

Computing the Monodromy Group of a Plane Algebraic Curve Using a New Numerical-modular Newton-Puiseux Algorithm

Poteaux Adrien

XLIM-DMI
UMR CNRS 6172
Université de Limoges, France

SNC'07
University of Western Ontario, Canada

Outline

- ① Computing the monodromy group of a plane algebraic curve
- ② A new numerical-modular Newton-Puiseux algorithm

The problem

- \mathcal{K} subfield of \mathbb{C} .
- $F \in \mathcal{K}[X, Y]$ squarefree and monic in Y .
- $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$ the associated curve.
- **Fiber** at x_0 : $\mathcal{F}(x_0) = \{\text{roots of } F(x_0, Y) = 0\}$.
- **Regular point** : $\#\mathcal{F}(x_0) = D_Y$.
- **Critical point** : $\#\mathcal{F}(x_0) < D_Y$.
- $\delta(x_0)$: distance between x_0 and its nearest critical point.

Regular points

Let x_0 regular and $\mathcal{F}(x_0) = \{y_1, y_2, \dots, y_{D_Y}\}$ the fiber at x_0 .

- Implicit function theorem : there exist D_Y series

$$Y_i(X) = \sum_{k=0}^{\infty} \alpha_{ik} (X - x_0)^k \text{ s.t. } F(X, Y_i(X)) = 0 \text{ in the neighborhood of } x_0 \text{ and } Y_i(x_0) = y_i.$$

- The convergence radius of this series is at least $\delta(x_0)$.
- If γ is a path which does not meet any critical point, we can analytically continue the Y_i along γ .

Critical points : Puiseux Series

There exist d series $Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$ s.t.

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

- $\zeta_e = \exp\left(\frac{2\pi i}{e}\right)$.
- e_1, \dots, e_s a partition of D_Y .

The integer e_i is the **ramification index**.

Critical points : Puiseux Series

There exist d series $Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$ s.t.

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

- $\zeta_e = \exp\left(\frac{2\pi i}{e}\right)$.
- e_1, \dots, e_s a partition of D_Y .

The integer e_i is the **ramification index**.

Examples at $x_0 = 0$:

- $G(X, Y) = Y^3 - X$

$$Y_1(X) = X^{\frac{1}{3}}, Y_2(X) = jX^{\frac{1}{3}}, Y_3(X) = j^2X^{\frac{1}{3}}.$$

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

$$Y_{1k}(X) = j^k X^{\frac{1}{3}} + \frac{1}{6} X^3 + \frac{5}{12} j^k X^{\frac{10}{3}} + \dots, k = 1, 2, 3.$$

$$Y_{2k}(X) = 1 + X^{\frac{1}{2}} \pm \frac{1}{2} X^{\frac{3}{2}} + \frac{3}{2} X^2 + \dots, k = 1, 2.$$

$$Y_{31}(X) = 2 - 3X^2 - \frac{9}{2} X^3 + \dots$$

Local monodromy

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

$$Y_{31}(X) = 2 - 3X^2 - \frac{9}{2}X^3 + \dots$$

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

$$Y_{2k}(X) = 1 + X^{\frac{1}{2}} \pm \frac{1}{2}X^{\frac{3}{2}} + \dots$$

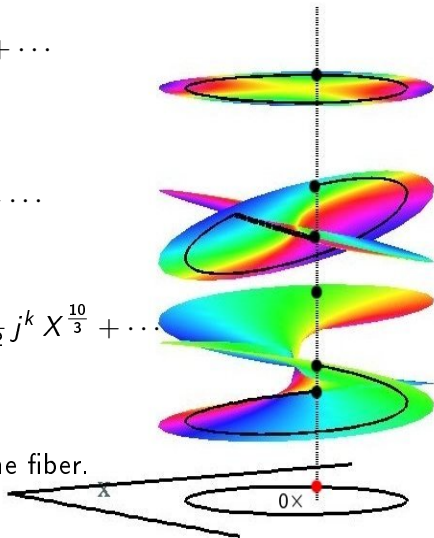
$\Rightarrow e = 2$: 2-cycle.

$$Y_{1k}(X) = j^k X^{\frac{1}{3}} + \frac{1}{6}X^3 + \frac{5}{12}j^k X^{\frac{10}{3}} + \dots$$

$\Rightarrow e = 3$: 3-cycle.

