

Calcul de développements de Puiseux : un nouvel algorithme symbolique-numérique

Poteaux Adrien

Laboratoire J.A. Dieudonné, UNSA
Projet Galaad, INRIA Sophia-Antipolis

JNCF 2008
22 octobre 2008

Résumé de l'épisode précédent

JNCF 2007 :

- Calcul de groupe de monodromie utilisant une approximation numérique des développements de Puiseux au-dessus des points critiques

(calcul symbolique) + (évaluation numérique) =

(temps de calcul catastrophiques) + (mauvaise précision)

- Principe d'un nouvel algorithme symbolique-numérique pour calculer ces approximations :
 - 1 Trouver la structure des solutions modulo p .
 - 2 Utiliser la structure pour faire des calculs numériques.

Résumé de l'épisode précédent

JNCF 2007 :

- Calcul de groupe de monodromie utilisant une approximation numérique des développements de Puiseux au-dessus des points critiques

(calcul symbolique) + (évaluation numérique) =

(temps de calcul catastrophiques) + (mauvaise précision)

- Principe d'un nouvel algorithme symbolique-numérique pour calculer ces approximations :
 - 1 Trouver la structure des solutions modulo p .
 - 2 Utiliser la structure pour faire des calculs numériques.

Travaux publiés (SNC'07)

Poteaux, *Computing monodromy groups defined by plane algebraic curves*

Résumé de l'épisode précédent

JNCF 2007 :

- Calcul de groupe de monodromie utilisant une approximation numérique des développements de Puiseux au-dessus des points critiques

(calcul symbolique) + (évaluation numérique) =

(temps de calcul catastrophiques) + (mauvaise précision)

- Principe d'un nouvel algorithme symbolique-numérique pour calculer ces approximations :
 - 1 Trouver la structure des solutions modulo p .
 - 2 Utiliser la structure pour faire des calculs numériques.

Travaux publiés (SNC'07)

Poteaux, *Computing monodromy groups defined by plane algebraic curves*

Aujourd'hui : description de l'algorithme numérique-modulaire

Développements de Puiseux
Algorithme symbolique-numérique



Factorisation
Calcul du genre



Calcul de groupe de monodromie



Théorie de Galois



Théorème d'Abel-Jacobi effectif



Calcul formel :
Intégration de fonctions algébriques
Étude d'EDO
Théorie de Galois différentielle



Physique : Équations KdV, KP

Problématique

- $K = \mathbb{Q}(\alpha)$ un corps de nombres
- $F(X, Y) \in K[X, Y]$ sans facteur carré, unitaire

Théorème (Puiseux)

Il existe d_Y séries $Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}}$ t.q. $F(X, Y_{ij}(X)) = 0$
pour tout $1 \leq j \leq e_i$, $1 \leq i \leq s$, avec

- ζ_{e_i} racine primitive de l'unité d'ordre e_i
- e_1, \dots, e_s partition de d_Y .

Partie singulière

$$\begin{aligned} Y_{ij}(X) &= \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}} \\ &= \sum_{k=0}^{r_{ij}} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}} + \text{termes suivants} \end{aligned}$$

r_{ij} est l'**indice de régularité**; $r_i = r_{ij}$ pour $1 \leq j \leq e_i$

Termes suivants : calculés par exemple via Newton quadratique
Kung & Traub 1978, *All Algebraic Functions Can Be Computed Fast*

Polygones de Newton génériques

$$F(X, Y) = \sum_{i,j} a_{ij} X^j Y^i$$

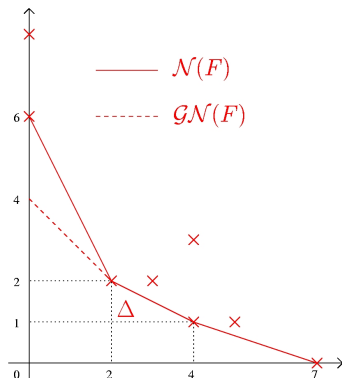
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

— $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de $\text{Supp}(F)$.

- - $\mathcal{GN}(F)$: pentes de $\mathcal{N}(F) \geq -1$.

