Improving Complexity Bounds for the Computation of Puiseux Series over Finite Fields

Adrien Poteaux[⋆] & Marc Rybowicz[†]

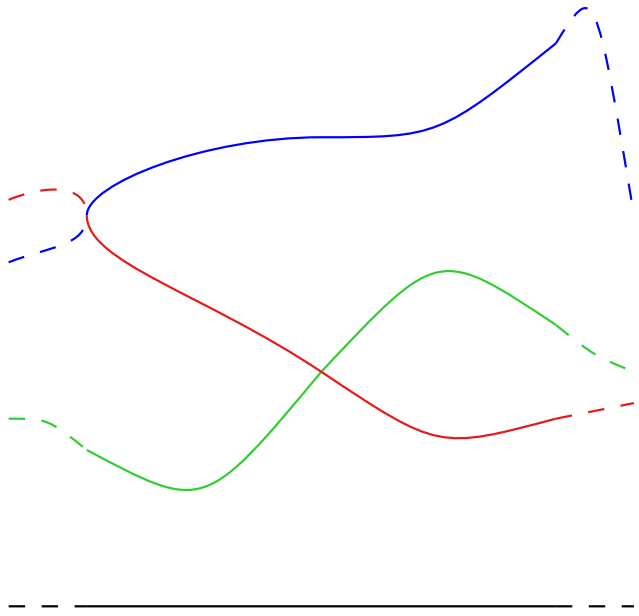
[⋆]: CFHP - CRISTAL - Université Lille 1

[†]: DMI - XLIM - Université de Limoges

ISSAC 2015, Bath, UK

July 8th, 2015

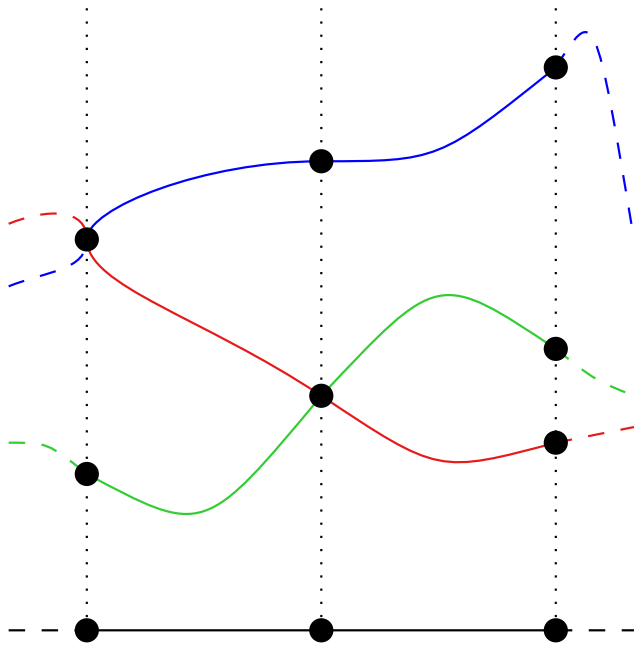
Roots of $F \in \mathbb{K}[X][Y]$ monic in Y



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

Roots of $F \in \mathbb{K}[X][Y]$ monic in Y

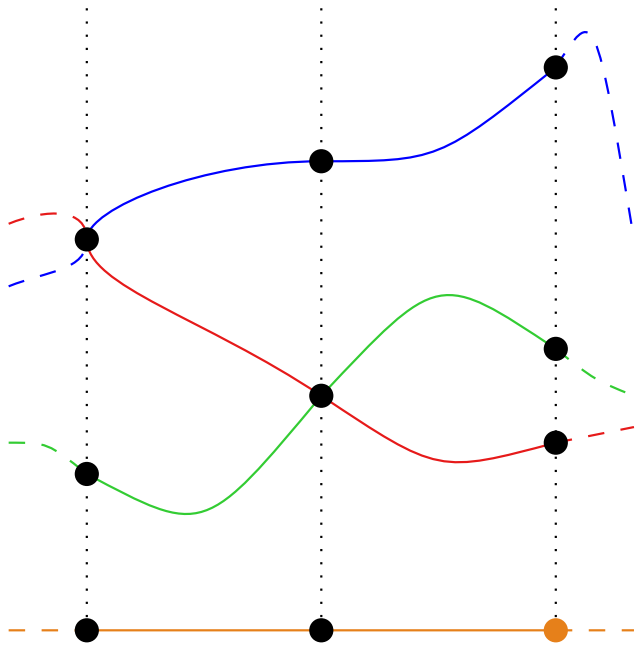
- **Fiber** of $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.



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

Roots of $F \in \mathbb{K}[X][Y]$ monic in Y

- **Fiber** of $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.
- **Regular point** : $\#\mathcal{F}(x_0) = d_Y$.

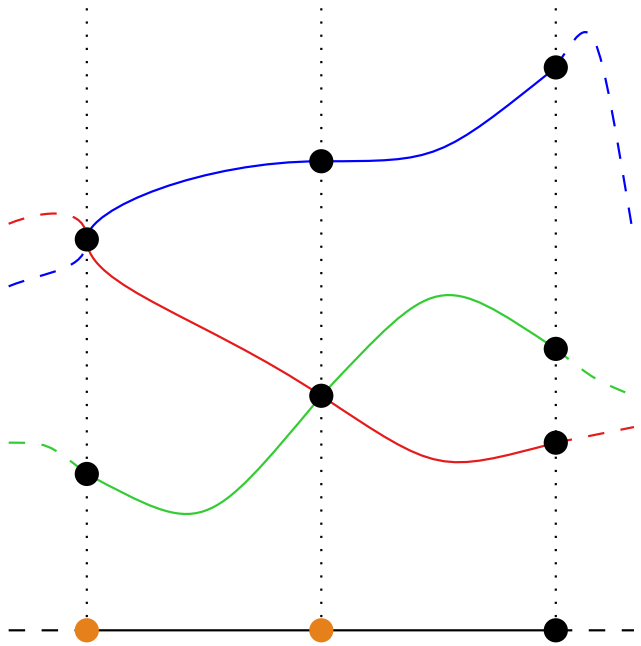


$$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$$

Roots of $F \in \mathbb{K}[X][Y]$ monic in Y

- **Fiber** of $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.
- **Regular point** : $\#\mathcal{F}(x_0) = d_Y$.
- **Critical point** : $\#\mathcal{F}(x_0) < d_Y$.

  $\Longrightarrow$ roots of $\Delta_Y(F)$.



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

Roots of $F \in \mathbb{K}[X][Y]$ monic in Y

- **Fiber** of $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.
- **Regular point** : $\#\mathcal{F}(x_0) = d_Y$.

