A Numerical-Modular Newton-Puiseux Algorithm to Compute Monodromy Groups

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

Floating Point Coefficient Puiseux Series

- $F = Y^d + a_{d-1}(X)Y^{d-1} + \cdots + a_0(X) \in \mathbb{Q}[X,Y]$ a squarefree polynomial.
- We denote by m the degree of F in X and by D its total degree.

Puiseux Theorem. *There exist positive integers $e_1, \ldots, e_s$ satisfying $\sum_{i=1}^{s} e_i = d$ so that, for each i $(1 \leq i \leq s)$ there exist e_i fractional power series :*

$$S_{ij}(X) = \sum_{k=0}^{\infty} \alpha_{ik}\, \zeta_{e_i}^{jk}\, X^{\frac{k}{e_i}} \quad \text{with} \quad F(X, S_{ij}(X)) = 0.$$

The S_{ij} are called *Puiseux series above 0* of F and the e_i are the *ramification indices*. The *singular part* of the expansion $S_{i_0 j_0}$ is its order N truncation, where N is minimal for the property that no other S_{ij} has the same partial sum.

Objective : *Compute floating point approximations of the series singular parts.*

- **Classical algorithm :** Compute singular parts symbolically using Newton-Puiseux algorithm, then approximate coefficients numerically.
Bit complexity for one branch : $O(d^{32}m^4)$ for the first step (Walsh 2000).
Experiments show an overwhelming coefficient growth and devastating numerical cancellations. Numerical evaluations may require a high number of digits.
- **Pure floating point computations :** Newton-Puiseux algorithm cannot be applied to approximate inputs since *exact information*, such as ramification indices, must be obtained from non-zero coefficients.

New method

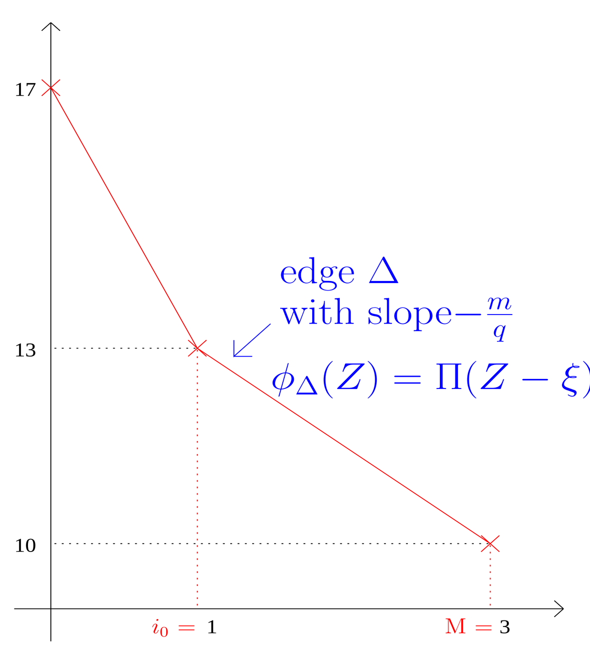
1. Apply Newton-Puiseux algorithm modulo a well-chosen prime number p to obtain the exact information required.
2. Use this information to guide a floating point Newton-Puiseux algorithm.

Complexity : $O(d^3 M(d) m^2)$ modular and floating point operations.
Experiments demonstrate efficiency and satisfactory accuracy.

Newton-Puiseux Algorithm.

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

- The *Newton polygon* $\mathcal{N}(F)$ is the lower convex hull of $\{(i,j) \in \mathbb{N}^2 \,|\, a_{ij} \neq 0\}$.
- The *characteristic polynomial* of an edge Δ of $\mathcal{N}(F)$ is $\phi_\Delta(Z) = \sum_{(i,j)\in\Delta} a_{ij} Z^{\frac{i-i_0}{q}}$.
- If ξ is a root of ϕ_Δ, we denote by M_ξ its multiplicity.




```
NewtonPuiseux(F, e, S, M)
If M = 1 then Return {S(X^(1/e))}
L ← {}
For each edge Δ of N(F) ∩ {(i,j) | i ≤ M}
  For each root ξ of φ_Δ(Z)
    F(X,Y) ← F(X^q, Y + ξ^(1/q) X^m)
    S(T) ← S(T^q) + ξ^(1/q) T^m
    L ← L ∪ {NewtonPuiseux(F, e*q, S, M_ξ)}
Return L
```

The function call NewtonPuiseux$(F,1,0,d)$ returns all (conjugacy classes of) Puiseux series singular parts above 0.

