

Calcul du groupe de monodromie d'une courbe algébrique plane

Poteaux Adrien

UPMC / INRIA Rocquencourt, équipe SALSA

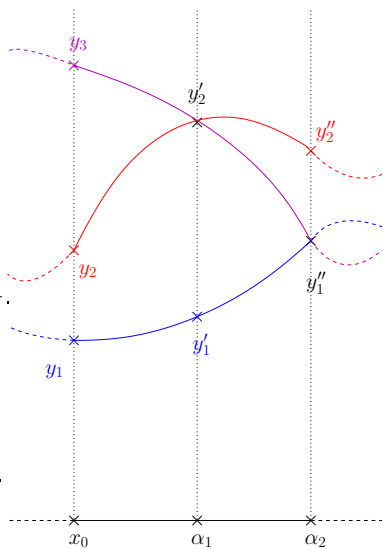
Séminaire de théorie des nombres
Institut de Mathématiques de Toulouse
22 février 2011

Notations

- $K = \mathbb{Q}(\alpha)$ un corps de nombres
- $F(X, Y) \in K[X, Y]$ squarefree
- $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$

Soit $x_0 \in \mathbb{C}$:

- **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** : $\#\mathcal{F}(x_0) < d_Y$.
- $\{\alpha_i\}_i = \{\text{racines de } \text{Res}_Y(F, F_Y)\}$.
- $\delta(x_0) = \min_{\alpha_i \neq x_0} |x_0 - \alpha_i|$.



Développement en série

- x_0 régulier; $\mathcal{F}(x_0) = \{y_1, \dots, y_{d_Y}\}$.

Théoreme (des fonctions implicites)

Il existe d_Y séries $Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k$ t.q.

$F(X, Y_i(X)) = 0$ sur un voisinage de x_0 et $Y_i(x_0) = y_i$.

Développement en série

- x_0 régulier; $\mathcal{F}(x_0) = \{y_1, \dots, y_{d_Y}\}$.

Théorème (des fonctions implicites)

Il existe d_Y séries $Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k$ t.q.

$F(X, Y_i(X)) = 0$ sur un voisinage de x_0 et $Y_i(x_0) = y_i$.

- x_0 critique

Théorème (Puiseux)

Il existe d_Y séries $Y_{ij}(X) = \sum_{k=n_j}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$ 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 de l'unité d'ordre e_i
- e_1, \dots, e_s partition de d_Y .

Exemples au-dessus de $X = 0$

- $F(X, Y) = Y^3 - X$:

$$\zeta_3^k X^{\frac{1}{3}}, \quad k = 1, 2, 3 \quad (e = 3)$$

- $H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$:

$$\zeta_3^k X^{\frac{1}{3}} + \frac{1}{6} X^3 + \frac{5}{12} \zeta_3^k X^{\frac{10}{3}} + \dots, \quad k = 1, 2, 3 \quad (e = 3)$$

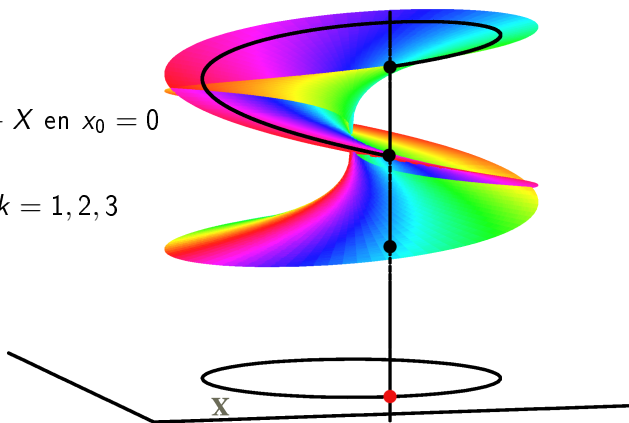
$$1 + \zeta_2^k X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^k X^{\frac{3}{2}} + \dots, \quad k = 1, 2 \quad (e = 2)$$

$$2 - 3X^2 - \frac{9}{2} X^3 + \dots \quad (e = 1)$$

Prolongement analytique autour d'un point critique

- $G(X, Y) = Y^3 - X$ en $x_0 = 0$

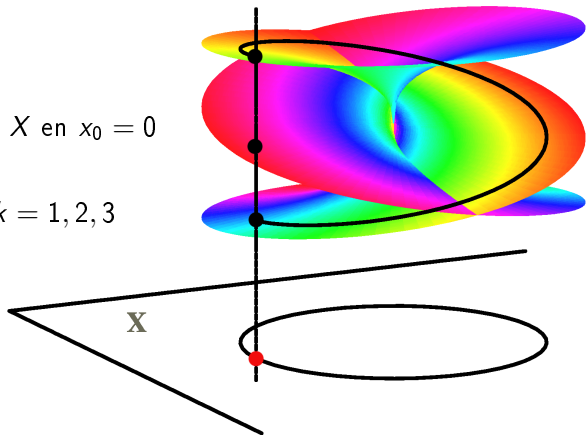
- $Y_k(X) = j^k X^{\frac{1}{3}}$, $k = 1, 2, 3$



