

Puiseux series computation: avoiding computations over \mathbb{Q}

Adrien Poteaux¹

Univ. Lille 1 - LIFL, computer algebra team

Symbolic Computation seminar, JKU, Linz

January 9th, 2011

¹joint work with Marc Rybowicz (University of Limoges)

Puiseux series: a generalization of formal power series

- $K = \mathbb{Q}(\gamma)$ a number field ; $F(X, Y) \in K[X, Y]$ squarefree.
- $R_F = \text{Res}_Y(F, F_Y)$
- $x_0 \in K$; solutions of $F(X, Y)$ above x_0 ?
 - $R_F(x_0) \neq 0$ (regular point): Taylor expansion

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

Puiseux series: a generalization of formal power series

- $K = \mathbb{Q}(\gamma)$ a number field ; $F(X, Y) \in K[X, Y]$ squarefree.
- $R_F = \text{Res}_Y(F, F_Y)$
- $x_0 \in K$; solutions of $F(X, Y)$ above x_0 ?
 - $R_F(x_0) \neq 0$ (regular point): Taylor expansion

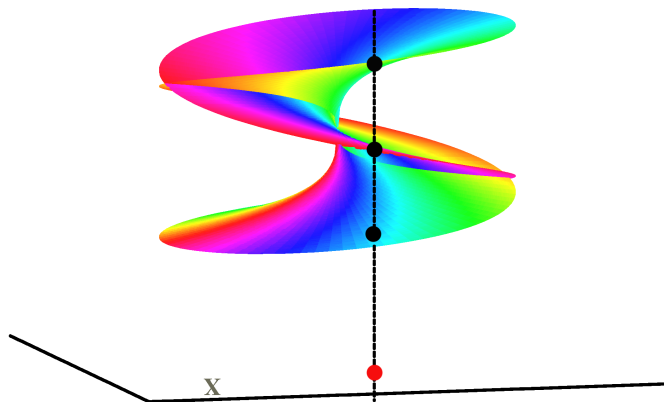
$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k ; 1 \leq i \leq d_Y$$

- $R_F(x_0) = 0$ (critical point): Puiseux expansion

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

- ζ_{e_i} primitive e_i -th root of unity,
- e_1, \dots, e_s partition of d_Y (ramification indices).

First example: $F(X, Y) = Y^3 - X$ above $x_0 \neq 0$

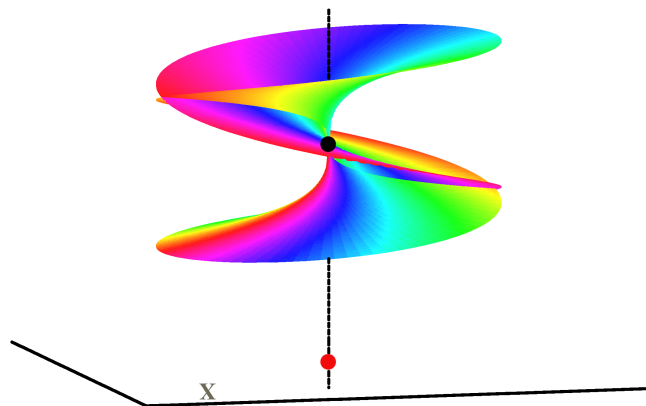


$$Y_1(X) = -0.215 - 0.373 i + (0.898 + 1.555 i)(X - 0.08) + \dots$$

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

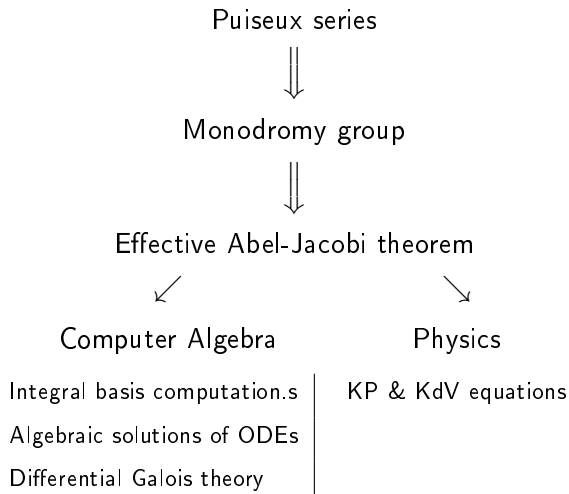
$$Y_3(X) = 0.431 + 1.795(X - 0.08) + \dots$$