How to choose p ? *We choose a prime number $p > d$ such that :*

- *the reduction modulo p of F can be formed. We denote it by $\bar{F}$.*
- *$\mathrm{Disc}_Y(F)$ and $\mathrm{Disc}_Y(\bar{F})$ have the same valuation in X.*

Then, characteristic exponents and intersection multiplicities of the branches corresponding to the Puiseux series will be preserved by reduction modulo p.

Applying NewtonPuiseux algorithm to $\bar{F}$ will provide root multiplicities of characteristic polynomials and slopes m/q for F whenever $q > 1$.

From modulo p to floating point Puiseux series.

The difficulty is to connect numerical computations to modular informations. We illustrate our method to make this connections with an example.

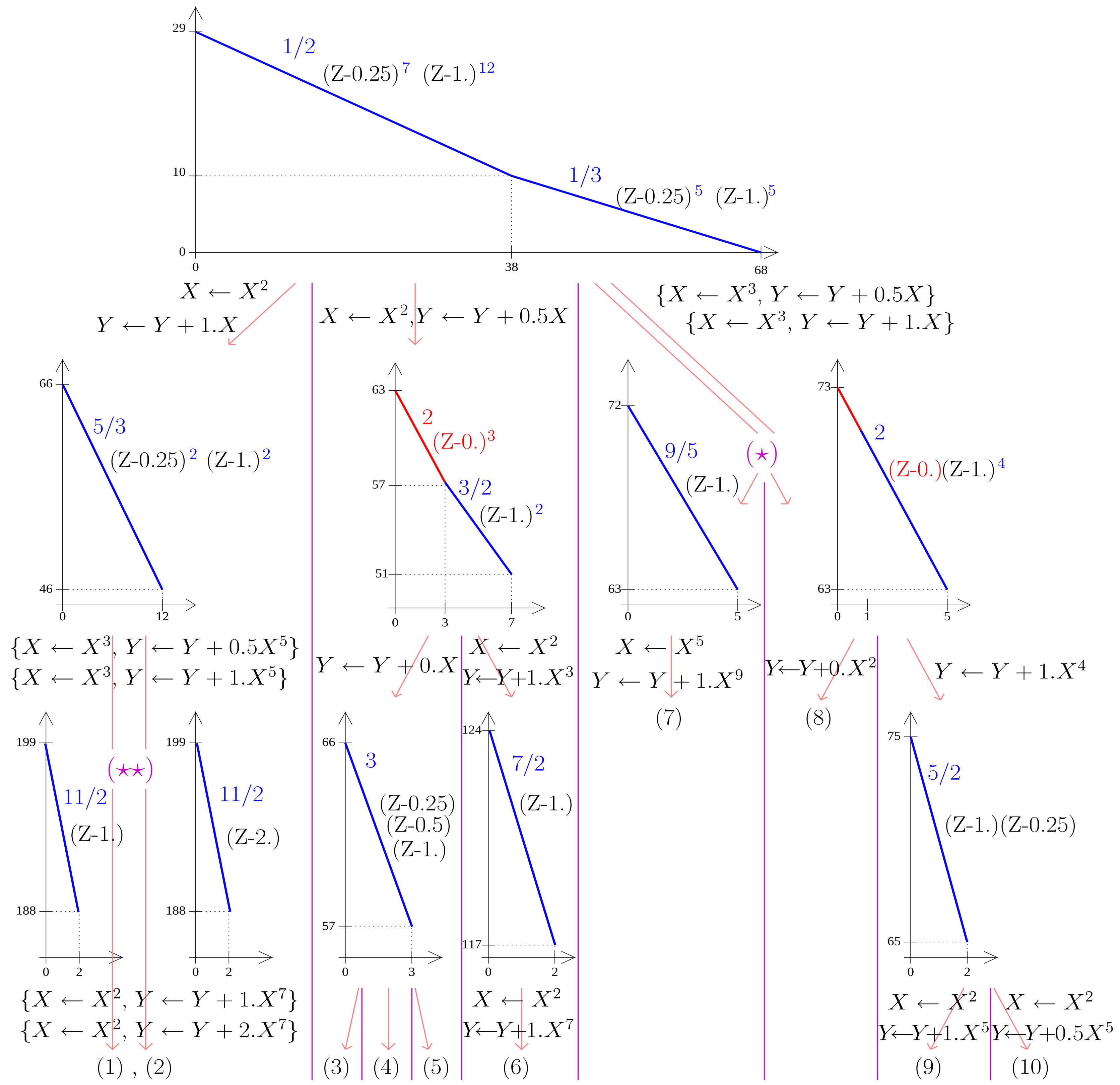
- We consider a polynomial $F(X,Y)$ of degree 68 in Y and 60 in X.
- Applying NewtonPuiseux to $\bar{F}$, we obtain the blue expansions below. Blue coefficients (represented by greek letters and $\cdot$) correspond to non-zero coefficients of the Puiseux series of F.
- Our criteria for p ensures that the (possibly) missing non-zero coefficients for expansions of F are the red ones.

