Algorithms Seminar 2006–2007,
F. Chyzak (ed.), INRIA

Available online at the URL
http://algo.inria.fr/seminars/.

Computing Monodromy Groups Defined by Plane Algebraic Curves

Adrien Poteaux
Xlim-Dmi, umr Cnrs 6172, Université de Limoges

April 23, 2007

Summary by Marc Mezzarobba

Abstract

This work deals with the numerical and symbolic-numerical computation of the monodromy of complex algebraic curves, with special emphasis on correct error control in presence of close singularities. The speaker's approach uses Puiseux expansions above singularities and analytic continuation along the edges of a minimal Euclidean spanning tree connecting them. This work is a first step toward an effective version of the Abel-Jacobi theorem relating an algebraic curve to its Jacobian variety.

1. Motivation and Problem Statement

1.1. The Abel-Jacobi Theorem.

An irreducible polynomial

$$F = Y^d + a_{d-1}(X)Y^{d-1} + \cdots + a_0(X) \in \mathbb{K}[X,Y] \qquad (d \geq 1) \tag{1}$$

over some subfield $\mathbb{K}$ of the complex numbers defines a plane affine algebraic curve

$$\mathcal{C} = \{(x,y) \in \mathbb{C}^2 : F(x,y) = 0\},$$

along with a ramified covering $\pi : \mathcal{C} \to \mathbb{C}$ of the complex plane and a compact Riemann surface $\hat{\mathcal{C}}$ canonically associated[1] to the curve $\mathcal{C}$. We seek to compute the *monodromy group* defined by this curve. The speaker's long-term goal, and the origin of his interest in this problem, is an effective version of the Abel-Jacobi theorem. Applications include the algebraic case of the Risch algorithm for indefinite integration, differential Galois group computations, and the study of some solution families of partial differential equations arising in physics, such as Korteweg-de Vries equations.

One concrete way to introduce this theorem is the following: a compact Riemann surface such as $\hat{\mathcal{C}}$ admits meromorphic functions. These necessarily have as many zeros as poles, when counted with multiplicities. Conversely, one may ask whether there exists a meromorphic function on $\mathcal{C}$ with prescribed zeros and poles satisfying the previous condition. For example, if the curve has genus zero, its set of meromorphic functions is $\mathbb{C}(X)$, so the answer is always positive.

Turning to the general case, recall that a divisor of $\mathcal{C}$ is a formal sum $\sum_P n_P P, n_P \in \mathbb{Z}$ of points of the curve. The degree of a divisor is the sum of its coefficients. A divisor that is the sum of the zeros of a meromorphic function (with multiplicities, and counting poles as zeros with negative multiplicity) is called a function divisor. Function divisors form a subgroup, denoted $\mathrm{Prin}(\mathcal{C})$, of the (Abelian) group $\mathrm{Div}^0(\mathcal{C})$ of degree zero divisors. So the former question amounts to decide whether a given divisor is a function divisor.

[1] Denote by S the set of critical points of π, as defined in §1.2. Then $\mathcal{C}' = \mathcal{C} \setminus (S \times \mathbb{C})$ is a (connected) finitely punctured compact Riemann surface and $\pi_{|\mathcal{C}'}$ is an unramified covering of $\mathbb{C} \setminus S$. "Stuffing the holes" (including that at infinity), we obtain $\hat{\mathcal{C}}$ and a map $\hat{\pi} : \hat{\mathcal{C}} \to \mathbb{P}^1\mathbb{C}$ extending $\pi_{|\mathcal{C}'}$.

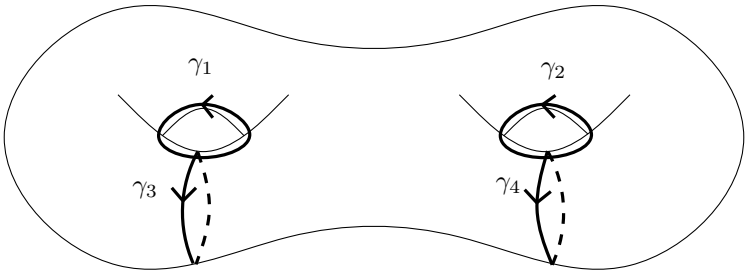

FIGURE 1. The canonical basis of homology, for a curve of genus 2.

