

Calcul du groupe de monodromie d'une courbe algébrique plane

Poteaux Adrien

XLIM
Université de Limoges

Séminaire ALGO du 23 avril 2007

Problématique

- $\mathcal{K}$ sous-corps de $\mathbb{C}$.
- $F = Y^d + a_{d-1}(X)Y^{d-1} + \dots + a_0(X) \in \mathcal{K}[X, Y]$ irréductible.
- $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$ la courbe affine associée.
- **Fibre** en x_0 : $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d$.
- **Point critique** : $\#\mathcal{F}(x_0) < d$.
- $\delta(x_0)$: distance entre x_0 et son plus proche point critique

Points réguliers

Soit x_0 régulier et $\mathcal{F}(x_0) = \{y_1, y_2, \dots, y_d\}$ la fibre en x_0 .

- Théorème des fonctions implicites : il existe d séries

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k \text{ t.q. } F(X, Y_i(X)) = 0 \text{ sur un}$$

voisinage de x_0 et $Y_i(x_0) = y_i$.

- Le rayon de convergence de ces séries est égal à $\delta(x_0)$.
- Si γ est un chemin qui ne passe par aucun point critique, les Y_i peuvent être prolongées analytiquement le long de γ .

x_0 point critique : Séries de Puiseux

Il existe d séries $Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$ t.q.

$F(X, Y_{ij}(X)) = 0$ pour tout $1 \leq j \leq e_i, 1 \leq i \leq s$, avec :

- $\zeta_e = \exp\left(\frac{2\pi i}{e}\right)$
- $e_1, \dots, e_s$ partition de d .

▷ e_i est l'**indice de ramification**

x_0 point critique : Séries de Puiseux

Il existe d séries $Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$ t.q.

$F(X, Y_{ij}(X)) = 0$ pour tout $1 \leq j \leq e_i$, $1 \leq i \leq s$, avec :

- $\zeta_e = \exp\left(\frac{2\pi i}{e}\right)$
- $e_1, \dots, e_s$ partition de d .

▷ e_i est l'**indice de ramification**

Exemples en $x_0 = 0$:

- $G(X, Y) = Y^3 - X$

$$\Rightarrow Y_1(X) = X^{\frac{1}{3}}, Y_2(X) = jX^{\frac{1}{3}}, Y_3(X) = j^2X^{\frac{1}{3}}.$$

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

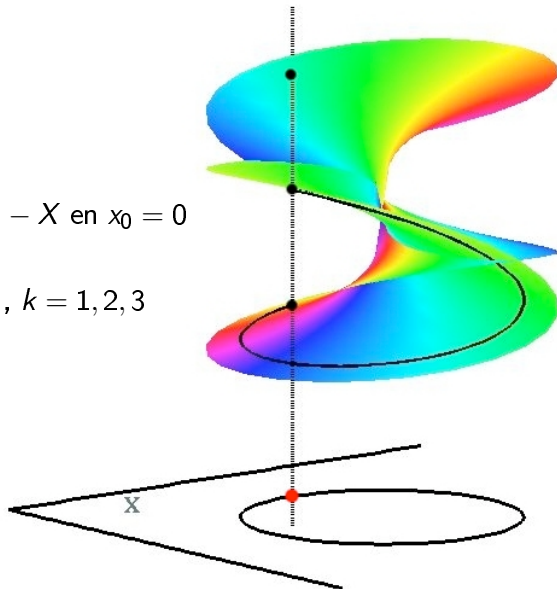
$$\Rightarrow Y_k(X) = j^k X^{\frac{1}{3}} + \frac{1}{6} X^3 + \frac{5}{12} j^k X^{\frac{10}{3}} + \dots, k = 1, 2, 3.$$

$$Y_4(X) = 1 + X^{\frac{1}{2}} \pm \frac{1}{2} X^{\frac{3}{2}} + \frac{3}{2} X^2 \pm \frac{19}{8} X^{\frac{5}{2}} + 2 X^3 + \dots$$

$$Y_6(X) = 2 - 3 X^2 - \frac{9}{2} X^3 + \dots$$

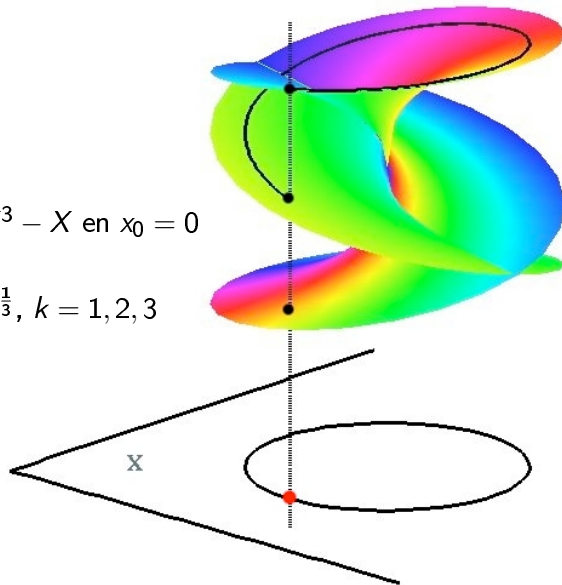
Monodromie locale

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



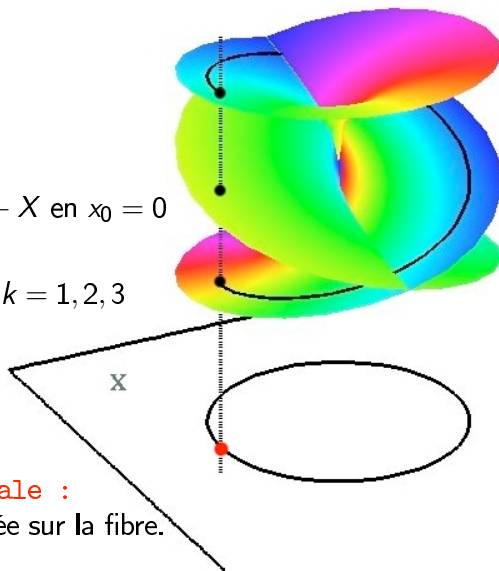
Monodromie locale

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



Monodromie locale

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



⇒ Monodromie locale :
permutation engendrée sur la fibre.

