

Calcul symbolique-numérique des séries de Puiseux

Poteaux Adrien

UPMC / INRIA Rocquencourt, équipe SALSA

Séminaire Vegas - Caramel, Loria

3 mars 2011

Développements en série

- $K = \mathbb{Q}(\gamma)$; $F(X, Y) \in K[X, Y]$ sans facteur carré.
- $R_F = \text{Res}_Y(F, F_Y)$
- $x_0 \in \overline{K}$; solutions de $F(X, Y)$ au-dessus de x_0 ?
 - $R_F(x_0) \neq 0$ (point régulier) : séries de Taylor.

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k ; 1 \leq i \leq d_Y$$

Développements en série

- $K = \mathbb{Q}(\gamma)$; $F(X, Y) \in K[X, Y]$ sans facteur carré.
- $R_F = \text{Res}_Y(F, F_Y)$
- $x_0 \in \overline{K}$; solutions de $F(X, Y)$ au-dessus de x_0 ?
 - $R_F(x_0) \neq 0$ (point régulier) : séries de Taylor.

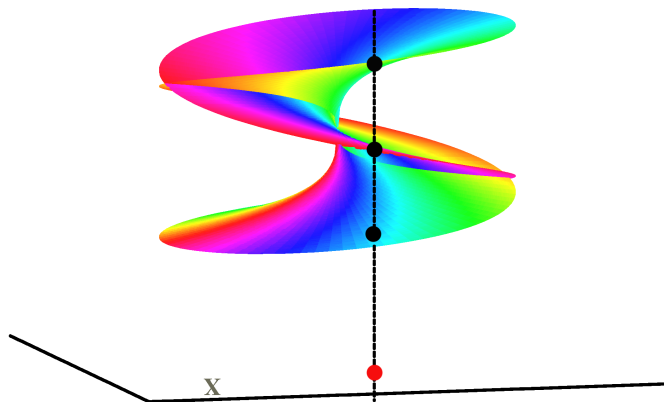
$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k ; 1 \leq i \leq d_Y$$

- $R_F(x_0) = 0$ (point critique) : séries de Puiseux

$$S_{ij}(X) = \sum_{k=n_i}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}} ; 1 \leq j \leq e_i, 1 \leq i \leq s$$