As a complex manifold, $\hat{\mathcal{C}}$ admits holomorphic differential one-forms (a.k.a. differentials of the first kind or differentials without poles). These can be integrated along cycles, and the value of such an integral depends only on the homology class of the cycle and the cohomology class of the differential. Let $(\omega_1, \ldots, \omega_g)$ be a basis of the cohomology space $H^1(\mathcal{C})$ ("a basis of the holomorphic differentials") and let $(\gamma_1, \ldots, \gamma_{2g})$ be the canonical basis of $H_1(\mathcal{C})$, made of (the classes of) the loops depicted on Figure 1. Integrals of ($\mathbb{Z}$-combinations of) the ω_i along ($\mathbb{Z}$-combinations of) the γ_j form a lattice $\Gamma \subset \mathbb{C}$. Now we are in position to state the theorem.

Theorem 1. *The Abel-Jacobi map*

$$\begin{array}{rcl} \mathrm{Div}^0(\mathcal{C})/\mathrm{Prin}(\mathcal{C}) & \to & \mathrm{Jac}(\mathcal{C}) = \mathbb{C}^g/\Gamma \\ P & \mapsto & \left(\int_O^P \omega_1, \ldots, \int_O^P \omega_g\right) \end{array}$$

is a group isomorphism.

To decide whether a divisor is a function divisor using this theorem, we have to compute the period lattice Γ above. Using an algorithm due to C. and M. Tretkoff, this can be reduced to computing the monodromy of the curve [5].

1.2. **Monodromy.** Above all but finitely many points a of the x-plane, the fiber $\pi^{-1}(a)$ has cardinality d. In that case, a is called a *regular point*. Points that are not regular (that is, such that the univariate polynomial $F(a, Y)$ has multiple roots) are said to be *critical*. If a is a regular point, the implicit function theorem states that there exist d analytic functions $y_1(x), \ldots, y_d(x)$ such that $\{y_i(a)\} = \pi^{-1}(a)$ and $F(x, y_i(x)) = 0$ for all i. Each of them parametrizes one sheet of the covering in a neighborhood of a.

Consider a path $\gamma : [0, 1] \to \mathbb{C} \setminus S$, and choose one analytic solution of equation (1) above $\gamma(0)$. One may continue analytically this solution along γ, yielding an analytic function defined in a neighborhood of $\gamma(1)$ which is still a solution of the equation. Now take γ to be a loop with basepoint a: then analytic continuation along γ—or any other path homotopic to γ—induces a permutation of the fiber $\pi^{-1}(a)$. The action of the fundamental group $\pi_1(\mathbb{C} \setminus S, a)$ thus defined on $\pi^{-1}(a)$ is called the monodromy of $\mathcal{C}$ with basepoint a. Up to conjugation, it does not depend on the choice of the basepoint.

The monodromy action of a loop enclosing exactly one critical point c is called the local monodromy around c. The whole monodromy may be represented by the local monodromy around each critical point with respect to a common basepoint. This is the expected output of an algorithm for monodromy computation.

2. Certified monodromy computation

2.1. **General strategy.** Many methods for monodromy computation are based upon its definition by means of analytic continuation. The idea is to choose a broken line path homotopic to a bunch of loops encompassing one critical point each; then to compute (in a way to be precised) the fiber above each vertex; and finally to connect the fibers above adjacent vertices, that is, to identify values corresponding to the same solution branch.

For example, the Maple `monodromy` function, by M. van Hoeij and B. Deconinck [5], connects the fibers heuristically using first-order Taylor expansions, adapting the step length depending on the observed precision. M. van Hoeij and M. Rybowicz developed another version which provides correct error control using interval arithmetic, but it is much slower. Another idea, studied among others by D.V. and G.V. Chudnovsky [1, 2, 4], is to compute a differential equation satisfied by the algebraic function $y(x)$. This allows for fast high-precision evaluation by binary splitting [3, 10], however, according to the speaker, the size of the differential equation compared to that of the algebraic one and the conversion cost can be prohibitive. Moreover, in most cases, the high precision is not really needed.