Prolongement analytique autour d'un point critique

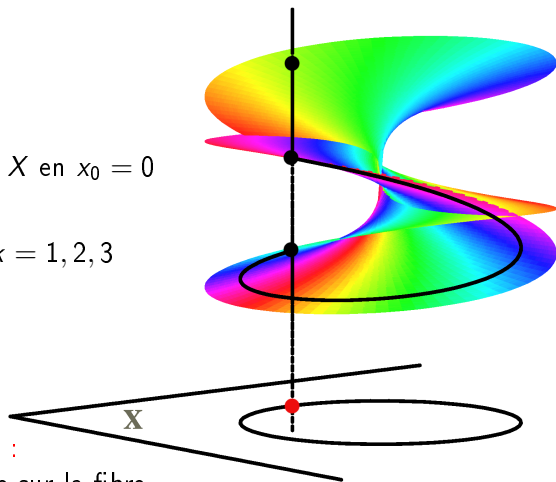
- $G(X, Y) = Y^3 - X$ en $x_0 = 0$

- $Y_k(X) = j^k X^{\frac{1}{3}}, k = 1, 2, 3$



Prolongement analytique autour d'un point critique

- $G(X, Y) = Y^3 - X$ en $x_0 = 0$
- $Y_k(X) = j^k X^{\frac{1}{3}}$, $k = 1, 2, 3$



⇒ **Monodromie locale :**
permutation engendrée sur la fibre.

Monodromie locale

$$H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$$

$$2 - 3X^2 - \frac{9}{2}X^3 + \dots$$

$\Rightarrow e = 1$: 1-cycle.

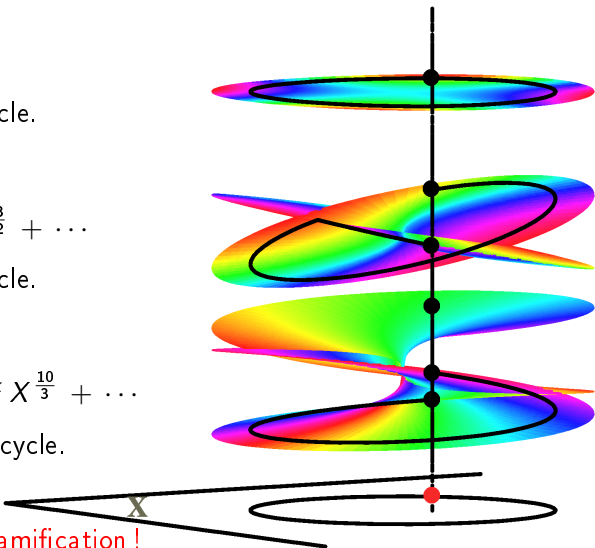
$$1 + \zeta_2^k X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^k X^{\frac{3}{2}} + \dots$$

$\Rightarrow e = 2$: 2-cycle.

$$\zeta_3^k X^{\frac{1}{3}} + \frac{1}{6} X^3 + \frac{5}{12} \zeta_3^k X^{\frac{10}{3}} + \dots$$

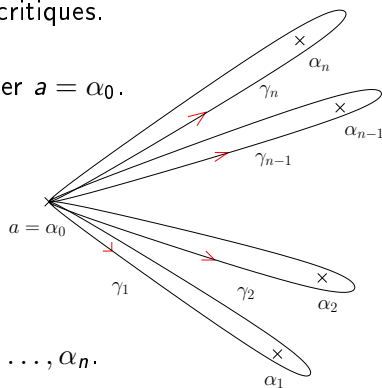
$\Rightarrow e = 3$: 3-cycle.

La monodromie locale
se lit sur les indices de ramification !



Groupe de monodromie

- On note $\alpha_1, \dots, \alpha_n$ les points critiques.
- On fixe un point de base régulier $a = \alpha_0$.



- On cherche les n permutations $\sigma_1, \dots, \sigma_n$ correspondant à $\alpha_1, \dots, \alpha_n$.

\implies ces permutations engendrent le groupe de monodromie.

Motivations

- Théorie de Galois

J. Harris 1979, *Galois groups of enumerative problems*

H. Volklein 1997, *Groups as Galois Groups*

Motivations

- Théorie de Galois
- Factorisation

Galligo & van Hoeij 2007, *Approximate bivariate factorization : a geometric viewpoint*

Galligo & Poteaux 2009, *Continuations and monodromy on random Riemann surfaces*

Galligo & Poteaux 2010, *Computing monodromy via continuation methods on random Riemann surfaces*

Motivations

- Théorie de Galois
- Factorisation
- Théorème d'Abel-Jacobi effectif

Calcul du groupe d'homologie à l'aide du groupe de monodromie

Deconinck & van Hoeij 2001, *Computing Riemann Matrices of Algebraic Curves*

Tretkoff & Tretkoff 1984, *Combinatorial Group Theory, Riemann Surfaces and Differential Equations*

Motivations

- Théorie de Galois
- Factorisation
- Théorème d'Abel-Jacobi effectif
 - Applications en calcul formel
 - Primitive de fonctions algébriques(partie logarithmique de l'intégrale).
Risch 1969, Davenport 1981, Trager 1984, Bronstein 1990, Bertrand 1995...
 - Solutions algébriques d'EDO
Baldassarri & Dwork 1979, *On Second Order Linear Differential Equations with Algebraic Solutions*
 - Calcul de groupe de Galois différentiel
Compoint & Singer 1998, *Relations linéaires entre solutions d'une équation différentielle*

Motivations

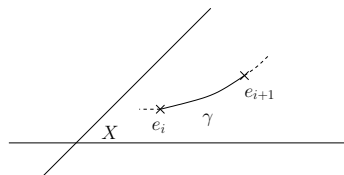
- Théorie de Galois
- Factorisation
- Théorème d'Abel-Jacobi effectif
 - Applications en calcul formel
 - Applications en physique
 - Calcul des solutions quasi-périodiques des équations KP.
Deconinck & Segur 1998, The KP Equation with Quasiperiodic Initial Data
 - Solutions solitons des équations KdV (Korteweg-de Vries) et NLS (Nonlinear Schrödinger).