Polynôme caractéristique :

$$\phi_{\Delta}(T) = \sum_{(i,j) \in \Delta} a_{ij} T^{\frac{i-j}{q}}$$



Algorithme de Newton-Puiseux rationnel

D. Duval 89, *Rational Puiseux Expansions*

Pour chaque arête Δ de $\mathcal{GN}(F)$

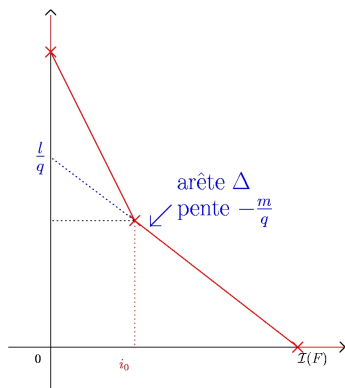
- $\phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$

- Pour chaque ϕ_k

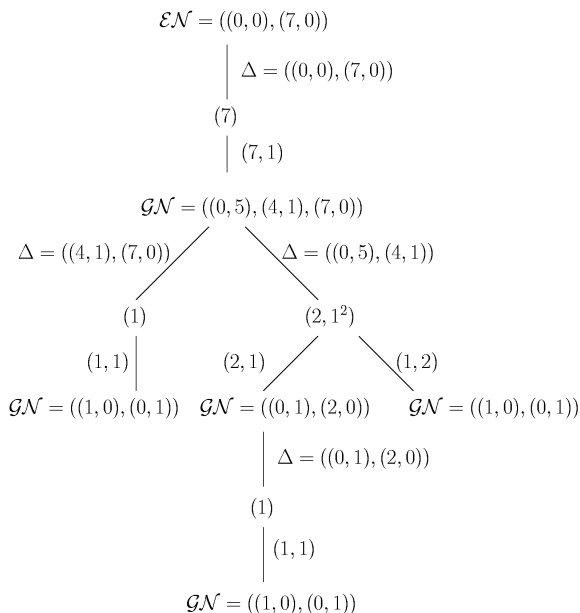
$$F(X, Y) \leftarrow \frac{F(\xi_k^u X^q, X^m(\xi_k^v + Y))}{X^l}$$

avec

- ξ_k t.q. $\phi_k(\xi_k) = 0$,
- (u, v) tel que $uq - vm = 1$.



Arbre des polygones



Calcul des développements de Puiseux

- Calcul numérique délicat
- Calcul symbolique : calcul dans des extensions de degré potentiellement élevé et croissance des coefficients

Complexité binaire $\tilde{O}(d_Y^{32} d_X^4)$ Walsh 2000

Calcul des développements de Puiseux

- Calcul numérique délicat
- Calcul symbolique : calcul dans des extensions de degré potentiellement élevé et croissance des coefficients

Complexité binaire $\tilde{O}(d_Y^{32} d_X^4)$ Walsh 2000

Une approche modulaire-numérique :

- 1 Calculer la partie singulière des séries de Puiseux modulo un bon premier p .

Cela nous donne l' **arbre des polygones** $\mathcal{T}(F)$, i.e. :

- Les polygones de Newton génériques,
- Les structures de multiplicité des ϕ_Δ .

- 2 Calculer numériquement les séries de Puiseux en suivant $\mathcal{T}(F)$.

Contributions

- Notion de *polygone de Newton générique*.
- Critère de bonne réduction (choix d'un bon p).
- Bornes sur le premier p .
- Complexité améliorée de la partie modulaire de notre algorithme.
- Calculs numériques suivant $\mathcal{T}(F)$.
- Prototype d'implémentation en Maple.

Partie symbolique : calculer $\mathcal{T}(F)$

Poteaux & Rybowicz, *On the good reduction of Puiseux series and complexity of the Newton-Puiseux algorithm over finite fields*, ISSAC'08

Bonne \mathfrak{p} -réduction

On note :

- σ l'anneau des entiers algébriques de K ,
- p un nombre premier,
- \mathfrak{p} un idéal premier de σ divisant p .

