Sur le calcul efficace des séries de Puiseux

Adrien Poteaux* & Marc Rybowicz†

*: CFHP - CO2 - CRIStAL - Université de Lille

†: DMI - XLIM - Université de Limoges

Séminaire de géométrie et algèbre effectives, IRMAR, Rennes

18 Décembre 2015

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$ $\rightsquigarrow$ $y_1 = 4,\ y_2 = 8$ $(\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow$ $y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2}$ $(\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow$ $y_1 = 1.618,\ y_2 = -0.618$ $(\mathbb{K} = \mathbb{C})$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$ $\rightsquigarrow$ $y_1 = 4,\ y_2 = 8$ $(\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow$ $y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2}$ $(\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow$ $y_1 = 1.618,\ y_2 = -0.618$ $(\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ polynômes ?

Exemple

$$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \rightsquigarrow \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$ $\rightsquigarrow$ $y_1 = 4,\ y_2 = 8$ $(\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow$ $y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2}$ $(\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow$ $y_1 = 1.618,\ y_2 = -0.618$ $(\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Taylor ?

Exemple

$$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \rightsquigarrow \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$$

$$(1 - X)\,Y - 1 \rightsquigarrow Y_1(X) = 1 + X + X^2 + \ldots \in \mathbb{K}[[X]]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$ $\rightsquigarrow$ $y_1 = 4,\ y_2 = 8$ $(\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow$ $y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2}$ $(\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow$ $y_1 = 1.618,\ y_2 = -0.618$ $(\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \rightsquigarrow \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$$

$$X^2\,(1 - X)\,Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \ldots \in \mathbb{K}((X))$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$ $\rightsquigarrow$ $y_1 = 4,\ y_2 = 8$ $(\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow$ $y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2}$ $(\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow$ $y_1 = 1.618,\ y_2 = -0.618$ $(\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \rightsquigarrow \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$

$X^2\,(1 - X)\,Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \ldots \in \mathbb{K}((X))$

$Y^3 - X$

$\rightsquigarrow Y_i(X) = \xi_3^i\,\sqrt[3]{X},\ \xi_3^3 = 1 \qquad \in \overline{\mathbb{K}}[X^{1/3}]$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$
  $\rightsquigarrow \quad y_1 = 4,\ y_2 = 8 \qquad (\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow \quad y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2} \qquad (\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow \quad y_1 = 1.618,\ y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Laurent ?

Exemple

$$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \quad \rightsquigarrow \quad \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$$

$$X^2\,(1 - X)\,Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \ldots \in \mathbb{K}((X))$$

$$(1 + X)^2\,Y^2 - 2\,(X + 1)\,Y - X + 1$$
$$\rightsquigarrow Y_i(X) = 1 + \xi_2^i\,X^{1/2} - X - \xi_2^i\,X^{3/2} + X^2 + \ldots \qquad \in \mathbb{K}[[X^{1/2}]]$$

Un problème classique : racines d'un polynôme

- $F \in \mathbb{K}[Y]$, $\mathbb{K} = \mathbb{Q}(\alpha)$ ou $\mathbb{K} = \mathbb{F}_{p^n} \rightsquigarrow$ éléments de $\overline{\mathbb{K}}$

Exemple

- $F(Y) = Y^2 - 3\,Y + 2 \rightsquigarrow y_1 = 1,\ y_2 = 2,$
- $F(Y) = Y^2 - Y + 1$
  $\rightsquigarrow \quad y_1 = 4,\ y_2 = 8 \qquad (\mathbb{K} = \mathbb{F}_{11})$
  $\rightsquigarrow \quad y_1 = \frac{1+\sqrt{5}}{2},\ y_2 = \frac{1-\sqrt{5}}{2} \qquad (\mathbb{K} = \mathbb{Q})$
  $\rightsquigarrow \quad y_1 = 1.618,\ y_2 = -0.618 \quad (\mathbb{K} = \mathbb{C})$

- $F \in \mathbb{K}[X][Y] \rightsquigarrow$ séries de Puiseux

Exemple

$$Y^2 - (2\,X + 3)\,Y + X^2 + 3\,X + 2 \quad \rightsquigarrow \quad \left.\begin{array}{l} Y_1(X) = 1 + X \\ Y_2(X) = 2 + X \end{array}\right\} \in \mathbb{K}[X]$$

$$X^2\,(1 - X)\,Y - 1 \rightsquigarrow Y_1(X) = X^{-2} + X^{-1} + 1 + X + \ldots \in \mathbb{K}((X))$$

$$X^2\,(1 + X)^2\,Y^2 - 2\,(X + 1)\,Y - X + 1$$
$$\rightsquigarrow Y_i(X) = X^{-1} + \xi_2^i\,X^{-1/2} - 1 - \xi_2^i\,X^{1/2} + \ldots \qquad \in \mathbb{K}((X^{1/2}))$$

Séries de Puiseux

Théorème (Puiseux, 1850)

Il existe $e_1, \cdots, e_s \in \mathbb{N}^\star$ *tels que* $d_Y = \sum_{i=1}^{s} e_i$ *et* F *(vu comme un polynôme univarié en* Y*) possède* d_Y *racines distinctes dans* $\overline{\mathbb{K}((X - x_0))}$ *qui peuvent s'écrire de la façon suivante :*

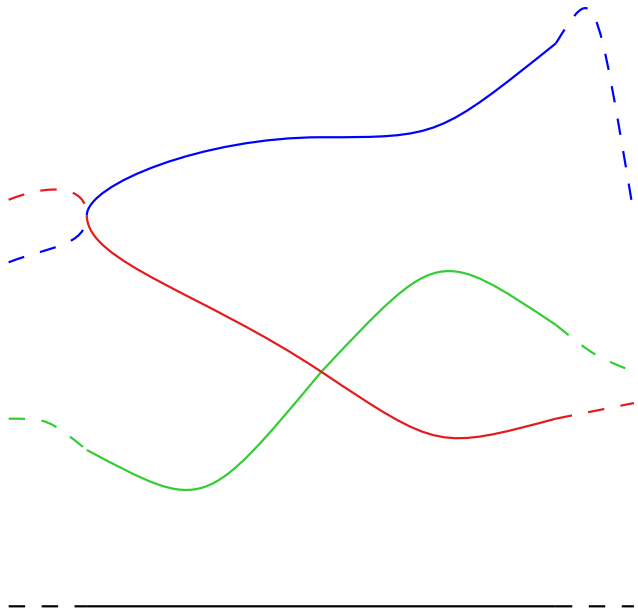
$$Y_{ij}(X) = \sum_{k=n_i}^{\infty} \alpha_{i,k}\, \zeta_{e_i}^{jk}\, (X - x_0)^{\frac{k}{e_i}}$$

avec :

- $0 \leq j \leq e_i - 1$, $1 \leq i \leq s$,
- $n_i \in \mathbb{Z}$, $\alpha_{i,n_i} \neq 0$
- ζ_{e_i} *racine primitive de l'unité d'ordre* e_i

De plus, $\{\alpha_{i,k}\}$ *appartiennent à une extension finie de* $\mathbb{K}$.