(1) $Y = \alpha X^{1/2} + \cdot X^{5/6} + \cdot X^{11/12}$
(2) $Y = \alpha X^{1/2} + \cdot X^{5/6} + \cdot X^{11/12}$
(3) $Y = \beta X^{1/2} + \gamma X + \cdot X^{3/2}$
(4) $Y = \beta X^{1/2} + \gamma X + \cdot X^{3/2}$
(5) $Y = \beta X^{1/2} + \gamma X + \cdot X^{3/2}$
(6) $Y = \beta X^{1/2} + \cdot X^{3/4} + \cdot X^{7/8}$
(7) $Y = \cdot X^{1/3} + \cdot X^{3/5}$
(8) $Y = \delta X^{1/3} + \cdot X^{2/3} + \cdot X$
(9) $Y = \delta X^{1/3} + \epsilon X^{2/3} + \cdot X^{5/6}$
(10) $Y = \delta X^{1/3} + \epsilon X^{2/3} + \cdot X^{5/6}$

From this, we deduce :

- slopes of Newton polygons of F and its successive transforms,
- root multiplicities of the characteristic polynomials.

With this information, we can follow the classical algorithm numerically.
We compute roots of ϕ_Δ with a numerical solver, then group them according to the multiplicities given by modular computations, and finally certify the result, thanks to a theorem by B. Smith (Smith 1970).
In the figure below, information provided by modular computations is in blue and potentially missing edges and roots are in red.



(⋆⋆) We get two numerical polynomials that we cannot relate to the polygons modulo p. But Newton polygons and multiplicities are the same, so we can perform both changes of variable. At the next step the multiplicity is one for both branches and we are done.

(⋆) We get two numerical polynomials defined by two roots of the same edge with the same multiplicity. We need to relate to the possible polygons modulo p : The polynomial which has the largest X^{72}-coefficient correspond to the left polygon.

Application: Monodromy Group

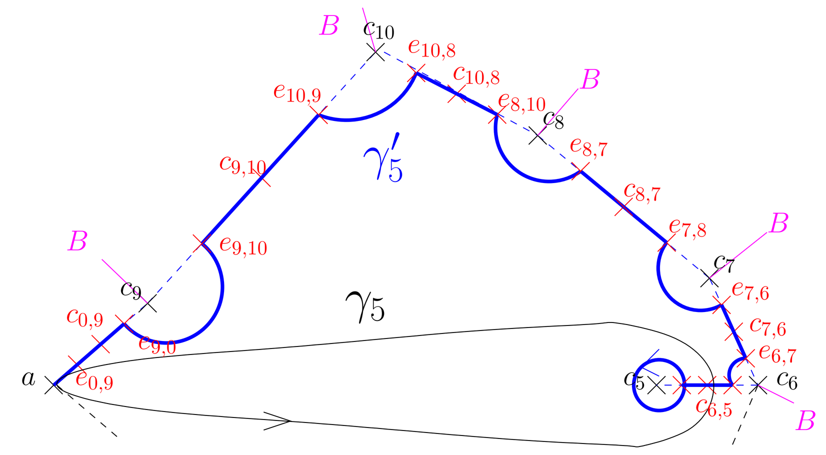
The curve $\mathcal{C} = \{(x,y) \in \mathbb{C}^2 \,|\, F(x,y) = 0\}$ along with the projection on the first coordinate x define a d-sheeted ramified covering $(\mathcal{C}, x)$ of the complex plane.

