Calcul symbolique-numérique des développements de Puiseux au dessus des points critiques partie modulaire

Adrien Poteaux

XLIM-DMI (UMR CNRS 6172)
Université de Limoges

Journées Gecko

Problématique

- But : évaluation numérique de fonctions algébriques près d'un point critique.
- Pourquoi ?
  - Utile dans le cadre du théorème d'Abel Jacobi.
  - Utile pour le calcul de la monodromie (Poteaux, SNC 2007).
- Comment ?
  - Calcul numérique des développements de Puiseux au dessus des points critiques.
  - Nécessité d'avoir des informations exactes
    $\Rightarrow$ obtenues par un calcul modulo p.
- Aujourd'hui : partie modulaire de l'algorithme
  - Critère de bonne réduction (choix du nombre premier p).
  - Déduction de l'arbre des polygones du calcul modulo p.
  - Complexité bit de l'algorithme de Newton-Puiseux modulo p.

Notations

- $F \in \mathcal{K}[X, Y]$ unitaire, sans carré où $\mathcal{K}$ sous-corps de $\mathbb{C}$.
- $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$ la courbe associée.
- **Fibre** en x_0 : $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier :** $\#\mathcal{F}(x_0) = D_Y$.
- **Point critique :** $\#\mathcal{F}(x_0) < D_Y$.
- $\delta(x_0)$: distance entre x_0 et son plus proche point critique.

Points réguliers

Soit x_0 régulier et $\mathcal{F}(x_0) = \{y_1, \ldots, y_{D_Y}\}$ la fibre en x_0.

- Théorème des fonctions implicites : il existe D_Y séries $Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik}(X - x_0)^k$ t.q. $F(x, Y_i(x)) = 0$ dans un voisinage de x_0 et $Y_i(x_0) = y_i$.
- Ces séries ont un rayon de convergence au moins égal à $\delta(x_0)$.
- Newton quadratique : N termes en $O\tilde{}(D_Y N)$ opérations dans $\mathcal{K}$ (pour une série).
  Kung & Traub 1978, *All algebraic functions can be computed fast*

Points critiques : Séries de Puiseux

- Il existe D_Y séries $Y_{ij}(X) = \sum_{k=1}^{\infty} \alpha_{ik}\, \zeta_{e_i}^{jk}\, (X - x_0)^{\frac{k}{e_i}}$ 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 e_i-ème de l'unité.
  - $e_1, \ldots, e_s$ partition de D_Y
- Les e_i sont les **indices de ramification**.
- Ces séries ont un rayon de convergence au moins égal à $\delta(x_0)$.

But : Calculer rapidement une évaluation numérique de ces séries.

Partie singulière

$$Y_{ij}(X) = \sum_{k=1}^{\infty} \alpha_{ik}\, \zeta_{e_i}^{jk}\, (X - x_0)^{\frac{k}{e_i}}$$

Définition

L'indice de régularité de Y_{ij} est le plus petit entier c_{ij} qui vérifie la propriété qu'aucune autre série de Puiseux de F ait pour somme partielle $\sum_{k=1}^{c_{ij}} \alpha_{ik}\, \zeta_{e_i}^{jk}\, (X - x_0)^{\frac{k}{e_i}}$

Définition

La partie singulière de la série S_{ij} est $\sum_{k=1}^{c_{ij}} \alpha_{ik}\, \zeta_{e_i}^{jk}\, (X - x_0)^{\frac{k}{e_i}}$

Remarque : termes suivant = partie régulière.

$\Rightarrow$ calculés via Newton quadratique.

Etat de l'art

- Newton (1676) : donne le principe.
- Puiseux (1850) : première procédure.
- Chystov (1986) : complexité binaire polynomiale.
- Duval (1989) : algorithme rationnel.
  - Minimise l'extension de $\mathcal{K}$ dans laquelle on travaille.
  - Calcul de la partie singulière : $O(d^8)$ opérations dans $\mathcal{K}$ où $d = \max(D_X, D_Y)$.
- Walsh (2000) : complexité binaire de la partie singulière :

  $\tilde{O}({D_Y}^{32}{D_X}^4)$ (pour l'algorithme classique).
- Walsh (1999) : taille polynomiale des coefficients pour certains développements rationnels.
- Utilisation de l'équation différentielle.