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

$$Y_6(X) = 2 - 3X^2 - \frac{9}{2}X^3 + \dots$$

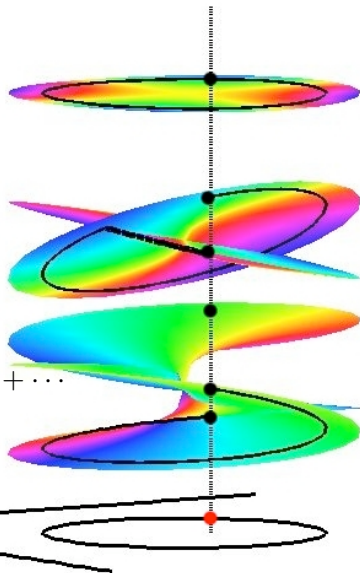
$\Rightarrow e = 1 : 1\text{-cycle.}$

$$Y_4(X) = 1 + X^{\frac{1}{2}} \pm \frac{1}{2}X^{\frac{3}{2}} + \dots$$

$\Rightarrow e = 2 : 2\text{-cycle.}$

$$Y_1(X) = j^k X^{\frac{1}{3}} + \frac{1}{6}X^3 + \frac{5}{12}j^k X^{\frac{10}{3}} + \dots$$

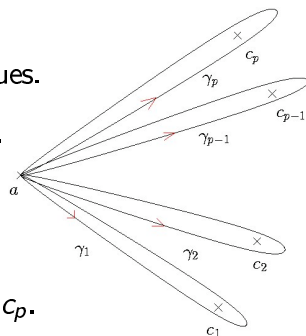
$\Rightarrow e = 3 : 3\text{-cycle.}$



La monodromie locale
se lit sur les
indices de ramification !

Monodromie globale

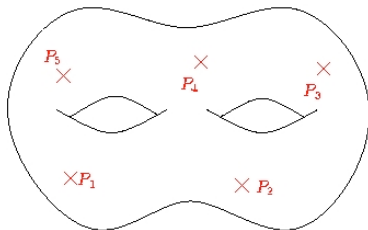
- On note $c_1, \dots, c_p$ les points critiques.
- On fixe un point de base régulier a .
- On cherche les p permutations $\sigma_1, \dots, \sigma_p$ correspondant à $c_1, \dots, c_p$.



- Ces permutations engendrent le groupe de monodromie.

Motivations

$\mathcal{C}$ est une surface de Riemann homéomorphe à une sphère à g poignées où g est le genre de la courbe.



- diviseur $D = \sum n_{\mathcal{P}} \mathcal{P}$: somme formelle de points.
- degré d'un diviseur : $\deg(D) = \sum n_{\mathcal{P}}$
- Diviseur de fonction $(f) = \sum v_{\mathcal{P}}(f) \mathcal{P}$: défini par les pôles et les zéros de f .

Questions liées aux diviseurs

- On note
- $\mathcal{F}$ l'ensemble des diviseurs de fonctions.
 - $\mathcal{D}_0$ l'ensemble des diviseurs de degré 0.

On a $\mathcal{F} \subset \mathcal{D}_0$ mais pas égalité.

Problèmes :

- Soit $D \in \mathcal{D}_0$. Comment déterminer si $D \in \mathcal{F}$?
- Existe-t-il $n \in \mathbb{Z}$ tel que $nD \in \mathcal{F}$?
- Etant donnés $D_1, \dots, D_k \in \mathcal{D}_0$, existe-t-il $n_1, \dots, n_k \in \mathbb{Z}$ tels que $n_1 D_1 + \dots + n_k D_k \in \mathcal{F}$?

Une résolution : le théorème d'Abel Jacobi

L'application d'Abel

$$\begin{aligned} \mathcal{A}: \quad \mathcal{D}_0/\mathcal{F} &\longrightarrow \mathbb{C}^g/\Gamma \\ \sum n_{\mathcal{P}}\mathcal{P} &\longmapsto \sum n_{\mathcal{P}} \left(\int_{\mathcal{O}}^{\mathcal{P}} \omega_1, \dots, \int_{\mathcal{O}}^{\mathcal{P}} \omega_g \right) \end{aligned}$$

est un isomorphisme de groupe.

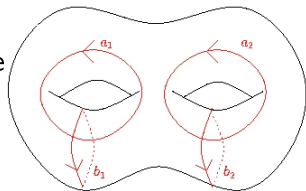
- les ω_i forment la base de l'espace des différentielles sans pôle.
- Γ est le réseau des périodes.
- $\mathcal{O}$ est un point de base sur la courbe.

$\Rightarrow$ Calculer l'application d'Abel donne les informations souhaitées sur les diviseurs !

