrow$ toutes les factorisations de $[A]$
der Put).

$\mathcal{E}(A) \rightsquigarrow$ élément particulier de $\mathcal{E}(A)$.

précis : $\mathrm{Com}(A_p) = K \otimes_C \mathcal{E}(A)$.

Décomposition isotypique

t d'irréductibilité :

$\chi(A_p)$ irréductible $\Leftrightarrow$ $[A]$ irréductible.

$A_p) = F_1^{m_1} \dots F_r^{m_r} \Rightarrow \exists P$ tel que $P[A] = \text{diag}([A^{[1]}], \dots, [A^{[r]}$

Cas $\chi(A_p) = F^m$

d'indécomposabilité :

$[A]$ indécomposable $\Leftrightarrow \chi_{\min}(A_p) = \chi(A_p)$.

ithme de van der Put :
ailler dans $K[X]/F$ et réduire le problème à $\chi_{\min}(A_p) = X^m$

natives rationnelles :

ape 1 : $[A] \sim \text{diag}([A^{[1]}], \ldots, [A^{[r]}]) \Rightarrow \exists\, T \in \mathcal{E}(A)$ "de spec
ximal", *i.e.*, $\chi(T) = F_1 \ldots F_r$.
heuristique : prendre un élément au hasard dans $\mathcal{E}(A)$.

ape 2 : $[A]$ indécomposable $\Leftrightarrow \mathcal{E}(A)$ ne contient pas d'
mpotents autres que I et O.
algorithme récursif ; voir Giesbrecht-Zhang *'03*.

Le cas indécomposable

de réductibilité :

$\chi_{\min}(A_p) = \chi(A_p) = F^m$ avec $m > 1 \Rightarrow [A]$ réductible.

Comment calculer la factorisation maximale ?

$i = 1, \ldots, m$, $v^i := F^i(A_p)$ et $E_i := \ker(v^i)$,

drapeau de K^n et dans une base adaptée, la matrice de v, *i.*
P, est triangulaire par blocs avec des zéros sur la diagonale

$\in \mathcal{E}(A) \Rightarrow P[A]$ est triangulaire par blocs.

II.
Factorisation de systèmes d' É. D. P. (D-finis) en caractéristique p.

en cours avec la participation d'A. Quadrat (INRIA - CAFE

Plan de la partie II

tèmes d'É. D. P. D-finis.

torisation en caractéristique p.

mple.

corps différentiel (partiel) (ou Θ-corps),
$C(x_1, x_2)$, $\Theta = (\frac{d}{dx_1}, \frac{d}{dx_2})$.

on : module différentiel (partiel) D-fini : $k[\partial_1, \partial_2]$-module
on fini sur k.

$$\begin{array}{l} (Y) = 0, \quad \Delta_1 := \partial_1 - A_1 \\ (Y) = 0, \quad \Delta_2 := \partial_2 - A_2 \end{array}$$ système intégrable.

ons d'intégrabilité : $[\Delta_1, \Delta_2] = 0$
$(A_2) - \partial_2(A_1) = A_1 A_2 - A_2 A_1$).

ique : étant donné un système linéaire d'É. D. P.,

uler une base involutive (ou de Janet),

ase du "quotient",

ude de cette base ⇒ intégrabilité.

nsi un test de D-finitude.

que : similarité avec la forme normale de B. Mourrain pour
algébriques de dimension zéro.

$$\begin{cases} \Delta_1(Y) = 0, & \Delta_1 := \partial_1 - A_1 \\ \Delta_2(Y) = 0, & \Delta_2 := \partial_2 - A_2 \end{cases}$$

définitions de réductible, décomposable ... + même P
ures partielles : Δ_i^p.
gs partiels : $\mathcal{E}_i(\Delta) := \{P \in \mathcal{M}_n(k) \,|\, \Delta_i P = P\Delta_i\}$.
g : $\mathcal{E}(\Delta) := \{P \in \mathcal{M}_n(K) \,|\, \forall i : \Delta_i P = P\Delta_i\} = \bigcap_i \mathcal{E}_i(\Delta)$.

$\Delta_j] = 0 \Rightarrow [\Delta_i, \Delta_j^p] = 0 \Rightarrow [\Delta_i^p, \Delta_j^p] = 0$.

s Δ_i^p appartiennent à $\mathcal{E}(\Delta)$ et commutent.

ser (presque) toute la théorie de la partie I.
ction simultanée de matrices qui commutent.

Exemple

$$A_1 = \begin{pmatrix} 1 & x_1 x_2 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} \frac{x_1 - 2x_1^3 x_2 f_2(x_2) - f_3(x_2) x_1 + x_1 x_2 (f_1(x_2) + f_2(x_2) x_1^2)}{x_1 x_2} & \frac{1}{2} f_2(x_2) x_2 x_1^4 + \frac{1}{2} f_3(x_2) x_1^2 + f_4(x_2) \\ -\frac{2 f_2(x_2)}{x_2} & f_1(x_2) + f_2(x_2) x_1^2 \end{pmatrix}$$

$= \partial_1 - A_1$
$= \partial_2 - A_2$ $\rightsquigarrow$ vérification $[\Delta_1, \Delta_2] = 0 \rightsquigarrow$ D-fini.