Calcul du groupe de monodromie

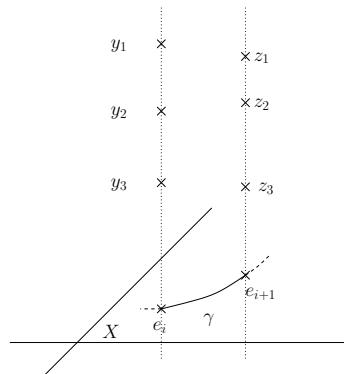
A. Poteaux 2007, *Computing monodromy groups defined by plane algebraic curves*

Méthode « relier les fibres »

- 1 Choix des chemins.
- 2 Choix des points de connexion.

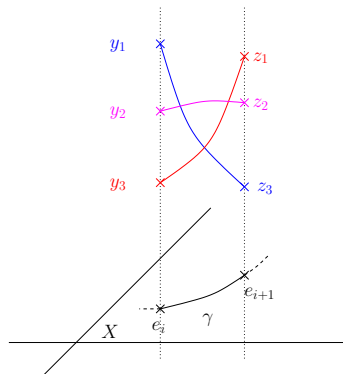


Méthode « relier les fibres »



- 1 Choix des chemins.
- 2 Choix des points de connexion.
- 3 Calcul des fibres.

Méthode « relier les fibres »



- 1 Choix des chemins.
- 2 Choix des points de connexion.
- 3 Calcul des fibres.
- 4 Méthode de connexion.

Monodromie : état de l'art (sketch)

1 Relier les fibres

→ Deconinck & van Hoeij 2001

- Fonction monodromy de Maple.
- Fibres reliées à l'aide des dérivées premières.
- Critère de connexion et contrôle de l'erreur heuristiques.

→ van Hoeij & Rybowicz (com. perso.)

- Théorème de Smith + arithmétique numérique/intervalles.
- Algorithme certifié mais trop lent

2 Equation différentielle

Monodromie : état de l'art (sketch)

1 Relier les fibres

2 Equation différentielle

- Intérêt : calcul rapide des développements à ordre élevé.

Chudnovsky & Chudnovsky 1986, 1990 ; van der Hoeven 2000 ;
Cormier-Singer-Trager-Ulmer 2002 ; Bostan & all 2007 ...

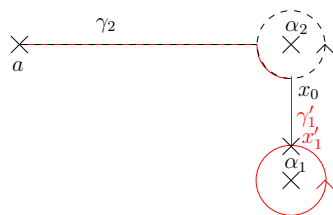
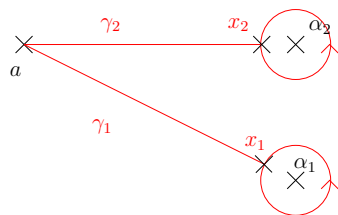
- Calcul de l'équation différentielle potentiellement coûteux.
- Taille de l'équation différentielle importante.
- On utilise des développements à ordre petit.

Stratégie employée

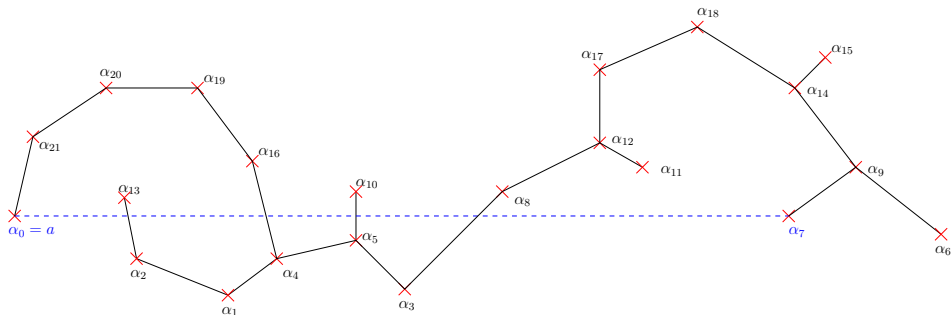
- 1 Choix des chemins : arbre de recouvrement minimum.
- 2 Méthode de connexion : développements en série tronqués et développements de Puiseux **au-dessus des points critiques**.
 - Bornes sur les ordres de troncation.
 - Donne la monodromie locale.
 - Utile pour l'application d'Abel (Deconinck & Patterson 2008).
- 3 Choix des points intermédiaires :
 - Compromis ordres de troncation / nombre de points.
 - Borne sur le nombre de points intermédiaires.

Utiliser un arbre de recouvrement minimum

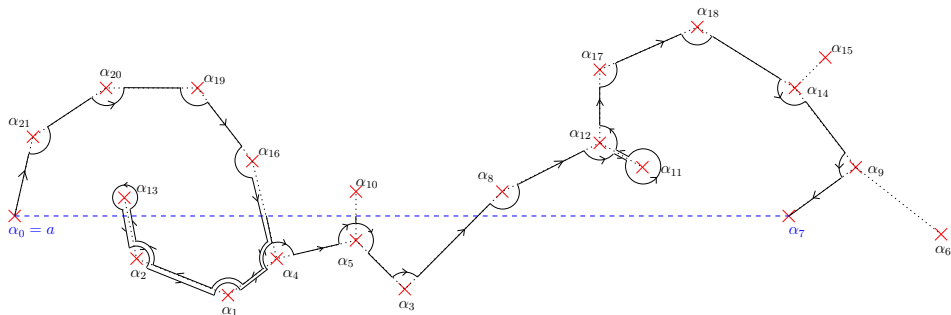
Intérêt : minimiser la longueur totale des chemins



