COMPUTING MONODROMY VIA CONTINUATION METHODS ON RANDOM RIEMANN SURFACES

ANDRÉ GALLIGO AND ADRIEN POTEAUX

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.

Keywords: Bivariate polynomial, Plane curve, Random Riemann surface, Absolute Factorization, Algebraic Geometry, Continuation methods, Monodromy, Symmetric group, Algorithms, Maple Code.

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 $1 \leq i \leq s$.

1.2. **Factorization.** Our main motivation is to analyze and develop further factorization algorithms for bivariate polynomials in $\mathbb{C}[x, y]$, which proceed

Date: November 2, 2010.

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. [CG05], [Gao03, GKM$^+$04] or [CL07] and their bibliography. The reader can also consider [Kal00] for an history of early algorithms. [BCGW93] was the first algorithmic paper using monodromy group action as developed below. The paper [GW97] considers point combinations, and an exponential search. The papers [SSH92, SS93a, Sas01] discuss another interesting algorithm based on zero-sum identities.

1.3. **Continuation or homotopy methods.** A continuation method was proposed in [CGvH$^+$01]; 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 [BCGW93], 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 [SVW01], 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 [SVW02]). Although the setting was different than 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. [DvH01, SVW02, CG05]. Monodromy also plays an important role in the factorization algorithms presented in [GW97, Rup00, SVW01, SVW02, CG05, CG06, LS09].

1.4. **A generic model.** In [GvH07], 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 $f = f_1 ... f_s$ 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. [TT84] and [DvH01].

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 on potential extensions of our geometric model.

These results and statements were announced in a presentation [GP09] at the conference SNC'09.

2. Computation of Monodromy generators

In this section, we keep the previous notations and describe algorithmically our main tool, the monodromy group with respect to the projection on the $x-$axis, its representation and its calculation. A previous implementation can be found in the package `algcurves` of Maple (see also [DvH01]), that our work aims to improve.

2.1. **Our setting.** The discriminant locus Δ of f is defined as the zero-set of $\mathrm{Res}_y(f, f'_y)$; it contains simple points, which are the projections of turning points of X - i.e. points with a vertical tangent, and multiple points, which are projections of the singularities of X. In other words, these are the solutions of the system $f = f'_y = f'_x = 0$. Multiplicity also appears when two (or more) turning points have the same projection (this does not happen in the generic case).

To define the monodromy, first select a base point $x = a$ e.g. $a = 0$ in the complex x-axis (considered as a real plane) minus the discriminant locus. Let E be the fiber of π above 0 (i.e. the d distinct y-values for which $f(0, y) = 0$). These y-values are now assigned an order, $(y_1, y_2, \ldots, y_d)$. This ordering of the d y-values labels the d sheets of the covering $X - \pi^{-1}(\Delta)$ of $\mathbb{C} - \Delta$.

For each point $\alpha \in \Delta$, one chooses a path γ_α in the complex x-plane which starts and ends at $x = 0$, encircles only $x = \alpha$ (counterclockwise) and avoids all points of Δ. The d-tuple $(y_1, y_2, \ldots, y_d)$ is then analytically continued around this path γ_α. When one returns to $x = 0$, a new d-tuple is found, which has the same entries as $(y_1, y_2, \ldots, y_d)$, but ordered differently: $(y_{\sigma_\alpha(1)}, y_{\sigma_\alpha(2)}, \ldots, y_{\sigma_\alpha(d)})$, where σ_α is a permutation acting on the set of labels $\{1, 2, \ldots, d\}$. We will say that the permutation σ_α is attached to the path γ_α. Note that for the same α but different choices of γ_α, we may obtain different permutations: for instance, on picture 1, we have $\gamma_3 = \gamma_1^{-1} \circ \gamma_2 \circ \gamma_1$, which leads, for the associated permutations, $\sigma_3 = \sigma_1^{-1} \circ \sigma_2 \circ \sigma_1 \neq \sigma_2$.

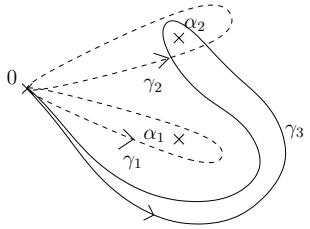


FIGURE 1. Different paths leads to different permutations

Here are some typical situations. If $x = \alpha$ is a simple point of Δ, hence the projection of a unique turning point of X, then σ_α is a transposition. If $x = \alpha$ is the projection of a double point (a node), then σ_α is the identity. If $x = \alpha$ is the projection of a cusp singularity then σ_α is the cyclic permutation of order 3. In our simple generic model, we will encounter only the two first cases.