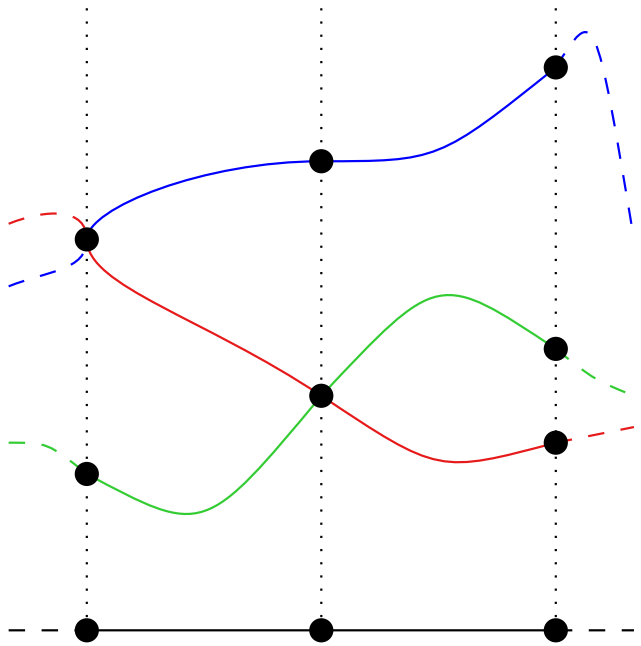
Racines de $F \in \mathbb{K}[X][Y]$



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

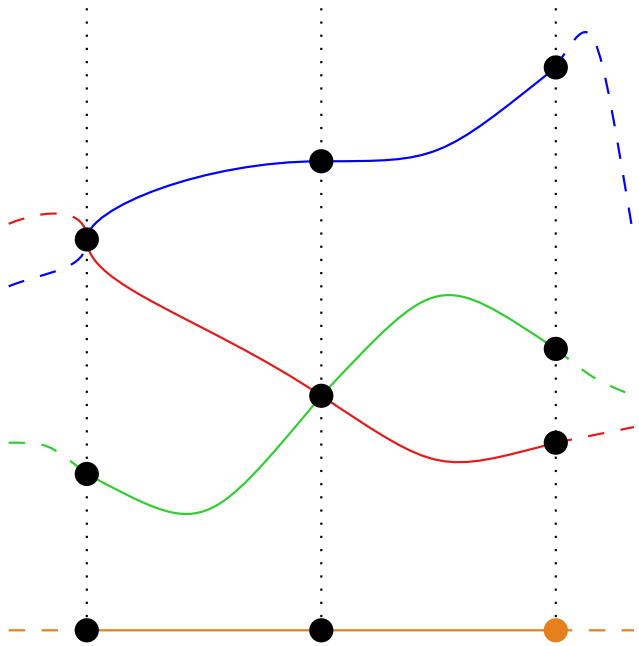
- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.

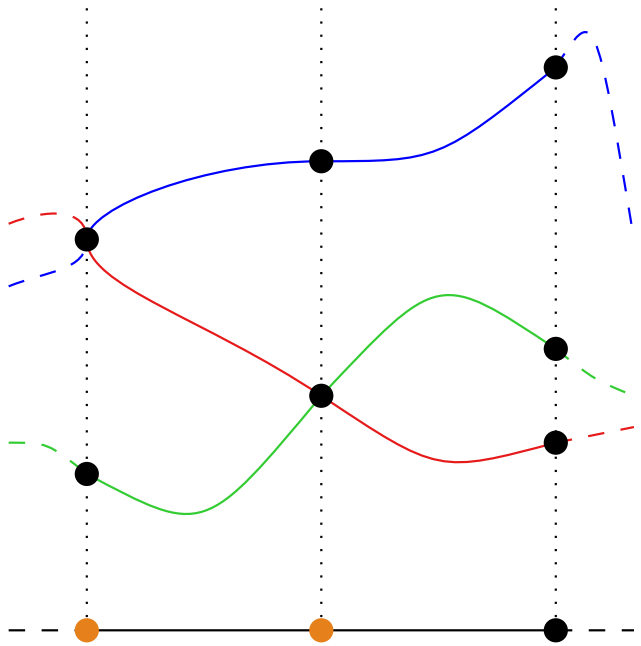


$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.
- **Point critique** : $\#\mathcal{F}(x_0) < d_Y$.

  $\Longrightarrow$ racines de $\mathrm{Res}_Y(F, F_Y)$.



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.

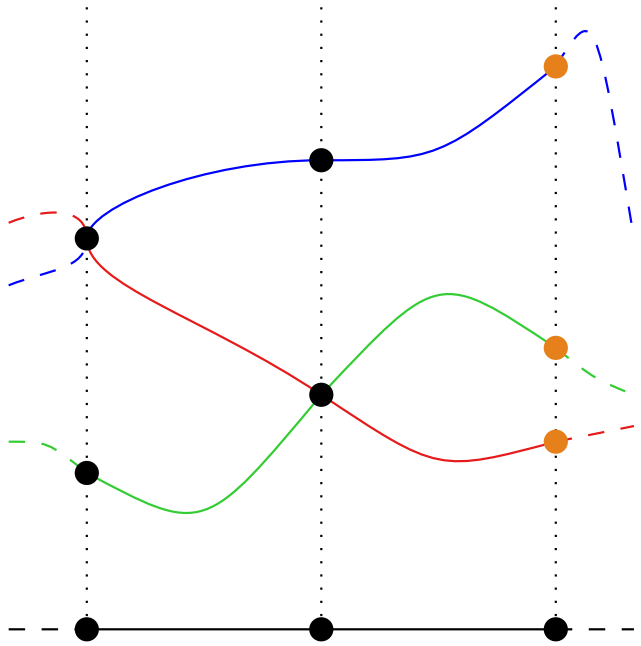
d_Y séries de Taylor :

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik}(X - x_0)^k$$

(Théorème des fonctions implicites)

- **Point critique** : $\#\mathcal{F}(x_0) < d_Y$.

$\Longrightarrow$ racines de $\mathrm{Res}_Y(F, F_Y)$.



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Racines de $F \in \mathbb{K}[X][Y]$

- **Fibre** en $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{racines de } F(x_0, Y) = 0\}$.
- **Point régulier** : $\#\mathcal{F}(x_0) = d_Y$.

d_Y séries de Taylor :

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k$$

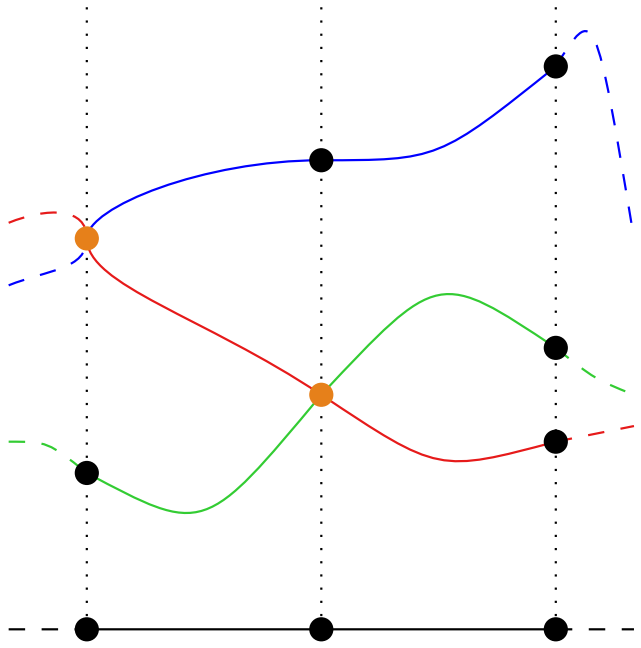
(Théorème des fonctions implicites)

- **Point critique** : $\#\mathcal{F}(x_0) < d_Y$.

$\Longrightarrow$ racines de $\mathrm{Res}_Y(F, F_Y)$.