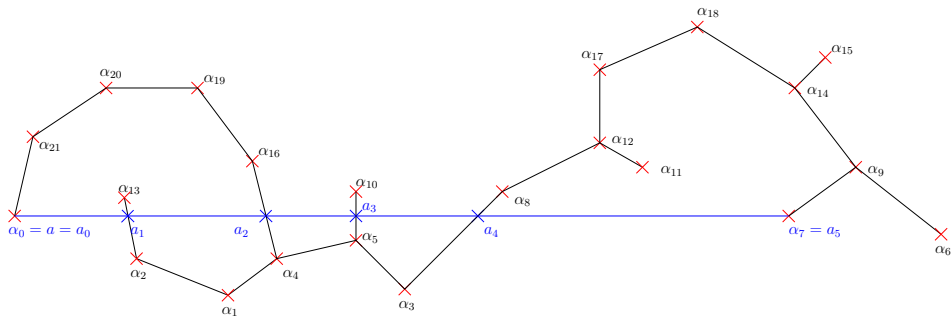
Objectif : « chemin dans l'arbre » homotope à γ_7



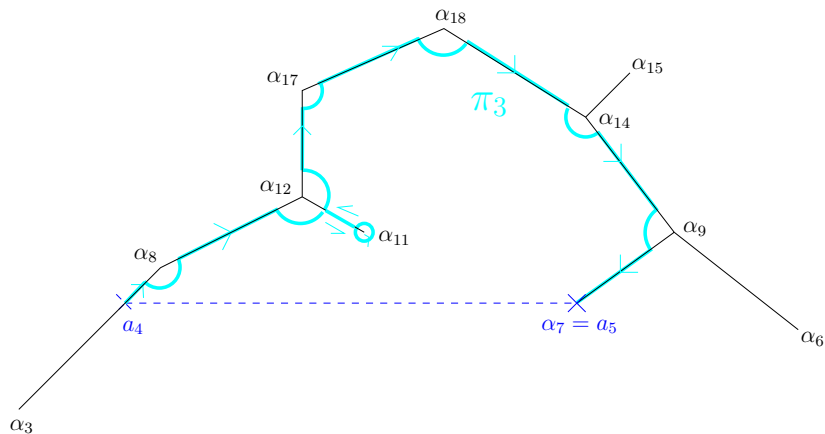
Objectif : « chemin dans l'arbre » homotope à γ_7



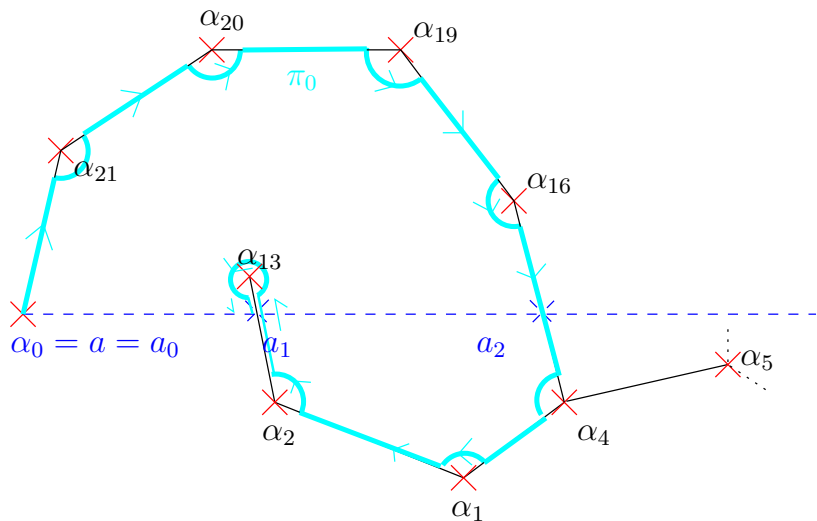
Découpage du segment $[a, \alpha_7]$



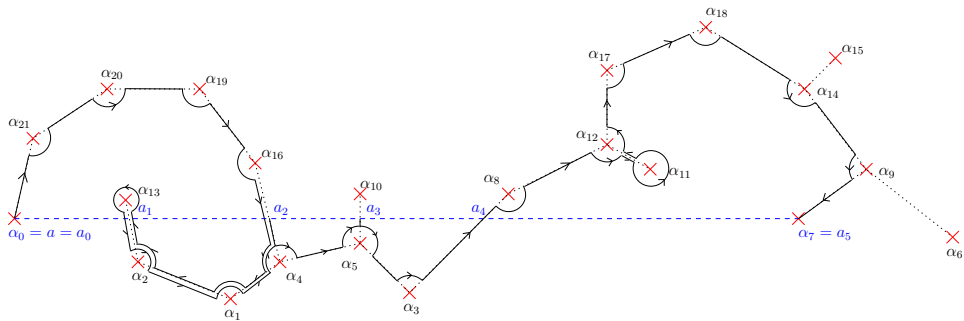
Segment $[a_i, a_{i+1}]$: un unique sens de contournement