First example: $F(X, Y) = Y^3 - X$ above $x_0 = 0$



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

Long term goal



Local monodromy and Puiseux series

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

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

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

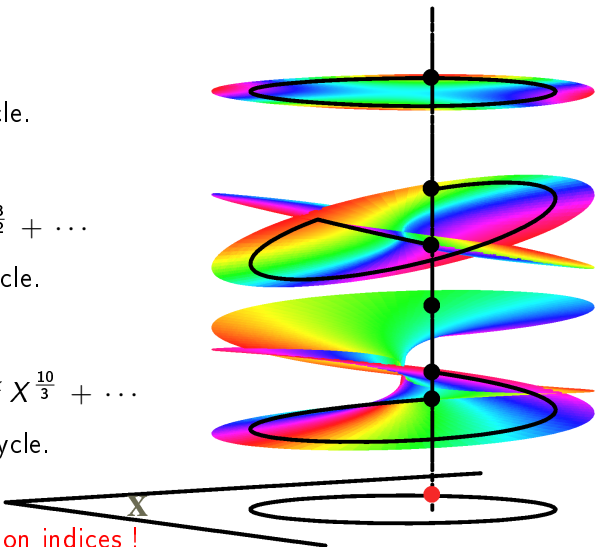
$$1 + \zeta_2^k X^{\frac{1}{2}} + \frac{1}{2} \zeta_2^k X^{\frac{3}{2}} + \dots$$

$\Rightarrow e = 2$: 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.

The local monodromy
is given by the ramification indices !



Using Puiseux expansions

- An evaluation of the Puiseux series gives:
 - the local monodromy,
 - analytic continuation around critical points.
- We want an exact structure,
- Numerical approximations of the coefficients is good enough.

Other motivations: a fundamental theoretical object

- Ramification indices \implies genus computation
(*Riemann Hurwitz formula*)

Other motivations: a fundamental theoretical object

- Genus computation
- Integral basis computation

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

- Determination of parametrizations of genus 0 curves

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

- Integration of algebraic functions

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

M. Bronstein 1990, *Integration of Elementary Functions*

Other motivations: a fundamental theoretical object

- Genus computation
- Integral basis computation
 - Determination of parametrizations of genus 0 curves
 - Integration of algebraic functions
- Connectivity queries

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

Computing Puiseux series: the singular part

$$\begin{aligned} S_{ij}(X - x_0) &= \sum_{k=n_i}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}} \\ &= \sum_{k=n_i}^{r_{ij}} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}} + \text{next terms} \end{aligned}$$

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 1978, *All Algebraic Functions Can Be Computed Fast*

Examples above de $X = 0$

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

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

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

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

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

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

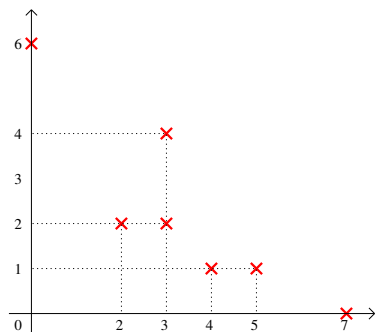
The Newton-Puiseux algorithm: main tools

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

Support of a polynomial

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

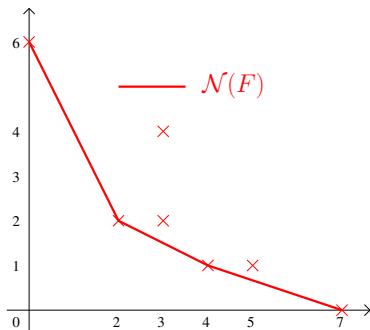
× $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$



Newton polygon

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

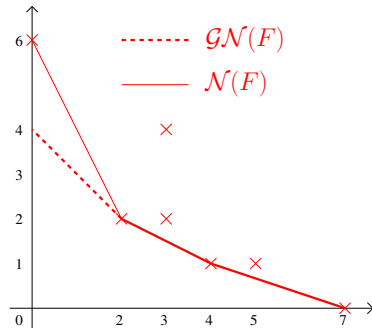
- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: lower part of the convex hull of $\text{Supp}(F)$.



Generic Newton polygon

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

- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: lower part of the convex hull of $\text{Supp}(F)$.
- - $\mathcal{GN}(F)$: slopes of $\mathcal{N}(F) \leq -1$.



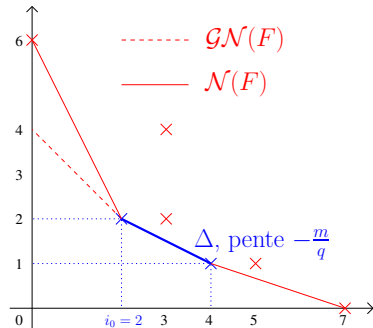
Characteristic polynomial

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

- × $\text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\}$
- $\mathcal{N}(F)$: lower part of the convex hull of $\text{Supp}(F)$.
- - $\mathcal{GN}(F)$: slopes of $\mathcal{N}(F) \leq -1$.

Characteristic polynomial:

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



Rational Newton-Puiseux Algorithm

D. Duval 1989, *Rational Puiseux Expansions*

For each edge Δ of $\mathcal{N}(F)$

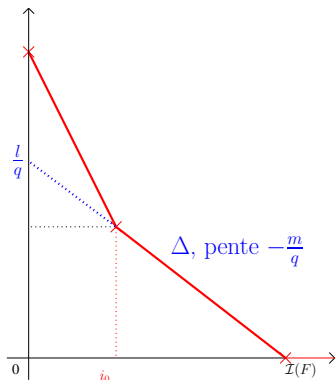
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- For each ϕ_k

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

with

- ξ_k s.t. $\phi_k(\xi_k) = 0$,
- (u, v) such that $uq - vm = 1$.