Séries de Puiseux :

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



$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Partie singulière

$$Y_{ij}(X) \quad = \quad \sum_{k=n_i}^{r_{ij}} \alpha_{ik}\, \zeta_{e_i}^{jk}\, X^{\frac{k}{e_i}} + \text{termes suivants}$$

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]

Exemple

$$F = \prod_{i=1}^{3}(Y - S_i(X)) + X^{19}Y \text{ avec}$$

- $S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2} + \ldots$
- $S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2} + \ldots$
- $S_3 = X + X^2 + X^3 + X^4 + \ldots$

Cet exposé : complexité arithmétique sur $\mathbb{F}_{p^n}$

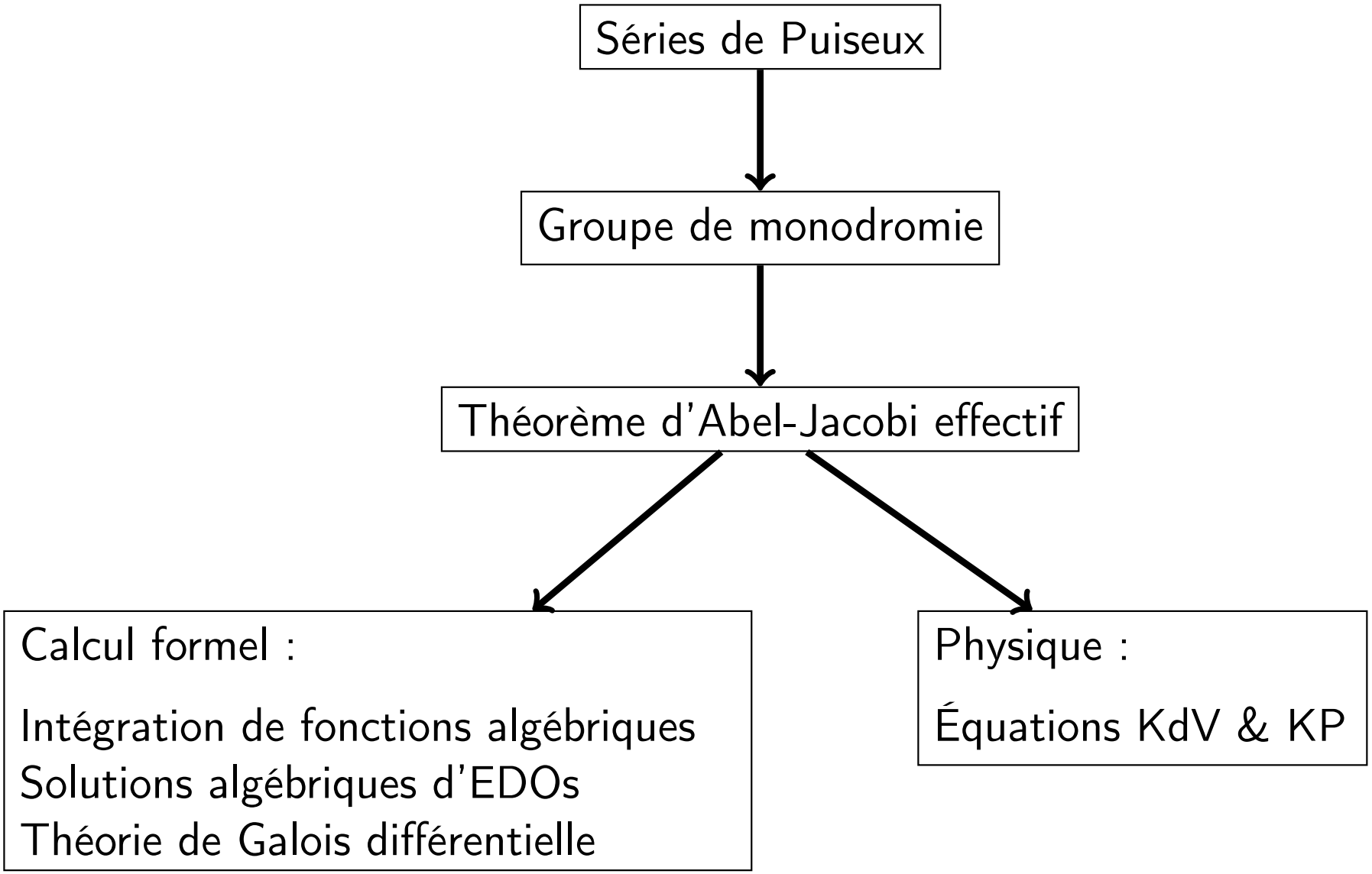
- Article associé : *Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields* (ISSAC'15)
- Les références numérotées / les numéros de pages sont celles de ce papier.

On ne considère pas :

- croissance des coefficients / complexité binaire sur $\mathbb{K} = \mathbb{Q}$
  - expliqué dans Chistov [12], Walsh [53,54]
  - stratégie symbolique / numérique P. & Rybowicz [39,41...]

On suppose $p > \deg_Y(F)$ (comme dans P. & Rybowicz [39,41])

Motivation initiale



Séries de Puiseux et monodromie locale

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

$$2 - 3\,X^2 - \tfrac{9}{2}\,X^3 + \cdots$$

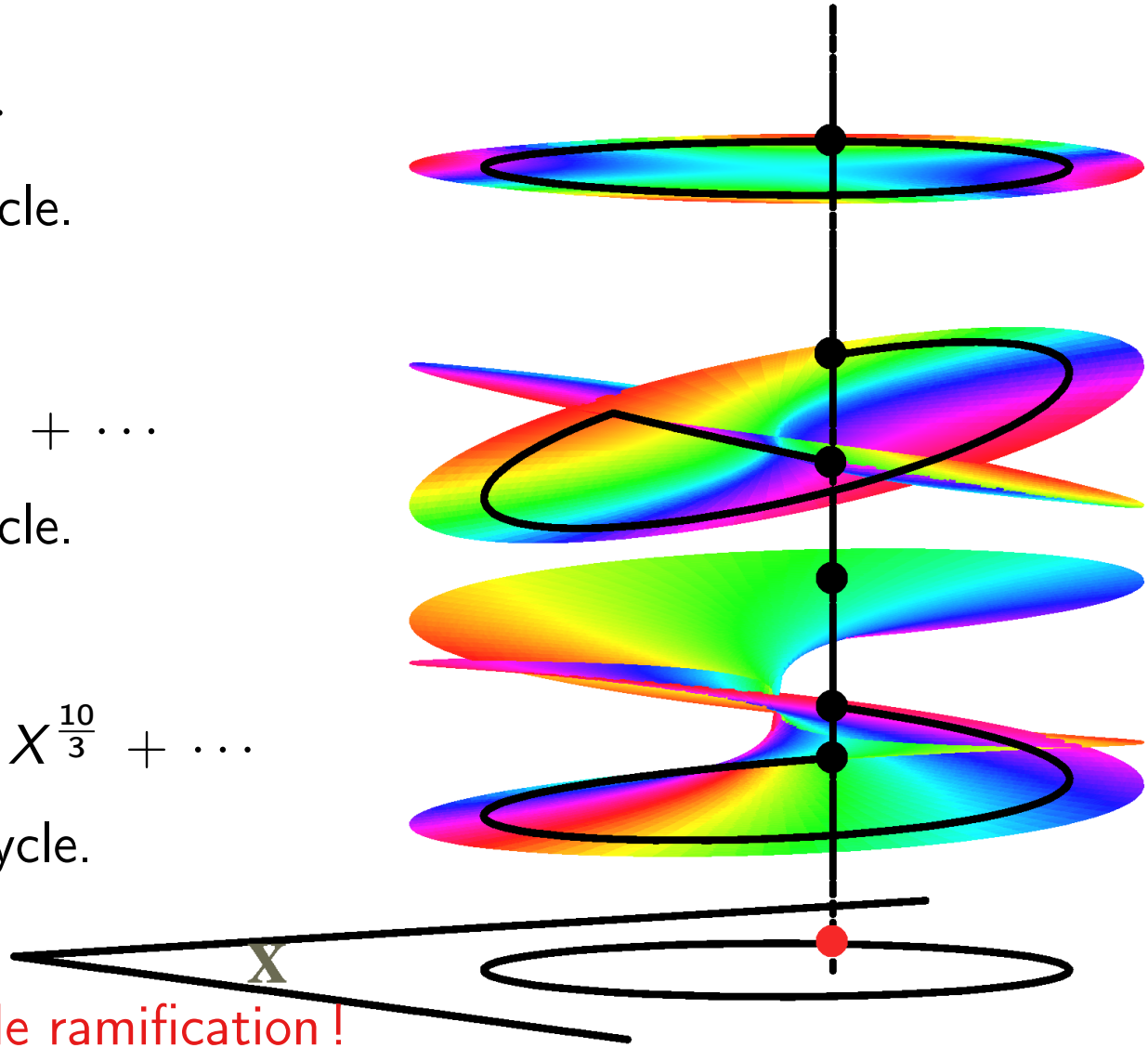
$$\Rightarrow\ e = 1 : \text{1-cycle.}$$