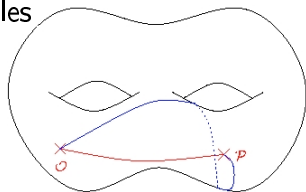
L'application d'Abel

$$\begin{aligned} \mathcal{A}: \quad \mathcal{D}_0/\mathcal{F} &\longrightarrow \mathbb{C}^g/\Gamma \\ \sum n_P \mathcal{P} &\longmapsto \sum n_P \left(\int_{\mathcal{O}}^{\mathcal{P}} \omega_1, \dots, \int_{\mathcal{O}}^{\mathcal{P}} \omega_g \right) \end{aligned}$$

- Il y a $2g$ cycles qui ne peuvent être contractés à un point.
 $\Rightarrow$ base de l'homologie.



- Périodes : intégrales des différentielles sans pôle sur cette base.



- Modulo les périodes, $\int_{\mathcal{O}}^{\mathcal{P}} \omega_i$ ne dépend pas du chemin choisi.

Applications d'une version effective du théorème

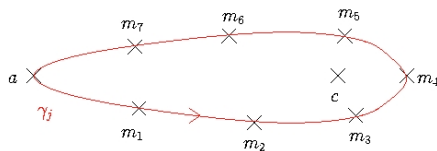
- Primitive de fonctions algébriques (partie logarithmique) :
Risch 69, Davenport 81, Trager 84, Bronstein 90, Bertrand 95...
- Etude symbolique d'EDO : existence et calcul des solutions algébriques, calcul du groupe de Galois différentiel.
Baldassarri-Dwork 79, Compoint-Singer 98...
- Calcul des solutions quasi-périodiques des équations KP (Kadomtsev-Petviashvili) : B. Deconinck et H. Segur 98
- Solutions solitons des équations KdV (Korteweg-de Vries) et NLS (Nonlinear Schrödinger).

Calcul des périodes

M. van Hoeij, B. Deconinck (1996) :

- Calcul de la monodromie.
- Calcul d'une base de l'homologie à l'aide d'une représentation de la monodromie (Tretkoff & Tretkoff, 1984).
- Calcul d'une base de l'espace des différentielles sans pôle (les ω_i).
- Calcul des périodes (intégrales des ω_i le long des cycles de l'homologie).

Résumé de la méthode employée



- 1 On choisit $a = m_0, m_1, \dots, m_k = a$ des points sur la boucle γ_j .
- 2 On calcule les fibres $F_i = \{y_{i,1}, \dots, y_{i,d}\}$ en m_i .
- 3 On connecte les éléments de F_i à ceux de F_{i+1} à l'aide de développements en série de Puiseux, de sorte que chaque couple corresponde au même prolongement.

Monodromie : état de l'art (sketch)

① Relier les fibres

◇ Van Hoeij & Deconinck (1999)

- 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 fiable mais trop lent

② Equation différentielle

③ Méthodes basées sur l'homotopie

Monodromie : état de l'art (sketch)

- ① Relier les fibres
- ② Equation différentielle
 - Intérêt : calcul rapide des développements à ordre élevé.
Chudnovsky & Chudnovsky, Van der Hoeven 2000,
Cormier-Singer-Trager-Ulmer 2002 ...
 - Temps de passage potentiellement coûteux.
 - Taille de l'équation différentielle importante.
 - On utilise des développements à ordre petit.
- ③ Méthodes basées sur l'homotopie

Monodromie : état de l'art (sketch)

- ➊ Relier les fibres
- ➋ Equation différentielle
- ➌ Méthodes basées sur l'homotopie

Problème formulable dans cette classe de problème.

Deux principaux inconvénients :

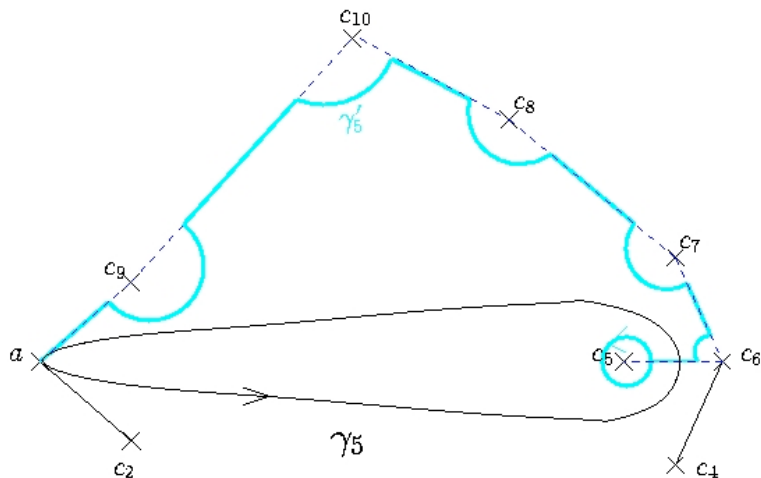
- Situation générale qui n'utilise pas toute l'information à notre disposition.
- Stratégie qui évite les points critiques : pas toujours faisable.