Our Newton-Puiseux Algorithm

For each edge Δ of $\mathcal{GN}(F)$

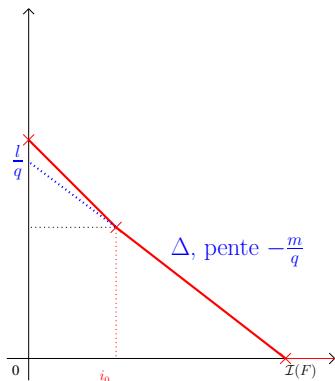
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- For each ϕ_k

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

with

- ξ_k s.t. $\phi_k(\xi_k) = 0$,
- (u, v) such that $uq - vm = 1$.



Rational Newton-Puiseux Algorithm: first turn

For each edge Δ of $\mathcal{N}_0(F)$

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

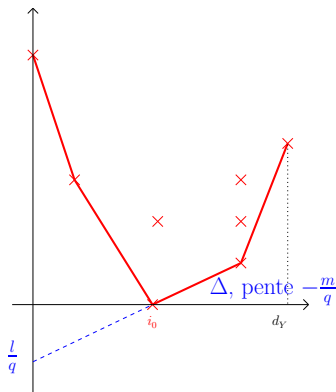
- For each ϕ_k

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

with

- ξ_k s.t. $\phi_k(\xi_k) = 0$,
- (u, v) such that $uq - vm = 1$.

First turn: initial polygon $\mathcal{N}_0(F)$



Our Newton-Puiseux Algorithm: first turn

For each edge Δ of $\mathcal{EN}(F)$

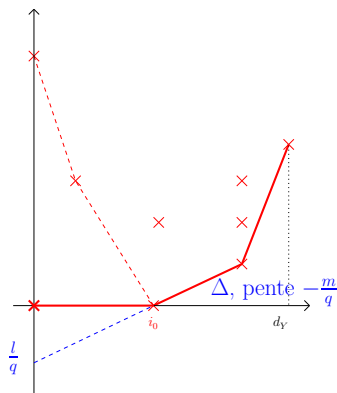
$$- \phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$$

- For each ϕ_k

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

with

- ξ_k s.t. $\phi_k(\xi_k) = 0$,
- (u, v) such that $uq - vm = 1$.



First turn: exceptional polygon $\mathcal{EN}(F)$

(lower part of the convex hull of $\text{Supp}(F) \cup \{(0, 0)\}$).

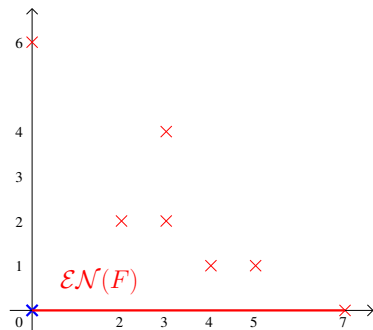
One example

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

One example

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

- Exceptionnal Newton polygon



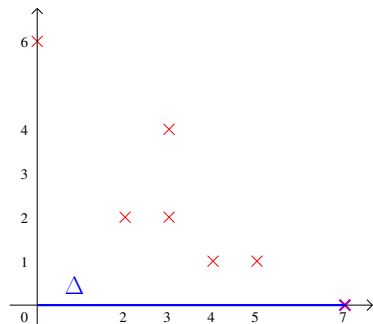
One example

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

One example

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

- Exceptionnal Newton polygon
- $\phi_{\Delta}(T) = T^7$.



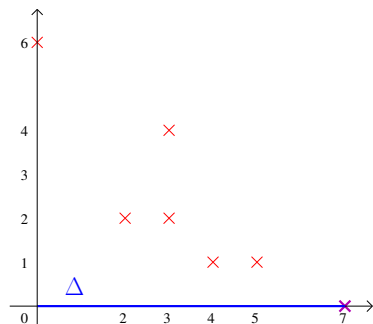
One example

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

One example

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

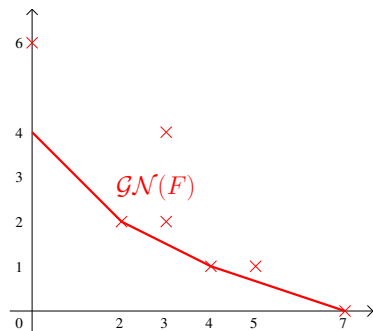
- Exceptionnal Newton polygon
- $\phi_{\Delta}(T) = T^7$.
- $m = 0, q = 1, l = 0, u = 1, v = 1$.
- $F(X, Y) \leftarrow F(X, Y)$



One example

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

- Generic Newton polygon



One example

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

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

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

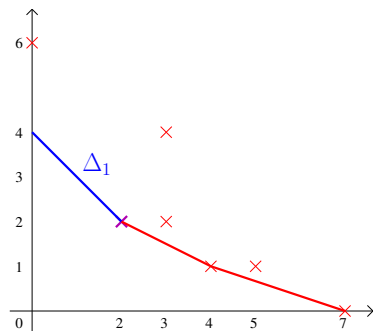
$$\mathcal{GN} = ((0, 4), (2, 2), (4, 1), (7, 0))$$