\Rightarrow Local monodromy :

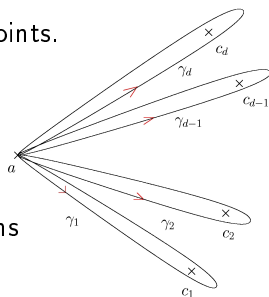
Permutation generated on the fiber.



We get it from **ramification indices** !

Global monodromy

- Let c_1, \dots, c_d denote the critical points.
- We fix a regular base point a .
- We will compute the d permutations $\sigma_1, \dots, \sigma_d$ generated by $\gamma_1, \dots, \gamma_d$.



- These permutations generate the monodromy group.

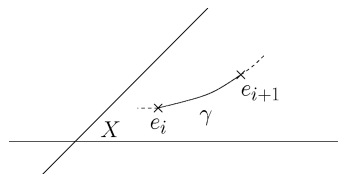
Motivations

- Galois theory.
- Multivariate polynomial factorization (Galligo-Van Hoeij 2007...).
- First step towards an effective Abel-Jacobi theorem.
 - Integration of algebraic functions (logarithmic part).
 - Applications in Physics (KP equations...).

Our long term goal :

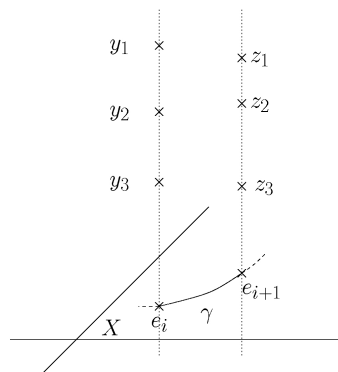
An implementation of the Abel map with provable accuracy bound.

Compute fibers and connect



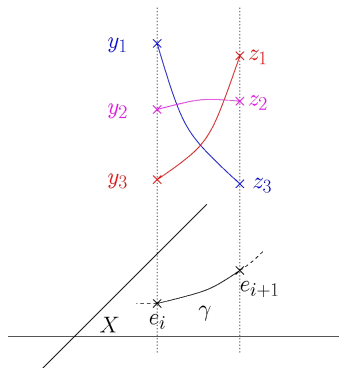
- 1 Choice of paths.
- 2 Choice of connection points.

Compute fibers and connect



- 1 Choice of paths.
- 2 Choice of connection points.

Compute fibers and connect



- 1 Choice of paths.
- 2 Choice of connection points.
- 3 Connection method.

Monodromy : state of art (sketch)

1 Compute fibers and connect

Van Hoeij & Deconinck (2001)

- Maple's `monodromy` command.
- Fibers connected with first order approximation.
- Heuristic connection criteria and error control.

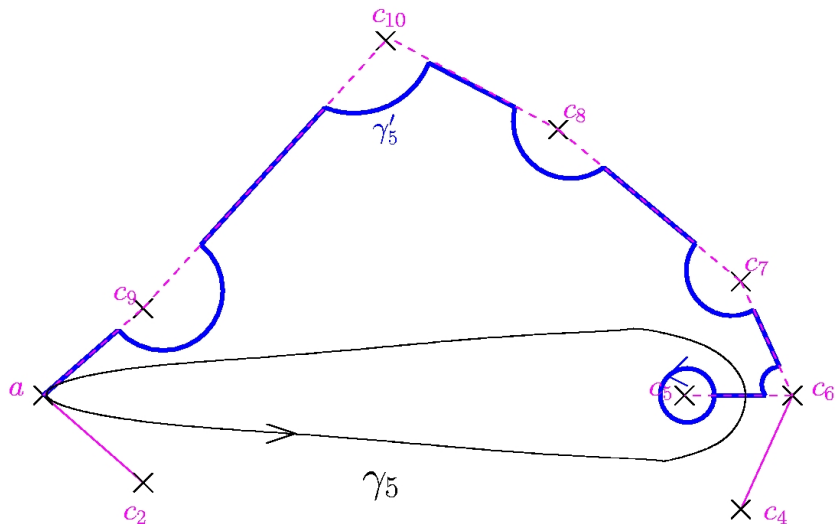
2 Differential equation

Chudnovsky & Chudnovsky, Van der Hoeven...