Contributions

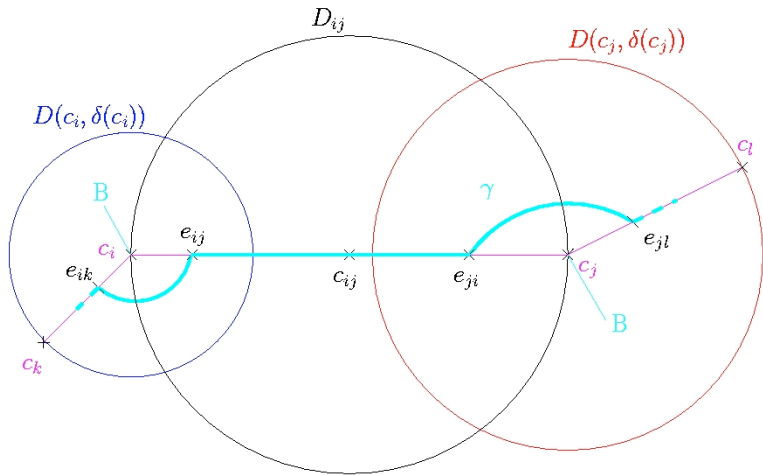
- Optimiser les chemins parcourus : borne sur le nombre de points intermédiaires.
- Connexions contrôlées.
- Utilisation de développements de Puiseux en des points critiques : algorithme numérique/modulaire.
- Prototype d'implémentation en Maple.

Utilisation d'un arbre de recouvrement minimum

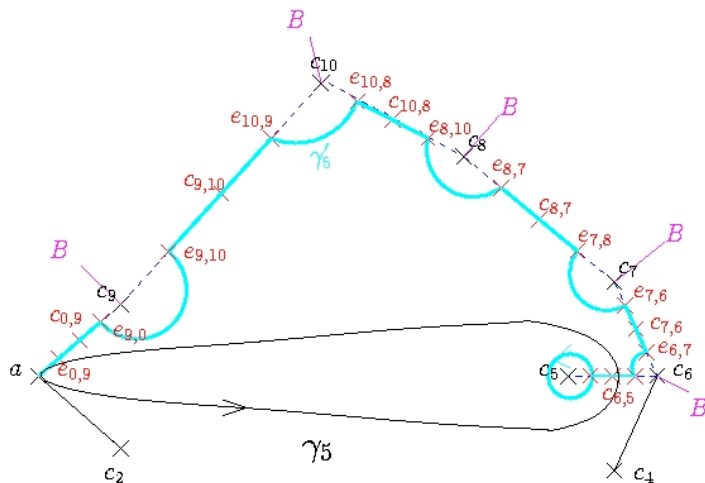
Un exemple : $F(x, y) = (x - 1)y^3 - 2x^3y^2 + xy + 1$.



Connexions le long de l'arbre



Nombres de points intermédiaires



$\Rightarrow$ A ce stade, on utilise $O(p) = O(D^2)$ points intermédiaires.

Théorème de Smith : racines isolées

Théorème

Soit P un polynôme de $\mathbb{C}[Z]$ possédant d racines distinctes. Soient $z_1, \dots, z_d$ des nombres complexes distincts. On pose :

$$\rho_i = d \left| \frac{f(z_i)}{\prod_{j \neq i} (z_i - z_j)} \right|.$$

Si les disques $D_i = D(z_i, \rho_i)$ sont 2 à 2 disjoints, alors pour tout i , il existe une unique racine de P dans D_i .

Idée : plus les z_i sont de bonnes approximations des racines de P , plus les rayons sont petits.

Contrôle de la connexion

On note :

- $Y_1(X), \dots, Y_d(X)$ les d séries de Puiseux au dessus de x_0 .
- $\tilde{Y}_1(X), \dots, \tilde{Y}_d(X)$ les séries tronquées.
- $x_1 \in D(x_0, \delta(x_0))$ et $\{y_1, \dots, y_d\} = \mathcal{F}(x_1)$.

On calcule :

- les $\tilde{y}_i$ approximations des y_i .
- ρ_i les rayons de Smith associés.
- $\varepsilon = \min_{i \neq j} |\tilde{y}_i - \tilde{y}_j|$.
- $r = \max(\rho_1, \dots, \rho_d)$.

On suppose que $\frac{\varepsilon}{2} - r > 0$. Alors :

Proposition

$|\tilde{Y}_i(x_1) - y_k| < \frac{\varepsilon}{2} - r \Rightarrow Y_i(x_1) = y_k$: on connecte $\tilde{Y}_i$ à $\tilde{y}_k$.

Contrôle de la connexion : ordre de troncation ?

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 $G(X, Y) = F(x_0 + X^e, Y)$.

Gestion du nombre de pas

- Si $\beta = \frac{1}{2}$, il suffit d'avoir $n \geq 1 - \log_2 \left(\frac{\varepsilon - 2r}{M} \right)$.
- Pour $[c_{kl}, c_k]$, nombre de points intermédiaires ajoutés :

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

Théorème

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.

$\Rightarrow$ borne cubique en la sortie.

Utilisation de développements au-dessus des points critiques

- Développement de Puiseux : $\sum_{k=1}^{\infty} \mu_k \zeta_e^k (X - c)^{\frac{k}{e}}$

Intérêt :

- Faire un tour autour d'un point critique est gratuit.
 - Contourner un point critique : 2 évaluations.
 - Contrôle numérique lors de l'intégration ultérieure.
-
- Newton : utilise des changements de variable successifs :

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

où u, v, q, m et l viennent d'une arête Δ du polygone de Newton et ξ est une racine du polynôme caractéristique de Δ

Polygone de Newton

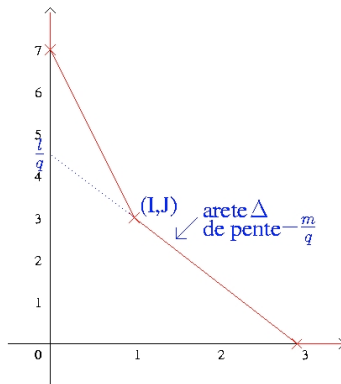
$$F(X, Y) \leftarrow \frac{F(\xi^v X^q, \xi^u X^m (1 + Y))}{X^I}$$

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

- polynôme caractéristique :

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

- ξ racine de φ .
- u, v tels que $uq - vm = 1$.