One example

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

- Generic Newton polygon

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



One example

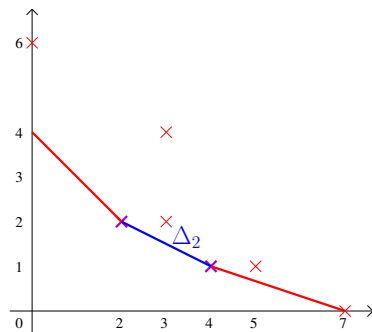
$$\begin{array}{c} \mathcal{E}\mathcal{N} = ((0, 0), (7, 0)) \\ \left| \begin{array}{l} \Delta = ((0, 0), (7, 0)) \\ (7) \\ (7, 1) \end{array} \right. \\ \mathcal{G}\mathcal{N} = ((0, 4), (2, 2), (4, 1), (7, 0)) \\ \swarrow \\ \Delta_1 = ((0, 4), (2, 2)) \\ (2) \end{array}$$

One example

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

- Generic Newton polygon

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

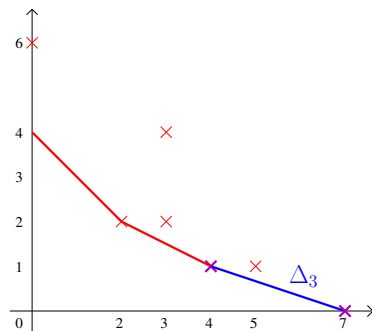


One example

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

- Generic Newton polygon

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

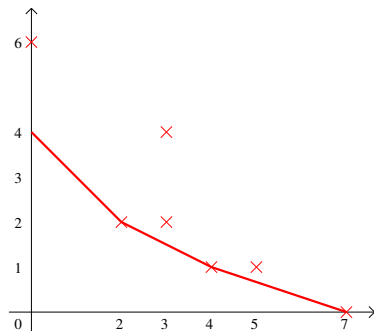


One example

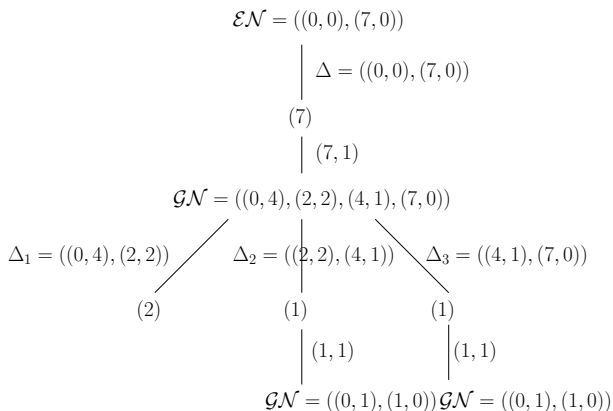
- $K = \mathbb{F}_7$
- $F(X, Y) = Y^7 + Y^5X + 5Y^4X + 5Y^4X^3 + 4Y^2X^2 + X^6$

- Generic Newton polygon

edge	$\phi_{\Delta_i}(T)$	next pol. F_i
Δ_1	$4T^2$	mult. 1 \implies End
Δ_2	$4 + 5T$	
Δ_3	$5 + T$	



One example

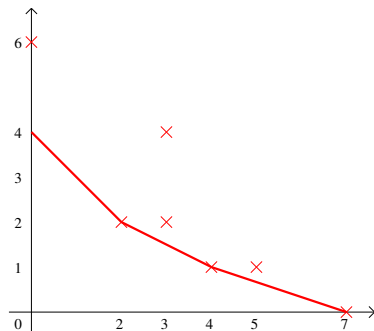


One example

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

- Generic Newton polygon

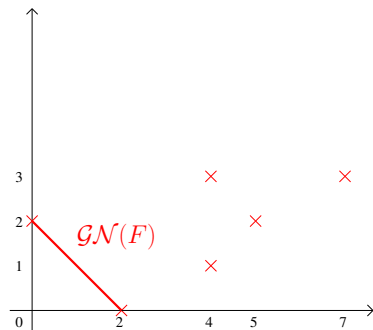
edge	$\phi_{\Delta_i}(T)$	next pol. F_i
Δ_1	$4T^2$	$\frac{F(X, XY)}{X^4}$
Δ_2	$4 + 5T$	mult. 1 \implies End
Δ_3	$5 + T$	



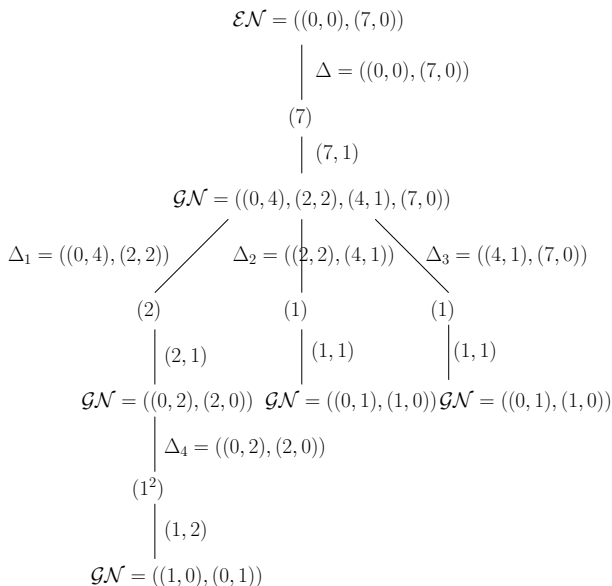
One example

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

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



Polygon tree



A symbolic algorithm \rightarrow too slow in practice

Two main problems:

