

Good Reduction of Puiseux Series and Complexity of the Newton-Puiseux Algorithm over Finite Fields

Adrien Poteaux and Marc Rybowicz

XLIM-DMI (UMR CNRS 6172)
Université de Limoges

ISSAC'08

The problem

- L a field
- $F(X, Y) \in L[X, Y]$ squarefree and monic in Y
- Hypothesis : $\text{Char}(L) = 0$ or $\text{Char}(L) > D_Y$

Theorem (Puiseux)

There exist D_Y series $S_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}}$ s.t.
 $F(X, S_{ij}(X)) = 0$ for all $1 \leq j \leq e_i, 1 \leq i \leq s$, with

- ζ_{e_i} primitive e_i -th root of unity,
- e_1, \dots, e_s partition of D_Y .

Motivation

Poteaux, SNC'07 *Computing Monodromy Groups defined by Plane Algebraic Curves* :

- New algorithm to compute monodromy groups using numerical approximations of Puiseux expansions

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

- Principles of a new symbolic-numeric algorithm to compute these approximations :
 - 1 Compute the singular part of Puiseux series modulo a well chosen prime number p
 - 2 Use this information to conduct numerical computation of Puiseux series

Today : symbolic part and complexity results

The symbolic part : compute the polygon tree $\mathcal{T}(F)$

Contributions :

- We introduce *generic Newton polygons* and *polygon trees*
- A criterion for a “good prime” p
- Bounds for the prime p
- Improved complexity bounds

The idea to compute $\mathcal{T}(F)$:

- Find a prime number p and a prime ideal \mathfrak{p} dividing p such as F has a good \mathfrak{p} -reduction
- Apply RNPuiseux algorithm to $\overline{F} = F \pmod{\mathfrak{p}}$

Singular part of Puiseux series

$$\begin{aligned} S_{ij}(X) &= \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}} \\ &= \sum_{k=0}^{r_{ij}} \alpha_{ik} \zeta_{e_i}^{jk} X^{\frac{k}{e_i}} + \text{next terms} \end{aligned}$$

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*

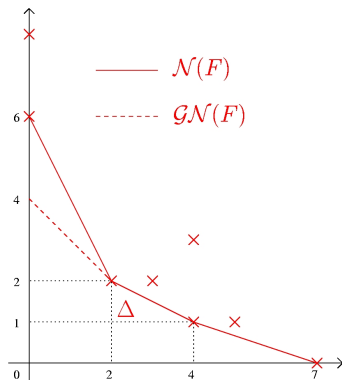
Generic Newton polygons

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

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

Characteristic polynomial :

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



RNPuiseux, the Rational Newton-Puiseux Algorithm

D. Duval 89, *Rational Puiseux Expansions*

For each edge Δ of $\mathcal{GN}(F)$

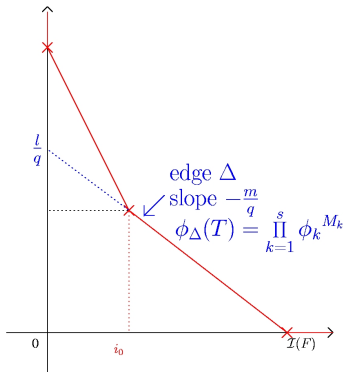
- $\phi_{\Delta} = \prod_{k=1}^s \phi_k^{M_k}$

- For each ϕ_k

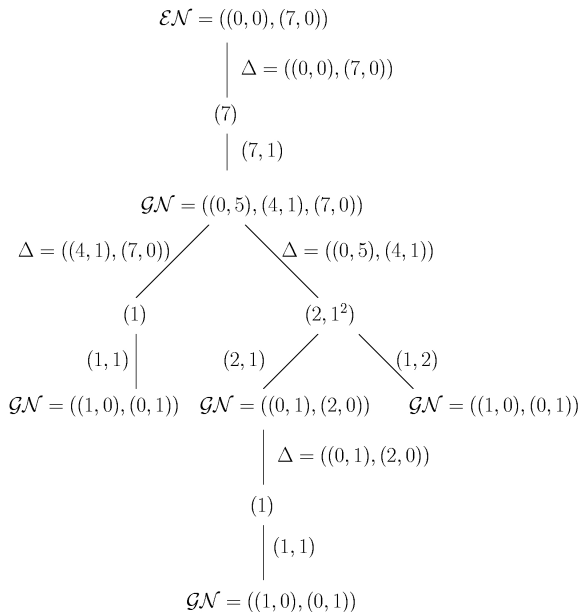
$$F(X, Y) \leftarrow \frac{F(\xi_k^u X^q, X^m(\xi_k^v + Y))}{X^l}$$