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

Un exemple : $F(X, Y) = Y^3 - X$ au-dessus de $x_0 \neq 0$

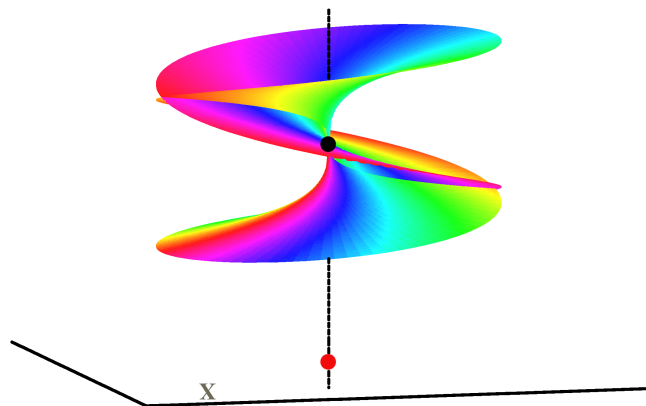


$$Y_1(X) = -0.215 - 0.373 i + (0.898 + 1.555 i)(X - 0.08) + \dots$$

$$Y_2(X) = -0.215 + 0.373 i - (0.898 - 1.555 i)(X - 0.08) + \dots$$

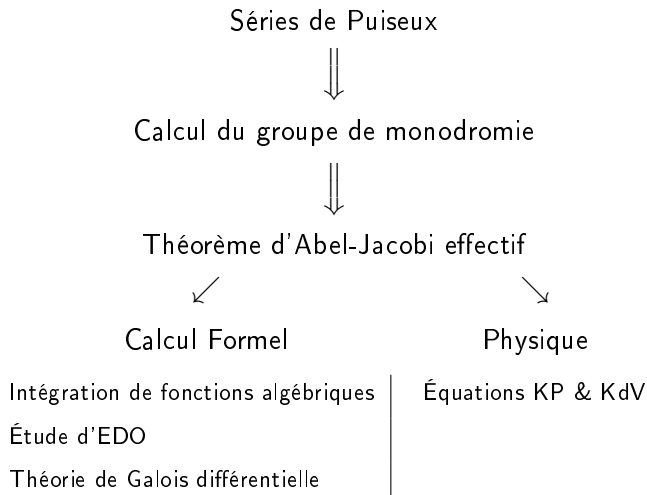
$$Y_3(X) = 0.431 + 1.795(X - 0.08) + \dots$$

Un exemple : $F(X, Y) = Y^3 - X$ au-dessus de $x_0 = 0$



$$Y_j(X) = \zeta_3^j X^{\frac{1}{3}}$$

Motivations



Monodromie locale et Puiseux

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

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

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

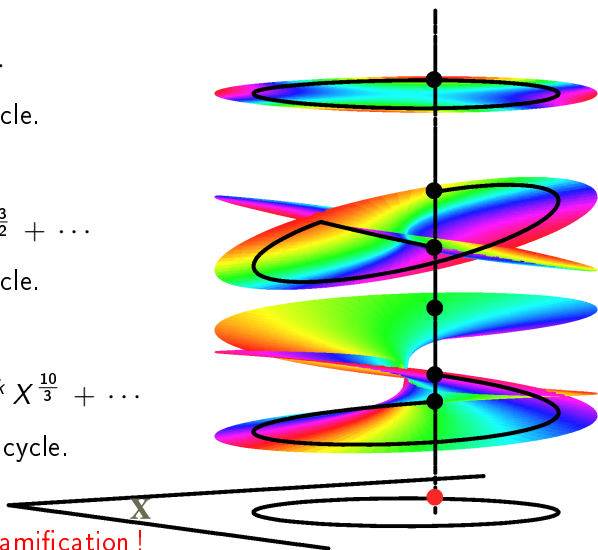
$$1 + \zeta_2^k X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^k X^{\frac{3}{2}} + \dots$$

$\Rightarrow e = 2$: 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 !



Utilisation des séries de Puiseux

- Évaluer les séries de Puiseux nous donne :
 - la monodromie locale,
 - le prolongement analytique près des points critiques.
- Structure exacte nécessaire
- Approximation numérique des coefficients suffisante.

Autres motivations : un outil théorique fondamental

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

Autres motivations : un outil théorique fondamental

- 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*

Autres motivations : un outil théorique fondamental

- Calcul du genre
- Calcul de bases intégrales
 - Détermination de paramétrisations de courbes de genre 0
 - Intégration de fonctions algébriques
- Connectivité dans les courbes algébriques

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

Calcul des séries de Puiseux

- Entrée : exacte.
- Sortie : approchée (structure exacte).

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

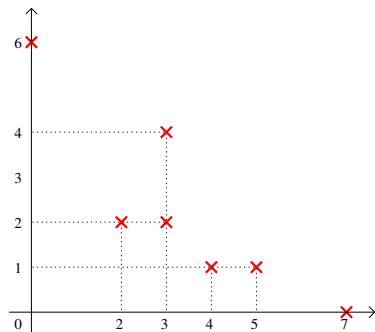
Principaux outils

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

Support d'un polynôme

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

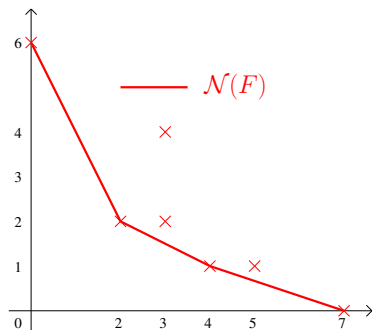
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$



