

# A Numerical-Modular Newton-Puiseux Algorithm to Compute Monodromy Groups of Plane Algebraic Curves

Adrien Poteaux  
 XLIM - DMI, UMR CNRS 6172  
 Université de Limoges  
 adrien.poteaux@unilim.fr

## 1. INTRODUCTION

This poster presents a symbolic-numeric method to compute the monodromy group of a plane algebraic curve viewed as a ramified covering space of the complex plane. Following the definition, our algorithm is based on analytic continuation of algebraic functions above paths in the complex plane. Our contribution is three-fold : first of all, we show how to use a minimum spanning tree to minimize the length of paths ; then, we propose a strategy that gives a good compromise between the number of steps and the truncation orders of Puiseux expansions, obtaining for the first time a complexity result about the number of steps; finally, we present an efficient numerical-modular algorithm to compute Puiseux expansions above critical points, which is a non trivial task. A number of figures and examples illustrate the poster.

### Motivations

- Galois theory, multivariate polynomial factorization. . .
- First step for an effective Abel-Jacobi Theorem [1]

### Notations

- $\mathcal{K}$  a subfield of  $\mathbb{C}$ ,
- $F = Y^d + a_{d-1}(X)Y^{d-1} + \dots + a_0(X) \in \mathcal{K}[X, Y]$  a squarefree polynomial,
- $\mathcal{C} = \{(x, y) \in \mathbb{C}^2 \mid F(x, y) = 0\}$  the associated curve,
- $D(x_0, \rho)$  the open disc with center  $x_0$  and radius  $\rho$ .

### Some definitions

- *Fiber* at  $x_0 \in \mathbb{C}$  :  $\mathcal{F}(x_0) = \{y \in \mathbb{C} \text{ s. t. } F(x_0, y) = 0\}$ .
- A point  $x_0$  is *regular* if  $\#\mathcal{F}(x_0) = d$ .
- A point  $x_0$  is *critical* if  $\#\mathcal{F}(x_0) < d$ .

Critical points are denoted  $c_1, \dots, c_p$ . They are roots of the discriminant of  $F$  in  $Y$ . We will denote  $\delta(x_0)$  the distance between  $x_0$  and its nearest critical point ( $x_0$  excepted). There exist  $d$  so-called *Puiseux series*

$$Y_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik} \zeta_{e_i}^{jk} (X - x_0)^{\frac{k}{e_i}}$$

such that  $F(X, Y_{ij}(X)) = 0$  for all  $1 \leq j \leq e_i$ ,  $1 \leq i \leq s$  where  $e_1, \dots, e_s$  is a partition of  $d$  and  $\zeta_{e_i} = \exp\left(\frac{2\pi\sqrt{-1}}{e_i}\right)$ . The integers  $e_i$  are called the *ramification indices*.

**Expansions above a regular point  $x_0$ .**

- **Implicit Function Theorem** : for each  $y_i \in \mathcal{F}(x_0)$ , there is an analytic function  $Y_i(X)$  such that  $F(X, Y_i(X)) = 0$  in a neighborhood of  $x_0$  and  $Y_i(x_0) = y_i$ .
- The convergence radius of  $Y_i$  is at least  $\delta(x_0)$
- If a path  $\gamma$  does not meet any critical point,  $Y_i(X)$  can be analytically continued along  $\gamma$ .

**Monodromy.** Let

- $a$  be a regular point,  $\mathcal{F}(a) = \{y_1, \dots, y_d\}$  be its fiber,
- $Y_1(X), \dots, Y_d(X)$  be the series at  $X = a$  defined by the Implicit Function Theorem,
- $\gamma_i : [0, 1] \rightarrow \mathbb{C}$  a loop in the  $x$ -plane with base  $a$  that encloses a *single* critical point  $c_i$ .

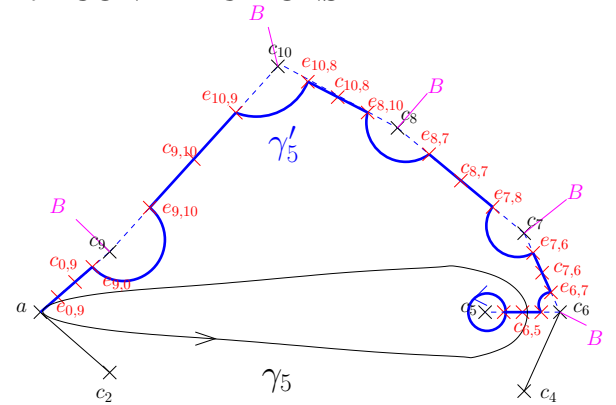
We analytically continue the  $Y_k(X)$  along  $\gamma_i$ . When  $t$  gets close to 1,  $\gamma_i(t)$  gets close to  $a$  and the values of the continuations  $\{Y_1(\gamma_i(t)), \dots, Y_d(\gamma_i(t))\}$  tend to the fiber at  $a$ , defining a permutation  $\sigma_i$  of  $\{1, \dots, d\}$  so that :

$$Y_k(\gamma_i(t)) \rightarrow y_{\sigma_i(k)} = Y_{\sigma_i(k)}(a).$$

**Definition 1** The *monodromy group*  $\mathcal{M}$  of the covering  $(\mathcal{C}, x)$  is the group generated by the  $\sigma_i$ .