with $\cdot \xi_k$ s.t. $\phi_k(\xi_k) = 0$,

- (u, v) such that $uq - vm = 1$.



Polygon Tree



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 .

Definition

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

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

where $\Delta_F = \text{Disc}_Y(F)$

Reduction of Puiseux Series

- L a finite extension of K generated by the Puiseux series coefficients,
- \mathfrak{O} the ring of algebraic integers of L ,
- \mathfrak{P} a prime ideal of $\mathfrak{O}_{\mathfrak{P}}$ dividing \mathfrak{p} ,
- $\mathfrak{O}_{\mathfrak{P}} = \{\alpha \in L \mid v_{\mathfrak{P}}(\alpha) \geq 0\}$.

Theorem

If F has local good \mathfrak{p} -reduction, then the Puiseux series coefficients of F above 0 are in $\mathfrak{O}_{\mathfrak{P}}$.

Proof : Use a theorem of Dwork & Robba 79
On Natural Radii of p -adic Convergence

Reduction of $\mathcal{T}(F)$

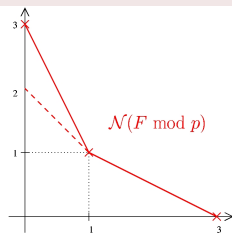
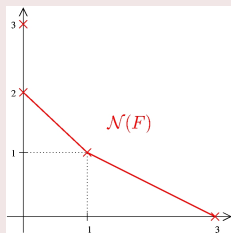
Theorem

If F has local good p -reduction, then $\mathcal{T}(F) = \mathcal{T}(\bar{F})$.

Not true with classical polygons :

Example

$$F(X, Y) = (Y - pX)(Y^2 - X) + X^3 \Rightarrow \text{tc}(\Delta_F) = 4$$



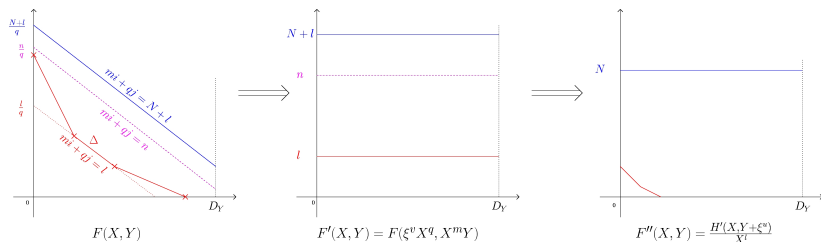
Choice of the prime number p

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



- $\delta_F = \sum_i r_i f_i.$

Lemma

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

Complexity of RNPuiseux 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 $\rightarrow \mathcal{O}(\delta_F D_Y [\delta_F + D_Y + t_0 \log p])$

Lemma

$$\delta_F \leq v_X(\Delta_F) \leq D_X(2D_Y - 2)$$

Theorem (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* : $\mathcal{O}(D_Y^6 D_X^2)$

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

Theorem

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

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

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

Conclusion

- A reduction criterion :
 - It gives us $\mathcal{I}(F)$
 - Probabilistic algorithms give small p
- Improved complexity bounds :
 - Truncations of powers of X
 - Substitutions can be made using “shifts”
 - Bound in term of output size δ_F
 - Bound for δ_F
- <http://arxiv.org/abs/0803.3027>
→ Proofs, examples and comments
- To do :
 - Extensions : non monic case, genus computation...
 - Implementation
 - Sharpen bounds

Numerical precision

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

A factor of the discriminant has 30 degree and coefficients $> 10^{13}$.

Number of correct digits for the singular part coefficients :

Digits	Symbolic + Numeric	Our algorithm
10	0	4
20	0	15
30	5	29