Algorithme de Newton-Puiseux : partie singulière

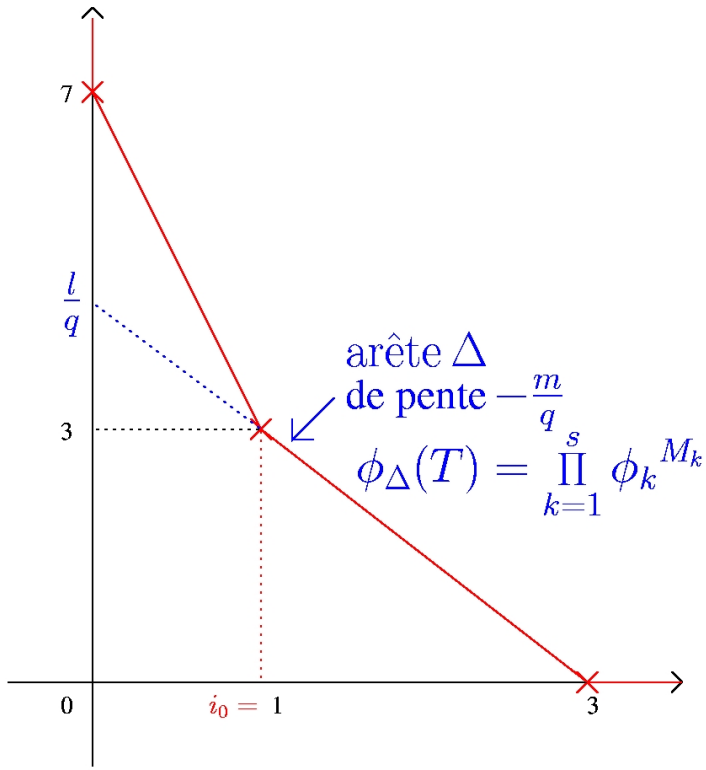
$$F(X,Y) = \sum_{i,j} a_{ij} X^j Y^i \ , \ P(X) = X \ , \ Q(X,Y) = Y$$

Pour chaque arête Δ

- u, v tels que $uq - vm = 1$.
- polynôme caractéristique :

$$\phi_\Delta(T) = \sum_{(i,j)\in\Delta} a_{ij} T^{\frac{i-i_0}{q}}$$

Pour chaque ϕ_k, ξ t.q. $\phi_k(\xi) = 0$.



- $F(X,Y) \leftarrow \dfrac{F(\xi^u X^q, \xi^v X^m(1+Y))}{X^l}$
- $P(X) \leftarrow P(\xi^u X^q)$
- $Q(X,Y) \leftarrow Q(\xi^u X^q, \xi^v X^m(1+Y))$

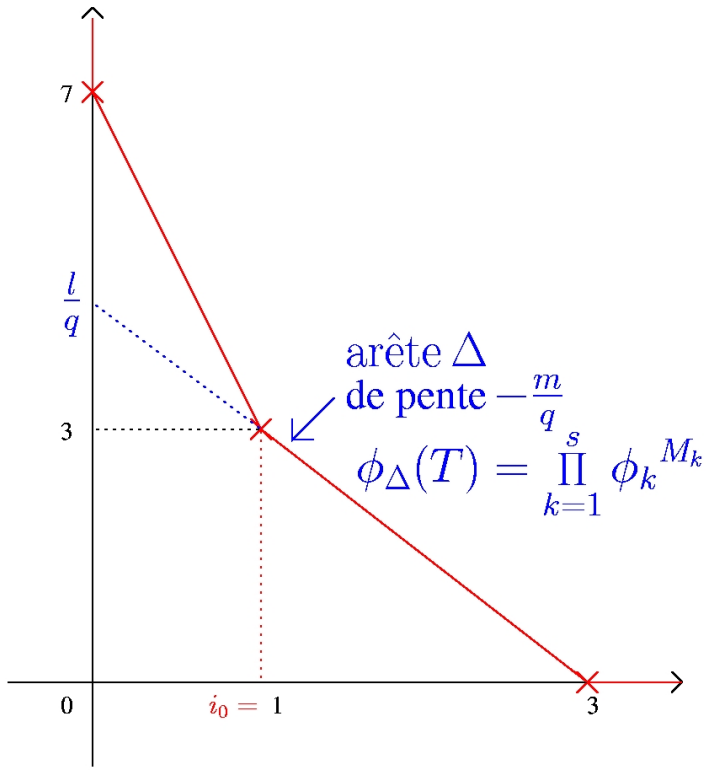
$$x(T) = P(T), y(T) = Q(T,0)$$

Algorithme numérique ?