Our investigation on the monodromy actions on a random Riemann surface includes Maple experimentations, observations and statistical distributions of the transpositions and permutations associated to the $d(d-1)$ critical points of such a complex curve. Already for $d = 10$ that means considering 90 discriminant points and organizing 90 paths in a limited portion of the complex plane; the Maple package `algcurves[monodromy]` described in [DvH01], which is satisfactory for rather small examples, is not sufficient for that task. So we had to rely on another program for our developments. Let us be more specific on the difficulties we encountered trying to use `algcurves[monodromy]` in our setting. In order to see how fibers are permuted, we have to follow paths homotopic to the ones showed in Figure 2. Unfortunately, for a large number of discriminant points, some paths automatically generated by the Maple command `algcurves[monodromy]`, with option `showpaths`, are not correct: for random polynomials of degree 10, it happens that they cross each other when they should not do so (see [DvH01, section 3.5]).

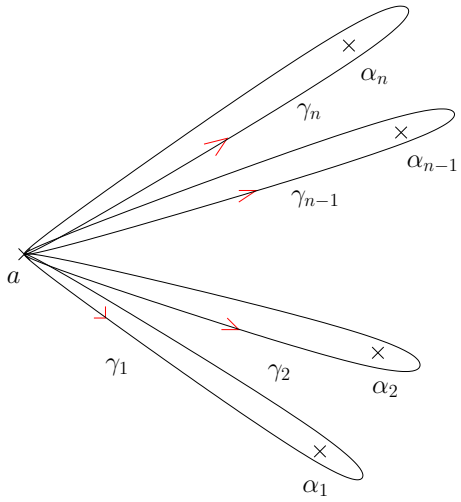


FIGURE 2. Paths encircling one point of the discriminant

To avoid this kind of bad behavior, we rely on algorithms described in the second author's thesis [Pot08, section 3.4.4] to compute the paths to be followed. We now briefly describe it, and also recall the main points of our monodromy computation strategy.

2.2. **Description of our monodromy algorithm.** This section will summarize our strategy to compute monodromy groups, it was first presented in [Pot07], and more details were provided in [Pot08].

Our method is of type "compute fibers and connect". For each path γ_i we want to follow, we take successive intermediary points on the loop, compute fibers above these points, and finally connect the successive fibers one to one in order to get the permutation σ_i generated by the path γ_i on the initial fiber. Two important features of our strategy are a minimization of the total path length and an elaborated use of truncated series expansions. The main steps of our program are:

(1) Compute the set of roots α_i of $\mathrm{Res}_y(f, f'_y)$.
(2) Construct paths in the complex x-plane homotopic to the γ_i of figure 2
(3) Choose intermediary points along these paths, and connect the successive fibers of each path one to one to get the monodromy.

We will now detail our strategy for the two last points.

2.2.1. *Choice of the paths.* To minimize the total path length, we first compute an Euclidean minimal spanning tree $\mathcal{T}$, and then create paths γ'_i following this tree and homotopic to the paths γ_i of figure 2 in $\mathbb{C}\backslash\{\alpha_1, \cdots, \alpha_n\}$. On first appearance, creating such paths may seem an easy task, but there are a lot of situations which are complicated, and need to be worked out to obtain a correct algorithm. For instance a claim of the second author in Proposition 3 of [Pot07] is not fully correct: one can create counter examples. To resolve the matter, an algorithm which computes the needed paths was developed in [Pot08, section 3.4.4]; let us briefly summarize it.

According to our connection method (see below), we want to use *paths in the tree* γ'_i, i.e. paths which are constituted only of segments of $\mathcal{T}$ and arcs of circles centered on a critical point α_k which link two connected edges of the tree $\mathcal{T}$ (see [Pot07, section 3.1] for more details). Thus, our aim is to know which sequence of oriented edges of $\mathcal{T}$ and oriented circles we have to follow in order to go around each critical point. The approach we give in [Pot08, section 3.4.4] is of type "divide and conquer". We will explain it with the help of figure 3 below, so the reader can easily follow the procedure.