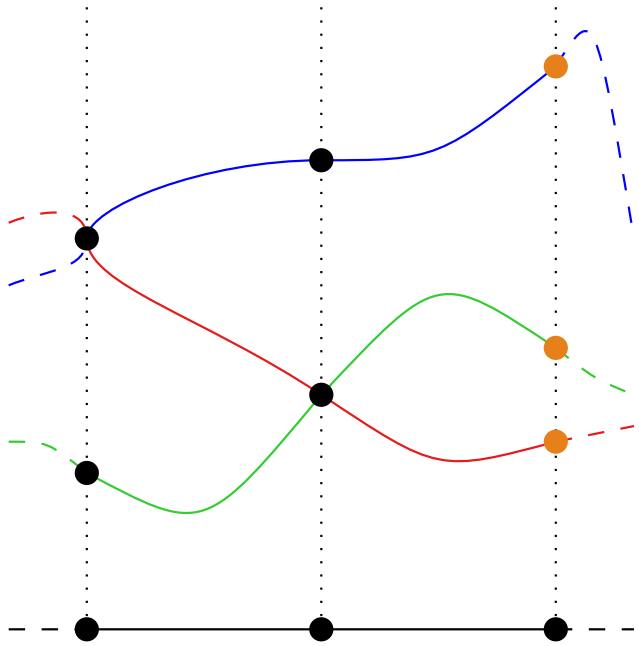
d_Y Taylor series :

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

(Implicit Function Theorem)

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

$\Longrightarrow$ roots of $\Delta_Y(F)$.



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

Roots of $F \in \mathbb{K}[X][Y]$ monic in Y

- **Fiber** of $x_0 \in \mathbb{C}$: $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.
- **Regular point** : $\#\mathcal{F}(x_0) = d_Y$.

d_Y Taylor series :

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

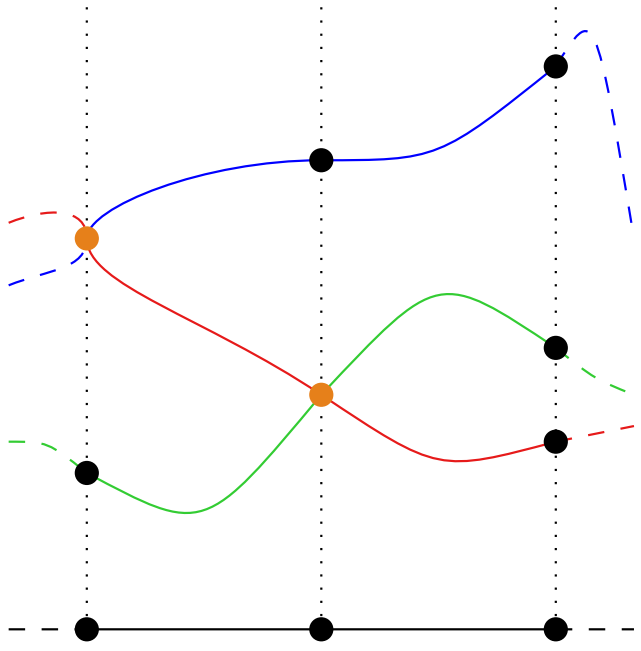
(Implicit Function Theorem)

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

$\Longrightarrow$ roots of $\Delta_Y(F)$.

Puiseux series :

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



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

Singular part

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

r_{ij} is the **regularity index**; $r_i = r_{ij}$ for $1 \leq j \leq e_i$

Next terms can be computed using quadratic Newton iterations

Kung & Traub [31]

Example

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

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

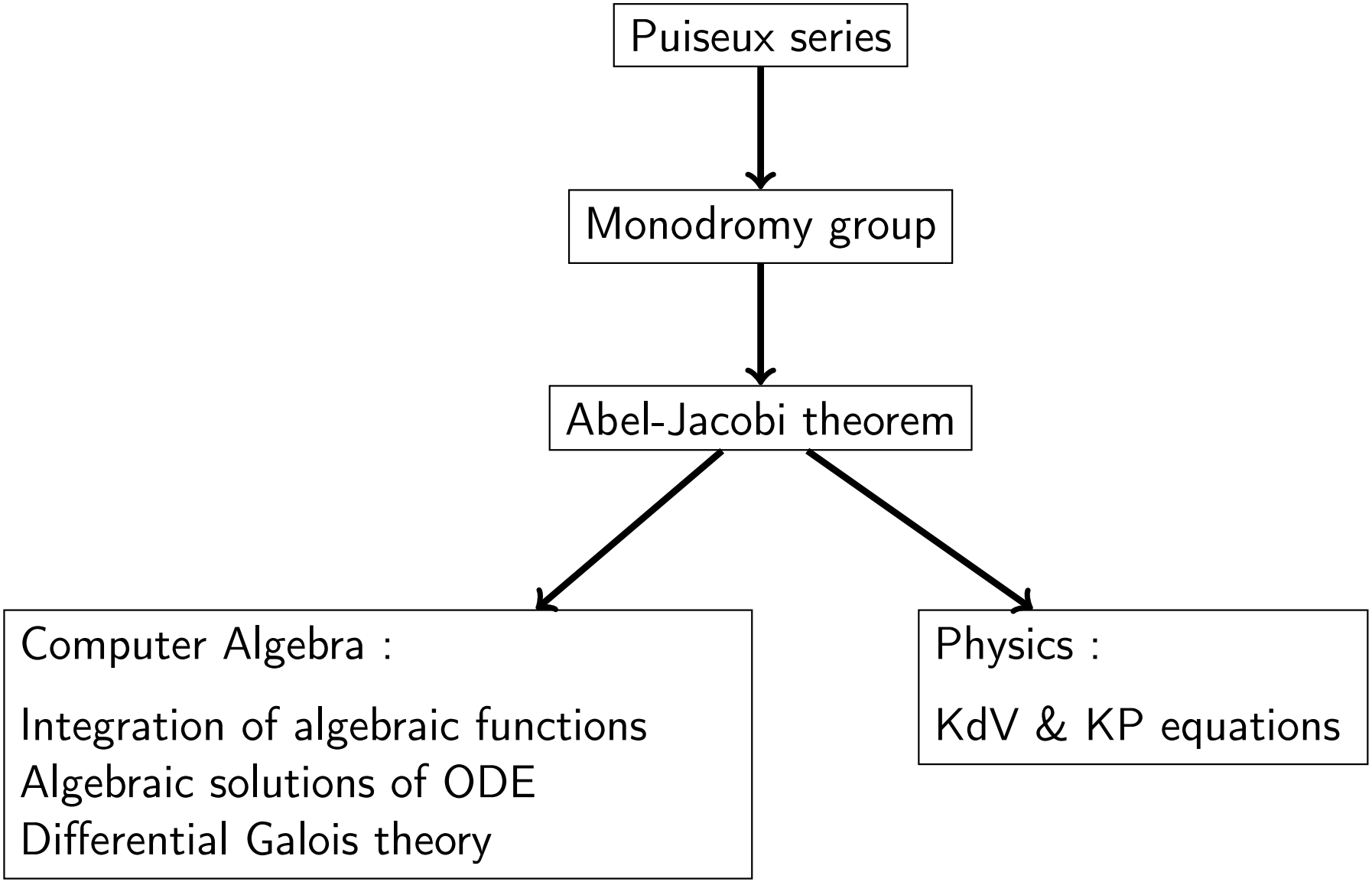
This paper : improving arithmetic complexity over $\mathbb{F}_{p^n}$