The strategy exposed here fits into this "compute-fibers-and-connect" pattern. Following the discussion above, in a regular point, the equation admits d (convergent) formal power series solutions $y(x)$. One can show that their convergence radius is at least the distance from a to the nearest critical point. We use every other vertex (disks on Figure 2) of the path as an *expansion point*, above which we compute Taylor expansions of the d solutions. Between two successive expansion points, in the intersection of the convergence disks, lie *connection points*. Fibers above connection points are computed numerically and compared with the values assumed there by expansions above nearby expansion points to make the connection. However, when the curve has singularities close to each other, the path needs to go between them at some point, which requires high orders of truncation. Existing methods based on this sole idea tend to require unacceptable expansion orders or even to become inaccurate in those cases. To solve this problem, the method presented here allows expansion points to be singular points.

2.2. **Puiseux expansions above critical points.** Indeed, it is still possible to give formal solutions of the equation (corresponding to asymptotic expansions of "actual" algebraic functions) in the neighborhood of a critical point c, in the form of Puiseux series with nonnegative support. (Recall that F is monic.) More precisely, there exist s classes

$$y_i(x) = \sum_{k=0}^{\infty} y_{i,k} \, (x-c)^{k/e_i}, \qquad e_1 + \cdots + e_s = d$$

of e_i Puiseux series with conjugate algebraic coefficients satisfying $F(x, y_i(x)) = 0$. The e_i are called the ramification indices.

Puiseux expansions above critical points are computed using the Newton-Puiseux algorithm as improved by D. Duval [6]. Then the local monodromy can be read "for free" on the Puiseux expansions. Indeed, (almost) like power series exapansions above ordinary points, they have a sector of convergence extending up to the next critical point. This means that, once we choose a determination for the e_i-th root functions, each Puiseux expansion defines an analytic function in a slit disk centered in c. The process of analytic continuation around c permutes cyclically the branches corresponding to conjugate Puiseux expansions. As in ordinary points, numerical evaluation inside the sector of convergence allows to connect the fibers. We can also "sidestep" the critical point by evaluating the expansion in two connection points.

Example. Take $F(X,Y) = (Y^3 - X)((Y-1)^2 - X)(Y - 2 - X^2) + X^2Y^5$. Since $F(0,y) = 0 \Rightarrow y \in \{0,1,2\}$ while $\deg_Y F = 6$, the point $x_0 = 0$ is critical. The Puiseux expansions of F above 0 are:

$$\begin{aligned} Y_{1,1} &= 2 - 3X^2 - \frac{9}{2}X^3 + \cdots \\ Y_{2,k} &= 1 + X^{1/2} + (-1)^k X^{3/2} + \cdots, && k \in \{1,2\} \\ Y_{3,k} &= j^k X^{1/3} + \frac{1}{6}X^3 + \frac{5}{12}j^k X^{10/3} + \cdots, && k \in \{1,2,3\}, j^3 = 1. \end{aligned}$$

Denoting solutions by their indices above, the local monodromy is thus

$$\big((1,1)\ (1,2)\ (1,3)\big)\big((2,1)\ (2,2)\big) \in \mathfrak{S}_6.$$

All this still applies if a happens to be an ordinary point: then the Puiseux expansions are usual power series expansions, the ramification indices are all 1 and the local monodromy is the identity permutation.

2.3. **Error control for numerical connection.** In a connection point x_1, Smith's theorem on isolation of complex roots of univariate polynomials [9] allows to compute small disks $D(\tilde{y}(x_1), \rho)$ containing each exactly one root of $F(x_1, Y)$. From the minimal distance between two of these disks, we get a truncation order n in the corresponding expansion points that ensures the nearest $\tilde{y}(x_1)$ to $\sum_{k=0}^{n} y_k (x_1 - x_0)^{k/e}$ is indeed that belonging to the same branch.