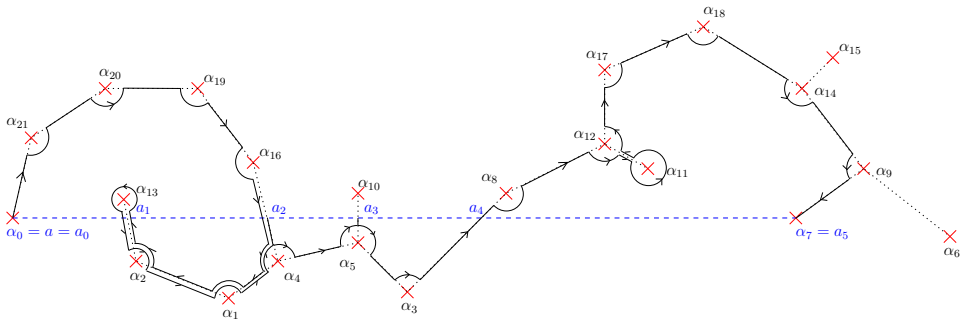


FIGURE 3. Path in the tree homotopic to $[a, \alpha_7]$ in $\mathbb{C}\backslash\{\alpha_1, \cdots, \alpha_n\}$

Considering the path γ_l, we search a path which is homotopic to $[a, \alpha_l]$ in $\mathbb{C}\backslash\{\alpha_1, \cdots, \alpha_n\}$.

- Let $a_0 = a, a_1, \cdots, a_{s-1}, a_s$ denote the successive intersection points between $[a, \alpha_l]$ and $\mathcal{T}$, ordered according to their appearance on the path $t\alpha_l + (1-t)a$. We will find paths homotopic to each segment $[a_i, a_{i+1}]$, and then connect end to end each of these paths.
- As the segment $[a_i, a_{i+1}]$ does not cross the tree, we must circle each critical point encountered by going in the same direction. This orientation can be guessed by counting the number of intersection between any half line starting at a point of $]a_i, a_{i+1}[$ and τ_i, the unique sequence of edges of $\mathcal{T}$ leading from a_i to a_{i+1}.
- Finally, we find the path in the tree homotopic to $[a_i, a_{i+1}]$ by following the tree from a_i to a_{i+1} according to the computed orientation, and never crossing the tree. This requires to know at each critical point α_k a permutation indicating the orientation of the edge connected to α_k. This can lead to a path with more edges than τ_i (see figure 3 between a_4 and a_5 for instance).

Several special cases need also to be analyzed further; by lack of space here, we do not explicitly describe them but they are all given in [Pot08].

2.2.2. *Connection method.* To connect the successive fibers of the path, we use truncated series expansions at controlled order and Puiseux expansions above critical points: the analytic continuation along one arc of circle around α_k of the path is given by evaluating the truncated Puiseux expansions above α_k in the two intermediary points defining the arc. Two intermediary points of a same edge are connected by using truncated Taylor series, introducing more intermediary points if needed. A good trade-off is worked out between

the number of intermediary points and the truncation orders involved. As computing Puiseux expansions can be costly, we use a modular-numeric algorithm. It was first described in [Pot07] and improved in [Pot08] (the modular part of the algorithm is also described in [PR08, PRb, PRa]). All details of our monodromy algorithm can be found in [Pot07] and [Pot08].

3. Description of analytic continuations

3.1. **Analytic Continuation Process.** Following [DvH01, section 3.6], we perform analytic continuation using first derivative order. From our combinatorial analysis (see section 5), we plan to use this process along about $2 \ln d$ paths, each one containing at least d points of Δ. For instance, for a polynomial f of degree 20, we will use 5 paths, each of them starting at 0, going to one point of the circle $C(0, 2)$, following this circle for an angle of $\frac{\pi}{3}$, and coming back to 0. See figure 4.