**Our goal is to compute a set of such generators.**

## 2. CONTRIBUTIONS



**Figure 1: Path homotopic to  $\gamma_5$**   
**Minimal spanning tree.** To minimize path lengths, we compute a Euclidean minimal spanning tree  $T$  for the set

$V = \{c_0 = a, c_1, \dots, c_p\}$ . For each  $i$ , we compute a path  $\gamma'_i$  along  $T$  homotopic to  $\gamma_i$  (see Figure 1).

#### Continuation strategy along $\gamma'_i$

1. Compute truncated Puiseux expansions at vertices  $c_k$  and midpoints  $c_{jk}$  of  $T$  (see Figure 1).
2. Choose  $e_{kj} \in D(c_k, \delta(c_k)) \cap D(c_{jk}, \delta(c_{jk}))$ .
3. Connect fibers at  $e_{jk}$  and  $e_{kj}$  using expansions at  $c_{jk}$ .
4. Connect fibers at  $e_{jk}$  and  $e_{kl}$  using expansion at  $c_k$  (continuation along arc of circles, see Figure 1).
5. Emulate a small loop around  $c_i$  using expansion at  $c_i$ .
6. Put end to end all these connections to compute  $\sigma_i$ .

Moreover, expansions above critical points will be useful in the construction of the Abel map [1]. Finally, truncated Puiseux series will provide :

- error bounds to get reliable connections,
- error bounds for integrals involved in Abel's map[1, 2].

**Connecting expansions and fibers.** In order to reliably connect Puiseux series to fibers above the  $e_{jk}$ , bounds for the truncation orders are required. Let  $S(X)$  be a Puiseux expansion above  $x_0$  with ramification index  $e$ , convergence radius  $\rho$  and  $\overline{S}^n(X)$  be its order  $n$  truncation. We can compute an upper bound  $M$  for  $\sup_{x \in D(x_0, \rho)} |S(x)|$  by using root bounds for univariate polynomials. Finally, denoting  $\beta = \left(\frac{|x_1 - x_0|}{\rho}\right)^{\frac{1}{e}}$ , we have :

**Proposition 1** *Let  $\eta$  be a positive real number. Then*

$$n \geq \frac{\ln\left(\frac{\eta}{M}\right) + \ln(1 - \beta)}{\ln(\beta)} - 1 \Rightarrow |S(x_1) - \overline{S}^n(x_1)| \leq \eta.$$

**Number of steps.** With such a bound, truncation orders may be too high. Therefore, we use intermediate points to decrease these numbers. Experiments shows that setting  $\beta = \frac{1}{2}$  gives a good compromise, introducing a logarithmic number of intermediate connection points for a half-edge of the tree. We obtain :

**Proposition 2** *If  $g$  is the genus of the curve and  $D$  is the total degree of  $F$ , the total number of intermediate points required to compute the monodromy by our method is in  $O(p \log \frac{LM}{L_m} + g)$ , and so in  $O(D^2 \log \frac{LM}{L_m})$ .*

**Corollary 1** *If  $F \in \mathbb{Z}[X, Y]$ , we need  $O(D^6 \log \|F\|_\infty)$  intermediate points.*

#### Numerical evaluation of Puiseux series above the $c_i$ .

*Naive idea* : Compute symbolically [3], evaluate numerically. Problems: • overwhelming coefficient swell.

- Bit complexity  $O(d^{32})$  [4].
- Numerical evaluations may still be inaccurate.

*Our idea*: a **modular-numeric algorithm** that proves efficient in practice.

Computations modulo a prime number  $p$  provide the exact information that we need in order to proceed reliably with floating point numbers.

The correspondence between polynomials modulo  $p$  and numerical polynomials is not easy to establish. Our algorithm makes this correspondence.

Our experiments show that approximations for the series coefficients are reasonably accurate, yielding accurate evaluations of algebraic functions in the neighborhood of critical points.

The poster presents an example to illustrate our method.

**Experimental results for this algorithm** computed with a Maple 10 prototype implementation. Symbolic computations are obtained with the **algcures** package.

Let  $F(X, Y) = (Y^3 - M_{10,6}(X))(Y^3 - M_{10,3}(X)) + Y^2 X^5$  where  $M_{a,d}(X) = X^d - 2(aX - 1)^2$ . We compute Puiseux expansions above roots of  $P(X)$ , a degree 30 irreducible factor of the discriminant of  $F$  in  $Y$ .

We compare the precision we get for the coefficient in  $X^{\frac{1}{2}}$  of the series computed for:

- the evaluation of the symbolic expansions,
- the expansions computed by our algorithm.

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

We also considered the family of polynomials defined by the following recursive expression :

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

where  $P_k(X) = \frac{1}{k^{3!}} X \left(X^k + (k-1)X - \frac{1}{k!}\right)$ . We compute Puiseux series above 0. They all have coefficients in  $\mathbb{Q}$  (case most favorable for the symbolic algorithm). Our algorithm is performed with a precision of ten digits. We consider computation times for the ramified part of all the expansions above 0. Moreover, we give the number of correct digits of the results.

Polynomial used	time for symbolic computations	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

### 3. REFERENCES

- [1] B. Deconinck and M. S. Patterson. Computing the Abel Map. *preprint*, 2007.
- [2] B. Deconinck and M. van Hoeij. Computing Riemann Matrices of Algebraic Curves. *Phys. D*, 152/153:28–46, 2001. Advances in Nonlinear Mathematics and Science.
- [3] D. Duval. Rational Puiseux Expansions. *Compositio Math.*, 70(2):119–154, 1989.
- [4] P. G. Walsh. A Polynomial-time Complexity Bound for the Computation of the Singular Part of an Algebraic Function. *Mathematics of Computation*, 69:1167–1182, 2000.