Segment $[a_i, a_{i+1}]$: un unique sens de contournement

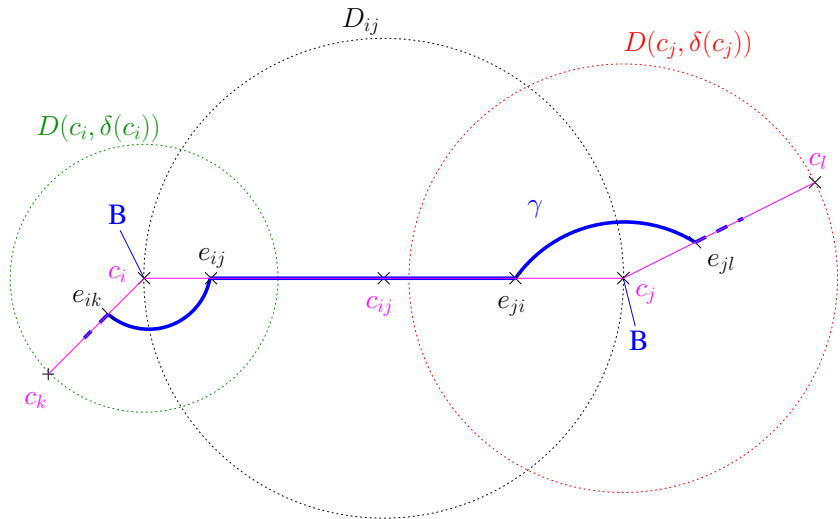


Résultat



Prolongement analytique le long de l'arbre

Connexions le long de l'arbre



Proposition

Soit

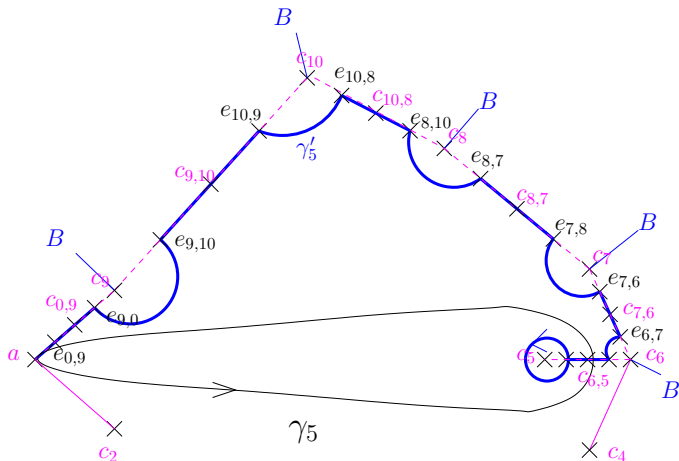
- $Y(X) = \sum_{k=0}^{\infty} \mu_k (X - x_0)^{\frac{k}{e}}$ une série de Puiseux,
- $\tilde{Y}(X) = \sum_{k=0}^n \mu_k (X - x_0)^{\frac{k}{e}}$ la série tronquée à l'ordre n ,
- $x_1 \in D(x_0, \delta(x_0))$,
- $M \geq \sup_{x \in D(x_0, \delta(x_0))} |Y(x)|$.
- $\eta \in \mathbb{R}^{+*}$ la précision requise,
- $\beta = \left(\frac{|x_1 - x_0|}{\delta(x_0)} \right)^{\frac{1}{e}}$,

Alors, $N \geq \frac{\ln\left(\frac{\eta}{M}\right) + \ln(1 - \beta)}{\ln(\beta)} - 1 \Rightarrow |Y(x_1) - \tilde{Y}(x_1)| \leq \eta$.

Cas régulier : formule de Cauchy.

Cas ramifié : considérer $G(X, Y) = F(x_0 + X^e, Y)$.

Nombre de points intermédiaires



\Rightarrow À ce stade, on a besoin de $O(n) = O(D^2)$ points intermédiaires.

Gestion du nombre de pas

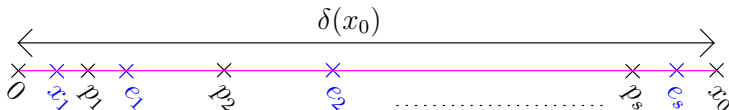
- $F(X, Y) = Y^3 - X^5 + 2(10X - 1)^2 \implies N \geq 102309$

Gestion du nombre de pas

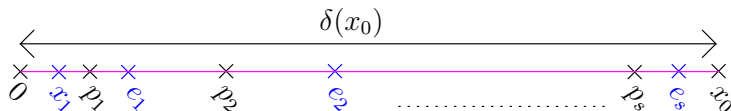
- $F(X, Y) = Y^3 - X^5 + 2(10X - 1)^2 \implies N \geq 102309$
- Si $\beta = \frac{1}{2}$, il suffit d'avoir $N \geq 1 - \log_2 \left(\frac{\epsilon - 2r}{M} \right)$.

Gestion du nombre de pas

- $F(X, Y) = Y^3 - X^5 + 2(10X - 1)^2 \implies N \geq 102309$
- Si $\beta = \frac{1}{2}$, il suffit d'avoir $N \geq 1 - \log_2 \left(\frac{\epsilon - 2r}{M} \right)$.



Gestion du nombre de pas



- Pour $[\alpha_{kl}, \alpha_k]$, nombre de points intermédiaires ajoutés :

$$s = \left\lceil \log_3 \left(\frac{\delta(c_{kl})}{\delta(c_k)} \right) + (e - 1) \log_3(2) \right\rceil + 1$$

Théoreme

Nombre total de points : $O(p \log \frac{L_M}{L_m} + g) = O(D^2 \log \frac{L_M}{L_m})$.

Corollaire

Si $F \in \mathbb{Z}[X, Y]$, on a $O(D^6 \log \|F\|_\infty)$ points intermédiaires.

\implies borne cubique en la sortie.