$$1 + \zeta_2^i\,X^{\frac{1}{2}} + \tfrac{1}{2}\,\zeta_2^i\,X^{\frac{3}{2}} + \cdots$$

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

$$\zeta_3^i X^{\frac{1}{3}} + \tfrac{1}{6}\,X^3 + \tfrac{5}{12}\,\zeta_3^i\,X^{\frac{10}{3}} + \cdots$$

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



La monodromie locale
correspond aux indices de ramification !

Calcul d'une série de Puiseux : idée et outils

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

$$\Longrightarrow \text{But : } Y(X) = \alpha\,X^{\frac{m}{q}} + \cdots \text{ s.t. } F(X,Y(X)) = 0$$

$$\begin{aligned} F(X,\alpha\,X^{\frac{m}{q}} + \cdots) \;&= \alpha^6\,X^{\frac{6\,m}{q}} + \alpha^5\,X^{\frac{5\,m}{q}+1} + 5\,\alpha^4\,X^{\frac{4\,m}{q}+3} \\ &\quad -2\,\alpha^4\,X^{\frac{4\,m}{q}+1} + 4\,\alpha^2\,X^{\frac{2\,m}{q}+2} + X^5 - 3\,X^4 + \cdots \end{aligned}$$

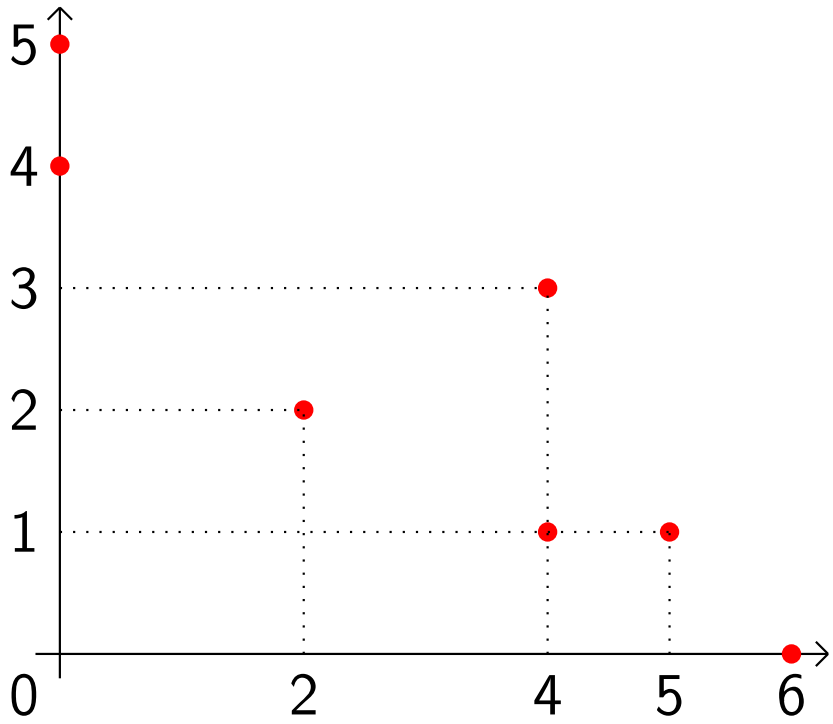
- On doit annuler au moins deux termes !

$$\Longrightarrow (m,q) \text{ t.q. deux exposants soient identiques}$$

Support d'un polynôme

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

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



Choix de (m, q) qui augmente l'ordre en X ?

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

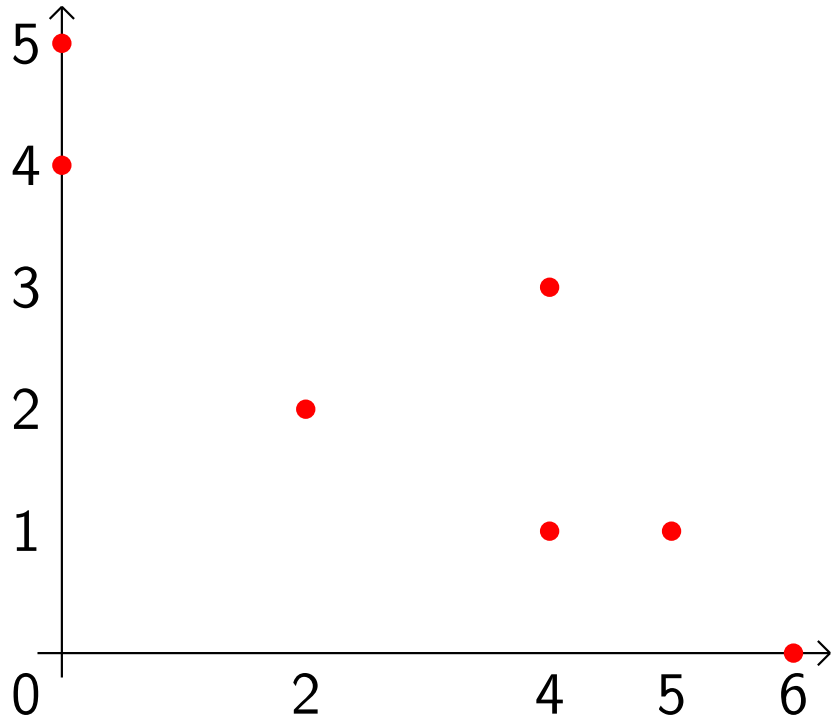
- Supp(F)$= \{(i,j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) pour annuler deux termes ?

$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite



Choix de (m, q) qui augmente l'ordre en X ?