Définition

F a une **bonne \mathfrak{p} -réduction locale** (en $x = 0$) si :

- $F \in \sigma_{\mathfrak{p}}[X, Y]$,
- $p > d_Y$,
- $\text{tc}(R_F) \not\equiv 0 \pmod{\mathfrak{p}}$.

où $R_F = \text{Resultant}_Y(F, F_Y)$

Réduction des séries de Puiseux

- L une extension finie de K engendrée par les coefficients des séries de Puiseux,
- \mathfrak{O} l'anneau des entiers algébriques de L ,
- \mathfrak{P} un idéal premier de \mathfrak{O} divisant \mathfrak{p} ,

Théorème

Si F a une bonne \mathfrak{p} -réduction locale, alors les coefficients des séries de Puiseux de F au-dessus de 0 sont dans $\mathfrak{O}_{\mathfrak{P}}$.

$$\mathfrak{O}_{\mathfrak{P}} = \{\alpha \in L \mid v_{\mathfrak{P}}(\alpha) \geq 0\}$$

Preuve : Utilise un théorème de Dwork & Robba 79

On Natural Radii of p -adic Convergence

Réduction de $\mathcal{T}(F)$

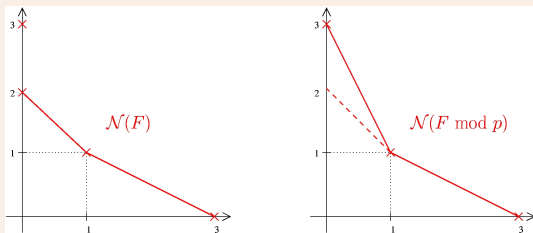
Théorème

Si F a une bonne p -réduction locale, alors $\mathcal{T}(F) = \mathcal{T}(\bar{F})$.

Faux avec les polygones classiques :

Exemple

$$F(X, Y) = (Y - pX)(Y^2 - X) + X^3 \Rightarrow \text{tc}(R_F) = 4$$



Choix du nombre premier p

- $K = \mathbb{Q}(\gamma)$, $w = [K : \mathbb{Q}]$, M_γ le polynôme minimal de γ
- $\text{ht}(Q) = \log \|Q\|_\infty$ où Q est un polynôme multivarié.

$\text{ht}(p)$ appartient à

- Stratégie déterministe
 $O(wd_Y(w\text{ht}(M_\gamma) + \text{ht}(F) + \log(wd_X d_Y)))$
- Stratégie de type Monte-Carlo, probabilité d'erreur $\leq \epsilon$
 $O(\log(d_Y w \log d_X) + \log(\text{ht}(F)) + \log(\text{ht}(M_\gamma)) + \log(\epsilon^{-1}))$
- Stratégie de type Las-Vegas, 2 itérations en moyenne
 $O(\log(d_Y w \log d_X) + \log(\text{ht}(F)) + \log(\text{ht}(M_\gamma)))$

Complexité de l'algorithme rationnel au-dessus de $L = \mathbb{F}_{p^{t_0}}$

Substitutions $\rightarrow \mathcal{O}(\delta_F^2 d_Y)$

Factorisations $\rightarrow \mathcal{O}(\delta_F [d_Y^2 + d_Y t_0 \log p])$

Total $\rightarrow \mathcal{O}(\delta_F d_Y [\delta_F + d_Y + t_0 \log p])$

Lemme

$$\delta_F \leq v_X(\Delta_F) \leq d_X(2d_Y - 2)$$

Théorème (Nombre d'opérations dans L)

$\rightarrow \mathcal{I}(\bar{F})$ au-dessus de 0 : $\mathcal{O}(d_Y^3 d_X^2 + d_Y^2 d_X t_0 \log p)$

$\rightarrow \mathcal{I}(\bar{F})$ au-dessus de l'ensemble des points critiques :

$$\mathcal{O}(d_Y^3 d_X^2 t_0 \log p)$$

D. Duval 89 *Rational Puiseux Expansions* : $\mathcal{O}(d_Y^6 d_X^2)$

Complexité binaire du calcul de $\mathcal{T}(F)$

- $F \in K[X, Y]$
- $K = \mathbb{Q}(\gamma)$
- $w = [K : \mathbb{Q}]$
- M_γ le polynôme minimal de γ

Théorème

Il existe un algorithme de type Monte-Carlo qui calcule $\mathcal{T}(F)$ en

$$\tilde{O}(d_Y^3 d_X^2 w^2 \log^2 \epsilon^{-1} [\text{ht}(M_\gamma) + \text{ht}(F)])$$

opérations binaires avec une probabilité d'erreur $\leq \epsilon$.