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

Un outil fondamental de la théorie des courbes algébriques

- Indices de ramification \implies calcul du genre
(*formule d'Hurwitz*)

Un outil fondamental de la théorie des courbes algébriques

- Calcul du genre
- Calcul de bases intégrales

M. van Hoeij 1994, *An Algorithm for Computing an Integral Basis in an Algebraic Function Field*

- Détermination de paramétrisations de courbes de genre 0

M. van Hoeij 1997, *Rational Parametrizations of Algebraic Curves using a Canonical Divisor*

- Intégration de fonctions algébriques

B. Trager 1984, *Integration of Algebraic Functions (PhD)*

M. Bronstein 1990, *Integration of Elementary Functions*

Un outil fondamental de la théorie des courbes algébriques

- Calcul du genre
- Calcul de bases intégrales
 - Détermination de paramétrisations de courbes de genre 0
 - Intégration de fonctions algébriques
- Calcul de cartes routières

J. Schwartz & M. Sharir 1983, On the "piano movers" problem II. General techniques for computing topological properties of real algebraic manifolds

Un outil fondamental de la théorie des courbes algébriques

- Calcul du genre
- Calcul de bases intégrales
 - Détermination de paramétrisations de courbes de genre 0
 - Intégration de fonctions algébriques
- Calcul de cartes routières
- Prolongement analytique
 - Calcul de groupe de monodromie

A. Poteaux 2007, Computing monodromy groups defined by plane algebraic curves

Objectif : version effective du théorème d'Abel-Jacobi

Nécessite : évaluation flottante rapide des séries de Puiseux.

Partie singulière

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

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

Exemples au-dessus de $X = 0$

- $F(X, Y) = Y^3 - X$:

$$0 + \zeta_3^k X^{\frac{1}{3}}, \quad k = 1, 2, 3 \quad (r = 1)$$

- $H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$:

$$0 + \zeta_3^k X^{\frac{1}{3}} + \frac{1}{6} X^3 + \dots, \quad k = 1, 2, 3 \quad (r = 1)$$

$$1 + \zeta_2^k X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^k X^{\frac{3}{2}} + \dots, \quad k = 1, 2 \quad (r = 1)$$

$$2 - 3X^2 - \frac{9}{2} X^3 + \dots \quad (r = 0)$$

L'algorithme de Newton-Puiseux

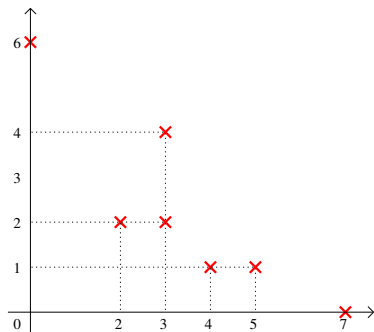
Principaux outils

$$F(X, Y) = Y^7 + Y^5 X - 2 Y^4 X + 5 Y^4 X^3 + 4 Y^2 X^2 + X^6$$

Support d'un polynôme

$$F(X, Y) = Y^7 X^0 + Y^5 X^1 - 2 Y^4 X^1 + 5 Y^3 X^4 - Y^3 X^2 + 4 Y^2 X^2 + Y^0 X^6$$

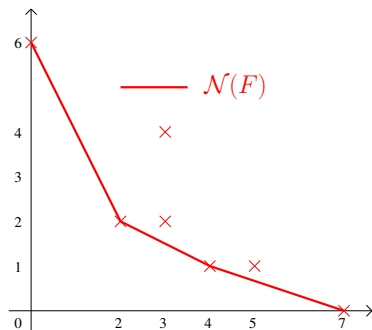
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$



Polygone de Newton

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

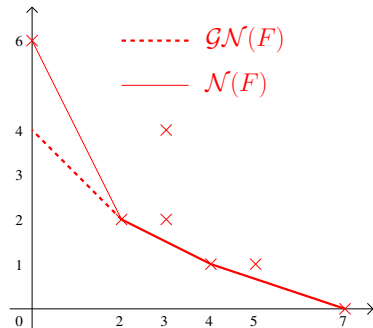
- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de $\text{Supp}(F)$.



Polygone de Newton générique

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

- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de $\text{Supp}(F)$.
- - $\mathcal{GN}(F)$: pentes de $\mathcal{N}(F) \leq -1$.



Polynôme caractéristique

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

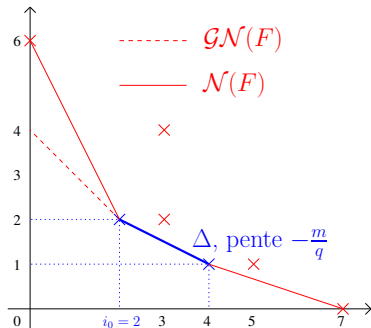
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

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

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

Polynôme caractéristique :

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



Algorithme de Newton-Puiseux rationnel

D. Duval 1989, *Rational Puiseux Expansions*

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

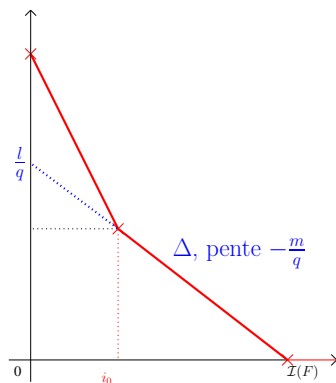
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- Pour chaque ϕ_k

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

avec

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



Notre variante

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

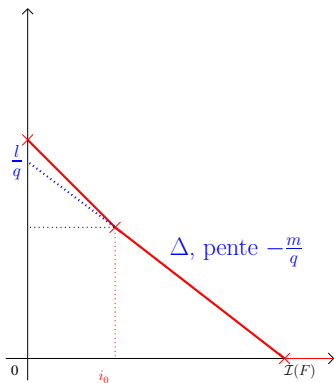
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- Pour chaque ϕ_k