Polygone de Newton

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

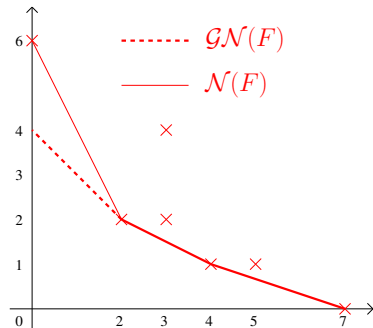
- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: partie inférieure de l'enveloppe convexe de $\text{Supp}(F)$.



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

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

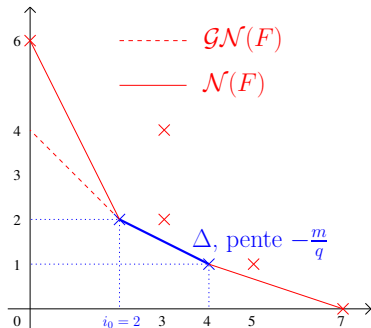
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

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

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

Polynôme caractéristique :

$$\phi_{\Delta}(T) = \sum_{(i,j) \in \Delta} a_{ij} T^{\frac{i-j_0}{q}}$$



Algorithme de Newton-Puiseux rationnel

D. Duval 1989, *Rational Puiseux Expansions*

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

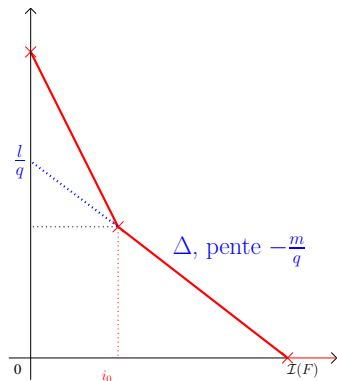
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- 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 $\mathcal{GN}(F)$

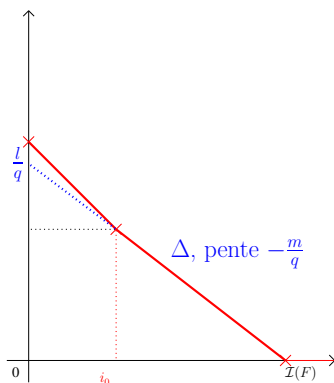
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- 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 $uq - vm = 1$.



Algorithme de Newton-Puiseux rationnel : premier tour

Pour chaque arête Δ de $\mathcal{N}_0(F)$

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

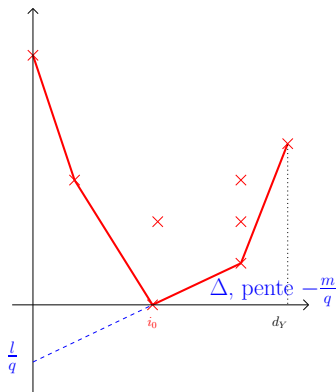
- Pour chaque ϕ_k

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

avec

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

Premier tour : polygone initial $\mathcal{N}_0(F)$



Notre variante : premier tour

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

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

- Pour chaque ϕ_k

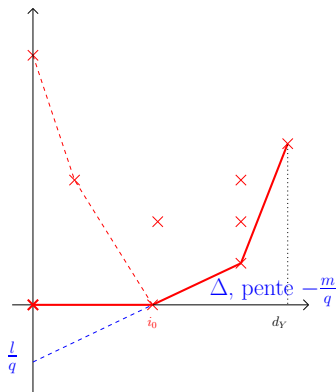
$$F(X, Y) \leftarrow \frac{F(\xi_k^v X^q, X^m(\xi_k^u + Y))}{X^l}$$

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 $\text{Supp}(F) \cup \{(0, 0)\}$).



