Theoretical Computer Science 412 (2011) 1492–1507

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Computing monodromy via continuation methods on random Riemann surfaces

André Galligo [a,*], Adrien Poteaux [b]

[a] Université de Nice-Sophia Antipolis, Laboratoire de Mathématiques. Parc Valrose, 06108 Nice Cedex 02, France

[b] UPMC, Univ Paris 06, INRIA, Paris-Rocquencourt center, SALSA Project, LIP6/CNRS UMR 7606, France

ARTICLE INFO

Keywords:
Bivariate polynomial
Plane curve
Random Riemann surface
Absolute factorization
Algebraic geometry
Continuation methods
Monodromy
Symmetric group
Algorithms
Maple code

ABSTRACT

We consider a Riemann surface X defined by a polynomial $f(x, y)$ of degree d, whose coefficients are chosen randomly. Hence, we can suppose that X is smooth, that the discriminant $\delta(x)$ of f has $d(d-1)$ simple roots, Δ, and that $\delta(0) \neq 0$, i.e. the corresponding fiber has d distinct points $\{y_1, \ldots, y_d\}$. When we lift a loop $0 \in \gamma \subset \mathbb{C}-\Delta$ by a continuation method, we get d paths in X connecting $\{y_1, \ldots, y_d\}$, hence defining a permutation of that set. This is called monodromy.

Here we present experimentations in Maple to get statistics on the distribution of transpositions corresponding to loops around each point of Δ. Multiplying families of "neighbor" transpositions, we construct permutations and the subgroups of the symmetric group they generate. This allows us to establish and study experimentally two conjectures on the distribution of these transpositions and on transitivity of the generated subgroups.

Assuming that these two conjectures are true, we develop tools allowing fast probabilistic algorithms for absolute multivariate polynomial factorization, under the hypothesis that the factors behave like random polynomials whose coefficients follow uniform distributions.

1. Introduction

1.1. d-covering

A square-free bivariate polynomial equation $f(x, y) = 0$ defines a reduced curve X in $\mathbb{C}^2$. Dividing out by the gcd of the coefficients of f viewed as a polynomial in y, we can assume that no irreducible component of X is a vertical line. The closure of each connected component of $X - Sing(X)$ corresponds to an algebraic curve whose equation is an irreducible factor of f; here $Sing()$ denotes the singular locus, which consists at most in a finite number of points of X.

This characterization can be analyzed further using a projection. Let d be the degree of f in y and call π the projection of X on the x-axis. Then, except for a finite number of values Δ, π is d to 1. More precisely, $X - \pi^{-1}(\Delta)$ is a d-covering of the x-axis minus Δ; moreover, X is the union of s connected coverings $X_i - \pi^{-1}(\Delta)$.

For x_0 not in Δ, the fiber $E = \pi^{-1}(x_0)$ consists of d distinct points, partitioned in s subsets $\{E_i\}_{i=1}^{s}$, with E_i lying on $X_i - \pi^{-1}(\Delta)$ for $1 \leq i \leq s$.

* Corresponding author.
E-mail addresses: galligo@unice.fr (A. Galligo), adrien.poteaux@lip6.fr (A. Poteaux).
URLs: http://www-math.unice.fr/~galligo/ (A. Galligo), http://www-salsa.lip6.fr/~poteaux/ (A. Poteaux).

0304-3975/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2010.11.047

1.2. Factorization

Our main motivation is to analyze and develop further factorization algorithms for bivariate polynomials in $\mathbb{C}[x, y]$ that proceed by continuation methods. Factoring multivariate polynomials, either in the exact or approximate setting, is an important problem in computer algebra. Thanks to Bertini's theorem, the bivariate case captures its essential issues. See e.g. [3,12,13] or [6] and their bibliography. The reader can also consider [20] for an history of early algorithms. [1] was the first algorithmic paper using monodromy group action as developed below. The paper [17] considers point combinations, and an exponential search. The papers [31,29,28] discuss another interesting algorithm based on zero-sum identities.