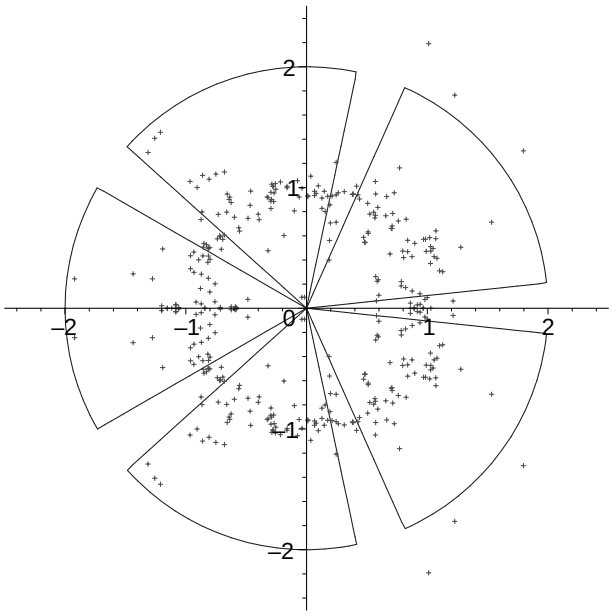
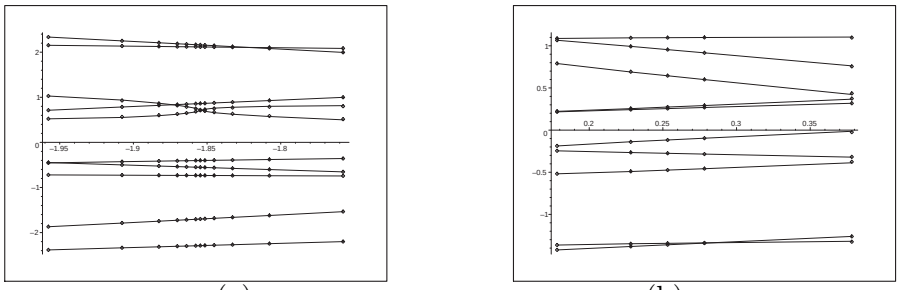


Figure 4. Paths and discriminant points for a curve of degree 20, defined by a dense polynomial with random integer coefficients between −100 and 100.

Our Maple algorithm to make an analytic continuation along each path γ uses the following scheme: starting from the fiber at a point x_k of γ, we approximate the fiber at the next point x_{k+1} using the first order Taylor expansion at x_k. Then, if this approximation is close enough to the fiber at x_{k+1}, we connect each approximation to its nearest point of the fiber. Otherwise, we use one more intermediary point between x_k and x_{k+1}.

The average complexity issues are discussed in section 8.

3.2. **Passing close to a critical point.** In our case, since we are studying random Riemann surfaces, the critical points we will encounter are turning points. If we consider the product of two such curves, we may also encounter intersection points. As the geometry of these two types of points



(a) (b)

FIGURE 5. Intermediary steps for (a) a turning point (b) an intersection point.

are different, we made experiments to get information on the behavior of our analytic continuation process; practical observations confirmed our natural intuition. The two pictures of figure 5 illustrate our observations: here we consider a polynomial F defined as the product of two random polynomials F_1 and F_2. Figure 5a represents the analytic continuation process along a path which is close to a root of $\mathrm{Res}_y(F_1, F'_{1y})$, whereas figure 5b represents the same for a root of $\mathrm{Res}_y(F_1, F_2)$. On these two pictures, we only represent the real parts of the complex numbers involved; points represent the computed fibers, whereas lines indicate the interpolated curve obtained by our approximations.

These pictures illustrate that the analytic continuation needs more steps when following a path who goes around a turning point than when it goes close to an intersection point.

3.3. **First derivative versus second derivative.** To improve the analytic continuation process, it could seem better to use more than the first derivative to predict the next fiber of the path. For instance, one may precompute the second derivative and get a better approximation in order to use less intermediary points. Unfortunately, in our experiments the number of intermediary points did not decrease significantly, whereas the time spent to evaluate the second derivative is sizeable when the degree increases. This is shown in the following table (the indicated times are total computing times for the analytic continuation along 3 loops for each polynomial, using respectively one or two derivatives in the analytic continuation process; we note however that our algorithm is a prototype and does not use fast algorithms).

degree	first derivative	two first derivatives
10	10.2 s	12.7 s
20	97 s	105 s
30	1046 s	1233 s
40	1100 s	1850 s

4. Distribution of critical points

In this section we study the distribution of critical points of a random Riemann surface X, with respect to the projection on the $x-$axis. This information will be used to formulate a conjecture on the limit distribution

of the sequence of transpositions attached to the ordered set of discriminant points of X.

4.1. **Distribution of roots of random polynomials.** Roots of random univariate polynomials have been studied by many authors, important results were achieved, e.g. by Kac [Kac48], Edelman-Kostan [EK95] in the real case, or by Erdos-Turan [ET50] in the complex case.

This was generalized by Shub-Smale [SS93b] and their coworkers, to the multivariate real case, by Zelditch-Schiffmann [SZ04] and their coworkers, and also by Bilu [Bil97] in the complex case. Let us also quote a recent joint work of the first author with C. d'Andrea and M. Sombra [DGS] which focused on effective bounds.