$\rightarrow$ 2 cas se présentent :

$) \neq 0 \Rightarrow$ système irréductible mod p,

$) = 0 \Rightarrow$ système décomposable mod p.

Cas irréductible

$$f_1 = x_2^4,\ f_2 = x_2,\ f_3 = x_2^6,\ f_4 = 2x_2^6 + 2x_2^4.$$

Algo. de I.

$= \cdots \rightsquigarrow \chi(\Delta_1^p) = (X+1)^2,$

$= \cdots \rightsquigarrow \chi(\Delta_2^p) = X^2 + (2x_2^{12} + x_2^3 + 2x_2^{15})X + x_2^{15} + x_2^{18} + 2x_2^{27} +$
uctible.

articulier, le système en question est donc irréductible !

Cas décomposable

$$f_1 = 2x_2,\ f_2 = 0,\ f_3 = 2x_2^6 + x_2,\ f_4 = x_2 + x_2^2.$$

Algo. de I.

$\cdots \rightsquigarrow \chi(\Delta_1^p) = (X+1)^2$,

$\cdots \rightsquigarrow \chi(\Delta_2^p) = (X + 2 + x_2^3 + x_2^{15})(X + 2x_2^3)$.

urbures partielles simultanément diagonalisables.

$\rightsquigarrow$ Système décomposable.

Calcul de la décomposition

sant Δ_2^p :

$_2$ vecteurs propres associés aux 2 facteurs de $\chi(\Delta_2^p)$,

atrice ayant pour colonnes v_1, v_2 diagonalise Δ_2^p et donc,
ès le I., $P[A_2]$ diagonale,

aussi $P[A_1]$ diagonale.

III.
Un algorithme modulaire pour le calcul de solutions exponentielles.

en collaboration avec M. van Hoeij (Florida State University

Plan de la partie III

blème et Motivations.
liminaires.
ns premiers.
luire le nombre de combinaisons à tester.

Problème

$$L = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0$$

trouver les facteurs à droite d'ordre 1 $\partial - r$, $r \in \overline{\mathbb{Q}}(x)$ lorsq
sont dans $C(x)$ avec $C \subset \overline{\mathbb{Q}}$.

ouver les solutions exponentielles y de l'équation différentie
iée $\rightsquigarrow$ lien $r = y'/y$.

oblème inclus dans celui de la factorisation.

Motivations

nme standard pour les facteurs d'ordre 1 (Beke) :

sir un exposant généralisé en chaque singularité.

ul de solutions polynomiales (*e.g.*, avec [ABP]).

x problèmes :

binatoire : au plus n^m combinaisons,

s : objets définis sur des extensions algèbriques de C.

: utiliser des méthodes modulaires pour éliminer des com
; surtout celles définies sur de grandes extensions.

Méthodes modulaires et factorisation

onter de la car. p à la car. 0 : (van der Put) pas d'algorithm
lets, inefficace ... Hensel ?

biner des factorisations mod plusieurs p : comment ? lesquelle

er de grands p : calculs de p-courbure, factorisation ... p
eux.

velle approche :

er seulement les racines du polynome caractéristique de la
oure pour un bon premier.

r ces racines à des informations locales en car. zéro.

Définitions : car. 0

$$L = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0$$

ılarités = racines de a_n + ∞.

$x\partial \rightsquigarrow L = \sum_{i=\nu}^{\infty} x^i p_i(\delta) \in \overline{\mathbb{Q}}((x))[\delta]$
quation indicielle = p_ν.

sant généralisé de L en $x = 0$: $e \in \overline{\mathbb{Q}}[x^{-1/k}]$ tel que 0 e
e de l'équation indicielle de $L_{\delta\to\delta+e}$.
$p(\int(e/x))\Sigma$ solution locale en 0.

tre local : $t_i = x - x_i$ ou $t_\infty = 1/x$.

e . *Si* $L = l(\partial - r)$, *alors* $\forall x_i \in \overline{S}, \exists\, e_{x_i} \in \overline{\mathbb{Q}}[t_i^{-1}]$ *tel que :*

$$r = \sum_{x_i \in \mathcal{S}} \frac{e_{x_i}}{t_i} - t_\infty e_\infty^* + \frac{Q'}{Q},$$

tion de Fuchs)

$$\deg(Q) + \sum_{x_i \in \overline{\mathcal{S}}} \mathrm{Const}(e_{x_i}) = 0.$$

Définitions : car. p

$(x) \rightarrow \overline{\mathbb{F}}_p(x^p)$,
$y \mapsto y^p + y^{(p-1)}$ surjective, additive, $\ker(\tau) = \{z'/z | z \neq$

ns : $\chi_p(L)$:= polynôme caractéristique de la p-courbure.
)) := {racines de $\chi_p(L)$ dans $\overline{\mathbb{F}}_p(x^p)$}.