$$F(X,Y) \leftarrow \frac{F(\xi^u X^q, \xi^v X^m (1+Y))}{X^l}$$

Certains informations doivent être connues de façon exacte :

- Les polygones de Newton
- Les multiplicités des racines de ϕ_Δ



Algorithme symbolique

- Calcul dans des extensions de degré potentiellement élevé.
- Croissance des coefficients.

Exemple : $F = (y^3 - x)\,((y-1)^2 - x)\,(y - 2 - x^2) + x^2\,y^5$ a pour discriminant $x^3\,P(x)$ avec $deg_x(P) = 23$.

Les coefficients de son développement de Puiseux à l'ordre 1 ont une taille de 136 chiffres !

Approche numérique-modulaire

1. Calcul de la partie singulière modulo un bon premier p.

   Cela nous donne :

   - Les pentes rationnelles $-\frac{m}{q}$ avec $q \neq 1$.
   - Les multiplicités des racines de $\phi_\Delta(T)$, sauf éventuellement une.

2. Ajout des pentes entières.

3. Calcul numérique des séries de Puiseux guidé par les informations modulaires.

Partie modulaire

1. Critère de bonne réduction.
2. Des séries modulo p à l'arbre de polygone.
3. Complexité binaire de l'algorithme modulaire.

Réductibilité des séries modulo p

On s'intéresse au calcul des séries de Puiseux au dessus de 0.

Théorème

Soit p un nombre premier tel que

- $p > D_Y$
- *On peut former la réduction $\overline{F}$ de F modulo p.*
- *$Disc_Y(F)$ et $Disc_Y(\overline{F})$ ont la même valuation X-adique.*

Alors les séries de Puiseux peuvent être réduites modulo p

Exemple : $F(X,Y) = Y^2 - X^3(X+p)$

Séries solutions :

$$S(X) = \sqrt{p}(-1)^j X^{\frac{3}{2}} + \frac{1}{2\sqrt{p}}(-1)^j X^{\frac{5}{2}} - \frac{1}{8p^{\frac{3}{2}}} X^{\frac{7}{2}} + \frac{1}{16p^{\frac{5}{2}}}(-1)^j X^{\frac{9}{2}} + \dots$$

Discriminant : $Disc_Y(F) = 4pX^3 + 4X^4$

Preuve :

Dwork & Robba (1979), *On natural radii of p-adic convergence* :

Théorème

Le rayon de convergence p-adique des séries de Puiseux est supérieur ou égal à la valeur absolue p-adique de la plus petite racine du discriminant.

$Disc_Y(F) = X^{\mu}(c_0 + \cdots + c_r X^r)$ avec $val_p(c_0) = 0$ et $val_p(c_i) \geq 0$.

Si $val_p(x) > 0$ et $x \neq 0$, alors $val_p(c_0 + c_1 x + \cdots + c_r x^r) = 0$.
$\Rightarrow$ Pas de racines du discriminant dans $D(0, 1^-)$
Les séries de Puiseux convergent p-adiquement sur $D(0, 1^-)$.

En tant que racine de F (dont les coefficients sont de valuation positive), les séries de Puiseux sont bornés p-adiquement par 1 .

Preuve :

$$S(X) = \sum_i \alpha_i X^{i/e}$$

.

1. $S(X)$ converge sur $D(0, 1^-)$.
2. $|S(x)|_p \leq 1$ pour $x \in D(0, 1^-)$.

Proposition

Soit $S \in \mathbb{C}_p[[X]]$ *convergente et bornée sur* $D(0, 1^-)$.
Alors $\sup\{|S(x)|_p, x \in D(0, 1^-)\} = \max_i |\alpha_i|_p$.

Conclusion : $\max_i |\alpha_i|_p \leq 1$, soit $val_p(\alpha_i) \geq 0 \ \forall i$ $\square$

Bonne réduction des séries

Pour pouvoir suivre l'algorithme numériquement, on a besoin :

- Des pentes des polygones.
- Des multiplicités des polynomes caractéristiques.