Calcul des développements de Puiseux

- Calcul numérique pur délicat.
- Calcul symbolique : deux principaux problèmes.
 - Croissance des coefficients (augmentation des temps de calcul et problème d'évaluation).
 - Calcul dans des extensions de degré potentiellement élevé.

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

Algorithme de Puiseux :

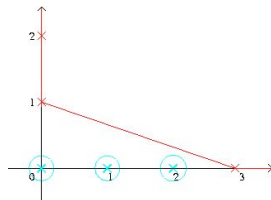
- Informations qui doivent être exactes :
 - Les polygones de Newton.
 - Les multiplicités des racines des polynômes caractéristiques.
- Informations que l'on peut traiter numériquement :
 - Les coefficients des développements calculés.

⇒ Idée :

On fait les calculs numériquement.
On obtient les informations exactes
à l'aide d'un calcul modulaire parallèle.

⇒ Difficulté :

Connecter les calculs numériques et les calculs modulo p .



Hypothèses sur le premier p utilisé

On suppose que le premier p utilisé vérifie les hypothèses suivantes :

- ① Les coefficients de F peuvent être réduits modulo p .
On note F_p l'image de F dans $\overline{\mathbb{F}}_p[X, Y]$.
- ② F_p est sans carré et $p > d$ (assure l'existence des séries).
- ③ La forme de la partie sans carré du discriminant est conservée.
- ④ La suite des polygones de Newton rencontrés est inchangée par réduction modulo p .

Partie ramifiée de l'algorithme

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

On note

- $\mathcal{I}(F)$ le plus petit i tel que $a_{i,0} \neq 0$.
- $\mathcal{N}(F)$ le polygone de Newton associé au polynôme F

But de l'algorithme : trouver $G(X, Y)$, $P(X)$, $Q(X, Y)$ et L t.q.

- $\mathcal{I}(G) = 1$
- $X^L G(X, Y) = F(P(X), Q(X, Y))$

Un exemple

```
r := RootOf(y^6-x,y) :F := evala(Norm((y-1-r^2-r^5)*(y+1-r^3-r^5)*  
(y-2-r^2-r^7)*(y+2-r^3-r^5)))+x^16*y^10 :
```

$$\deg_y(F) = 24, \deg_x(F) = 22, tdeg(F) = 26.$$

253 monômes. $\max |a_{ij}| = 1603614$

$$\begin{aligned} F := & 4096 - 34071x^{11}y^8 - 30241x^{11}y^6 + 170364x^{11}y^5 + 222144x^{11}y^4 + 91714x^{11}y^3 + \\ & 152439x^{11}y^2 + 5616x^{11}y + 3x^{12}y^{12} - 48x^{12}y^{11} - 534x^{12}y^{10} - 1434x^{12}y^9 + 4239x^{12}y^8 + \\ & 31212x^{12}y^7 + 74500x^{12}y^6 + 65364x^{12}y^5 - 58749x^{12}y^4 - 123408x^{11}y^7 - 21702x^{14}y - 198400y^6 + \\ & 55962x^2y^{14} + 9000x^2y^{11} - 727956x^2y^4 + 137664x^2y^3 + 15576x^{14}y^5 + 54x^{10}y^{13} - 46914x^2y^9 + \\ & 2818x^{16}y^3 - 114416x^3 + 57600xy^2 + 2715x^{16}y^2 + x^{16}y^{10} + 648x^{14}y^7 - 6x^2y^{21} - \\ & \vdots \\ & + 122361x^{10}y^8 + 1603614x^3y^7 - 1049406x^3y^5 - 242536x^3y^6 + 102144y^4 - 12x^{14}y^9 + \\ & 678084x^2y^{10} + 34x^{16}y^6 - 6144x - 1166511x^2y^8 + 309936x^{10}y^2 + 25047x^{14}y^4 - 6336x^2y + \\ & 195504x^2y^2 - 7224x^2y^{16} + 23612x^{14}y^3 - 131606x^{10}y^3 - 184053x^{10}y^6 - 342x^2y^{17} + 123990x^2y^7 + \\ & 126060x^4 - 351461x^5 + 319163x^6 - 311700x^{10}y^4 + 116478x^{10}y^7 - 930x^2y^{13} \end{aligned}$$

Algorithme symbolique en $x = 0$

$F(0, Y)$ a 4 racines de multiplicité 6 : -2,-1,1,2.

On a donc 4 polynômes à regarder :

- $F_1(X, Y) = F(X, Y + 1)$
- $F_2(X, Y) = F(X, Y + 2)$
- $F_3(X, Y) = F(X, Y - 1)$
- $F_4(X, Y) = F(X, Y - 2)$

On traite chaque polynôme séparément.

Regardons $F_1(X, Y)$.

Première transformation

$$P_1(X) \leftarrow X, Q_1(X) \leftarrow Y.$$

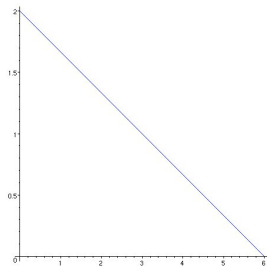
On calcule $\mathcal{N}(F_1)$.

