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 $Y$

$C = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$
Roots of $F \in \mathbb{K}[X][Y]$ monic in $Y$

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

$C = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$
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**: $\#\mathcal{F}(x_0) = d_Y$.

$\mathcal{C} = \{(x, y) \in \mathbb{C}^2 | F(x, y) = 0\}$
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**: $\#\mathcal{F}(x_0) < d_Y$.  
  $\implies$ 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**: $\# \mathcal{F}(x_0) < d_Y$.

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

$C = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$
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**: $\# \mathcal{F}(x_0) < d_Y$.

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

Puiseux series:

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

$C = \{(x, y) \in \mathbb{C}^2 | F(x, y) = 0\}$
Singular part

\[ Y_{ij}(X) = \sum_{k=n_i}^{r_{ij}} \alpha_{ik} \zeta_{e_j}^k X^{\frac{k}{e_j}} + \text{next terms} \]

\( r_{ij} \) 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

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

- \( S_1 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 - X^{15}/2 \)
- \( S_2 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 + X^{15}/2 \)
- \( S_3 = X + X^2 + X^3 + X^4 \)
This paper: improving arithmetic complexity over $\mathbb{F}_{p^n}$

We do not consider:

- coefficient growth problem / bit complexity over $K = \mathbb{Q}$
  - 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

Puiseux series

Monodromy group

Abel-Jacobi theorem

Computer Algebra:
Integration of algebraic functions
Algebraic solutions of ODE
Differential Galois theory

Physics:
KdV & KP equations

adrien.poteaux@univ-lille1.fr
State of the art (about arithmetic complexity)

- Newton-Puiseux like algorithm
  - Duval [22, 23] $\rightarrow O(D^8)$
  - P. & Rybowicz [39, 40] $\rightarrow O^\sim(D^5)$

- Factorisation in $\mathbb{F}_q[[X]][Y]$ or $\overline{\mathbb{F}}_q[[X]][Y]$ (Montes algorithm)
  - Bauch, Nart & Stainsby [3] : $O^\sim(D^5)$, irreducibility test $O^\sim(D^4)$
  - 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

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

\[ \Rightarrow \text{We’re looking } Y(X) = \alpha X^{m/q} + \cdots \text{ s.t. } F(X, Y(X)) = 0 \]

\[ F(X, \alpha X^{m/q} + \cdots) = \alpha^6 X^{6m/q} + \alpha^5 X^{5m/q+1} + 5 \alpha^4 X^{4m/q+3} \]

\[ -2 \alpha^4 X^{4m/q+1} + 4 \alpha^2 X^{2m/q+2} + X^5 - 3 X^4 + \cdots \]

- Some of these terms must cancel!

\[ \Rightarrow (m, q) \text{ s.t. at least two exponents are the same} \]
Support of the polynomial

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

- \( \text{Supp}(F) = \{(i, j) \in \mathbb{N}^2 \mid a_{ij} \neq 0\} \)
Choice of \((m, q)\) that increases the \(X\)-order?

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

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

\((m, q)\) for cancelling two terms?
\(\therefore\) at least two points on \(mi + qj = l\)

\((m, q)\) for increasing the \(X\)-order?
\(\therefore\) no other point under the line
Choice of \((m, q)\) that increases the \(X\)-order?

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

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

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

\(\sim\) at least two points on \(mi + qj = l\)

* increasing the \(X\)-order?

\(\sim\) no other point under the line

\((\Delta_1) i + 2j = 6\) is such a line
Choice of \((m, q)\) that increases the \(X\)-order?

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

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

\((m, q)\) for cancelling two terms?

\(\sim\) at least two points on \(mi + qj = l\)

\((\Delta_1) i + 2j = 6\) is such a line

\((\Delta_2) i + j = 4\) is too
Newton polygon

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

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

\( \mathcal{N}(F) \) : lower part of convex hull of \( \text{Supp}(F) \).
Choice of $\alpha$ that increases the $X$-order?

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

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

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

$$F(T^2, \alpha T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2) T^6 - 3T^8 + \alpha^5 T^7 + (5\alpha^4 + 1) T^{10} + \ldots$$
Characteristic polynomial

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

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

\[ \mathcal{N}(F) : \text{lower part of convex hull of Supp}(F). \]

\[ F(T^2, \alpha T) = (\alpha^6 - 2\alpha^4 + 4\alpha^2)T^6 - 3T^8 + \alpha^5T^7 + (5\alpha^4 + 1)T^{10} + \ldots \]

Characteristic polynomial:

\[ \phi_{\Delta_1}(\beta) = \beta^2 - 2\beta + 4 \]
Rational Newton-Puiseux algorithm Duval [22,23]

For each edge $\Delta$ of $\mathcal{N}(F)$

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

- For each factor $\phi_k$, compute a RNP-shift:

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

with

\begin{itemize}
  \item $\xi$ s.t. $\phi_k(\xi) = 0$,
  \item $(u, v)$ such that $uq - vm = 1$.
\end{itemize}

- Recursive calls for $\{H_{\Delta,\xi}(X, Y)\}_{\Delta,\xi}$
ISSAC’08 results

(we denote $v_F = v_X(\Delta_Y(F))$)

P. & Rybowicz [39, 40]:

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

$\implies$ complexity bounded by $O^\sim(v_F^2 d_Y) \subset O^\sim(d_X^2 d_Y^3) \subset O^\sim(D^5)$
Contributions : improving Newton-Puiseux algorithm

- Abhyankhar’s trick : less steps ($O(d_X d_Y) \rightarrow O^\sim(d_Y)$) requires the polynomial to be distinguished.