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

avec

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



Notre variante

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

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

- Pour chaque ϕ_k

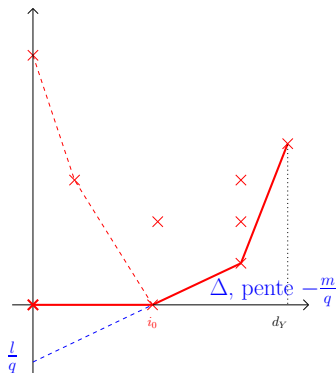
$$F(X, Y) \leftarrow \frac{F(\xi_k^v X^q, X^m(\xi_k^u + Y))}{X^l}$$

avec

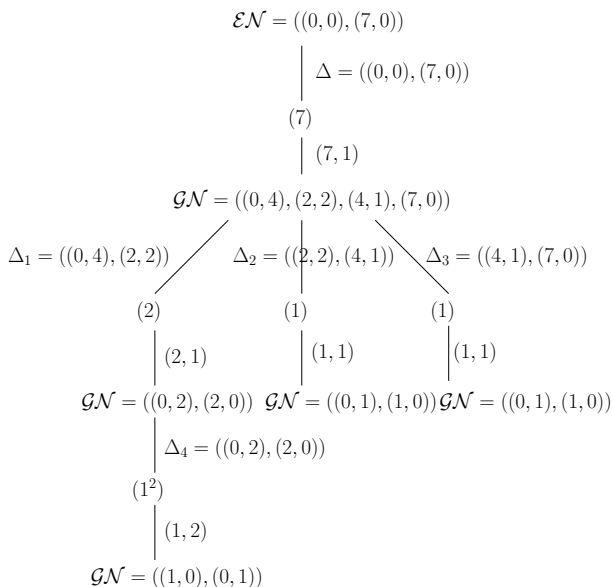
- ξ_k t.q. $\phi_k(\xi_k) = 0$,
- (u, v) tel que $uq - vm = 1$.

Premier tour : polygone exceptionnel $\mathcal{EN}(F)$

(partie inférieure de l'enveloppe convexe de $\text{Supp}(F) \cup \{(0, 0)\}$).



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 $\mathcal{O}(d_Y^{32} d_X^4)$

Walsh 2000, *A Polynomial-time Complexity Bound for the Computation of the Singular Part of an Algebraic Function*

Calcul des développements de Puiseux

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

Complexité binaire $\mathcal{O}(d_Y^{32} d_X^4)$

Walsh 2000, *A Polynomial-time Complexity Bound for the Computation of the Singular Part of an Algebraic Function*

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 $\mathcal{T}(F)$.

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

Poteaux & Rybowicz 2008, *On the good reduction of Puiseux series and complexity of the Newton-Puiseux algorithm over finite fields*

Poteaux & Rybowicz 2010, *On the good reduction of Puiseux series and Applications*

Poteaux & Rybowicz, *Complexity bounds for the rational Newton-Puiseux algorithm over finite fields and related problems*

Bonne \mathfrak{p} -réduction

Soient :

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

Définition

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

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

où $R_F = \text{Res}_Y(F, F_Y)$

Principaux résultats

Si F a une bonne p -réduction, alors :

Théorème 1 : on peut réduire les séries de Puiseux modulo \mathfrak{P} divisant p

Theorem 2 : $\mathcal{T}(F) = \mathcal{T}(F \bmod p)$ (*faux avec les polygones classiques*)

Autres résultats

- Bornes pour le premier p : taille logarithmique en l'entrée avec des algorithmes probabilistes. [▶ tailles](#)
- Bornes de complexité améliorées pour l'algorithme de Newton-Puiseux rationnel sur les corps finis

de $O(D^8)$ à $\tilde{O}(D^5)$

- Complexité binaire pour le calcul de $\mathcal{T}(F)$:

$\tilde{O}(D^5)$ avec un petit p

[▶ Détails](#)

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

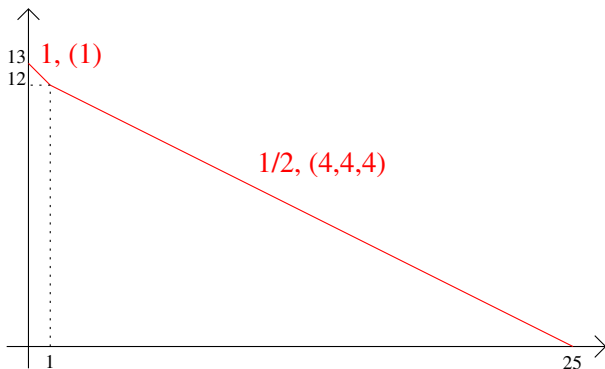
Suivre $\mathcal{T}(F)$ numériquement : un exemple

Développements de Puiseux de F :