We do not consider :

- coefficient growth problem / bit complexity over $\mathbb{K} = \mathbb{Q}$
  - explained in Chistov [12], Walsh [53,54]
  - symbolic / numeric strategy P. & Rybowicz [39,41...]

We assume $p > \deg_Y(F)$ (as in P. & Rybowicz [39,41])

Our initial motivation



State of the art (about arithmetic complexity)

- Newton-Puiseux like algorithm
  - Duval [22, 23] $\rightarrow O(D^8)$
  - P. & Rybowicz [39, 40] $\rightarrow \tilde{O}(D^5)$
- Factorisation in $\mathbb{F}_q[[X]][Y]$ or $\overline{\mathbb{F}_q}[[X]][Y]$ (Montes algorithm)
  - Bauch, Nart & Stainsby [3] : $\tilde{O}(D^5)$, irreducibility test $\tilde{O}(D^4)$
  - see also Pauli [37, 38], Ford & Veres [25]
- Hensel-like methods
  - Sasaki, Inaba, Kako [28, 44, 45]
  - Berthomieu, Quintin, Lecerf [5] (particular case)

Computing Puiseux series : tools and idea

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

$\Longrightarrow$ We're looking $Y(X) = \alpha\,X^{\frac{m}{q}} + \cdots$ s.t. $F(X, Y(X)) = 0$

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

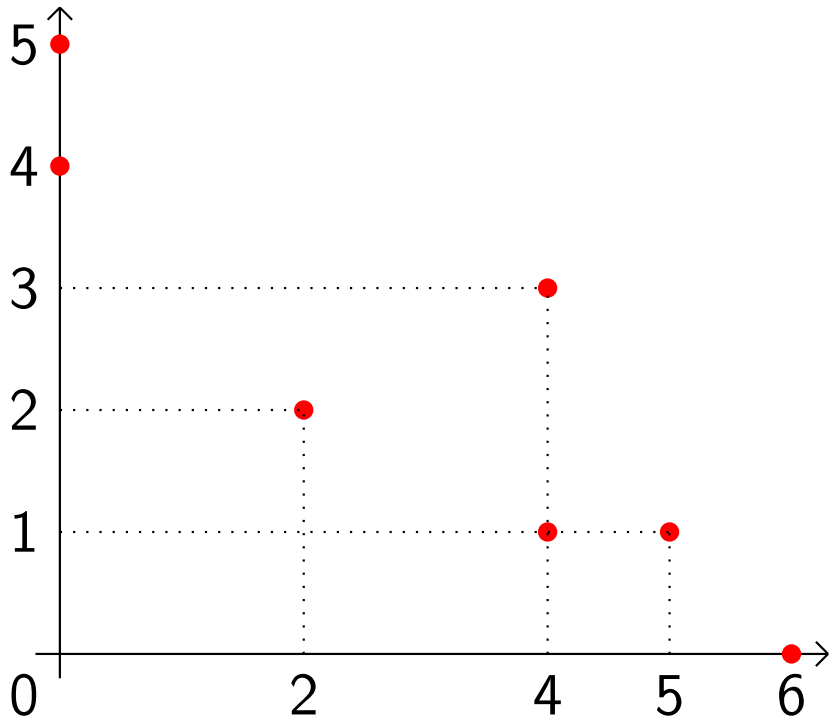
- Some of these terms must cancel !

  $\Longrightarrow$ (m, q) s.t. at least two exponents are the same

Support of the polynomial

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

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



Choice of (m, q) that increases the X-order ?

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

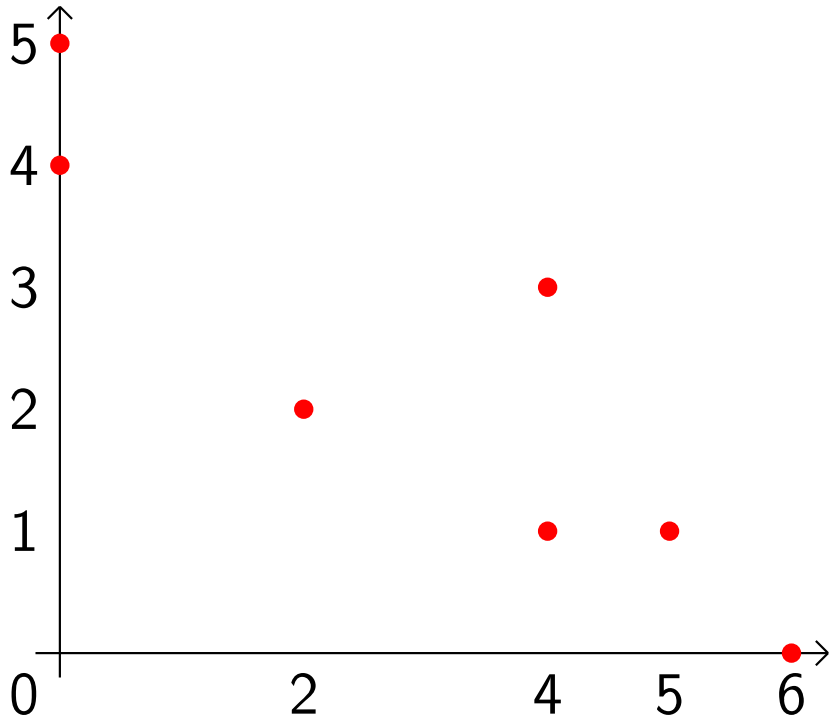
- Supp(F)$= \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$

$*$ (m, q) for cancelling two terms ?

$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

$*$ increasing the X-order ?

$\rightsquigarrow$ no other point under the line



Choice of (m, q) that increases the X-order ?