- Factorisation of $F$ in $\mathbb{F}_q[[X]][Y]$ during the algorithm
  - reduces $d_Y$ in recursive calls,
  - fulfills previous requirement.

\[ \implies O^\sim(D^4) \text{ algorithm.} \]

- 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 $\phi_{\Delta}(T) = (T - \xi)^{d_Y}$

$\implies$ 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 $\phi_\Delta(T) = (T - \xi)^{d_Y}$

$\implies$ number of steps in $O(\rho \log(d_Y))$.

Example 2 p. 303:

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

$$S_2 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 + X^{15/2}$$

$$S_3 = X + X^2 + X^3 + X^4$$
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 $\phi_{\Delta}(T) = (T - \xi)^{d_Y}$

$\implies$ number of steps in $O(\rho \log(d_Y))$.

Example 2 p. 303:

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

$$S_2 = X + X^2 + X^3 + 17X^4 + X^5 + X^6 + X^7 + X^{15/2}$$

$$S_3 = X + X^2 + X^3 + X^4$$
Weierstrass preparation theorem.

After a RNP-shift:

- $G(0, Y) = Y^d p(Y)$ avec $p(0) \neq 0$,
- Hensel lemma:
  
  $G = HP$ 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: $O^*(d_Y N)$
Complexity

\[ s_k = \#\{(\Delta, \xi)\} \]

1. Abhyankar : bivariate shift \( O^\sim(N \, d_Y) \)

2. RNP-shift : one for each \((\Delta, \xi)\) \( s_k \, O^\sim(N \, d_Y) \)

3. Weierstrass Preparation \( s_k \, O^\sim(N \, d_Y) \)

4. Recursive calls.

- Total : \( \sum_k s_k \in O(\rho \log(dy)) \) \( O^\sim(\rho \, N \, d_Y) \)

- \( N = v_F(= v_X(\Delta_Y(F))) \) \( O^\sim(\rho \, v_F \, d_Y) \subset O^\sim(d_X \, d_Y^3) \)

- Factorisations P. & Rybowicz [39,40] \( O^\sim(d_Y^3 + d_Y^2 \log(q)) \)

A better complexity?
A sharp count: family of examples

Example (example 3, p. 305)

\[ F(X, Y) = \prod_{k=1}^{N} (Y - S_k) \] \textit{with}

\[ S_1(X) = 2X \]
\[ S_2(X) = X + 2X^2 \]
\[ \ldots \ldots \ldots \]
\[ S_{N-1}(X) = X + X^2 + \cdots + X^{N-2} + 2X^{N-1} \]
\[ S_N(X) = X + X^2 + \cdots + X^{N-2} + X^{N-1} + 2X^n \]

\[ \rho = d_Y = N, \ d_X \in \Theta(N^2). \ v_X(\Delta_Y(F)) \in \Theta(N^3) = \Theta(d_X d_Y). \]

Cost is \[ N^3 \times (N + (N - 1) + \cdots + 3 + 2) \simeq N^5. \]

\[ \implies \text{complexity in } \Theta(d_X d_Y^3). \]
Theoretically, we have in $L[[X]][Y]$:

\[ F = F_1 \ast F_2 \ast F_3 \]
Factorisation according to the Newton polygon

\[ F(X, Y) \]

\[ G(X, Y) = F(X^q, Y X^m)/X^l \]

\[ (\Delta_3) \ m i + q j = l \]

\[ X^{md} P(X^{1/q}, X^{-m/q} Y) \]

\[ X^{md3} G_3(X^{1/q}, X^{-m/q} Y) \]

\[ Hensel lemma \]

\[ G(X, Y) = P(X, Y) G_3(X, Y) \]

\[ G(0, Y) = Y^d g_3(Y) \]
Factorisation according to the Newton polygon

\[ F(X, Y) \]

\[ G(X, Y) = F(X^q, Y X^m)/X^l \]

\[(\Delta_3) \quad m i + q j = l\]

\[ G(X, Y) = P(X, Y) G_3(X, Y) \quad \text{Hensel lemma} \]

\[ G(0, Y) = Y^d g_3(Y) \]
Factorisation according to the Newton polygon

\[
F(X, Y) = \frac{d}{X} \left( G(X, Y) - F(X, Y) \right)
\]

Hensel lemma

\[
G(X, Y) = P(X, Y) \cdot G_3(X, Y) \mod X^n \mod X
\]

Lebreton, Schost, van der Hoeven [34]
Conclusion

- A better worst case complexity for Puiseux series above 0.
  \[ O^\sim(D^5) \Rightarrow O^\sim(D^4) \]

- 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!