On a donc besoin de préserver :

- les pentes non entières (mônomes introduisant la ramification).
- la différenciation des racines des polynomes caractéristiques.

Il faut donc que les termes de tête des différences de racines ne soient pas réduits à 0 modulo p, et donc que la valuation du discriminant reste inchangée.

Exemple : $F \in \mathcal{K}[X, Y]$, $D_Y = 21, D_X = 22$

(1) $Y = X^{1/2} - 23X + X^{3/2}$ (4) $Y = X^{1/3}$

(2) $Y = X^{1/2} - 23X + 2X^{3/2}$ (5) $Y = 5X^{1/3} + X^{2/3} + X^{5/6}$

(3) $Y = X^{1/2} - 23X + 46X^{3/2}$ (6) $Y = 5X^{1/3} + X^{2/3} + 2X^{5/6}$

Coefficient de plus bas degré du discriminant : $-2^{92}3^{71}5^{244}11^{4}31^{24}$

Du modulaire au numérique : un exemple

1. Calcul des séries modulo $p = 23$:

(1)	$Y = X^{1/2} + X^{3/2}$	(4)	$Y = X^{1/3}$
(2)	$Y = X^{1/2} + 2X^{3/2}$	(5)	$Y = 5X^{1/3} + X^{2/3} + X^{5/6}$
(3)	$Y = X^{1/2} + X^{2}$	(6)	$Y = 5X^{1/3} + X^{2/3} + 2X^{5/6}$

2. On ajoute les pentes entières :

(1)	$Y = X^{1/2} + \alpha X + X^{3/2}$	(4)	$Y = X^{1/3}$
(2)	$Y = X^{1/2} + \alpha X + 2X^{3/2}$	(5)	$Y = 5X^{1/3} + X^{2/3} + X^{5/6}$
(3)	$Y = X^{1/2} + \alpha X + \beta X^{3/2}$	(6)	$Y = 5X^{1/3} + X^{2/3} + 2X^{5/6}$

3. On reconstruit l'arbre des polygones à partir de ces séries

Complexité binaire de l'algorithme rationnel modulo p

Algorithme rationnel :

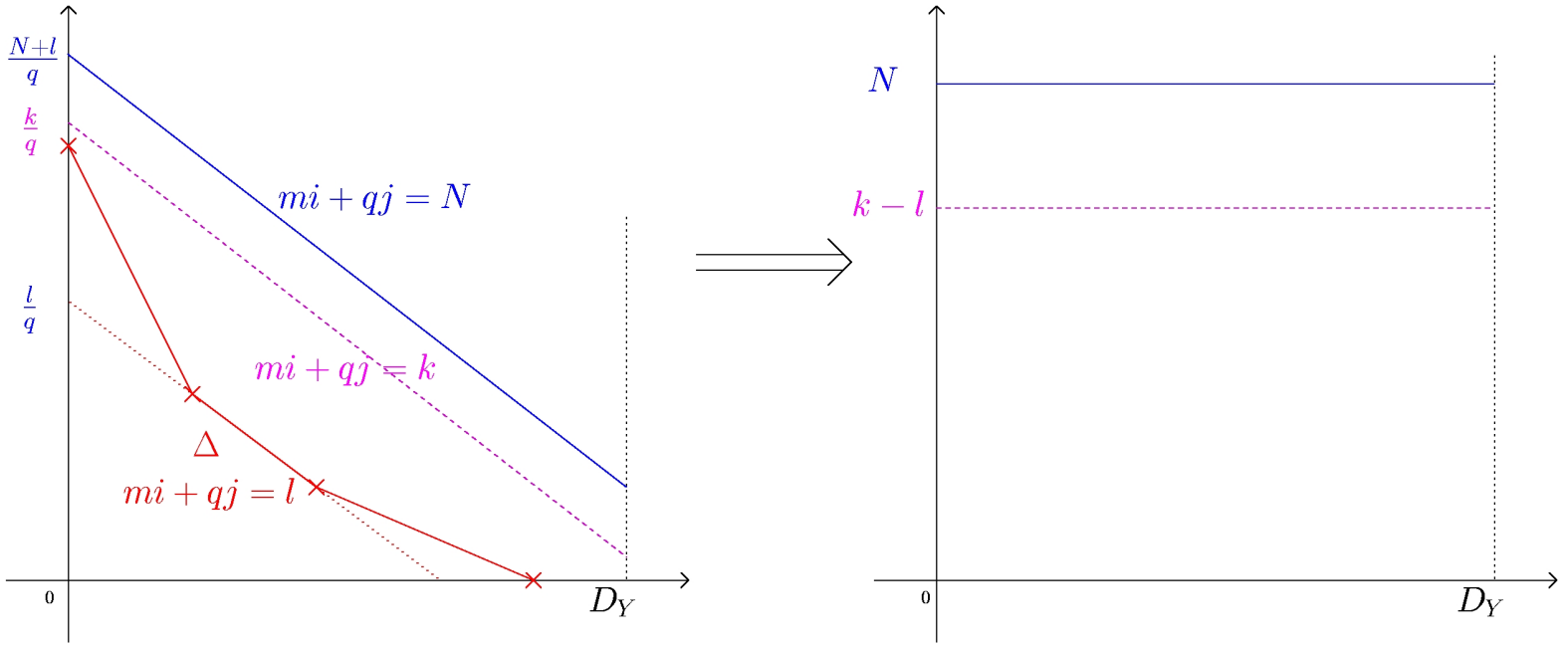
- Calcule un représentant par classe de conjugaison.
- $X_i(T) = \lambda T^{e_i}$, $Y_i(T) = \sum_{k=0}^{\infty} \alpha_{i,k} T^k$, $\alpha_{i,k} \in \mathcal{K}_i$, $1 \leq i \leq r$.
- Si $f_i = [\mathcal{K}_i : \mathcal{K}]$, on a $\sum_{i=0}^{r} e_i f_i = D_Y$.