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

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

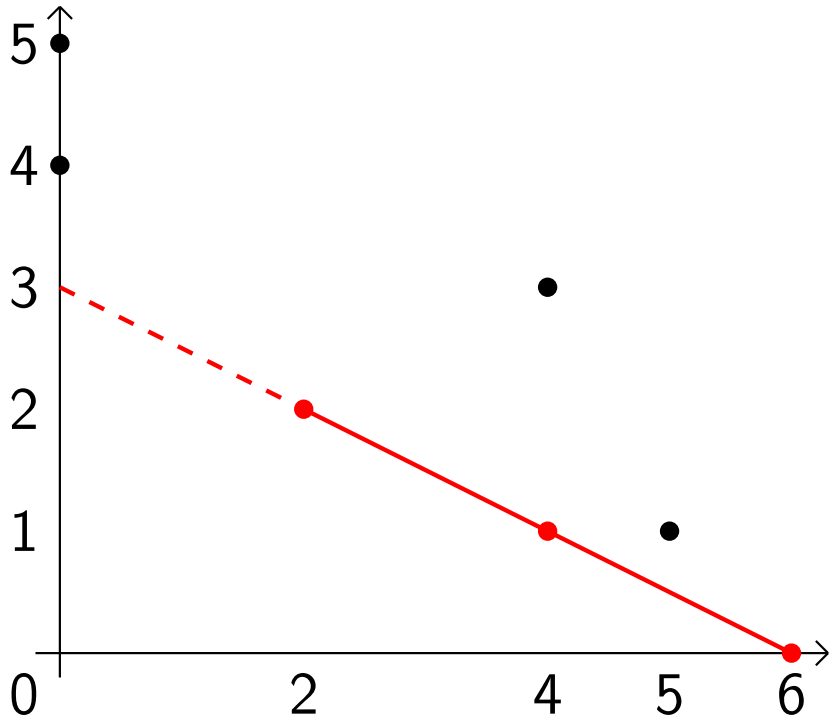
$*$ (m, q) for cancelling two terms ?

$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

$*$ increasing the X-order ?

$\rightsquigarrow$ no other point under the line

(Δ_1) $i + 2\,j = 6$ is such a line



Choice of (m, q) that increases the X-order ?

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

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

$*$ (m, q) for cancelling two terms ?

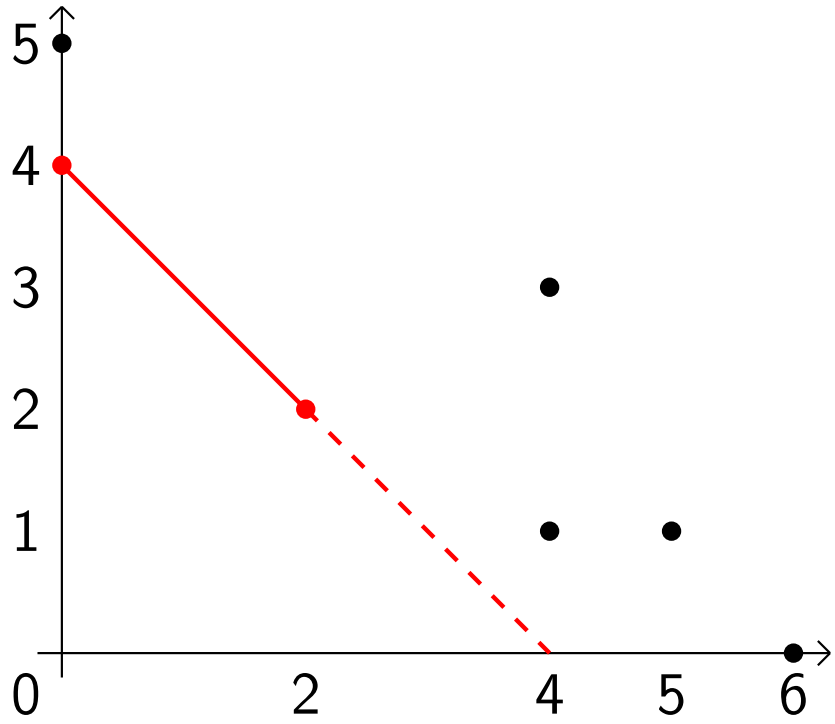
$\rightsquigarrow$ at least two points on $m\,i + q\,j = l$

$*$ increasing the X-order ?

$\rightsquigarrow$ no other point under the line

(Δ_1) $i + 2\,j = 6$ is such a line

(Δ_2) $i + j = 4$ is too

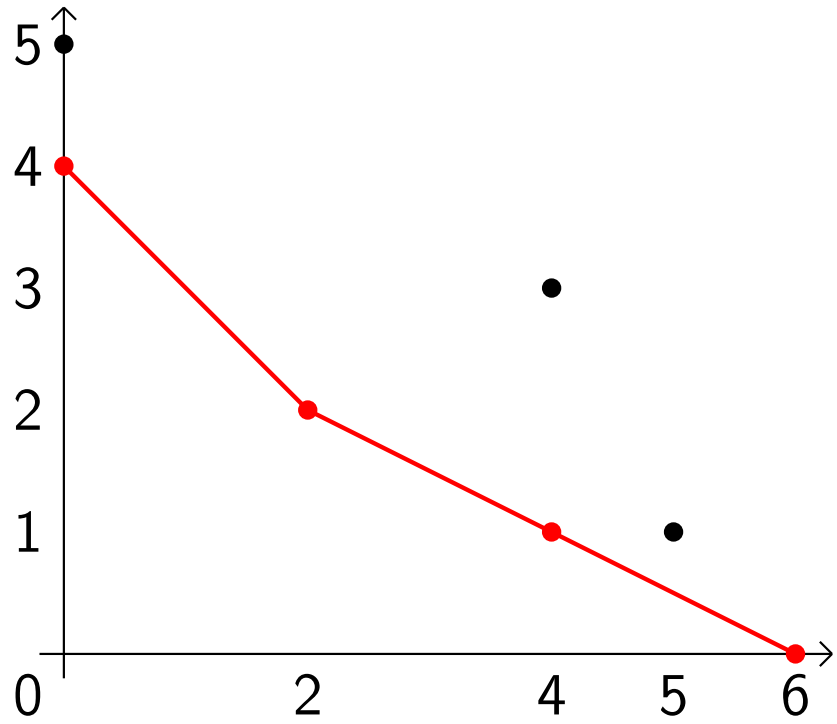


Newton polygon

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

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

— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).



Choice of α that increases the X-order ?