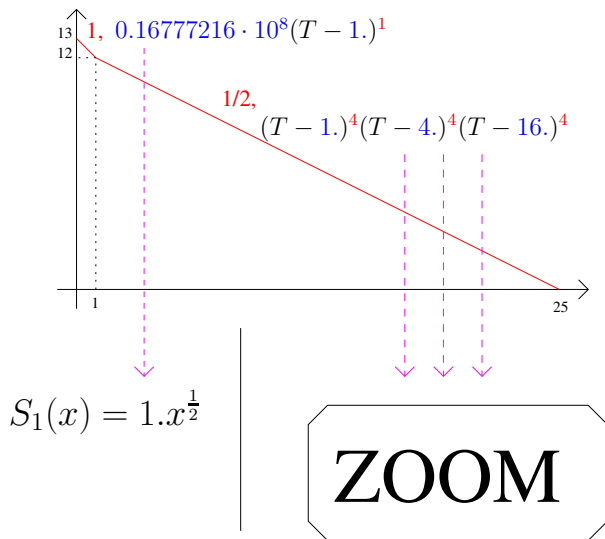
- $S_1(X) = X + \dots$
- $S_2(X) = 4X^{\frac{1}{2}} + X^{\frac{7}{8}} + \dots$
- $S_3(X) = 2X^{\frac{1}{2}} + 2X + \dots$
- $S_4(X) = 2X^{\frac{1}{2}} + X + X^{\frac{7}{6}} + \dots$
- $S_5(X) = X^{\frac{1}{2}} + 2X + X^{\frac{5}{4}} + \dots$
- $S_6(X) = X^{\frac{1}{2}} + X + \dots$
- $S_7(X) = X^{\frac{1}{2}}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

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

Premier polygone de Newton



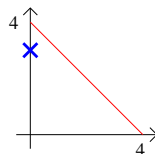
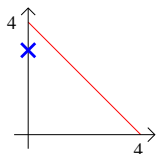
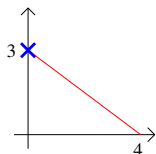
Premier polygone de Newton



Tri selon les polygones

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

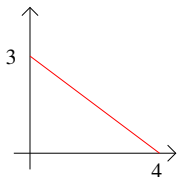
$\{G_1, G_2, G_3\}$



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

Tri selon les polygones

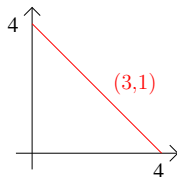
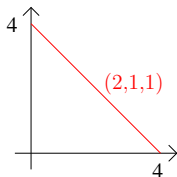
G_3



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

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

$\{G_1, G_2\}$



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 $S_i.$

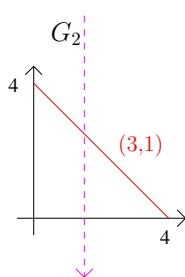
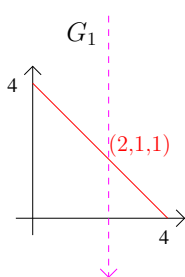
Tri selon les multiplicités

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, 0.0000000074101187358617089031,
0.0000000027761147770454585021]



Résultat

```
mypuiseux(F, x, y, x, 0);
```

```
[[[x = T, y = 1.0 T], [x = T2, y =  
1.00000000000000046423 T2 + 1.0000000000000014628 T], [x = T2, y =  
4.0000000000000002662 T2 + 1.0000000000000014628 T], [x = T4, y =  
0.999999999999999869303 T5 + 2.0000000000000040470 T4 +  
1.0000000000000014628 T2], [x = T2, y = 1.9999999999993502275 T2 +  
2.00000000000000757425 T], [x = T6, y = 1.00000000000036976678 T7 +  
1.00000000000047325425 T6 + 2.0000000000000757425 T3], [x = T8, y =  
0.99999999999483964356 T7 + 4.0000000000009297336 T4]]]
```

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

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

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 seconde	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

Conclusion

- Séries de Puiseux : algorithme symbolique-numérique
 - Réduction modulo un petit $p \rightarrow$ calcul de $\mathcal{T}(F)$.
 - Calculs numériques suivant $\mathcal{T}(F)$: filtre à deux étages.

\implies Les séries de Puiseux peuvent être utilisées en pratique !
- Calcul du groupe de monodromie :
 - Chemins optimisés.
 - Compromis nombre de pas / ordres de troncation
 - \rightarrow borne sur le nombres d'étapes.
 - Développements en des points critiques : utilisation de l'algorithme numérique-modulaire.
- Perspectives
 - Contrôle des erreurs numériques. Amélioration du second filtre.
 - Théorème d'Abel-Jacobi effectif **et** certifié.
 - Implémentation efficace.

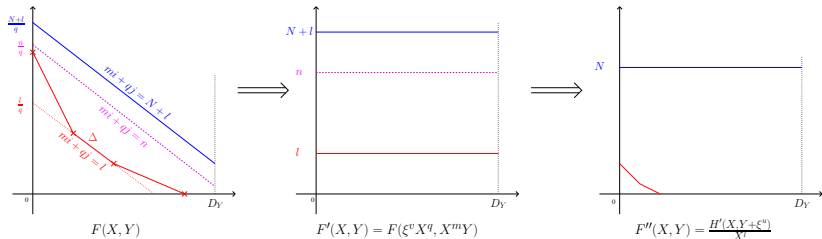
Choix du premier p

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

$\text{ht}(p)$ appartient à

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

Complexité de RNP : substitutions



- $\delta_F = \sum_i r_i f_i.$

Lemme

- Les calculs peuvent se faire modulo x^{δ_F+1} .
- Une substitution = N "shifts" $\subset O(NM(d_Y))$ opérations de corps.

Complexité de RNP sur $L = \mathbb{F}_{p^{t_0}}$

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)

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

$\rightarrow \mathcal{T}(\bar{F})$ au-dessus de l'ensemble des points critiques :
 $\mathcal{O}(d_Y^3 d_X^2 t_0 \log p)$

D. Duval 1989, *Rational Puiseux Expansions* : $\mathcal{O}(d_Y^6 d_X^2)$

Complexité binaire pour l'algorithme the Monte-Carlo

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

Théoreme

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

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

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

← retour