- Degree of the extension field
- Coefficient growth

One example

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

$$R_H(X) = X^3 P(X), \deg_X(P) = 23; \beta \text{ s.t. } P(\beta) = 0$$

Singular parts of Puiseux series of H above β :

- $S_i(X) = \alpha_{i,0}, 1 \leq i \leq 4.$
- $S_i(X) = \alpha_{i,0} + \alpha_{i,1}(X - \beta)^{\frac{1}{2}}, 5 \leq i \leq 6.$
- Degree of the extension field
 - $i = 5, 6: K(\alpha_{i,0}) = K(\alpha_{i,1}) = K(\beta) \rightarrow$ extension of **degree 23**,
 - $i = 1, \dots, 4: [K(\alpha_{i,0}) : K(\beta)] = 4 \rightarrow$ extension of **degree 92**,
- Coefficient growth

One example

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

$$R_H(X) = X^3 P(X), \deg_X(P) = 23; \beta \text{ s.t. } P(\beta) = 0$$

Singular parts of Puiseux series of H above β :

- $S_i(X) = \alpha_{i,0}, 1 \leq i \leq 4.$
- $S_i(X) = \alpha_{i,0} + \alpha_{i,1}(X - \beta)^{\frac{1}{2}}, 5 \leq i \leq 6.$
- Degree of the extension field
 - $i = 5, 6: K(\alpha_{i,0}) = K(\alpha_{i,1}) = K(\beta) \rightarrow$ extension of degree 23,
 - $i = 1, \dots, 4: [K(\alpha_{i,0}) : K(\beta)] = 4 \rightarrow$ extension of degree 92,
- Coefficient growth
 - $\alpha_{i,0} \rightarrow$ rational number with 98 digits,
 - $\alpha_{i,1} \rightarrow$ rational number with 132 digits.

One example

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

$$R_H(X) = X^3 P(X), \deg_X(P) = 23; \beta \text{ s.t. } P(\beta) = 0$$

Singular parts of Puiseux series of H above β :

- $S_i(X) = \alpha_{i,0}, 1 \leq i \leq 4.$
- $S_i(X) = \alpha_{i,0} + \alpha_{i,1}(X - \beta)^{\frac{1}{2}}, 5 \leq i \leq 6.$
- Degree of the extension field
 - $i = 5, 6: K(\alpha_{i,0}) = K(\alpha_{i,1}) = K(\beta) \rightarrow$ extension of degree 23,
 - $i = 1, \dots, 4: [K(\alpha_{i,0}) : K(\beta)] = 4 \rightarrow$ extension of degree 92,
- Coefficient growth
 - $\alpha_{i,0} \rightarrow$ rational number with 98 digits,
 - $\alpha_{i,1} \rightarrow$ rational number with 132 digits.

> `t0:=time():algcures[puiseux](H,X=RootOf(P),Y,0):time()-t0;`

13.388

(on a eeePC)

A symbolic algorithm \rightarrow too slow in practice

- Degree of the extension field
 - working over a factor of the resultant: up to $d_X(2d_Y - 1)$.
 - factorisations during the algorithm: up to d_Y . \rightarrow up to $O(D^3)$
- Coefficient growth
 - Walsh: $\|\alpha_{ik}\| \leq 2(h+1)(h(d_X+1)(d_Y+1))^{6d_X d_Y^2}$

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

A symbolic algorithm \rightarrow too slow in practice

- Degree of the extension field
 - working over a factor of the resultant: up to $d_X(2d_Y - 1)$.
 - factorisations during the algorithm: up to d_Y . \rightarrow up to $O(D^3)$
- Coefficient growth
 - Walsh: $\|\alpha_{ik}\| \leq 2(h+1)(h(d_X+1)(d_Y+1))^{6d_X d_Y^2}$

Bit complexity ?

- Chystov: “it’s polynomial”
- Walsh: $O(d_Y^{32} d_X^4 \text{ht}(F)^2)$; $\text{ht}(F) = \log(h)$

Chistov 1986, *Polynomial complexity of the Newton-Puiseux algorithm*

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

A symbolic algorithm \rightarrow too slow in practice

- Degree of the extension field
 - working over a factor of the resultant: up to $d_X(2d_Y - 1)$.
 - factorisations during the algorithm: up to d_Y . \rightarrow up to $O(D^3)$
- Coefficient growth
 - Walsh: $\|\alpha_{ik}\| \leq 2(h+1)(h(d_X+1)(d_Y+1))^{6d_X d_Y^2}$

Bit complexity ?

