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.

$$F(X, S_{ij}(X)) = 0 \text{ for all } 1 \leq j \leq e_i, 1 \leq i \leq s,$$

with

- $\zeta_{e_i}$ primitive $e_i$-th root of unity,
- $e_1, \ldots, e_s$ 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

  \[(\text{symbolic computation over number field}) + (\text{numerical evaluation}) = (\text{awfully long computation}) + (\text{bad accuracy})\]

- 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 $p$-reduction
- Apply RNPuiseux algorithm to $\overline{F} = F \mod p$
Singular part of Puiseux series

\[ S_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^k X^{\frac{k}{e_i}} \]

\[ = \sum_{k=0}^{r_{ij}} \alpha_{ik} \zeta_{e_i}^k X^{\frac{k}{e_i}} + \text{next terms} \]

\( r_{ij} \) is the \textbf{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, \textit{All Algebraic Functions Can Be Computed Fast}
Generic Newton polygons

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

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

- \( \mathcal{N}(F) \) : lower part of the convex hull of \( \text{Supp}(F) \).
- \( G\mathcal{N}(F) \) : slopes of \( \mathcal{N}(F) \) \( \geq -1 \).

Characteristic polynomial :

\[ \phi_\Delta(T) = \sum_{(i,j) \in \Delta} a_{ij} T^{\frac{i-i_0}{q}} \]
For each edge $\Delta$ of $\mathcal{GN}(F)$

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

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

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

\[ \mathcal{E}N = ((0, 0), (7, 0)) \]
\[ \Delta = ((0, 0), (7, 0)) \]
\[ (7) \]
\[ (7, 1) \]

\[ \mathcal{G}N = ((0, 5), (4, 1), (7, 0)) \]
\[ \Delta = ((4, 1), (7, 0)) \]
\[ (1) \]
\[ (1, 1) \]
\[ \mathcal{G}N = ((1, 0), (0, 1)) \]

\[ \Delta = ((4, 1), (7, 0)) \]
\[ (2, 1^2) \]
\[ (2, 1) \]
\[ (1, 2) \]
\[ \mathcal{G}N = ((0, 1), (2, 0)) \]
\[ \mathcal{G}N = ((1, 0), (0, 1)) \]

\[ \Delta = ((0, 5), (4, 1)) \]
\[ (2, 1) \]
\[ (1, 2) \]

\[ \mathcal{G}N = ((0, 1), (2, 0)) \]
\[ \mathcal{G}N = ((1, 0), (0, 1)) \]

\[ \Delta = ((0, 1), (2, 0)) \]
\[ (1) \]
\[ (1) \]
\[ (1, 1) \]
\[ \mathcal{G}N = ((1, 0), (0, 1)) \]
Good $p$-reduction

We denote :

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

**Definition**

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

- $F \in \mathcal{o}_p[X, Y]$,
- $p > D_Y$,
- $tc(\Delta_F) \not\equiv 0 \mod p$.

where $\Delta_F = \text{Disc}_Y(F)$
Reduction of Puiseux Series

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

**Theorem**

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

**Proof**: Use a theorem of Dwork & Robba 79

*On Natural Radii of \( p \)-adic Convergence*
Reduction of $\mathcal{I}(F)$

**Theorem**

*If $F$ has local good $p$-reduction, then $\mathcal{I}(F) = \mathcal{I}(\overline{F})$.***

**Not true with classical polygons:**

**Example**

$$F(X, Y) = (Y - pX)(Y^2 - X) + X^3 \Rightarrow tc(\Delta_F) = 4$$
Choice of the prime number $p$

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

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

- $O(wD_Y (\text{wht}(M_\gamma) + \text{ht}(F) + \log(wD_X D_Y)))$
  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 \( x^{\delta_F + 1} \)
- One substitution = \( N \) "shifts" \( \subset O(NM(D_Y)) \) field operations.
Complexity of RNPuiseux over $L = \mathbb{F}_{p^{t_0}}$

Substitutions $\rightarrow \mathcal{O}^\sim(\delta_F^2 D_Y)$

Factorisations $\rightarrow \mathcal{O}^\sim(\delta_F[D_Y^2 + D_Y t_0 \log p])$

Total $\rightarrow \mathcal{O}^\sim(\delta_F D_Y[\delta_F + D_Y + t_0 \log p])$

**Lemma**

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

**Theorem (Number of operations in $L$)**

$\rightarrow \mathcal{T}(\overline{F})$ above 0 : $\mathcal{O}^\sim(D_Y^3 D_X^2 + D_Y^2 D_X t_0 \log p)$

$\rightarrow \mathcal{T}(\overline{F})$ above all critical points : $\mathcal{O}^\sim(D_Y^3 D_X^2 t_0 \log p)$

D. Duval 89 *Rational Puiseux Expansions* : $O(D_Y^6 D_X^2)$
Bit Complexity for the Monte-Carlo algorithm

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

**Theorem**

There exists a Monte-Carlo algorithm which compute $T(F)$ in

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

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 $\delta_F$
  - Bound for $\delta_F$

  → 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:

<table>
<thead>
<tr>
<th>Digits</th>
<th>Symbolic + Numeric</th>
<th>Our algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>20</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>30</td>
<td>5</td>
<td>29</td>
</tr>
</tbody>
</table>