1.3. Continuation or homotopy methods

A continuation method was proposed in [5]; it consists essentially in following a path in X accumulating sufficiently many points on the same connected component, say X_1. An approximate interpolation provides a candidate factor f_1 of f; then an approximate division is performed. Other authors proceed directly to the (parallel) interpolation of all s factors, but this requires to estimate first the correct partition of a fiber E. In the first algorithmic paper using monodromy for factorization [1], one needs to consider a set of representatives for the generators of the fundamental group, which consists of a huge number of transpositions or other permutations.

Our study was initially motivated and inspired by the paper [32], which deals with a more general question of applying homotopy techniques to solve systems of polynomials equations, and contains a way to confirm whether a potential decomposition of the fiber is valid (this is described in [33]). Although the setting was different from ours (exact inputs, approximations with a great precision and with slightly different monodromy actions and loops than the ones considered here) , we borrowed the following important experimental observation which inspired our study: the partition of the fiber E can be recovered from only a small number of permutations of E corresponding to the monodromy action.

As above, denote by X the curve in $\mathbb{C}^2$ defined by $f(x, y) = 0$, by π the projection on the x-axis and choose a generic (i.e. random) fiber $E = \pi^{-1}(a)$ in X which has d points. To simplify the notations, we let $a = 0$. We denote by $\Delta \in \mathbb{C}$ the discriminant locus of π: Δ is the set of roots of the resultant in y of f and its derivative in y f'_y. The action of the fundamental group $\pi_1(\mathbb{C} - \Delta)$ on E defines the monodromy group G, which can be explicitly calculated. When f is irreducible, the orbit of G is the whole fiber E, while when $f = f_1 \cdots f_s$ is composite, the orbits of G provide the s-partition of E by the subsets formed by the roots of the factors f_i. This is the key combinatorial information which allows one to recover the factorization of f via x-adic Hensel lifting. See e.g. [9,33,3]. Monodromy also plays an important role in the factorization algorithms presented in [17,27,32,33,3,4,21].

1.4. A generic model

In [16], the following sub-generic situation was considered (it is the one encountered in several application and benchmark examples): the polynomial to be factored is a product $f = f_1 \cdots f_s$ such that the curves $X_i = f_i^{-1}(0)$ are all smooth and intersect transversely in double points (nodes), and that the projections of the critical points on the x-axis are all distinct. As the X_i are smooth and cut transversely, the discriminant points of f are either simple (turning points of one X_i) or double points (corresponding to projections of intersection points of two components X_i and X_j).

Our aim is to analyze and improve this approach. Here we will also assume that the coefficients of the factors f_i are independent random variables following a uniform (or a reduced normal distribution). As a consequence, with a high probability, $X_i := f_i^{-1}(0)$ will be smooth complex curves intersecting transversely, and f will be monic in y of degree d, hence f_i will be also monic in y.

A main task is to better investigate what happens on a single random Riemann surface. This question has its own interest and deserves to be studied for itself; it is also related to the so-called effective Abel-Jacobi problem and its applications in Physics, see e.g. [35] and [9].

1.5. Organization

The paper is organized as follows. We first present the monodromy action in our particular setting and describe an algorithmic approach and a Maple implementation for its computation (Section 2). We then expose in Section 3 our choices for the implementation of the continuation procedure. In Section 4, classical and recent results on the distribution of the roots of random polynomials which are useful for our purpose are recorded; then, we formulate a conjecture on the distribution of transpositions attached to the set of discriminant points; we also indicate the heuristic reasoning which guided the formulation. In Section 5, we report results on transition to transitivity of subgroups generated by products of transpositions and propose a conjecture directly related to our problem. We present, in Section 6, a methodology and some experiments to support our conjectures and approach of the problem. In Section 7, we report experiments showing the robustness of the studied strategy of factorization with respect to small perturbations of the input data. Section 8 discusses the expected average complexity of our approach. Finally, we conclude by discussing possible extensions of our geometric model.

These results and statements were announced in a presentation [15] at the conference SNC'09.