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

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

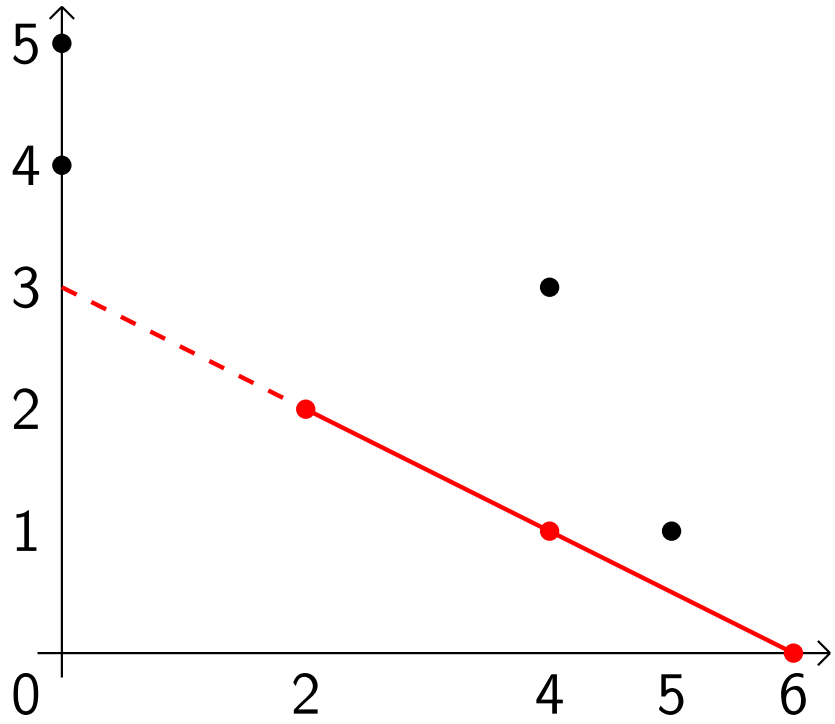
$*$ (m, q) pour annuler deux termes ?

$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite

(Δ_1) $i + 2\,j = 6$ est une telle droite



Choix de (m, q) qui augmente l'ordre en X ?

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

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

$*$ (m, q) pour annuler deux termes ?

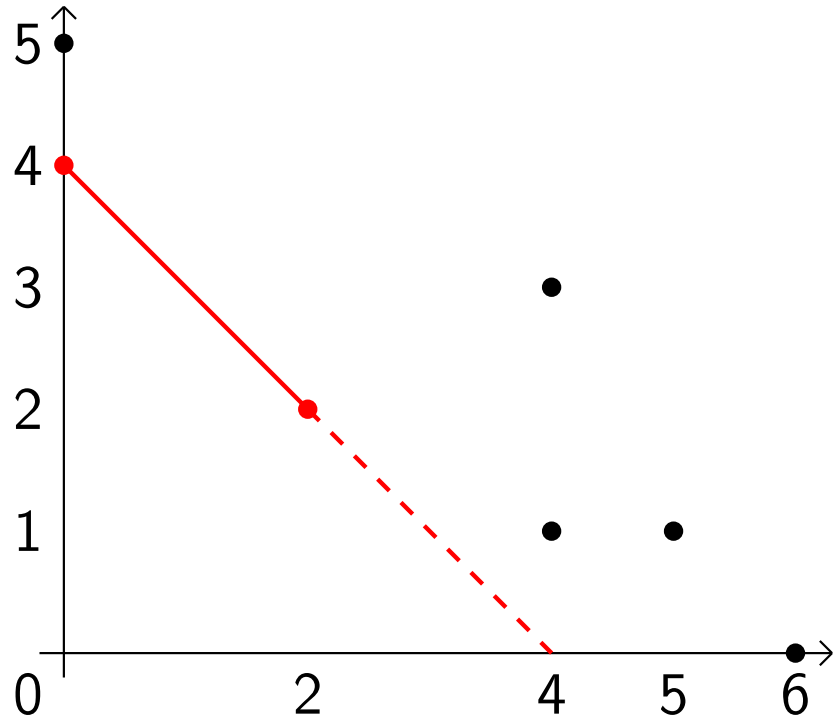
$\rightsquigarrow$ au moins 2 points sur $m\,i + q\,j = l$

$*$ augmenter l'ordre en X ?

$\rightsquigarrow$ pas d'autre point sous cette droite

(Δ_1) $i + 2\,j = 6$ est une telle droite

(Δ_2) $i + j = 4$ aussi

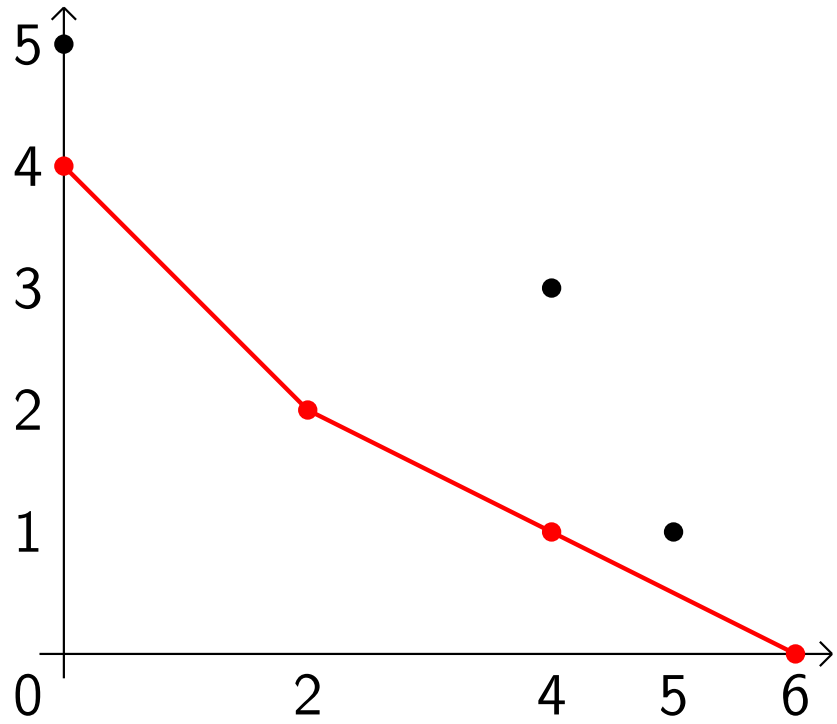


Polygone de Newton

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

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

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



Choix de α qui augmente l'ordre en X ?

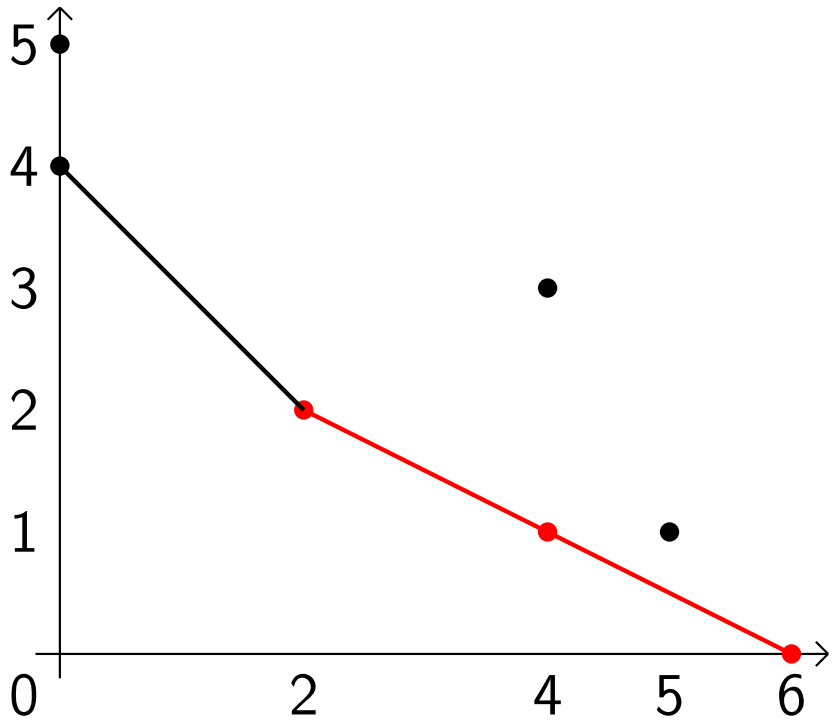
$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