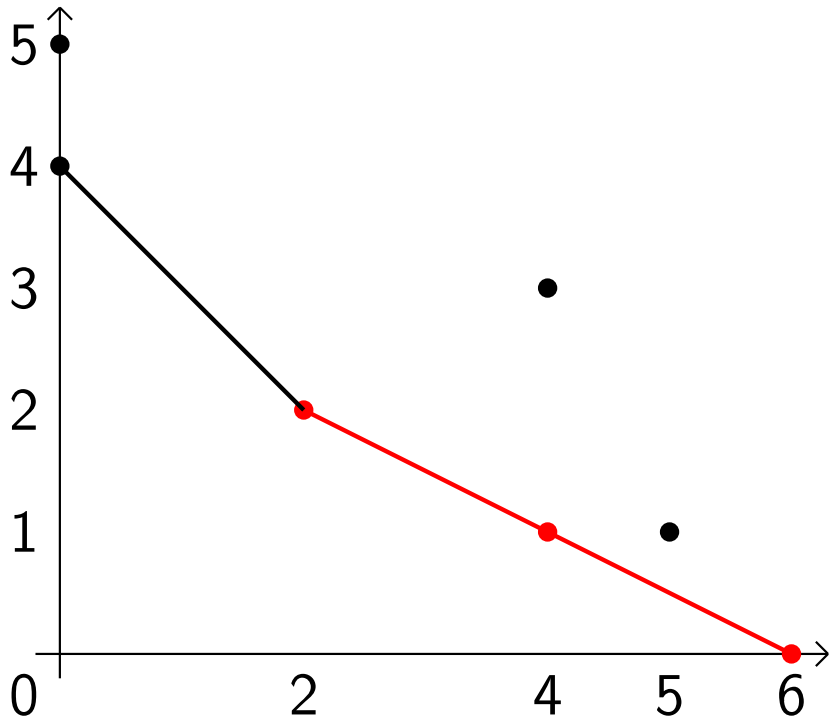
$$F(X,Y) = Y^6 + Y^5X + 5\,Y^4X^3 - 2\,Y^4X + 4\,Y^2X^2 + X^5 - 3\,X^4$$

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

— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).

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

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

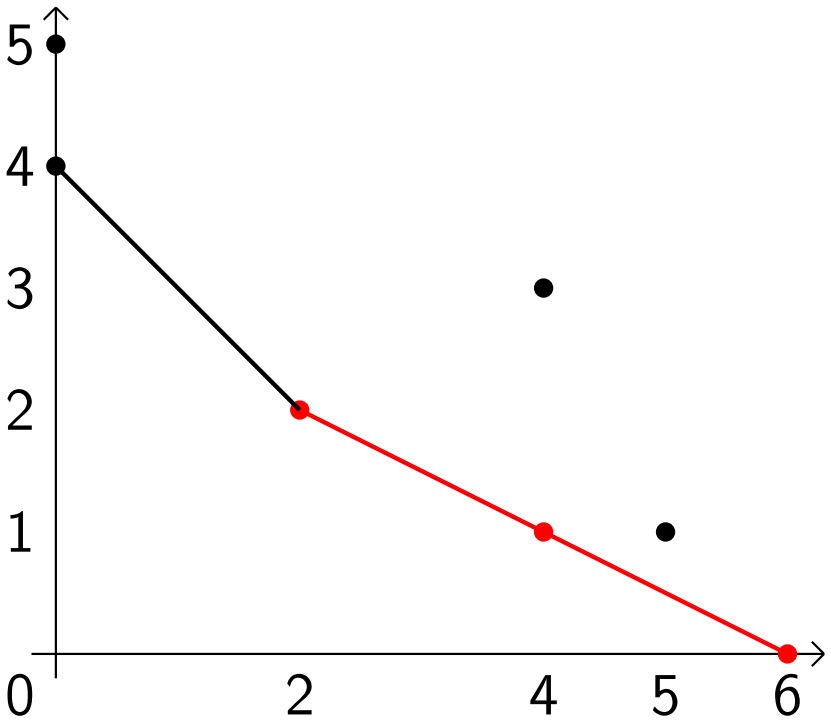


Characteristic polynomial

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

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

— $\mathcal{N}(F)$: lower part of convex hull of Supp(F).



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

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

Characteristic polynomial :

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

Rational Newton-Puiseux algorithm Duval [22,23]

For each edge Δ of $\mathcal{N}(F)$

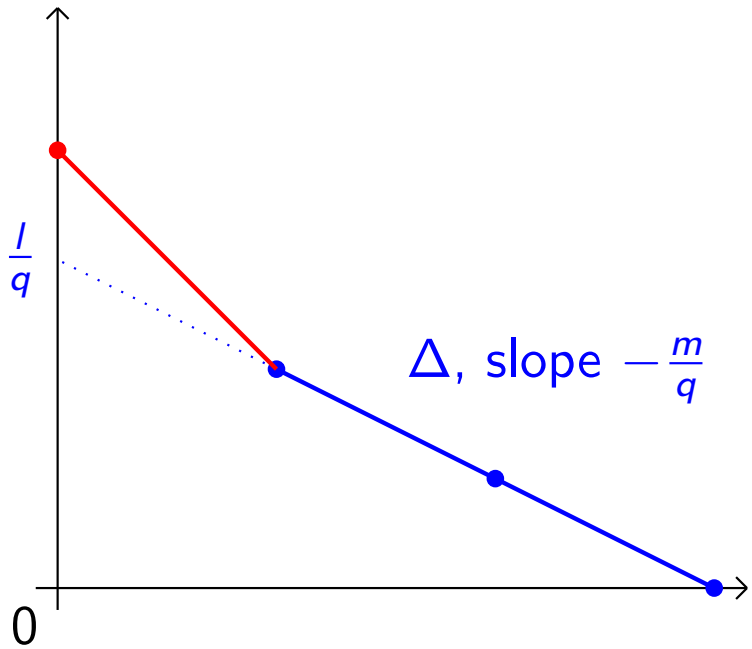
– Factor $\phi_\Delta = \prod_{k=1}^{s} \phi_k^{M_k}$

– For each factor ϕ_k, compute a RNP-shift : $\frac{l}{q}$

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

with
- ξ s.t. $\phi_k(\xi) = 0$,
- (u,v) such that $uq - vm = 1$.

– Recursive calls for $\{H_{\Delta,\xi}(X,Y)\}_{\Delta,\xi}$



ISSAC'08 results

(we denote $v_F = \mathrm{v}_X(\Delta_Y(F))$)

P. & Rybowicz [39, 40] :

- One RNP-substitution mod X^N : $\tilde{O}(N\, d_Y)$,
- We can bound N by v_F,
- The number of steps is bounded by v_F.

$\Longrightarrow$ complexity bounded by $\tilde{O}(v_F^2\, d_Y) \subset \tilde{O}({d_X}^2 {d_Y}^3) \subset \tilde{O}(D^5)$

Contributions : improving Newton-Puiseux algorithm

- Abhyankhar's trick : less steps ($O(d_X d_Y) \rightarrow \tilde{O}(d_Y)$)
  - $\rightarrow$ requires the polynomial to be distinguished.
- Factorisation of F in $\mathbb{F}_q[[X]][Y]$ during the algorithm
  - $\rightarrow$ reduces d_Y in recursive calls,
  - $\rightarrow$ fullfills previous requirement.

$$\Longrightarrow \tilde{O}(D^4) \text{ algorithm.}$$

- Fast factorisation of F according to its Newton polygon

Less steps ?