A chaque étape, opérations la plus coûteuse :

- Calcul de $F(\xi^v X^q, \xi^u X^m(1+Y))$.

Une opération dans $\mathbb{F}_q$: $O(M(\log q) \log\log q)$ opérations binaires.

Transformation sur le polygone



$$F_k(X,Y) := \sum_{mi+qj=k} a_{ij} X^j Y^i.$$

$F_{k,1}(X,Y) = F(X^q, X^m Y)/X^l$ (transformation géométrique).

$F_{k,2}(X,Y) = \xi^{\frac{vk}{q}} F_{k,1}(X, \xi^{\frac{-mv}{q}}(Y+1))$ (shift).

Changements de variable

Notons $M_{i,k}$ le coût du k-ième changement de variable associé à la i-ième branche, et M_i le coût des développements successifs pour la i-ième branche.

$$\begin{aligned} M_{i,k} &= N_k \text{ shifts} \\ &= O(ND_Y \log D_Y) \text{ opérations dans } \mathbb{F}_q. \\ &= O(ND_Y f_i \log D_Y \log f_i \log p) \text{ opérations binaires.} \end{aligned}$$

$$\begin{aligned} M_i &= \sum_{k=1}^{N} M_{i,k} \\ &= O(N^2 D_Y f_i \log D_Y \log f_i \log p) \text{ opérations binaires.} \end{aligned}$$

Coût de l'ensemble des changements de variables :

$$\begin{aligned} \sum_{i=1}^{s} M_i &= O(N^2 D_Y \sum_{i=1}^{r} f_i (\log D_Y)^2 \log p) \\ &= O(N^2 {D_Y}^2 (\log D_Y)^2 \log p) \end{aligned}$$

$\Rightarrow$ borne quadratique en la sortie.

Application à la partie singulière

Proposition

On peut borner par le nombre de termes N nécessaires pour séparer les racines par la valuation du discriminant en Y

Donc $N \leq val_X(Disc_Y(F)) = O(D_X D_Y)$.

Théorème

Le nombre d'opérations binaires pour calculer la partie singulière des développements de Puiseux de $F \in \mathbb{F}_p[X, Y]$ est borné par $O({D_Y}^4 {D_X}^2 (\log D_Y)^2 \log p)$.

Conclusion-Perspectives

- Choix du premier p :
  - Critère de réduction : problème du calcul du discriminant. Méthode probabiliste ?

- Complexité : quadratique en la sortie. Acceptable en pratique.
  - Complexité pour trouver p (ou taille du p).
  - Affiner la borne pour N (introduction des e_i).