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

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

$$F(T^2, \alpha\,T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\,T^6$$

$$-3\,T^8 + \alpha^5\,T^7 + (5\alpha^4 + 1)\,T^{10} + \ldots$$

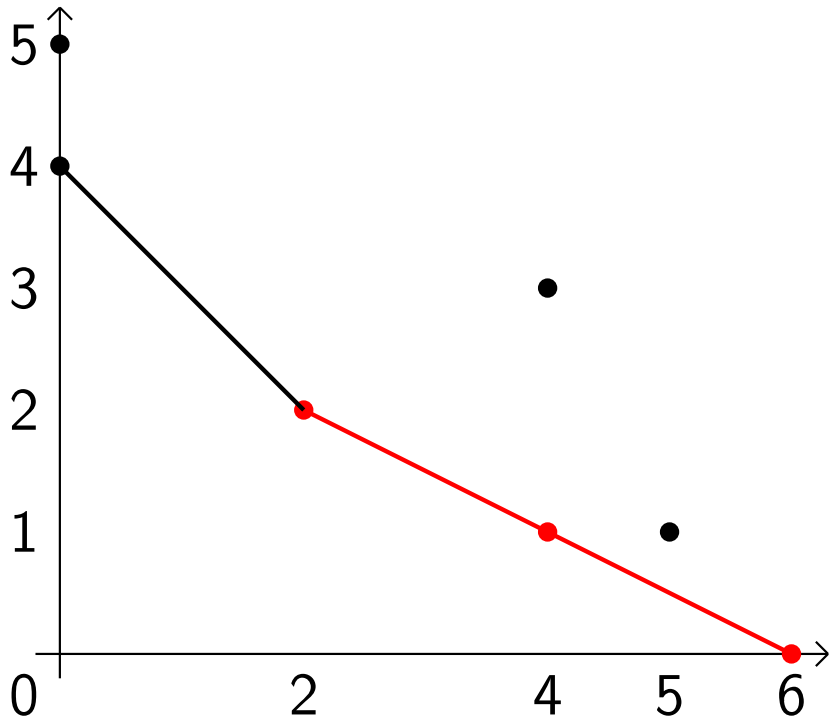


Termes suivants ?

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

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

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



$$F(T^2, \alpha\,T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\,T^6$$

$$-3\,T^8 + \alpha^5\,T^7 + (5\alpha^4 + 1)\,T^{10} + \ldots$$

Termes suivants ?

$$F(X,Y) \leftarrow F(X^q, Y + \alpha\,X^m)$$

Polynôme caractéristique

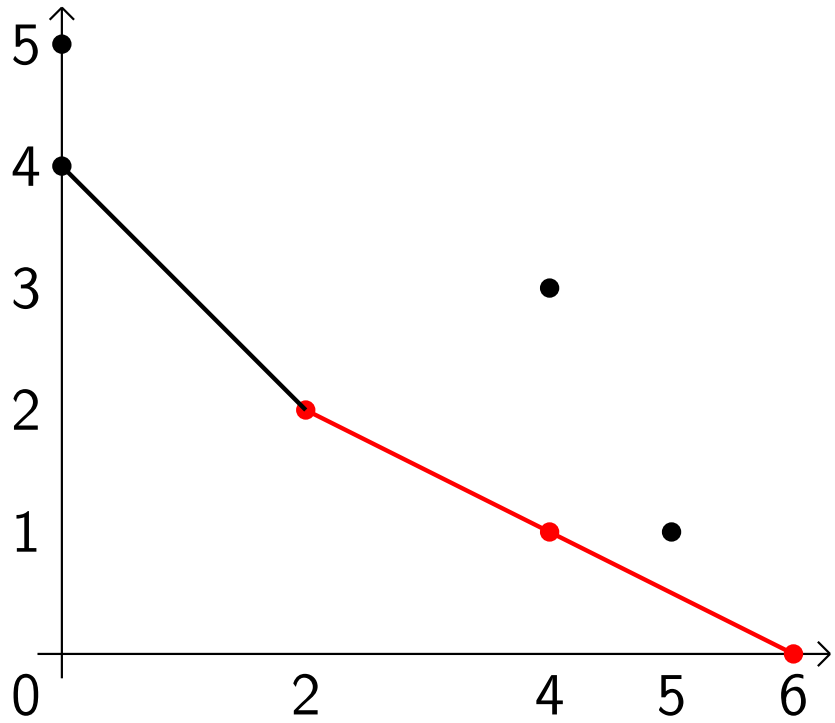
$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

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

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

$$F(T^2, \alpha\, T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)\, T^6$$

$$-3\, T^8 + \alpha^5\, T^7 + (5\alpha^4 + 1)\, T^{10} + \ldots$$



Polynôme caractéristique :

$$\phi_{\Delta_1}(\beta) = \beta^2 - 2\,\beta + 4$$

Algorithme de Newton-Puiseux rationnel Duval [22,23]

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

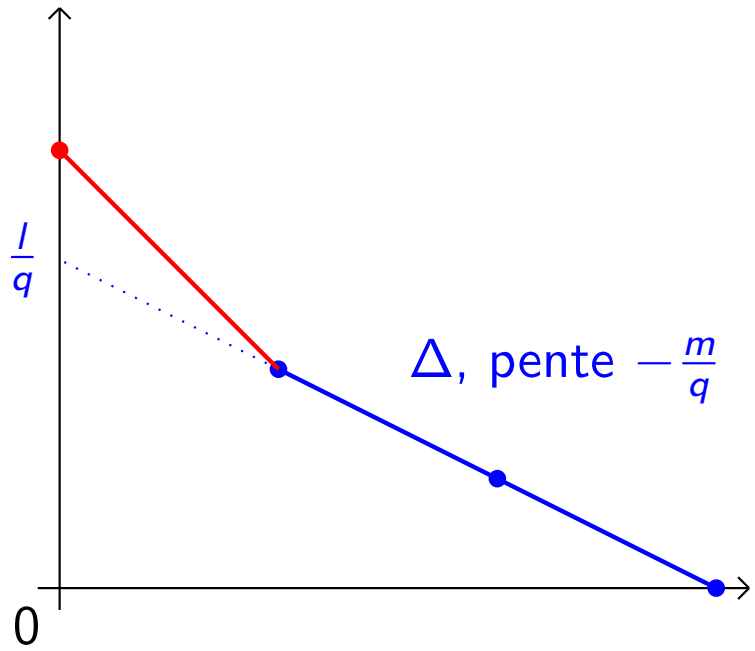
- Factoriser $\phi_\Delta = \prod_{k=1}^{s} \phi_k^{M_k}$
- Pour chaque facteur ϕ_k, RNP-shift :

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

avec

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

- Appels récursifs : $\{H_{\Delta,\xi_k}\ ;\ M_k > 1\}_{\Delta,\xi_k}$



Développements de Puiseux rationnels

Définition (Duval, 1989)

- *F irréductible dans $\mathbb{K}[X,Y]$: « un développement par place »*

$$R_i(T) = (X_i(T), Y_i(T)) = \left(\lambda_i T^{e_i}, \sum_{k=n_i}^{\infty} \beta_{i,k} T^k\right) \in \overline{\mathbb{K}}((T))^2$$

avec

  - $e_i > 0$, $n_i \in \mathbb{Z}$, $\lambda_i \neq 0$, *et* $\beta_{i,n_i} \neq 0$,
  - *paramétrisation irréductible :* $R_i(T) \notin \overline{\mathbb{K}}((T^\kappa))$ *pour* $\kappa > 1$
  - $R_i(T)$ *invariant par l'action du groupe de Galois* $\mathcal{G}(\overline{\mathbb{K}}/\mathbb{K})$

- *$F = F_1 \cdots F_r$ sans carré :* $\{$*dvts de Puiseux rationnels de* $F_k\}$

Si l'on note : - ρ le nombre de développements rationnels.