The idea : Decrease d_Y at each step

How ? Compute potential common roots at once

Abhyankar [1] : if F is monic,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- We cannot have $\mathcal{N}(G) = \Delta$, $q = 1$ and $\phi_\Delta(T) = (T-\xi)^{d_Y}$

$$\Longrightarrow \text{number of steps in } O(\rho \log(d_Y)).$$

Less steps ?

The idea : Decrease d_Y at each step

How ? Compute potential common roots at once

Abhyankar [1] : if F is monic,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- We cannot have $\mathcal{N}(G) = \Delta$, $q = 1$ and $\phi_\Delta(T) = (T-\xi)^{d_Y}$

$$\Longrightarrow \text{number of steps in } O(\rho \log(d_Y)).$$

Example 2 p. 303 :

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

Less steps ?

The idea : Decrease d_Y at each step

How ? Compute potential common roots at once

Abhyankar [1] : if F is monic,

- $G(X,Y) = F(X, Y + A_{d_Y-1}(X)/d_Y) = Y^{d_Y} + \sum_{k=0}^{d_Y-2} B_k(X)\, Y^k$
- We cannot have $\mathcal{N}(G) = \Delta$, $q = 1$ and $\phi_\Delta(T) = (T-\xi)^{d_Y}$

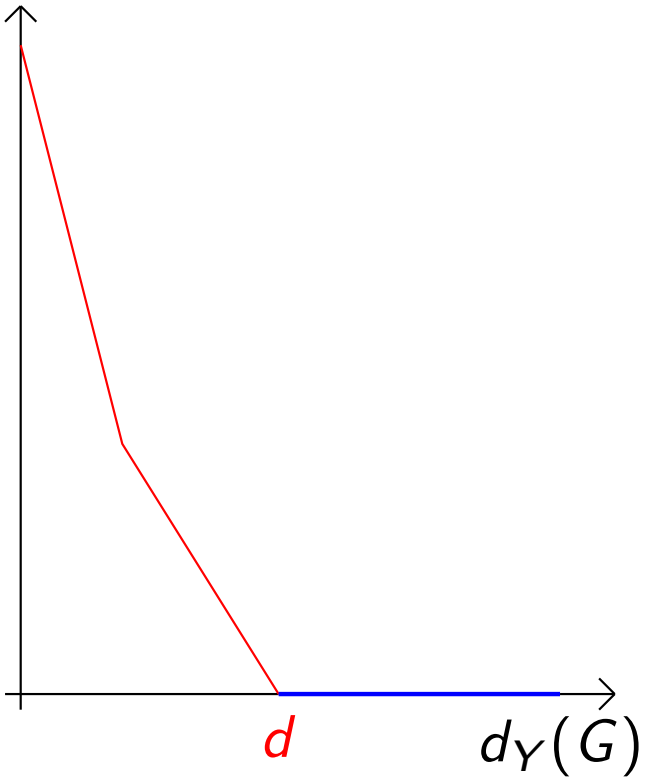
$$\Longrightarrow \text{number of steps in } O(\rho \log(d_Y)).$$

Example 2 p. 303 :

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

Weierstrass preparation theorem.

After a RNP-shift :



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

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

  - H monic in Y,
  - $H(0, Y) = Y^d$,
  - $P(0, Y) = p(Y)$.
- Algorithm :
  1. Hensel lemma modulo X^{N+1},
  2. Next calls with $H(X, Y)$.
- Complexity : $\tilde{O}(d_Y\, N)$

Complexity

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

1. Abhyankar : bivariate shift — $\tilde{O}(N\, d_Y)$
2. RNP-shift : one for each (Δ, ξ) — $s_k\, \tilde{O}(N\, d_Y)$
3. Weierstrass Preparation — $s_k\, \tilde{O}(N\, d_Y)$
4. Recursive calls.

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

A sharp count : family of examples

Example (example 3, p. 305)

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

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

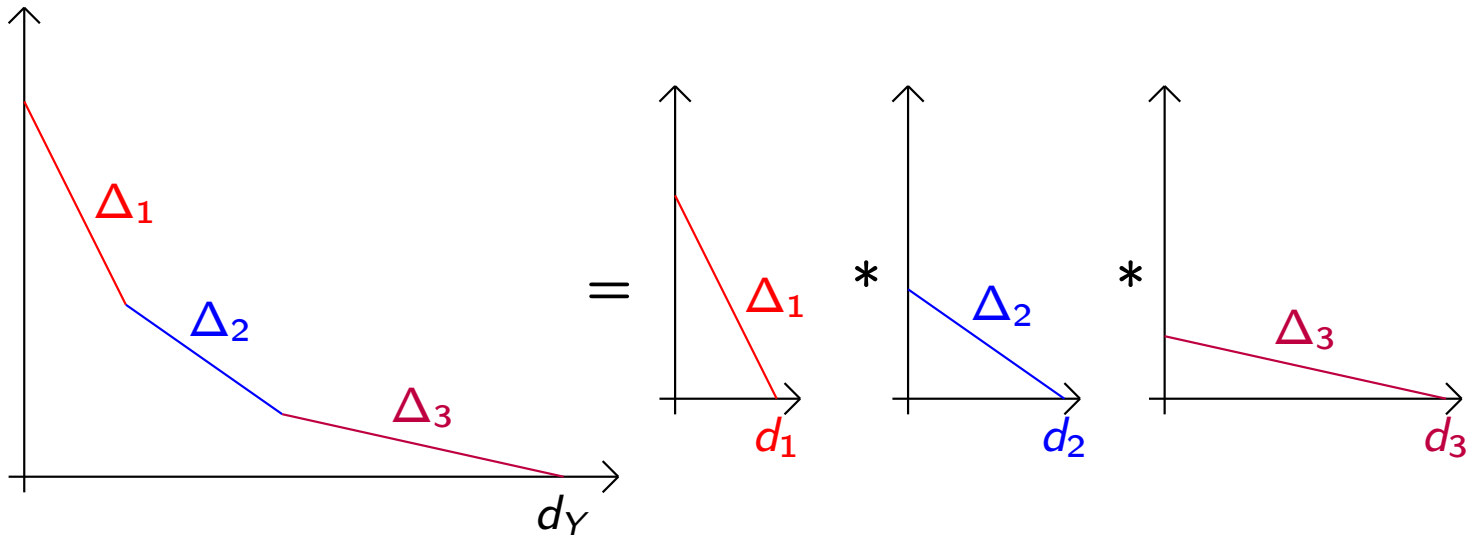
- $\rho = d_Y = N$, $d_X \in \Theta(N^2)$. $\mathrm{v}_X(\Delta_Y(F)) \in \Theta(N^3) = \Theta(d_X d_Y)$.
- Cost is $N^3 \times (N + (N-1) + \cdots + 3 + 2) \simeq N^5$.