- Let a be a *regular* (non critical) point. The polynomial $F(a,Y)$ has d distinct roots $\{y_1, \ldots, y_d\}$, the fiber $\mathcal{F}(a)$ at a.
- Implicit Function Theorem : there exists d analytic functions $Y_k(x)$ such that $F(x, Y_k(x)) = 0$ in a neighborhood of a and $Y_k(a) = y_k$.
- Let $\gamma_i : [0,1] \to \mathbb{C}$ be a loop in the x-plane starting and ending at a that encloses the single critical point c_i
- The d functions $Y_1, \ldots, Y_d$ can be analytically continued along γ_k.
- There exists a permutation σ_i so that $Y_k(\gamma_i(t)) \xrightarrow{t \to 1} y_{\sigma_i(k)} = Y_{\sigma_i(k)}(a)$

Objective: *Design a reliable algorithm to compute the monodromy group of $(\mathcal{C}, x)$, i.e. the group generated by the σ_i.*

New method

- Use a Euclidean minimal spanning tree to decrease path length.
- Perform analytic continuation with floating point Puiseux series *above critical points* and power series above regular points.
- Devise a trade-off between truncation orders and number of steps to improve performances. Obtain a bound for the number of steps.

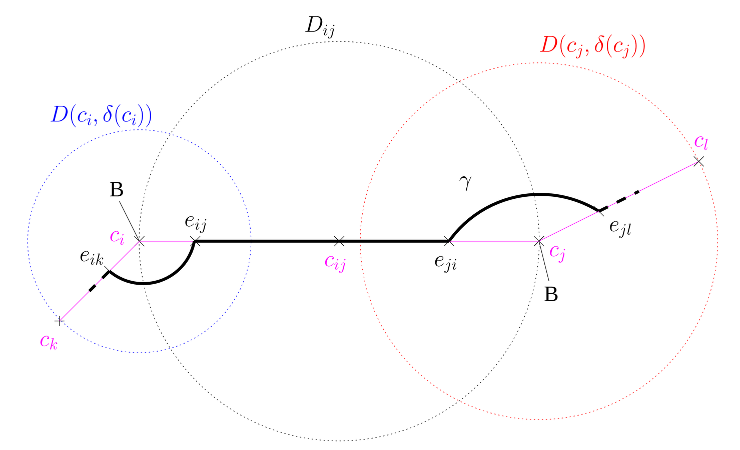


Let $c_1, \ldots, c_p$ be the critical points.

Minimal spanning tree
We use a tree of minimal length to connect the vertices $\{a, c_1, \ldots, c_p\}$. For each i, we compute a path γ_i' along T homotopic to the loop γ_i.

Continuation strategy along γ_i'

1. Choose $e_{kj} \in D(c_k, \delta(c_k)) \cap D(c_{jk}, \delta(c_{jk}))$.
2. Connect fibers at e_{jk} and e_{kj} using series expansions at c_{jk}.
3. Connect fibers at e_{jk} and e_{kl} using Puiseux series at c_k (branch cut must be well chosen).
4. Emulate a small loop around c_i using Puiseux series at c_i.
5. Put end to end all these connections to compute σ_i.



Bounds for truncation order. *Let*

- *$S(X) = \sum_{k=0}^{\infty} \alpha_k X^{\frac{k}{e}}$ be a Puiseux series above 0 and $\overline{S}^n(X) = \sum_{k=0}^{n} \alpha_k X^{\frac{k}{e}}$,*
- *$\rho \in \mathbb{R}^{+*}$ be smaller than the convergence radius of $S(X)$,*
- *$x_1 \in D(0,\rho)$, $\beta = \left(\frac{|x_1|}{\rho}\right)^{\frac{1}{e}}$, M be an upper bound for $\sup_{x \in D(0,\rho)} |S(x)|$,*
- *$\eta \in \mathbb{R}^{+*}$ be the precision required.*

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

We get an upper bound for M from root bounds for univariate polynomials.

Decreasing truncation orders. Experiments show that enforcing $\beta = \frac{1}{2}$ gives a good trade-off between number of steps and orders of truncation. It introduces a logarithmic number of intermediate connection and expansion points.

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