- Chystov: “it’s polynomial”
- Walsh: $\tilde{O}(d_Y^{32} d_X^4 \text{ht}(F)^2)$; $\text{ht}(F) = \log(h)$

(symbolic computation over number field) + (numerical evaluation) =
(awfully long computation) + (bad accuracy)

Numerical computations ?

Direct computation: almost useless ; one example:

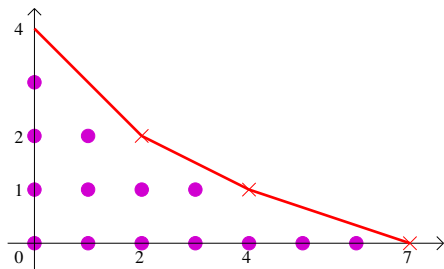
- $H(X, Y) = (Y^3 - X)((Y - 1)^2 - X)(Y - 2 - X^2) + X^2 Y^5$
- $R_H(X) = X^3 P(X)$, $\tilde{\alpha} = -.5060254677 - .4773219060 i$; $P(\tilde{\alpha}) \simeq 0$
- $\tilde{H} = H(X + \tilde{\alpha}, y)$; series above $(0, 0.4060249175 + 0.9045013397 i)$:
 $S(X) = 0.4060311143 + 0.9044983677 i - (0.3092659089 + 0.3655481764 i)X +$
 $(0.2648309844 + 0.08652658304 i)X^2 + \dots$
- convergence radius of $S(X)$: $.1649995849 \cdot 10^{-6}$

Numerical computations ?

Direct computation: almost useless

Guessing the structure ? two difficulties:

Finding the *correct* Newton polygon



Factorising “well” ϕ_{Δ}

$$x^2 - 2.0x + 0.9999$$

$$\stackrel{?}{=} (x - 0.99)(x - 1.01)$$

$$\stackrel{?}{=} (x - 1.)^2$$

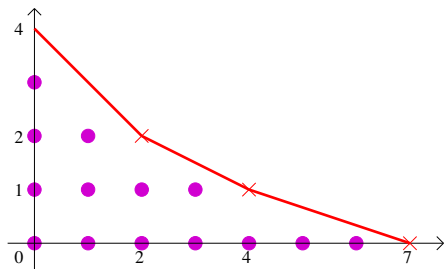
\implies Multiplicity structure ?

Numerical computations ?

Direct computation: almost useless

Guessing the structure ? two difficulties:

Finding the *correct* Newton polygon



Factorising “well” ϕ_Δ

$$x^2 - 2.0x + 0.9999$$

$$\stackrel{?}{=} (x - 0.99)(x - 1.01)$$

$$\stackrel{?}{=} (x - 1.)^2$$

\implies Multiplicity structure ?

\implies We need the polygon tree !

A new symbolic-numeric algorithm:

- 1 Compute the singular part of Puiseux series modulo a well chosen prime number p

This give us the **polygon tree** $\mathcal{T}(F)$, i.e.:

- Generic Newton polygons,
 - Multiplicity structures of the ϕ_{Δ} .
- 2 Use this information to conduct a numerical computation of the Puiseux series coefficients.

Good \mathfrak{p} -reduction

We denote:

- \mathfrak{o} the ring of algebraic integers of K ,
- p be a prime number,
- \mathfrak{p} a prime ideal of \mathfrak{o} dividing p .

Définition

F has *local (at $X = 0$) good \mathfrak{p} -reduction* if:

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

Main results

If F has a good \mathfrak{p} reduction, then

Theorem 1: we can reduce Puiseux series modulo \mathfrak{P} dividing \mathfrak{p}

Theorem 2: $\mathcal{T}(F) = \mathcal{T}(F \bmod \mathfrak{p})$ (*not true with classical polygons*)

Other results

- Bounds for the prime number p : size logarithmic in the input with probabilistic algorithms. [▶ sizes](#)
- Improved complexity bounds for the rational Newton-Puiseux algorithm above finite fields

from $O(D^8)$ to $\mathcal{O}(D^5)$

- Bit complexity to compute $\mathcal{T}(F)$: $\simeq \mathcal{O}(D^5)$ using a small p

[▶ Details](#)

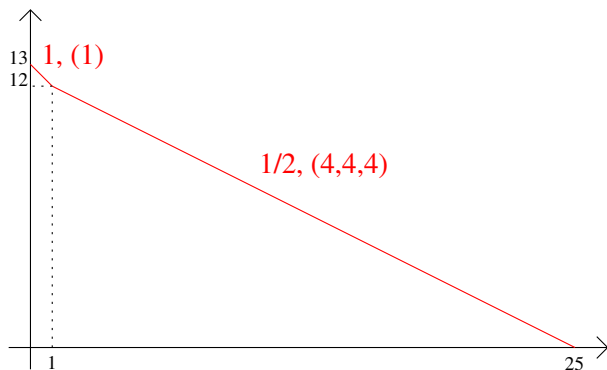
Following $\mathcal{T}(F)$: one example

Puiseux series of F :