$\Longrightarrow$ complexity in $\Theta(d_X {d_Y}^3)$.

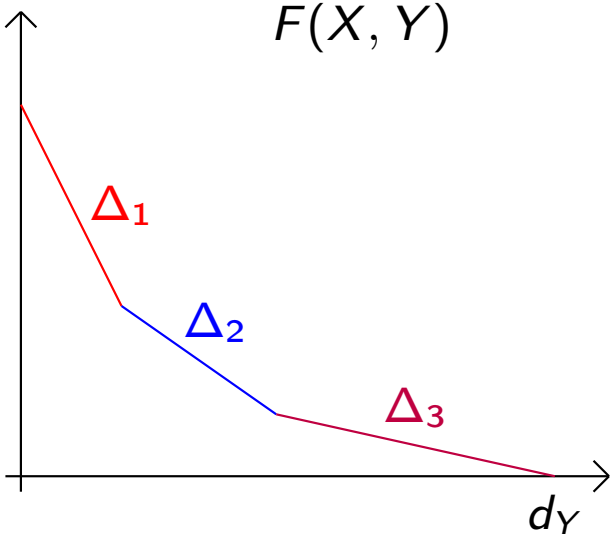
Factorisation according to the Newton polygon

Theoretically, we have in $L[[X]][Y]$:

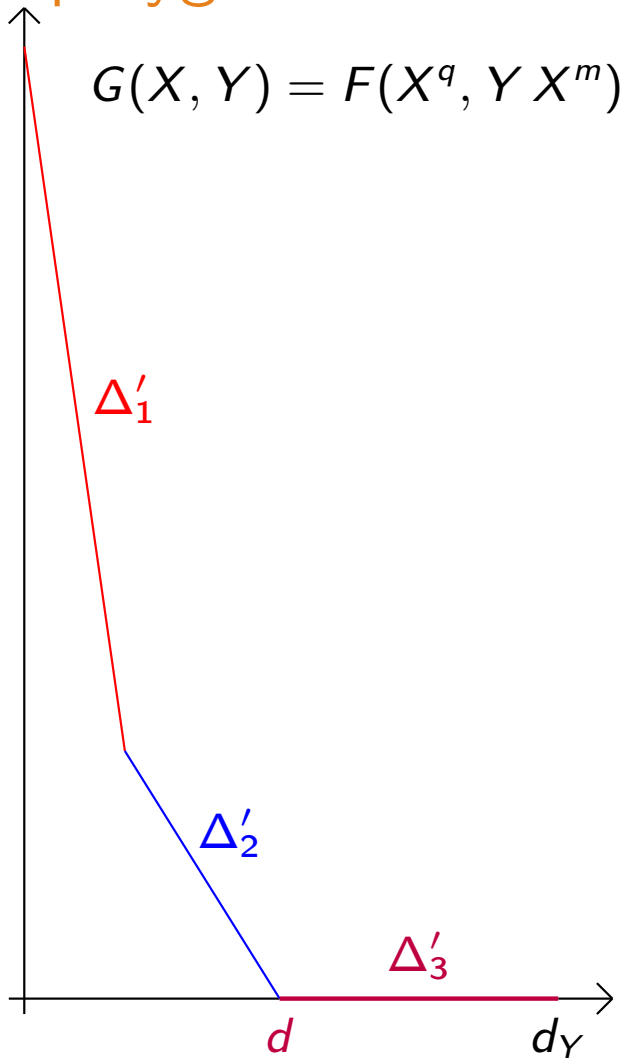
$$F = F_1 * F_2 * F_3$$

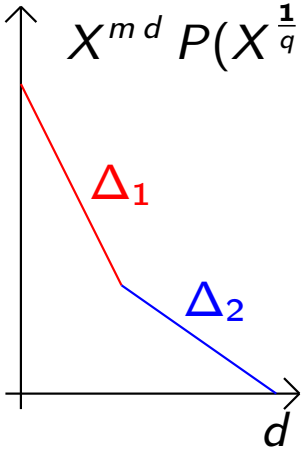


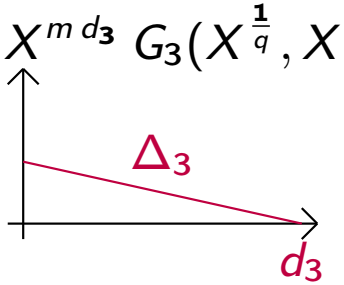
Factorisation according to the Newton polygon