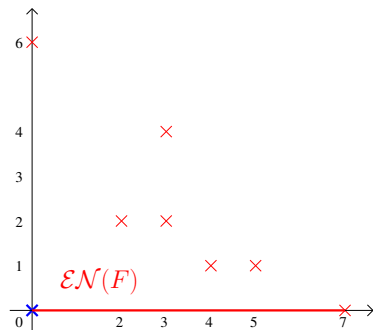
Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton exceptionnel



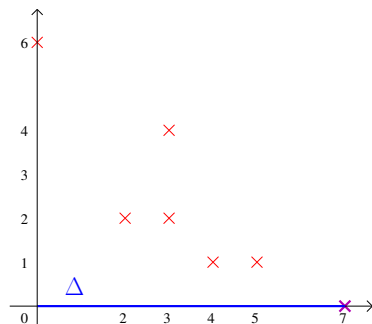
Un exemple

$$\mathcal{EN} = ((0, 0), (7, 0))$$

Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton exceptionnel
- $\phi_{\Delta}(T) = T^7$.



Un exemple

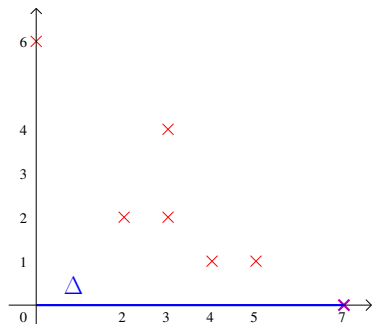
$$\mathcal{E}\mathcal{N} = ((0, 0), (7, 0))$$

$$\begin{array}{c} | \\ \Delta = ((0, 0), (7, 0)) \\ (7) \end{array}$$

Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

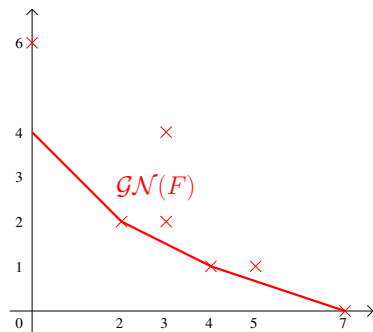
- Polygone de Newton exceptionnel
- $\phi_{\Delta}(T) = T^7$.
- $m = 0, q = 1, l = 0, u = 1, v = 1$.
- $F(X, Y) \leftarrow F(X, Y)$



Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton générique



Un exemple

$$\mathcal{EN} = ((0, 0), (7, 0))$$

$$\left| \begin{array}{l} \Delta = ((0, 0), (7, 0)) \\ (7) \end{array} \right.$$

$$\left| \begin{array}{l} (7) \\ (7, 1) \end{array} \right.$$

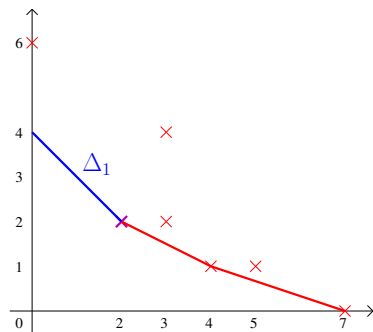
$$\mathcal{GN} = ((0, 4), (2, 2), (4, 1), (7, 0))$$

Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton générique

arête	$\phi_{\Delta_i}(T)$	nouveau pol. F_i
Δ_1	$4T^2$	



Un exemple

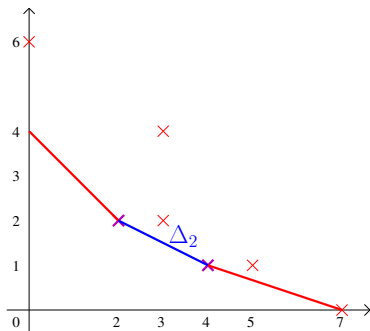
$$\begin{array}{c} \mathcal{E}\mathcal{N} = ((0, 0), (7, 0)) \\ \left| \begin{array}{c} \Delta = ((0, 0), (7, 0)) \\ (7) \\ (7, 1) \end{array} \right. \\ \mathcal{G}\mathcal{N} = ((0, 4), (2, 2), (4, 1), (7, 0)) \\ \swarrow \\ \Delta_1 = ((0, 4), (2, 2)) \\ (2) \end{array}$$

Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton générique

arête	$\phi_{\Delta_i}(T)$	nouveau pol. F_i
Δ_1	$4T^2$	
Δ_2	$4 + 5T$	

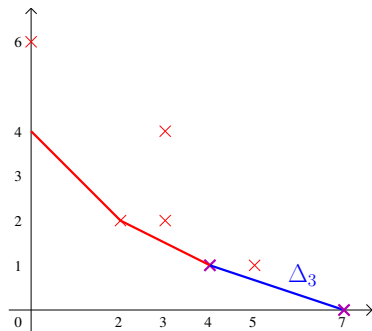


Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Polygone de Newton générique

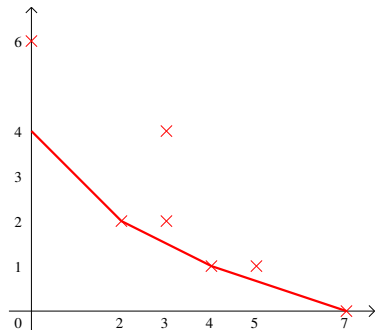
arête	$\phi_{\Delta_i}(T)$	nouveau pol. F_i
Δ_1	$4T^2$	
Δ_2	$4 + 5T$	
Δ_3	$5 + T$	



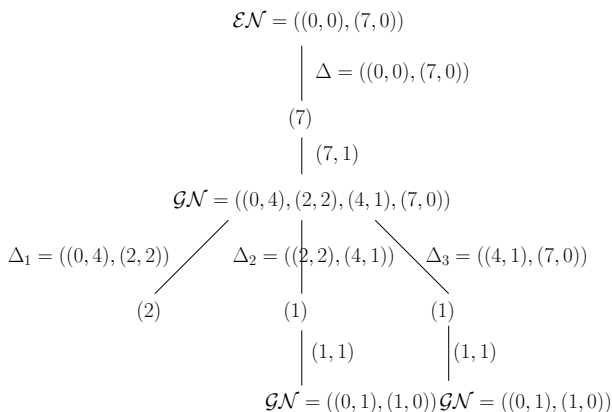
Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5 X + 5 Y^4 X + 5 Y^4 X^3 + 4 Y^2 X^2 + X^6$
- Polygone de Newton générique

arête	$\phi_{\Delta_i}(T)$	nouveau pol. F_i
Δ_1	$4 T^2$	mult. 1 \implies Fin
Δ_2	$4 + 5 T$	
Δ_3	$5 + T$	



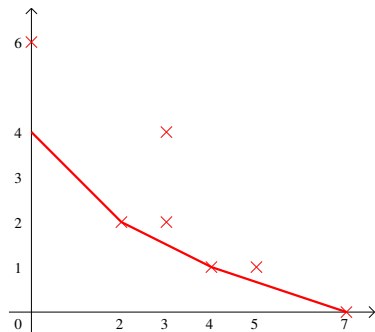
Un exemple



Un exemple

- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5 X + 5 Y^4 X + 5 Y^4 X^3 + 4 Y^2 X^2 + X^6$
- Polygone de Newton générique

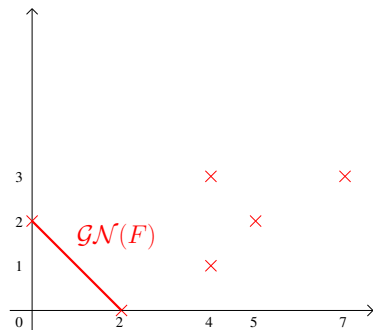
arête	$\phi_{\Delta_i}(T)$	nouveau pol. F_i
Δ_1	$4 T^2$	$\frac{F(X, X Y)}{X^4}$
Δ_2	$4 + 5 T$	mult. 1 \implies Fin
Δ_3	$5 + T$	