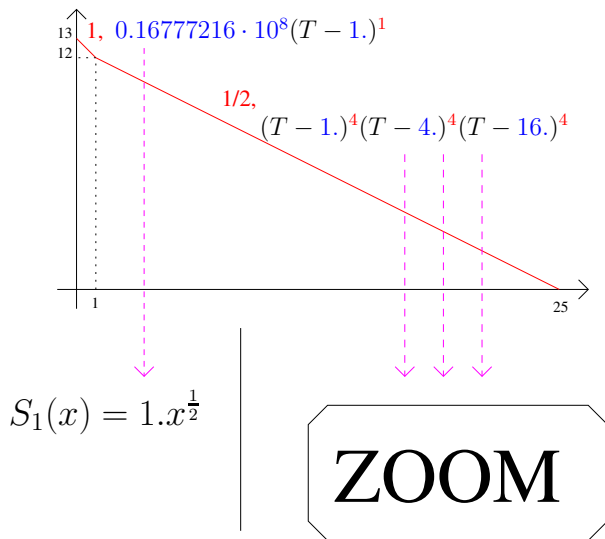
- $S_1(X) = X + \dots$
- $S_2(X) = 4X^{\frac{1}{2}} + X^{\frac{7}{8}} + \dots$
- $S_3(X) = 2X^{\frac{1}{2}} + 2X + \dots$
- $S_4(X) = 2X^{\frac{1}{2}} + X + X^{\frac{7}{6}} + \dots$
- $S_5(X) = X^{\frac{1}{2}} + 2X + X^{\frac{5}{4}} + \dots$
- $S_6(X) = X^{\frac{1}{2}} + X + \dots$
- $S_7(X) = X^{\frac{1}{2}}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

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

First Newton polygon



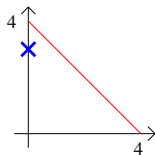
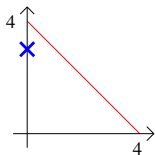
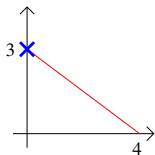
First Newton polygon



Sorting polynomials according to their Newton polygons

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

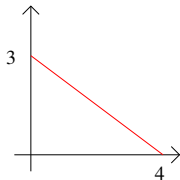
$\{G_1, G_2, G_3\}$



polynomial	coefficient in X^3
G_1	0.
G_2	0.
G_3	-17199267840000.0

Sorting polynomials according to their Newton polygons

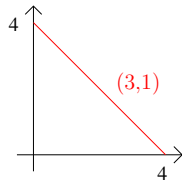
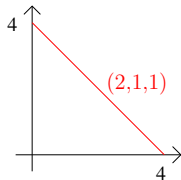
G_3



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

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

$\{G_1, G_2\}$



Sorting polynomials according
to multiplicity structures

Sorting polynomials according to multiplicity structures

Multiplicity structures:

- $(2, 1, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 1$
- $(3, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 2$

Sorting polynomials according to multiplicity structures

Multiplicity structures:

- $(2, 1, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 1$
- $(3, 1) \Rightarrow \deg(\text{pgcd}(\phi, \phi')) = 2$

Characteristic polynomials:

$$\phi_1 = 1049760000.0 - 2361960000.0 T + 1837080000.0 T^2 - 590490000.0 T^3 + 65610000.0 T^4$$

$$\phi_2 = 1719926784.0 - 6019743744.0 T + 7739670528.0 T^2 - 4299816960.0 T^3 + 859963392.0 T^4$$

- 1 $S_i \leftarrow \text{Syl}(\phi_i, \phi'_i)$
- 2 Compute singular values of the S_i

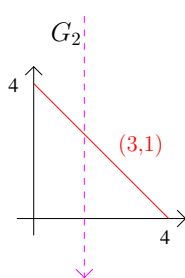
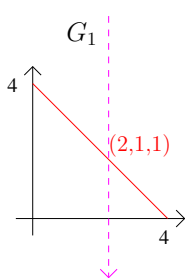
Sorting polynomials according to multiplicity structures

Singular values associated to ϕ_1 :

[710694508.4327095884, 5827385163.0346368216, 3038236185.2953794346, 1140210769.8445335036, 40759543.641844042087, 1882790.0681572535369, 3.8263754075532025314 $\cdot 10^{-11}$]

Singular values associated to ϕ_2 :

[37445022322.189717034, 24644791488.066781055, 12101920587.793187214, 3915075466.8959244453, 31534726.725839766232, 0.0000000074101187358617089031, 0.0000000027761147770454585021]



Results

```
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 =  
0.99999999999999869303 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 + 2.00000000000000757425 T3], [x = T8, y =  
0.99999999999483964356 T7 + 4.00000000000009297336 T4]]]
```

A good practical numerical behaviour: one example

$$M_{a,d} = x^d - 2(ax - 1)^2$$

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

coefficient in $x^{1/2}$ of the Puiseux series above 0:

Digits	numerical evaluation	our algorithm
10	0	4
20	0	15
30	5	29

Conclusion

- Reduction criterion:
 - We can compute $\mathcal{T}(F)$
 - Probabilistic algorithms \rightarrow small p
- Use $\mathcal{T}(F)$ to guide floating point computations:
 - Two stage filter
 - Use SVD

\implies Puiseux series may be used in practice !