$(\Delta_3)\ m\,i + q\,j = l$

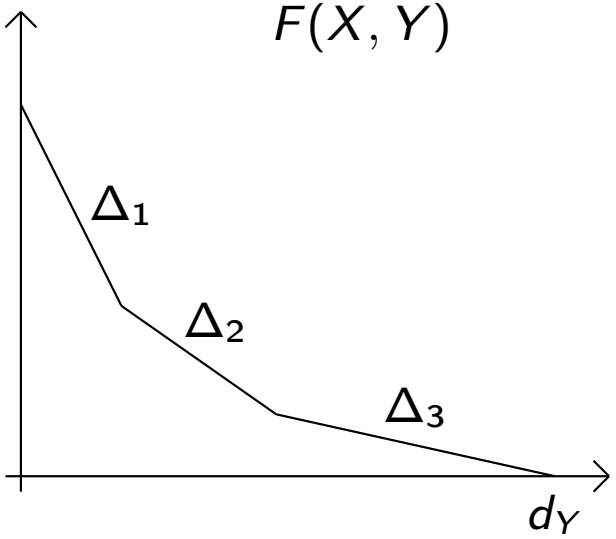




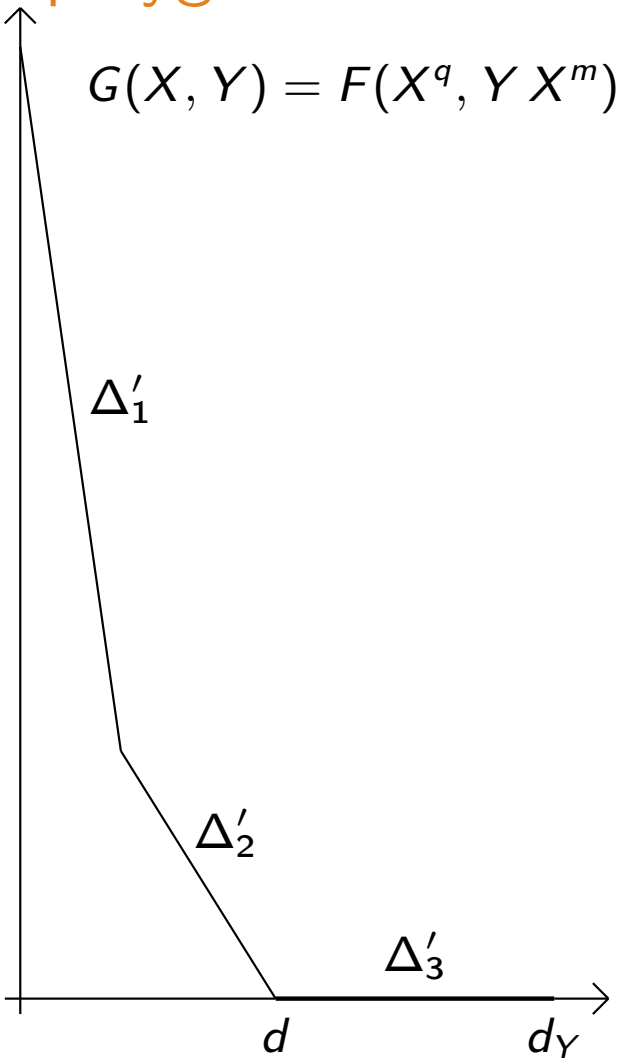


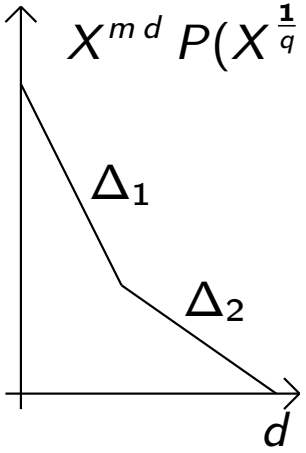
$$G(X,Y) = P(X,Y)\,G_3(X,Y) \quad \xleftarrow{\text{Hensel lemma}} \quad G(0,Y) = Y^d\,g_3(Y)$$

Factorisation according to the Newton polygon

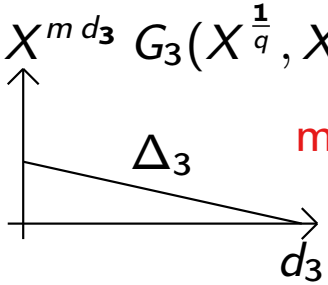


$(\Delta_3)\ m\,i + q\,j = l$





$\bmod X^N$

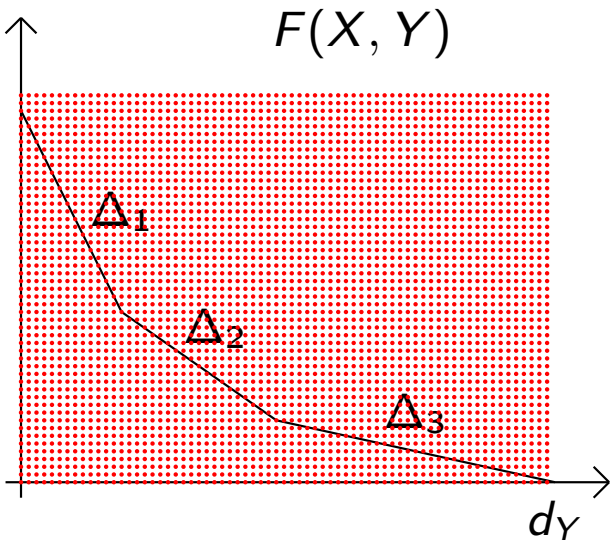


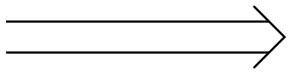
$\bmod X^N$

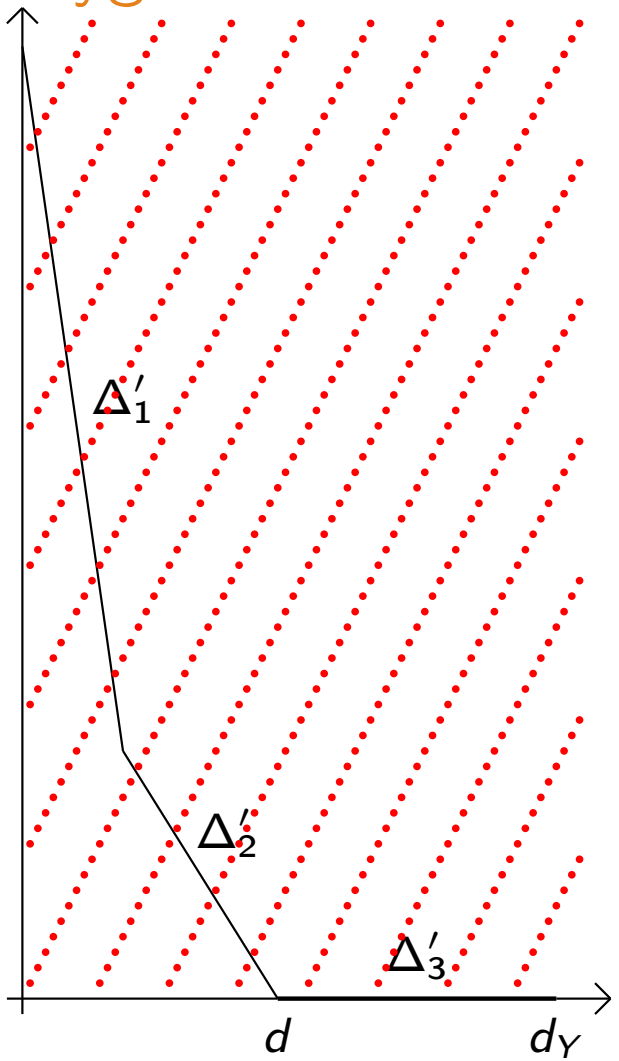
$G(X,Y) = P(X,Y)\,G_3(X,Y)$ $\Longleftarrow$ Hensel lemma $G(0,Y) = Y^d\,g_3(Y)$

$\bmod X^{q\,N}$

Factorisation according to the Newton polygon







Lebreton, Schost, van der Hoeven [34]

Conclusion

- A better worst case complexity for Puiseux series above 0.

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

- No complexity result for *all* critical points
  - Factorisation is too costly,
  - Should work with D5 algorithm

    Della Dora, Dicrescenzo, Duval [20]

- Fast factorisation according to $\mathcal{N}(F)$ using Lebreton, Schost, van der Hoeven [34]

Thank you !