Un exemple

- $K = \mathbb{F}_7$
- $F_1(X, Y) = X^3 Y^7 + X^2 Y^5 + 5 X^3 Y^4 - 2 X Y^4 + 4 Y^2 + X^2$

- $\phi_\Delta(T) = 1 + 4 T^2$ irréductible
- Mult. 1 \implies Fin



Calcul d'une approximation des séries de Puiseux

- Calcul numérique délicat

- $H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$
- $R_H(X) = X^3 P(X)$, $\deg_X(P) = 23$; α t.q. $P(\alpha) = 0$.
- $\tilde{\alpha} = -.5060254677 - .4773219060 I$ (Maple, Digits 10).
- $\tilde{H} = H(X + \tilde{\alpha}, y)$
- Série solution au-dessus de $(0, 0.4060249175 + 0.9045013397 I)$:
$$Y(X) = 0.4060249175 + 0.9045013397 I - (11442.48178 - 28086.23142 I)X + (0.1342799379 \cdot 10^{14} - 0.2787302439 \cdot 10^{14} I)X^2 + \dots$$
- rayon de convergence de $Y(X)$: $0.1063792606 \cdot 10^{-6}$

Calcul d'une approximation des séries de Puiseux

- Calcul numérique délicat
- (calcul symbolique) + (évaluation numérique) =
(temps de calcul importants) + (mauvaise précision)
 - $H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$
 - $R_H(X) = X^3 P(X)$, $\deg_X(P) = 23$; α t.q. $P(\alpha) = 0$.
 - Séries de Puiseux au-dessus de α : extension de degré 23!
 - Coefficient constant : fractions rationnelles de 98 chiffres!
 - Complexité binaire : $\tilde{O}(d_Y^{32} d_X^4)$

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

Un nouvel algorithme symbolique-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 Utiliser ces informations pour guider le calcul flottant des coefficients des séries de Puiseux.

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

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

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

Poteaux & Rybowicz, AAECC 2011, *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 \mathfrak{p} -réduction, alors :

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

Theorem 2 : $\mathcal{T}(F) = \mathcal{T}(F \bmod \mathfrak{p})$ (*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 $\mathcal{T}(F)$

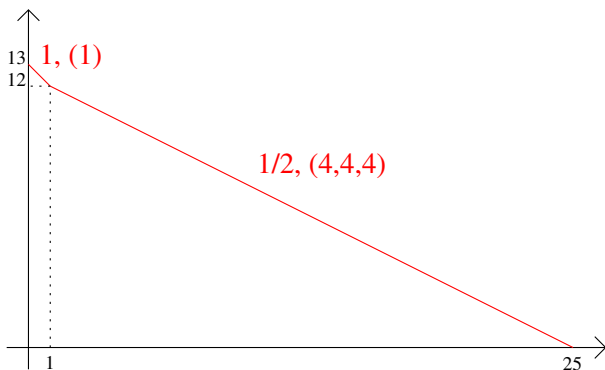
Suivre $\mathcal{T}(F)$ numériquement : un exemple

Développements de Puiseux de F :