- $\mathbb{K}_i$ le corps des coefficients de R_i et $f_i = [\mathbb{K}_i : \mathbb{K}]$.

Théorème :

$$\sum_{i=1}^{\rho} e_i f_i = d_Y$$

Lien avec la factorisation.

Développements de Puiseux rationnels :

$$F = \prod_{i=1}^{\rho} F_i \text{ avec } F_i \text{ irréductible dans } \mathbb{K}[[X]][Y]$$

Action du groupe de Galois :

$$F_i = \prod_{j=1}^{f_i} F_{ij} \text{ avec } F_{ij} \text{ irréductible dans } \overline{\mathbb{K}}[[X]][Y]$$

Séries de Puiseux :

$$F_{ij} = A_{d_Y} \prod_{k=0}^{e_i-1} \left(Y - S_{ij}(X^{1/e_i}\zeta_{e_i}^k) \right) \text{ avec } S_{ij} \in \overline{\mathbb{K}}[[X]]$$

État de l'art (Newton-Puiseux)

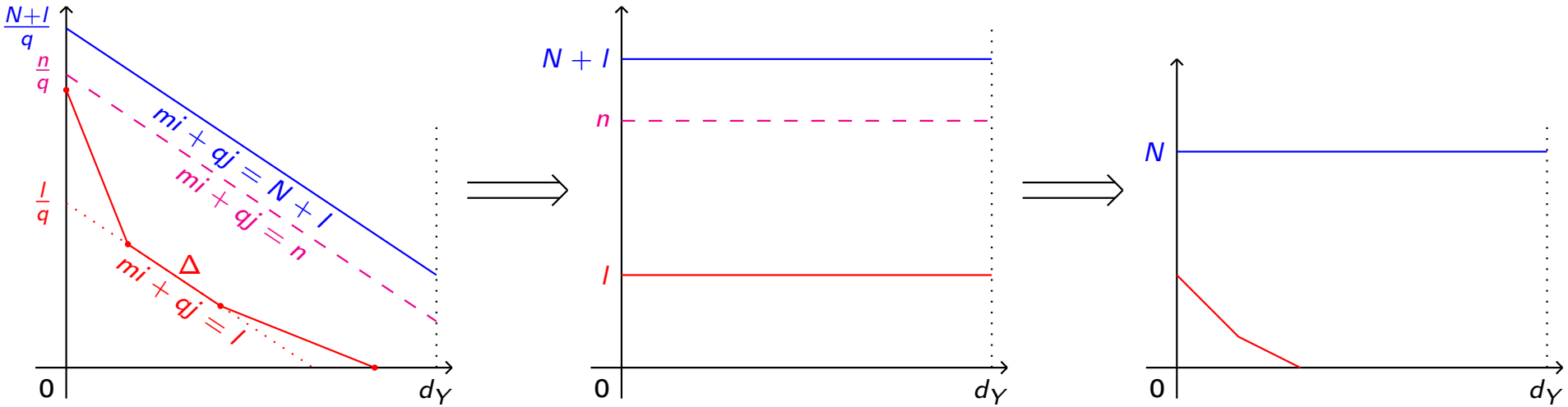
- Newton (1676) : donne le principe.
- Puiseux (1850) : première procédure.
- Chystov 1986 [12] : complexité binaire polynomiale.
- Duval 1989 [23] : algorithme rationnel $\rightarrow$ $O(D^8)$ op. dans $\mathbb{K}$.
- Walsh 2000 [54] : $\tilde{O}(d_Y{}^{32} d_X{}^4)$ (algo classique).
- Walsh 1999 [53] : taille polynomiale des coefficients de certains développements rationnels.
- P. & Rybowicz 2008 [39, 40] : algorithme en $\tilde{O}(D^5)$ op. dans $\mathbb{K}$.

État de l'art (complexité arithmétique)

- variantes de l'algorithme Newton-Puiseux
  - Duval [22, 23] $\rightarrow O(D^8)$
  - P. & Rybowicz [39, 40] $\rightarrow \tilde{O}(D^5)$
- Factorisation dans $\mathbb{F}_q[[X]][Y]$ ou $\overline{\mathbb{F}_q}[[X]][Y]$ (algorithme de Montes)
  - Bauch, Nart & Stainsby [3] : $\tilde{O}(D^5)$, test d'irreducibilité test $\tilde{O}(D^4)$
  - voir aussi Pauli [37, 38], Ford & Veres [25]
- méthodes à la Hensel
  - Sasaki, Inaba, Kako [28, 44, 45]
  - Berthomieu, Quintin, Lecerf [5] (cas particulier)

on note $v_F = \mathrm{v}_X(\mathrm{Disc}_Y(F))$; P. & Rybowicz [39, 40] :

- Un RNP-shift mod X^N : $\tilde{O}(N\, d_Y)$,



$F(X, Y)$ $\qquad$ $F'(X, Y) = F(\xi^v X^q, X^m Y)$ $\qquad$ $F''(X, Y) = \frac{F'(X, Y+\xi^u)}{X^l}$

- Borne de troncation : $N \leq v_F$,
- Nombre d'étapes borné par v_F.

$\Longrightarrow$ complexité en $\tilde{O}(v_F^2\, d_Y) \subset \tilde{O}(d_X{}^2 d_Y{}^3) \subset \tilde{O}(D^5)$

Contributions : amélioration de l'algorithme Newton-Puiseux

- astuce d'Abhyankhar : moins d'étapes ($O(d_X d_Y) \to \tilde{O}(d_Y)$)

  $\to$ polynôme distingué nécessaire.

- Factorisation de F dans $\mathbb{F}_q[[X]][Y]$ au fur et à mesure de l'algorithme

  $\to$ réduit d_Y pour les appels récursifs,

  $\to$ rend le polynôme distingué.

  $\Longrightarrow$ nouvel algorithme en $\tilde{O}(D^4)$.

- Factorisation rapide de F selon le polygone de Newton

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T-\xi)^{d_Y}$

$$\Longrightarrow \text{nombre d'étapes en } O(\rho \log(d_Y)).$$

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T-\xi)^{d_Y}$

$$\Longrightarrow \text{nombre d'étapes en } O(\rho \log(d_Y)).$$

Exemple 2 p. 303 :

$$S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2}$$
$$S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2}$$
$$S_3 = X + X^2 + X^3 + X^4$$

Moins d'étapes ?