Une seule arête :

$m = 1, q = 3, l = 6, u = 0, v = -1$
et $\xi = 1$ de multiplicité 2.

$$F_1(X, Y) \leftarrow \frac{F_1(X^3, X(1 + Y))}{X^6}.$$

$$P_1(X) \leftarrow P_1(X^3), Q_1(X, Y) \leftarrow Q_1(X^3, X(1 + Y)).$$



Deuxième transformation

On calcule $\mathcal{N}(F_1)$.

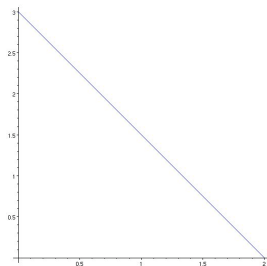
Une seule arête :

$m = 3$, $q = 2$, $l = 6$, $u = -1$, $v = -1$
et $\xi = 1$ de multiplicité 1.

$$F_1(X, Y) \leftarrow \frac{F_1(X^2, X^3(1 + Y))}{X^6}.$$

$$P_1(X) \leftarrow P_1(X^2), \quad Q_1(X, Y) \leftarrow Q_1(X^2, X^3(1 + Y)).$$

La multiplicité de ξ est 1 : on aura donc $\mathcal{I}(F_1) = 1$.



Résultats symboliques

En faisant de même pour F_2 , F_3 et F_4 , on obtient les développements de Puiseux suivants :

- $[X = T^6, Y = 1 + T^2 + T^5]$
- $[X = T^6, Y = 2 + T^2 + T^7]$
- $[X = T^6, Y = -1 + T^3 + T^5]$
- $[X = T^6, Y = -2 + T^3 + T^5]$

Approche numérique-modulaire

On fait des calculs numériques et des calculs modulo $p = 1009$ en même temps.

- On note F_p la réduction de F modulo p .
- Racines de $F_p(0, Y)$ dans $\mathbb{F}_p$:
1, 2, 1007 et 1008 de multiplicités 6.

Premier problème :

calculer numériquement les racines de $F(0, Y)$ avec multiplicités.

⇒ Utilisation d'une version généralisée du théorème de Smith.

Théorème de Smith : racines multiples

Théorème

Soient $P(Z) \in \mathbb{C}[Z]$ et $(z_1, M_1), \dots, (z_L, M_L)$ des éléments de $\mathbb{C}$ donnés avec multiplicité.

On peut calculer des nombres $\rho_1, \dots, \rho_L$ tels que :

Si les disques $D(z_k, \rho_k)$ ne s'intersectent pas, alors chaque disque $D(z_k, \rho_k)$ contient exactement M_k racines de $P(Z)$ (comptées avec multiplicité).

Théorème de Smith : racines multiples

Théorème

Soient $P(Z) \in \mathbb{C}[Z]$ et $(z_1, M_1), \dots, (z_L, M_L)$ des éléments de $\mathbb{C}$ donnés avec multiplicité.

On peut calculer des nombres $\rho_1, \dots, \rho_L$ tels que :

Si les disques $D(z_k, \rho_k)$ ne s'intersectent pas, alors chaque disque $D(z_k, \rho_k)$ contient exactement M_k racines de $P(Z)$ (comptées avec multiplicité).

Idée :

- On calcule des approximations des racines à l'aide d'un solver.
- On regroupe les racines selon la multiplicité donnée par le calcul modulo p .
- On calcule les rayons donnés par Smith
 - S'il y a intersection, on recommence en augmentant la précision des calculs.
 - Sinon, le théorème certifie le regroupement de racines.

Application à notre exemple

```
P :=eval(F,x=0) :s :=[fsolve(P,y,complex)] ;  
s := [-2., -2., -2., -2., -2., -2., -1.000000000, -1.000000000, -1.000000000,  
-1.000000000, -1.000000000, -1.000000000, 1., 1., 1., 1., 1., 1., 2., 2., 2., 2., 2.]  
s :=grouproots(s) ;  
s := [[-2., 6], [2., 6], [-1.000000000, 6], [1., 6]]  
smith(s,P,y) ;  
[0., 0., 0., 0.]
```

Application à notre exemple

```
P :=eval(F,x=0) :s :=[fsolve(P,y,complex)] ;  
s := [-2., -2., -2., -2., -2., -2., -1.000000000, -1.000000000, -1.000000000,  
-1.000000000, -1.000000000, -1.000000000, 1., 1., 1., 1., 1., 1., 2., 2., 2., 2., 2., 2.]  
s :=grouproots(s) ;  
s := [[-2., 6], [2., 6], [-1.000000000, 6], [1., 6]]  
smith(s,P,y) ;  
[0., 0., 0., 0.]
```

Etape suivante : on traite les racines par multiplicité.

On note :

```
Fp1 :=Eval(Fp,y=y+1) mod p :Fp2 :=Eval(Fp,y=y+2) mod p :  
Fp3 :=Eval(Fp,y=y+1007) mod p :Fp4 :=Eval(Fp,y=y+1008) mod p :  
f1 :=eval(F,y=y+1.) :f2 :=eval(F,y=y+2.) :  
f3 :=eval(F,y=y-1.) :f4 :=eval(F,y=y-2.) :
```

et on initialise

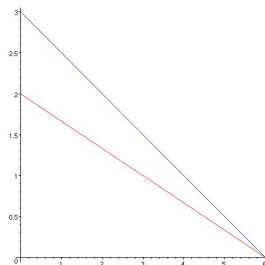
```
P1,P2,P3,P4 :=x$4 : Q1,Q2,Q3,Q4 :=y$4 :
```

Première transformation

On calcule $\mathcal{N}(H)$, $H \in \{F_{p1}, F_{p2}, F_{p3}, F_{p4}\}$.