Perspectives

- ① Certified implementation ?
 - Error bounds on the coefficients, analyze accuracy
 - Error bounds for SVD sufficient ? Other method ?

Perspectives

① Certified implementation ?

② A better second filter ?

- Context:

- We consider: $\{\phi_i\}_{1 \leq i \leq s}$ a set of approximate polynomials.

- We know: $\{d_j\}_{1 \leq j \leq s}$ the set of multiplicity structures.

- We want:

1. Connections between the two sets,

2. Root approximations with correct multiplicities.

- Idea:

- connection part \rightarrow Sum Of Squares ? (certifies that there is no close polynomial with a given multiplicity),

- root approximation \rightarrow Newton-like method.

Perspectives

- ① Certified implementation ?
- ② A better second filter ?
- ③ Computing *real* Puiseux series ?

SOS may help...

Perspectives

- 1 Certified implementation ?
- 2 A better second filter ?
- 3 Computing *real* Puiseux series ?
- 4 A (purely) numerical algorithm ?
 - ⇒ definition of a Puiseux series ?
 - similar to agcd ?
 - something else ?

Perspectives

- 1 Certified implementation ?
- 2 A better second filter ?
- 3 Computing *real* Puiseux series ?
- 4 A (purely) numerical algorithm ?
- 5 Factorisation during the algorithm ?

Abhyankar 2007, *Newton's theorem*:

Factorisation of F during the Newton-Puiseux algorithm

→ avoid to make substitutions in the whole polynomial ?

- Factorisation *à la Hensel*,
- We have bounds for the degree in X .

Perspectives

- 1 Certified implementation ?
- 2 A better second filter ?
- 3 Computing *real* Puiseux series ?
- 4 A (purely) numerical algorithm ?
- 5 Factorisation during the algorithm ?
- 6 A fast algorithm ? Additional ideas:
 - No substitution \rightarrow multi-evaluation of the series in F, F_Y, \dots
 - No factorisation \rightarrow D5
 - Relax computations.

$$\tilde{O}(D^{\frac{\omega+5}{2}}) ?$$

Perspectives

- 1 Certified implementation ?
- 2 A better second filter ?
- 3 Computing *real* Puiseux series ?
- 4 A (purely) numerical algorithm ?
- 5 Factorisation during the algorithm ?
- 6 A fast algorithm ?

Merci de votre attention !

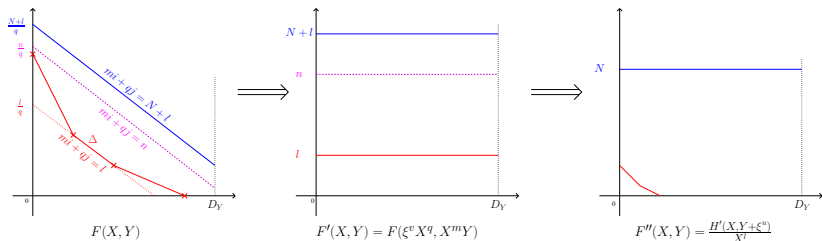
Choice of the prime number p

- $K = \mathbb{Q}(\gamma)$, $w = [K : \mathbb{Q}]$, M_γ the minimal polynomial of γ
- $\text{ht}(Q) = \log \|Q\|_\infty$ where Q is a multivariate polynomial.

$\text{ht}(p)$ belongs to

- $O(wd_Y(w\text{ht}(M_\gamma) + \text{ht}(F) + \log(wd_X d_Y)))$
Deterministic strategy
- $O(\log(d_Y w \log d_X) + \log(\text{ht}(F)) + \log(\text{ht}(M_\gamma)) + \log(\epsilon^{-1}))$
Monte-Carlo strategy with probability of error $\leq \epsilon$
- $O(\log(d_Y w \log d_X) + \log(\text{ht}(F)) + \log(\text{ht}(M_\gamma)))$
Las-Vegas strategy with an average of 2 iterations.

Complexity of RNP : substitution



- $\delta_F = \sum_i r_i f_i.$

Lemme

- All computations can be made modulo x^{δ_F+1}
- One substitution = N "shifts" $\subset O(NM(d_Y))$ field operations.

Complexity of RNP over $L = \mathbb{F}_{p^{t_0}}$

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 (Number of operations in L)

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

$\rightarrow \mathcal{T}(\bar{F})$ above all critical points : $\mathcal{O}(d_Y^3 d_X^2 t_0 \log p)$

D. Duval 89, *Rational Puiseux Expansions* : $O(d_Y^6 d_X^2)$

Bit Complexity for the Monte-Carlo algorithm

- $F \in K[X, Y]$
- $K = \mathbb{Q}(\gamma)$
- $w = [K : \mathbb{Q}]$
- M_γ the minimal polynomial of γ

Théorème

There exists a Monte-Carlo algorithm which compute $\mathcal{T}(F)$ in

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

bit operations with a probability of error $\leq \epsilon$.

◀ back