Proposition 1. *Let $y(x_1) = \sum_{k=0}^{\infty} y_k (x_1 - x_0)^{k/e}$ be a Puiseux expansion of a solution of (1) above x_0. Let ρ be the distance from x_0 to the next critical point and let M be a bound on the values of y on the disk $D(x_0, \rho)$. Then for any $x_1 \in D(x_0, \rho)$, the tail of the Puiseux expansion satisfies*

$$n \geq \frac{\lg \frac{M(x_0)}{\epsilon} + \lg \frac{1}{1-\beta}}{\lg \frac{1}{\beta}} - 1 \quad \Rightarrow \left| \sum_{k=n}^{\infty} y_k (x_1 - x_0)^{k/e} \right| \leq \epsilon \tag{2}$$

where $\beta = \left(\frac{|x_1 - x_0|}{\rho}\right)^{1/e}$.

A suitable M may be computed from Mignotte bounds on the roots of univariate polynomials [7]. Similar bounds are used in other parts of the algorithm that require numerical values for roots of polynomials.

3. Efficiency issues

3.1. **Global monodromy and choice of the path.** Since we can obtain the local monodromy in any critical point simply by looking at the Puiseux expansions, all we need to compute the global monodromy is to express the local monodromies using the same base point. The complexity of the computation depends on the path we choose to do this connection.

First, we can bound the total number of continuation steps as follows. Suppose the base point a is given. Compute a minimal spanning tree for the usual Euclidean distance of the set formed by a and the critical points. Use the critical points and the middles of the edges as expansion points, and put one connection point near each end of each edge (figure 2). From the definition of the tree, expansions above the middle of an edge are convergent up to its ends, so this is sufficient for continuation along the edge. Continuation along several successive edges is performed by "sidestepping" the vertices as mentioned in §2.2. Now the monodromy matrix around c w.r.t. the common basepoint a is the conjugate of that w.r.t. a connection point e lying near c by the matrix connecting the fibers $\pi^{-1}(a)$ and $\pi^{-1}(e)$—which we obtain by analytic continuation along

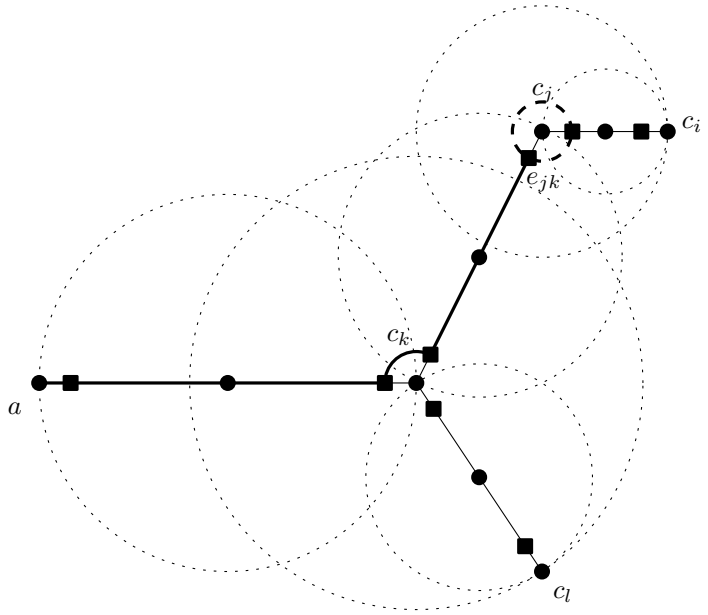

FIGURE 2. Choice of the path along which to perform analytic continuation. Disks ● are expansion points, squares ■ are connection points, dotted circles are convergence circles of Puiseux expansions. In bold, the path giving the local monodromy around c_j with basepoint a.

the path from a to e in the spanning tree. Thus, if $p \leq D^2$ (where D is the total degree of F) is the number of critical points, $2p+1$ expansions and $2p$ evaluations are enough to compute the global monodromy.

However, it turns out that minimizing the number of steps is not the best way to go. Indeed, bigger steps and steps reaching near singularities require high truncation orders. To decrease the sum of truncation orders along the path, we keep β away from 1 in Proposition 1, introducing additional steps (along the edges of the tree) as needed. Experiments show that setting $\beta = 1/2$ is a good compromise. Enforcing this value, Equation (2) becomes $n \geq \lg(M/\epsilon)$, and we get the following theorem.