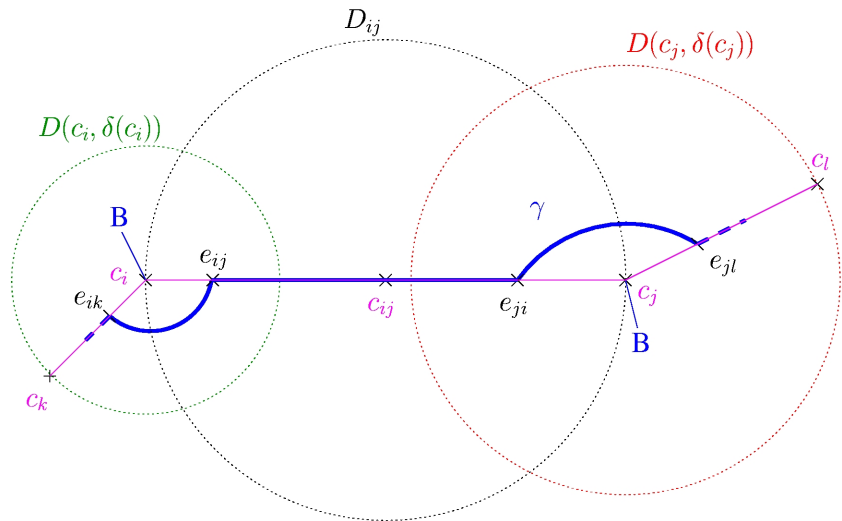
Contributions

- 1 Choice of paths : Euclidean minimum spanning tree.
- 2 Connection method : truncated series expansions and Puiseux series *above critical points*.
 - Certified connections.
 - Local monodromy for free.
 - Useful for Abel's map (Deconinck and Patterson 2007).
 - A new numerical-modular algorithm to compute singular part of Puiseux series.
- 3 Choice of connection points : trade-off between truncation orders and number of steps. Bound for the number of steps.

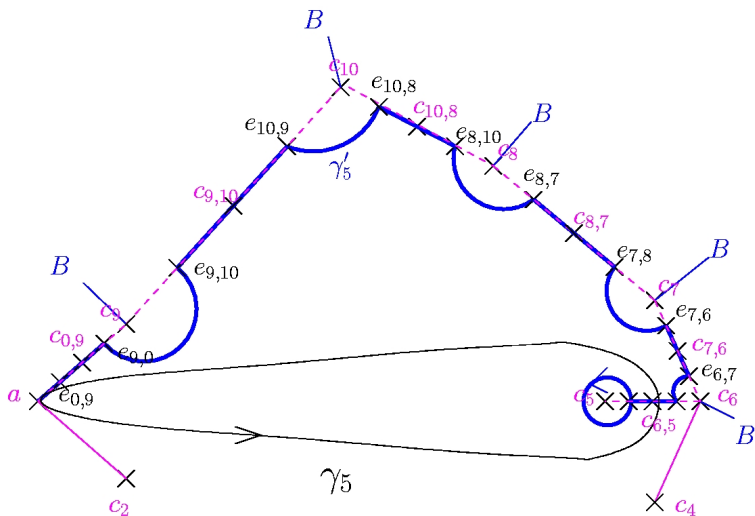
Euclidean Minimum Spanning Tree



Connections along the tree



Number of connection points



\Rightarrow At this point, we need $O(d) = O(D^2)$ connection points.