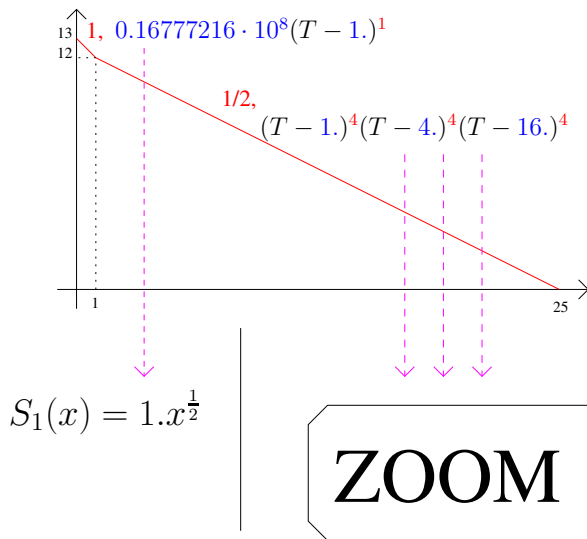
- $S_1(X) = X + \dots$
- $S_2(X) = 4X^{\frac{1}{2}} + X^{\frac{7}{8}} + \dots$
- $S_3(X) = 2X^{\frac{1}{2}} + 2X + \dots$
- $S_4(X) = 2X^{\frac{1}{2}} + X + X^{\frac{7}{6}} + \dots$
- $S_5(X) = X^{\frac{1}{2}} + 2X + X^{\frac{5}{4}} + \dots$
- $S_6(X) = X^{\frac{1}{2}} + X + \dots$
- $S_7(X) = X^{\frac{1}{2}}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

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

Premier polygone de Newton



Premier polygone de Newton



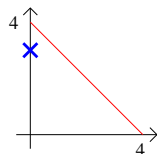
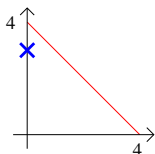
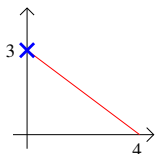

$$S_1(x) = 1.x^{\frac{1}{2}}$$

ZOOM

Tri selon les polygones

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

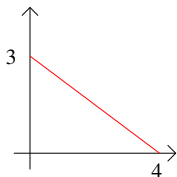
$\{G_1, G_2, G_3\}$



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

Tri selon les polygones

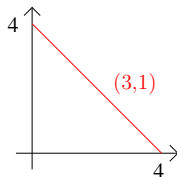
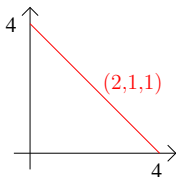
G_3



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

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

$\{G_1, G_2\}$



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

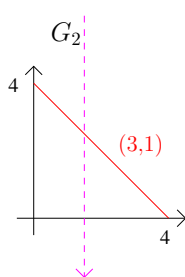
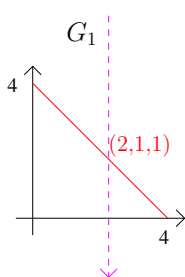
Tri selon les multiplicités

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]]]
```

Un bon comportement numérique apparent : un exemple

$$F(X, Y) = (Y^3 - M_{10,6}(X))(Y^3 - M_{10,3}(X)) + Y^2 X^5$$

où $M_{a,d} = X^d - 2(aX - 1)^2$.

coefficient en $X^{1/2}$

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

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
- \implies Les séries de Puiseux peuvent être utilisées en pratique !

Perspectives

- Contrôle des erreurs numériques ; amélioration du second filtre.
- Implémentation efficace.
- Nouvel algorithme ?

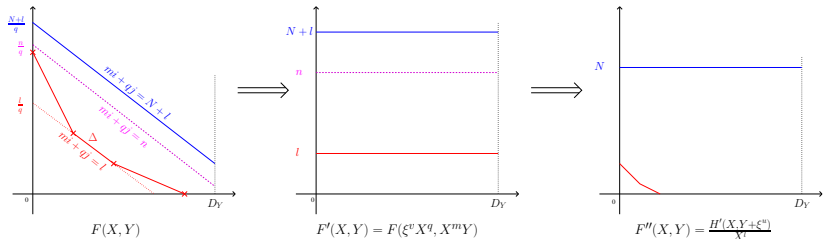
Choix du premier p

- $K = \mathbb{Q}(\gamma)$, $w = [K : \mathbb{Q}]$, 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

Théorème

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