Partie numérique : suivre $\mathcal{T}(F)$

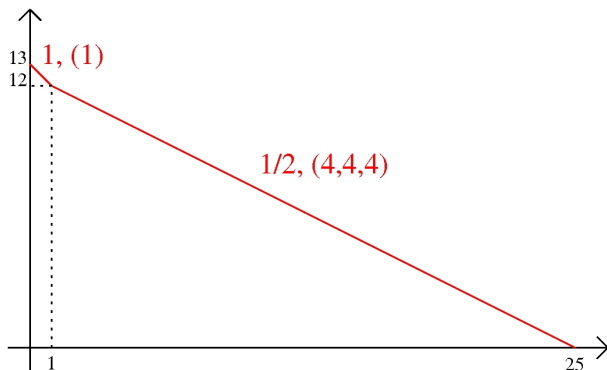
Suivre $\mathcal{T}(F)$ numériquement : un exemple

Développements de Puiseux de F :

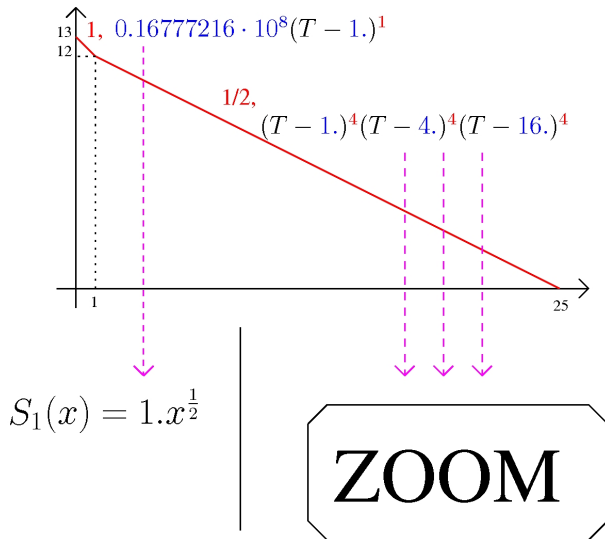
- $S_1(X) = X + \dots$
- $S_2(X) = 4X^{\frac{1}{2}} + X^{\frac{7}{8}} + \dots$
- $S_3(X) = 2X^{\frac{1}{2}} + 2X + \dots$
- $S_4(X) = 2X^{\frac{1}{2}} + X + X^{\frac{7}{6}} + \dots$
- $S_5(X) = X^{\frac{1}{2}} + 2X + X^{\frac{5}{4}} + \dots$
- $S_6(X) = X^{\frac{1}{2}} + X + \dots$
- $S_7(X) = X^{\frac{1}{2}} + 4X + \dots$

$d_Y = 25, d_X = 26$; $1 \leq \text{coefficients} \leq 10^{13}$; *Digits* = 20.

Premier polygone de Newton



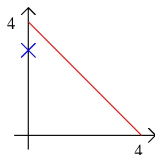
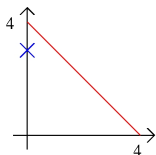
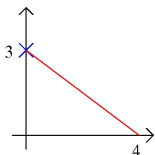

Premier polygone de Newton



Tri selon les polygones

$$G_i(X, Y) \leftarrow \frac{F(X^2, X(Y + \xi_i^{1/2}))}{X}, \quad \xi_1 = 1. \quad \xi_2 = 4. \quad \xi_3 = 16.$$

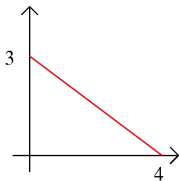
$\{G_1, G_2, G_3\}$



polynôme	coefficient en X^3
G_1	0.
G_2	0.
G_3	-17199267840000.0

Tri selon les polygones

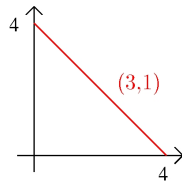
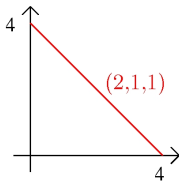
G_3



$$\phi_3 = 17199267840000.0(T - 1.)^1$$

$$S_2(x) = 4.x^{\frac{1}{2}} + 1.x^{\frac{7}{8}}$$

$\{G_1, G_2\}$



Tri selon les structures
de multiplicité

Tri selon les multiplicités

Structures de multiplicité :