$L_1 L_2 \Rightarrow \chi_p(L) = \chi_p(L_1)\chi_p(L_2)$,

$\partial - r \mapsto \tau(r)$ surjection entre l'ensemble des facteurs à dro
re 1 et $\mathcal{R}(\chi_p(L))$.

e . $L \in \overline{\mathbb{Q}}(x)[\partial]$ *et* p *tel que* $L[p]$ *existe.*
$L_2 \Rightarrow L[p] = L_1[p]L_2[p]$. *(*$L_i$ *unitaire)*

est d'irréductibilité,

est de non existence de solutions exponentielles.

Bons nombres premiers

peut être réduit mod p & $a_n[p] \neq 0$,

ngularités réductibles mod p,

ngularités distinctes restent distinctes mod p.

sition . *Si p est un bon premier et si $L = L_1.(\partial - r)$ alors*
ne racine s de $\chi_p(L)$ et des exposants généralisés e_{x_i} tels qu

$$s = \sum \tau(\frac{e_{x_i}}{t_i}) - \tau(t_\infty e^*_\infty).$$

Comment réduire le nombre de combinaisons ?

é, ? $\partial - r$ avec $r \in C(x)$.

ie : $L = l(\partial - r) \rightsquigarrow L[p] = l[p](\partial - r[p]) \rightsquigarrow \tau(r[p]) \in \mathcal{R}(\chi_p(L))$

cipe de l'algorithme :

uler $\mathcal{R}(\chi_p(L))$ pour un bon premier p.
parer les parties polaires pour sélectionner les bonnes com
ns.
arder que ces combinaisons et faire l'algorithme de Beke.

Exemple 1 (simple)

$$- \frac{2x^2-x+4}{2x^2}\partial^2 - \frac{3x^3-4x^2-3x-2}{2x^4}\partial + \frac{2x^3-3x-2}{2x^4}.$$

nts généralisés : 0, $\frac{5}{2}+\frac{1}{x}$, $2+\frac{1}{x}$ en 0, $-t_\infty^{-1}$, $-t_\infty^{-\frac{1}{2}}$, $t_\infty^{-\frac{1}{2}}$ en

rithme de Beke : 3 combinaisons à tester.

$c = x^p$).

$= (\lambda^2 + \lambda/c^2 + 2/c + 1/c^4)(\lambda + 2) \rightsquigarrow$ 1 racine $\lambda = 1 \rightsquigarrow$ exc
x $\frac{5}{2}+\frac{1}{x}$ et $2+\frac{1}{x}$ en 0 $\rightsquigarrow$ 1 seule combinaison à tester.

décider si $\exists Q$, $\deg(Q) = 0$ t. q. $L(Q(x).e^x) = 0 \rightsquigarrow e^x$.

Exemple 2 (plus difficile)

$x^3-2)^5\partial^3+(x^3-2)(2x^{10}-12x^7+108x^5+24x^4-216x^2$
$)\partial-2x(190x^6-274x^3-27x-212)$.

rités : $\alpha := \mathrm{RootOf}(x^3-2)$ et ∞.
nts généralisés : $2, \frac{1}{36}\frac{\alpha^2}{(x-\alpha)}-\frac{1}{18}\alpha$ et $-\frac{1}{36}\frac{\alpha^2}{(x-\alpha)}+4+\frac{1}{18}\alpha$ en
$\frac{4}{3}$ à l'∞.

rithme de Beke : 81 difficiles combinaisons à tester.

$x^3-2=(x+2)(x^2+3x+4) \bmod p$
vient 3 et $\beta := \mathrm{RootOf}(x^2+3x+4)$ en caractéristique p.

nts généralisés mod p : 2, $\frac{4}{x+2}-1$, $-\frac{4}{x+2}$ en 3, 2, $\frac{\beta^2}{(x-\beta)}$
$\frac{\beta^2}{-\beta)}+4+2\beta$ en β et 0 (multiplicité 2), 2 en l'∞.

une seule racine : $s := \frac{4c^4+2c+1}{c^6+c^3+4}$ $(c = x^p)$.

oix $\frac{4}{x+2}-1$ en 3, $\frac{\beta^2}{(x-\beta)}+3\beta$ en β et n'importe quoi à l'∞
$\frac{\alpha^2}{-\alpha)}-\frac{1}{18}\alpha$ en $\alpha \rightsquigarrow$ plus que 3 combinaisons à tester !

élimination de toutes les combinaisons difficiles.

n de Fuchs $\rightsquigarrow$ 1 combinaison $\rightsquigarrow$ 1 solution.