Theorem 2. *Let p be the number of critical points of equation* (1)*; and let L_{min}, L_{max} be the smallest, resp. the largest distance between two of them. There is an algorithm that computes the monodromy defined by* (1) *using $O(p \lg(L_{max}/L_{min}))$ expansion and connection points, all expansion orders being bounded by $\lg(M/\epsilon)$, with the notations of Proposition 1.*

Note that M and ϵ depend on the behaviour of $y(x)$ in each expansion point.

3.2. **Towards an efficient algorithm for Puiseux series computation.** The main cost of the algorithm outlined above comes from the manipulation of Puiseux expansions above critical points. The Newton-Puiseux algorithm and its variant mentioned above compute them by performing changes of variable in the algebraic equation, guided by the form of the so-called Newton polygon of the equation, until they manage to reduce the expansion to the regular case. In order not to "miss" the multiplicities of roots of polynomials that determine the ramification type, one uses exact arithmetic on algebraic numbers. This is slow, due to the growth of the coefficients and the degrees of algebraic extensions involved. Even the numerical evaluation to connect fibers is costly, because

large cancellations can occur. However, the speaker does not wish to give up expansions above singularities: not only do they provide the local monodromy and a way to sidestep critical points, but they also give useful information for error control in other parts of the effective Abel-Jacobi theorem.

To overcome this, he suggests a hybrid numeric-modular algorithm. The idea is to compute the coefficients of the expansion numerically, while performing in parallel an exact computation modulo some suitable prime. Indeed, only the Newton polygons and the multiplicities of roots of characteristic polynomials defined by their edges really need to be exact: in other words, if all Newton polygons appearing in the course of the Newton-Puiseux algorithm are known, then it is possible to compute expansions with approximate coefficients but correct ramification by numerical methods. The difficult part is to ensure that the structure of the modular computation correctly mirrors that of the complex one. Work is in progress to devise an algorithm that outputs a "good" prime for which no degeneracy happens (at least with high probability), and to control the accuracy of the numerical part of the algorithm. A prototype heuristic implementation of these ideas in Maple already gives unexpectedly good results.

Other questions currently under investigation include understanding more precisely the good performance of the numeric-modular strategy and studying the complexity of the overall algorithm.

References

[1] Chudnovsky (David V.) and Chudnovsky (Gregory V.). – On expansion of algebraic functions in power and Puiseux series, I. *Journal of Complexity*, vol. 2, 1986.

[2] Chudnovsky (David V.) and Chudnovsky (Gregory V.). – On expansion of algebraic functions in power and Puiseux series, II. *Journal of Complexity*, vol. 3, 1987.

[3] Chudnovsky (David V.) and Chudnovsky (Gregory V.). – Computer algebra in the service of mathematical physics and number theory. In *Computers in mathematics (Stanford, CA, 1986)*. p. 109–232. – Dekker, New York, 1990.

[4] Cormier (Olivier), Singer (Michael F.), Trager (Barry M.), and Ulmer (Felix). – Linear differential operators for polynomial equations. *Journal of Symbolic Computation*, vol. 34, n° 5, 2002, pp. 355–398.

[5] Deconinck (Bernard) and van Hoeij (Mark). – Computing Riemann matrices of algebraic curves. *Physica D*, vol. 152/153, 2001, pp. 28–46. – Advances in nonlinear mathematics and science.

[6] Duval (Dominique). – Rational Puiseux expansions. *Compositio Mathematica*, vol. 70, n° 2, 1989, pp. 119–154.

[7] Mignotte (Maurice). – *Mathematics for Computer Algebra*. – Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[8] Poteaux (Adrien). – Computing monodromy groups defined by plane algebraic curves. – 2007. To appear in SNC '07.

[9] Smith (Brian T.). – Error bounds for zeros of a polynomial based upon Gerschgorin's theorems. *Journal of the ACM*, vol. 17, n° 4, October 1970, pp. 661–674.

[10] Van der Hoeven (Joris). – Fast evaluation of holonomic functions. *Theoretical Computer Science*, vol. 210, n° 1, 1999, p. 199–216.