Truncation orders

Let

- $Y(X) = \sum_{k=0}^{\infty} \mu_k (X - x_0)^{\frac{k}{e}}$ a Puiseux series,
- $\tilde{Y}(X) = \sum_{k=0}^n \mu_k (X - x_0)^{\frac{k}{e}}$ its order n truncation,
- $x_1 \in D(x_0, \rho)$ with $\rho < \delta(x_0)$,
- $M \geq \sup_{x \in D(x_0, \rho)} |Y(x)|$,
- $\eta \in \mathbb{R}^{+*}$ the required precision,
- $\beta = \left(\frac{|x_1 - x_0|}{\delta(x_0)} \right)^{\frac{1}{e}}$,

Proposition

$$n \geq \frac{\ln\left(\frac{\eta}{M}\right) + \ln(1 - \beta)}{\ln(\beta)} - 1 \Rightarrow |Y(x_1) - \tilde{Y}(x_1)| \leq \eta$$

With $F(X, Y) = Y^3 - X^5 + 2(10X - 1)^2$, we get

$$\beta \approx 0.9999 \text{ and } n \geq 257636.$$

Number of connection points

- If $\beta = \frac{1}{2}$, we only need $n \geq 1 - \log_2 \left(\frac{\eta}{M} \right)$.
- For $[c_{jk}, c_k]$, logarithmic number of connection points :

$$O \left(\log_3 \left(\frac{\delta(c_{jk})}{\delta(c_k)} \right) \right).$$

Theorem

If $F \in \mathbb{Z}[X, Y]$, we need $O(D^6 \log \|F\|_\infty)$ connection points to compute the monodromy group.

\Rightarrow bound cubic in the size of the output.

- 1 Minimize the length of the paths.
- 2 Series expansions : trade-off between truncation orders and number of steps. Bound for the number of steps.
- 3 Puiseux series *above critical points* : a fast numerical-modular algorithm.

Newton-Puiseux algorithm : singular part

- Symbolic algorithm :
Bit complexity $O(D_Y^{32} D_X^4)$ (Walsh 2000)
- Purely numerical computation difficult :

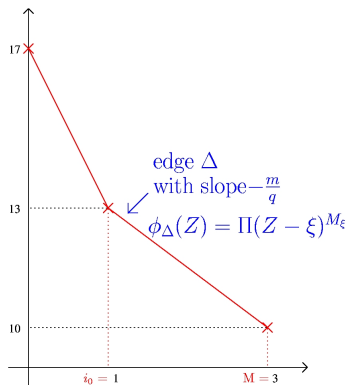
$$F(X, Y) \leftarrow F(X^q, Y + \xi^{\frac{1}{q}} X^m)$$

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

- Characteristic polynomial:

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

- ξ root of ϕ_{Δ} .



A numerical-modular algorithm

- 1 Compute singular part of Puiseux series modulo a good p .

This gives us :

- Rational exponents $\frac{m}{q}$ with $q \neq 1$.
- Multiplicities of roots of $\phi_{\Delta}(Z)$ when it has several factors.

Choice of p : can be deduced from the discriminant.

- 2 Guide numerical computations by this modular information.

Complexity for the singular part :

$O^{\sim}(D_Y^4 D_X^2)$ modular and floating point computations.

Numerical precision

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

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

Running time

$$G_n(X, Y) = \left(Y^{\lceil \frac{n}{2} \rceil} - P_{\lceil \frac{n}{2} \rceil}(X) \right) G_{\lfloor \frac{n}{2} \rfloor}(X, Y)$$

$$\text{with } P_{n_0}(X) = \frac{1}{n_0^3!} X \left(X^{n_0} + (n_0 - 1) X - \frac{1}{n_0!} \right).$$

Polynomial	Running time for symbolic	Our algorithm	
		time	precision
G_8	0.031 s	0.029 s	9
G_{12}	0.041 s	0.099 s	9
G_{16}	2.3 s	0.221 s	9
G_{20}	0.751 s	0.550 s	9
G_{24}	2.889 s	0.920 s	9
G_{28}	8.509 s	1.719 s	9
G_{32}	30.820 s	5.040 s	9

Prime number used : $p = 100019$.

Conclusions

- Modular computations yield an efficient algorithm for floating point Puiseux series above critical points.
- Monodromy groups can be computed using controlled number of steps and truncation orders.
- Paths can be optimized.

Future work

- Control round-off errors and analyze accuracy.
- Refine the monodromy algorithm.
- Finalize complexity.
- Improve implementation.