On obtient 2 polygones de multiplicité 2.

On regarde les coefficients des f_k en X^2 :



Première transformation

On calcule $\mathcal{N}(H)$, $H \in \{F_{p1}, F_{p2}, F_{p3}, F_{p4}\}$.

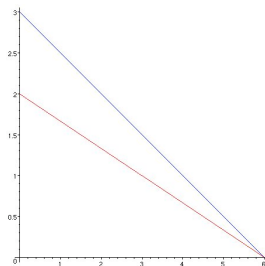
On obtient 2 polygones de multiplicité 2.

On regarde les coefficients des f_k en X^2 :

```
[seq(abs(coeff(coeff(i,x,2),y,0)),i=g)] ;
```

```
[46656.00000, 2985984.0, 0, 0]
```

f_3 et f_4 correspondent au polygone bleu, soit à F_{p3} et F_{p4} . On traite ces polynômes séparément des autres.



Première transformation

On calcule $\mathcal{N}(H)$, $H \in \{F_{p1}, F_{p2}, F_{p3}, F_{p4}\}$.

On obtient 2 polygones de multiplicité 2.

On regarde les coefficients des f_k en X^2 :

```
[seq(abs(coeff(coeff(i,x,2),y,0)),i=g)] ;
```

```
[46656.00000, 2985984.0, 0, 0]
```

f_3 et f_4 correspondent au polygone bleu, soit à F_{p3} et F_{p4} . On traite ces polynômes séparément des autres.

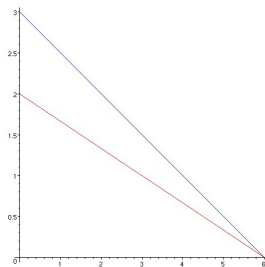
polygone rouge :

$m, q, l, u, v = 1, 3, 6, 0, -1$

$\xi_p = 1$ de multiplicité 2.

$\xi_1 = 1.$,

$\xi_2 = 0.9999609860 + 0./.$



Première transformation

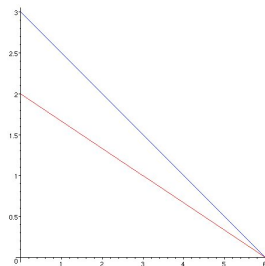
On calcule $\mathcal{N}(H)$, $H \in \{F_{p1}, F_{p2}, F_{p3}, F_{p4}\}$.

On obtient 2 polygones de multiplicité 2.

On regarde les coefficients des f_k en X^2 :

```
[seq(abs(coeff(coeff(i,x,2),y,0)),i=g)] ;
```

```
[46656.00000, 2985984.0, 0, 0]
```



f_3 et f_4 correspondent au polygone bleu, soit à F_{p3} et F_{p4} . On traite ces polynômes séparément des autres.

polygone rouge :

$m, q, l, u, v = 1, 3, 6, 0, -1$

$\xi_p = 1$ de multiplicité 2.

$\xi_1 = 1.$,

$\xi_2 = 0.9999609860 + 0.i.$

polygone bleu :

$m, q, l, u, v = 1, 2, 6, 0, -1$

$\xi_p = 1$ de multiplicité 3.

$\xi_3 = 0.9999727626 + 0.i,$

$\xi_4 = 1..$

Polynômes f_1 et f_2 (polygone rouge)

Pour $k \in \{1, 2\}$:

$$f_k(X, Y) \leftarrow \frac{f_k(\xi_k^{-1}X^3, X(1+Y))}{X^6}, \quad F_{pk}(X, Y) \leftarrow \frac{F_{pk}(\xi_p^{-1}X^3, X(1+Y))}{X^6}$$

$$P_k(X) \leftarrow P_k(\xi_k^{-1}X^3), \quad Q_k(X, Y) \leftarrow Q_k(\xi_k^{-1}X^3, X(1+Y)).$$

Polynômes f_1 et f_2 (polygone rouge)

Pour $k \in \{1, 2\}$:

$$f_k(X, Y) \leftarrow \frac{f_k(\xi_k^{-1}X^3, X(1+Y))}{X^6}, F_{pk}(X, Y) \leftarrow \frac{F_{pk}(\xi_p^{-1}X^3, X(1+Y))}{X^6}$$

$$P_k(X) \leftarrow P_k(\xi_k^{-1}X^3), Q_k(X, Y) \leftarrow Q_k(\xi_k^{-1}X^3, X(1+Y)).$$

On calcule $\mathcal{N}(F_{p1})$ et $\mathcal{N}(F_{p2})$.

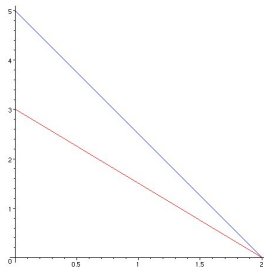
2 polygones différents :

```
[seq(abs(coeff(coeff(i,x,3),y,0)),i=g2)] ;
```

```
[419904.0000, 95.27800000]
```

On connecte f_1 à F_{p1} et f_2 à F_{p2} .

Les multiplicités obtenues sont 1 : on passe en numérique pur.