- $(2, 1, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 1$
- $(3, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 2$

Polynômes caractéristiques :

$$\phi_1 = 1049760000.0 - 2361960000.0 T + 1837080000.0 T^2 - 590490000.0 T^3 + 65610000.0 T^4$$

$$\phi_2 = 1719926784.0 - 6019743744.0 T + 7739670528.0 T^2 - 4299816960.0 T^3 + 859963392.0 T^4$$

- 1 $S_i \leftarrow \text{Syl}(\phi_i, \phi'_i)$
- 2 Calcul des valeurs singulières des S_i

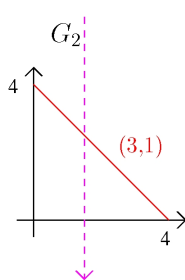
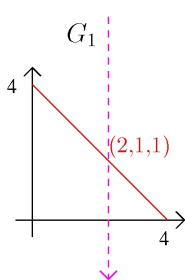
Tri selon les multiplicités

Valeurs singulières associées à ϕ_1 :

[710694508.4327095884, 5827385163.0346368216, 3038236185.2953794346, 1140210769.8445335036, 40759543.641844042087, 1882790.0681572535369, 3.8263754075532025314 $\cdot 10^{-11}$]

Valeurs singulières associées à ϕ_2 :

[37445022322.189717034, 24644791488.066781055, 12101920587.793187214, 3915075466.8959244453, 31534726.725839766232, 0.00000000074101187358617089031, 0.00000000027761147770454585021]



Exemples

Exemple 1

$$M_{a,d} = x^d - 2(ax - 1)^2, F_1(x, y) = y^3 - M_{10,5}(x)$$

coefficient en $x^{16/3}$:

Digits	évaluation numérique	algorithme numérique-modulaire
10	0	7
40	0	36
50	6	47

Algorithme de monodromie :

- version symbolique/numérique : 0.950 secondes. Précision de 40 chiffres nécessaires pour avoir un résultat correct.
- version numérique/modulaire : 0.839 secondes. Digits 10.

Exemple 2

$$F_2(x, y) = (y^3 - M_{10,6}(x))(y^3 - M_{10,3}(x)) + y^2 x^5$$

coefficient en $x^{1/2}$

Digits	évaluation numérique	algorithme numérique-modulaire
10	0	4
20	0	15
30	5	29

Exemple 3

$$G_n(x, y) = \left(y^{\lceil \frac{n}{2} \rceil} - P_{\lceil \frac{n}{2} \rceil}(x) \right) G_{\lfloor \frac{n}{2} \rfloor}(x, y)$$

où

$$P_{n_0}(x) = \frac{1}{n_0 3!} x \left(x^{n_0} + (n_0 - 1)x - \frac{1}{n_0!} \right).$$

Polynôme considéré	algorithme symbolique temps en secondes	algorithme numérique-modulaire	
		temps en secondes	précision
G_8	0.031	0.029	9
G_{12}	0.041	0.099	9
G_{16}	2.3	0.221	9
G_{20}	0.751	0.550	9
G_{24}	2.889	0.920	9
G_{28}	8.509	1.719	9
G_{32}	30.820	5.040	9

Résumé

- Critère de réduction :
 - Permet de calculer $\mathcal{T}(F)$
 - Algorithmes probabilistes \rightarrow petit p
- Utilisation de $\mathcal{T}(F)$ pour le calcul numérique :
 - Filtre à deux étages
 - Utilisation de la SVD
- Bornes de complexité améliorées
- Complexité binaire pour le calcul de $\mathcal{T}(F)$

Perspectives

- Extensions : complexité (calcul du genre)
- Contrôle des erreurs numériques (implémentation certifiée)
- Autres utilisations de la stratégie modulaire-numérique.