Idée : Réduire d_Y à chaque étape

Comment ? Calcul direct des racines communes

Abhyankar [1] : Si F est unitaire,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- On ne peut avoir $\mathcal{N}(G) = \Delta$, $q = 1$ et $\phi_\Delta(T) = (T-\xi)^{d_Y}$

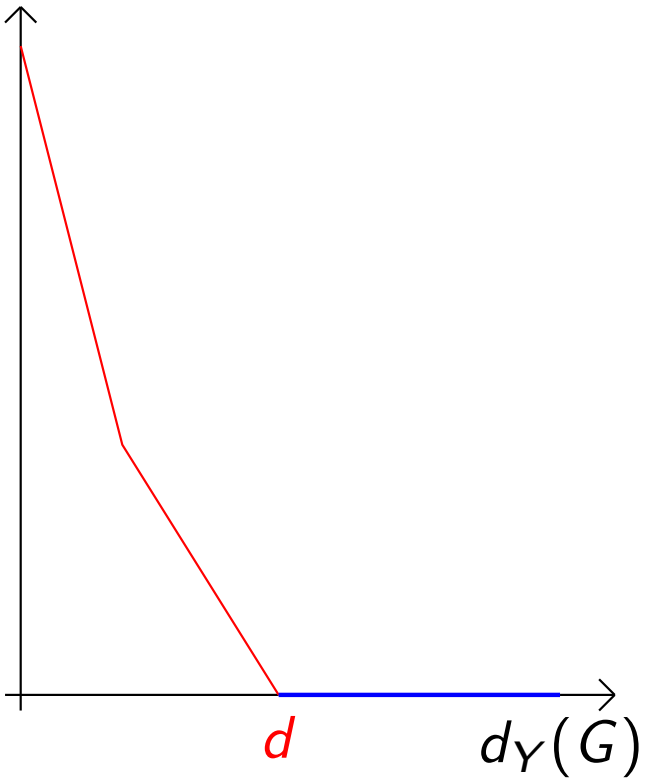
$$\Longrightarrow \text{nombre d'étapes en } O(\rho \log(d_Y)).$$

Exemple 2 p. 303 :

$$S_1 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 - X^{15/2}$$
$$S_2 = X + X^2 + X^3 + 17\,X^4 + X^5 + X^6 + X^7 + X^{15/2}$$
$$S_3 = X + X^2 + X^3 + X^4$$

Théorème de préparation de Weierstrass.

Après un RNP-shift :



- $G(0, Y) = Y^d\, p(Y)$ avec $p(0) \neq 0$,
- Lemme de Hensel :

  $G = H\, P$ in $\mathbb{F}_q[[X]][Y]$ avec :

  - H unitaire en Y,
  - $H(0, Y) = Y^d$,
  - $P(0, Y) = p(Y)$.
- Algorithme :
  1. Lemme de Hensel modulo X^{N+1},
  2. Appels récursifs avec $H(X, Y)$.
- Complexité : $\tilde{O}(d_Y\, N)$

Complexité

$s_k = \#\{(\Delta, \xi)\}$

1. Abhyankar : shift bivarié — $\tilde{O}(N\, d_Y)$
2. RNP-shift : un par (Δ, ξ) — $s_k\, \tilde{O}(N\, d_Y)$
3. Théorème de préparation de Weierstrass — $s_k\, \tilde{O}(N\, d_Y)$
4. Appels récursifs.

- Total : $\sum_k s_k \in O(\rho \log(dy))$ — $\tilde{O}(\rho\, N\, d_Y)$
- $N = v_F(= \mathrm{v}_X(\mathrm{Disc}_Y(F)))$ — $\tilde{O}(\rho\, v_F\, d_Y) \subset \tilde{O}(d_X\, {d_Y}^3)$
- Factorisations P. & Rybowicz [39,40] — $\tilde{O}({d_Y}^3 + {d_Y}^2 \log(q))$

Calcul de complexité fin : famile d'exemples

Exemple (exemple 3, p. 305)

$$F(X,Y) = \prod_{k=1}^{N} (Y - S_k) \ \textit{avec}$$

$$\begin{aligned}
S_1(X) &= 2X \\
S_2(X) &= X + 2X^2 \\
\dots &\quad \dots \quad \dots \\
S_{N-1}(X) &= X + X^2 + \cdots + X^{N-2} + 2X^{N-1} \\
S_N(X) &= X + X^2 + \cdots + X^{N-2} + X^{N-1} + 2X^N
\end{aligned}$$

- $\rho = d_Y = N$, $d_X \in \Theta(N^2)$. $\quad v_F \in \Theta(N^3) = \Theta(d_X d_Y)$.
- Cost is $N^3 \times (N + (N-1) + \cdots + 3 + 2) \simeq N^5$.

$\Longrightarrow$ complexité en $\Theta(d_X {d_Y}^3)$.

Conclusion

- Une meilleure complexité (pire des cas) au-dessus de $x = 0$.

$$O^{\sim}(D^5) \Longrightarrow O^{\sim}(D^4)$$

- Ne marche pas sur *tous* les points critiques.
  - Factorisation trop coûteuse,
  - Devrait passer avec un algorithme à la D5

    Della Dora, Dicrescenzo, Duval [20]

Vers un algorithme dichotomique

Adrien Poteaux* & Martin Weimann†

* : CFHP - CO2 - CRIStAL - Université de Lille

† : LMNO - Université de Caen

Séminaire de géométrie et algèbre effectives, IRMAR, Rennes

18 Décembre 2015

Idées :

- Diminuer le coût des substitutions : algorithme dichotomique.

  1. $F = G \cdot H \mod X^n$; $d_Y(G) \simeq d_Y(H)$, $n \in O(\frac{v_F}{d_Y}) \subset O(d_X)$.
     - Possible via les idées du papier D^4 modulo X^n,
     - Complexité en $O(\rho\, v_F \log(d_Y)^c) \subset \tilde{O}(v_F\, d_Y)$
  2. Hensel adapté [1] $\rightarrow F = G \cdot H \mod X^{v_F}$ $\tilde{O}(v_F\, d_Y)$
  3. $\log(d_Y)$ appels récursifs $\rightsquigarrow$ factorisation analytique mod X^{v_F}
  4. Puiseux, cas irréductible $\tilde{O}(v_F\, d_Y)$

- Factorisations trop coûteuses $\rightsquigarrow$ calculs « à la D5 »

1. $G(0, Y)$ et $H(0, Y)$ ne sont pas premiers entre eux

Lemme de Hensel adapté

- G et H sans racines communes, i.e. premiers dans $K(X)[Y]$,
- Euclide dans $K(X)[Y]$: $U_0\,G + V_0\,H = 1$,

  $U_0, V_0 \in K(X)[Y]$, $d_Y(U_0) < d_Y(H)$ et $d_Y(V_0) < d_Y(G)$
- $k = -\min(\mathrm{v}_X(U_0), \mathrm{v}_X(V_0)) \rightsquigarrow\ U\,G + V\,H = X^k \mod X^n$.

On définit :

- $\tilde{G} = G + X^{n-k}\alpha \cdot V$ et $\tilde{H} = H + X^{n-k}\alpha \cdot U \mod X^{2n-2k}$
- $\tilde{U} = U - (X^{n-k}\beta + 2\,X^{n-2k}\,\alpha \cdot U \cdot V) \cdot U \mod X^{2n-4k}$
- $\tilde{V} = V - (X^{n-k}\beta + 2\,X^{n-2k}\,\alpha \cdot U \cdot V) \cdot V \mod X^{2n-4k}$

Alors :

- $F = \tilde{G} \cdot \tilde{H} \mod X^{2n-2k}$
- $\tilde{U} \cdot \tilde{G} + \tilde{V} \cdot \tilde{H} = X^k \mod X^{2n-4k}$

OK si $n > 4\,k$!

(G, H) pour avoir k petit

- Pour une étape 1 *rapide*, il faut $k \in O(v_F/d_Y)$
- Par définition, $k = \min\{k_0 \in \mathbb{N} \mid X^{k_0} \in (G, H)\}$
- En général, $k \leq \mathrm{v}_X(\mathrm{Res}_Y(G, H))$ Trop grand !
- On peut construire (et calculer) G, H t.q. $k \in O(v_F/d_Y)$

  $\Longrightarrow$ Mélange de RNP-shift et de Hensel (factorisation analytique).

  - Requiert des arguments non triviaux de théorie de la singularité.
  - Work in progress !

Merci !