Polynômes f_3 et f_4 (polygone bleu)

Pour $k \in \{3, 4\}$:

$$f_k(X, Y) \leftarrow \frac{f_k(\xi_k^{-1}X^2, X(1+Y))}{X^6}, \quad F_{pk}(X, Y) \leftarrow \frac{F_{pk}(\xi_p^{-1}X^2, X(1+Y))}{X^6}$$

$$P_k(X) \leftarrow P_k(\xi_k^{-1}X^2), \quad Q_k(X, Y) \leftarrow Q_k(\xi_k^{-1}X^2, X(1+Y)).$$

Polynômes f_3 et f_4 (polygone bleu)

Pour $k \in \{3, 4\}$:

$$f_k(X, Y) \leftarrow \frac{f_k(\xi_k^{-1}X^2, X(1+Y))}{X^6}, \quad F_{pk}(X, Y) \leftarrow \frac{F_{pk}(\xi_p^{-1}X^2, X(1+Y))}{X^6}$$

$$P_k(X) \leftarrow P_k(\xi_k^{-1}X^2), \quad Q_k(X, Y) \leftarrow Q_k(\xi_k^{-1}X^2, X(1+Y)).$$

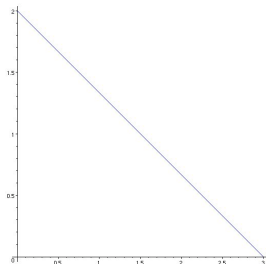
On calcule $\mathcal{N}(F_{p3})$ et $\mathcal{N}(F_{p4})$.

2 polygones identiques :

on fait le même changement de variable
pour les deux polynômes.

Les multiplicités obtenues sont 1 :

on passe en numérique pur.



Résultats

- $[X = 1.000000000 T^6, Y = 1. T^5 + 1. T^2]$
- $[X = (.9998501012 - 0. I) T^6, Y = .9999388687 T^2 + .9998166174 T^7]$
- $[X = (1.000041304 - .3333608699 e^{-11} I) T^6, Y = 1. T^3 + 1. T^5]$
- $[X = (1.000184747 - .3167392738 e^{-10} I) T^6, Y = (1.000184747 - .3167392738 e^{-10} I) T^5 + (1.000092369 - .1583550098 e^{-10} I) T^3]$

Exemples : monodromie

$M_{a,d}(X) := X^d - 2(aX - 1)^2$: 2 racines à distance $< 2a^{-\frac{d+2}{2}}$.

On considère $F(X, Y) = Y^3 - M_{10,5}(X)$.

- Fonction de Maple : 0.802 secondes. Digits 10.
- Version symbolique/numérique : 0.950 secondes. Précision de 40 chiffres nécessaire pour avoir un résultat correct.

Exemples : monodromie

$M_{a,d}(X) := X^d - 2(aX - 1)^2$: 2 racines à distance $< 2a^{-\frac{d+2}{2}}$.

On considère $F(X, Y) = Y^3 - M_{10,5}(X)$.

- Fonction de Maple : 0.802 secondes. Digits 10.
- Version symbolique/numérique : 0.950 secondes. Précision de 40 chiffres nécessaire pour avoir un résultat correct.

Algorithme Newton-Puiseux au dessus des racines de $M_{10,5}(X)$ jusqu'au terme en $X^{\frac{16}{3}}$:

Digits	Symbolique + Numerique	Mon algorithme
10	0	7
40	0	36
50	6	47

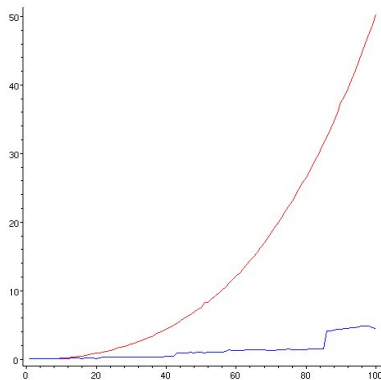
- Version numérique/modulaire : 0.839 secondes. Digits 10.

$F(X, Y) = (Y^3 - M_{10,6}(X))(Y^3 - M_{10,3}(X)) + Y^2X^5$: le discriminant possède un facteur $P(X)$ de degré 30 et avec des coefficients $> 10^{13}$.

Partie ramifiée de l'algorithme de Newton-Puiseux :

Digits	Symbolique + Numerique	Mon algorithme
10	0	4
20	0	15
30	5	29

Temps de calcul



$$F(x, y) = Y^3 - M_{10,5}(X)$$

au-dessus des racines de $M_{10,5}(X)$

Temps de calcul

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

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

Polynôme	temps de calcul symbolique	Mon algorithme	
		temps	précision
G_8	0.031 s	0.029 s	9
G_{12}	0.041 s	0.099 s	9
G_{16}	2.3 s	0.221 s	9
G_{20}	0.751 s	0.550 s	9
G_{24}	2.889 s	0.920 s	9
G_{28}	8.509 s	1.719 s	9
G_{32}	30.820 s	5.040 s	9

Premier utilisé : $p = 100019$.

Conclusions

- Chemins optimisés.
- Stratégie nombre de pas / ordre de troncation : borne sur le nombres d'étapes.
- Développements en des points critiques : algorithme numérique-modulaire.

Perspectives

- Pourquoi le calcul modulaire-numérique semble marcher si bien ?
- Finaliser l'algorithme :
 - Choix du premier p (travail en cours).
 - Contrôle de la précision.
- Théorème d'Abel Jacobi effectif.