These results roughly say:

Fact 1. *Let g be a degree d univariate polynomial in $\mathbb{C}[x]$ and denote by M some measure of the size of its coefficients. When d goes to infinity, if $M = o(d)$, then the roots of g concentrate uniformly on the unit circle of $\mathbb{C}$.*

and

Fact 2. *For a bivariate polynomial $g(x, y)$, under the same kind of limited growth condition of the coefficients of g, it also holds for the discriminant of f in that its roots concentrate uniformly on the unit circle of $\mathbb{C}$.*
Moreover the critical points of g, with respect to the x-projection, concentrate uniformly on the product of the two unit circles in $\mathbb{C}^2$.

Now let us introduce some notation to be more precise.

Let

$$g(x) = a_0 + \cdots + a_d x^d = a_d(x - \rho_1 \,\mathrm{e}^{\mathrm{i}\,\theta_1}) \cdots (x - \rho_d \,\mathrm{e}^{\mathrm{i}\,\theta_d}) \in \mathbb{C}[x]$$

for some $a_i \in \mathbb{C}$ with $a_0 a_d \neq 0$, $\rho_i > 0$ and $0 \leq \theta_i < 2\pi$. The *angle discrepancy of g* is defined as

$$\Delta_{\mathrm{a}}(g) := \sup_{0 \leq \alpha < \beta < 2\pi} \left| \frac{\#\{i : \alpha \leq \theta_i < \beta\}}{d} - \frac{\alpha - \beta}{2\pi} \right|$$

where $\#$ is the cardinality of a set. For $0 < \varepsilon < 1$, the *radius discrepancy of g* is

$$\Delta_{\mathrm{r}}(g; \varepsilon) := \frac{1}{d} \#\Big\{ i : 1 - \varepsilon < \rho_i < \frac{1}{1 - \varepsilon} \Big\}.$$

Set $|g| := \sup\{|g(z)| : z \in \mathbb{C}, |z| = 1\}$.

Theorem 1 (Erdos-Turan [ET50])**.** *Let $g(x) = a_0 + \cdots + a_d x^d \in \mathbb{C}[x]$ with $a_0 a_d \neq 0$, then for $0 < \varepsilon < 1$*

$$(1) \quad \Delta_{\mathrm{a}}(g) \leq 16 \sqrt{\frac{1}{d} \log\left(\frac{|g|}{\sqrt{a_0 a_d}} \right)} \quad , \quad 1 - \Delta_{\mathrm{r}}(g; \varepsilon) \leq \frac{2}{\varepsilon d} \log\left(\frac{|g|}{\sqrt{a_0 a_d}} \right).$$

The hardest part is the estimate for the angle discrepancy. The estimate for the radius distribution was found by H.P. Hughes and A. Nikeghbali [HN08] and is a simple consequence of Jensen's formula.

Figure 6 is an illustration, with a random polynomial of degree 200 obtained calling the Maple function `randpoly(x,degree=200,dense)`. In that

case, the (integer) coefficients are chosen uniformly between $-N$ and N for a fixed N. One can also make a polynomial with random complex coefficients but the result is similar.

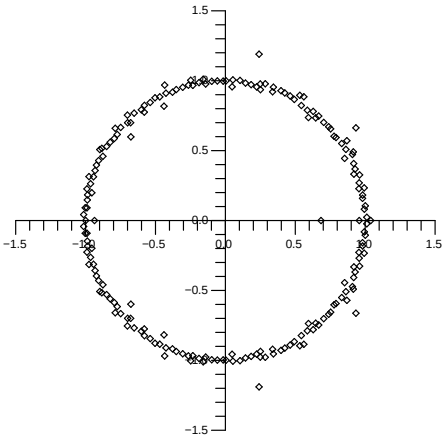


FIGURE 6. Roots of a random polynomial of degree 200

For the multivariate case we quote [DGS]. Let $N(-)$ denote the Newton polytope, $MV(-)$ the mixed volume and $V(-)$ the set of roots. For a system of polynomials $\mathbf{g} = (g_1, \ldots, g_n)$ in $\mathbb{Z}[x_1, \ldots, x_n]$ and $0 < \varepsilon < 1$, we define the *radius discrepancy* as

$$\Delta_{\mathrm{r}}(\mathbf{g}; \varepsilon) := \frac{\#\{\xi \in V(\mathbf{g}) : 1 - \varepsilon < |\xi_i| < \frac{1}{1-\varepsilon} \text{ for all } i\}}{\#V(\mathbf{g})},$$

where as usual the ξ's are counted with their corresponding multiplicity.

For $1 \leq j \leq n$ we consider a standard projection $\pi_j : \mathbb{R}^n \to \mathbb{R}^{n-1}$, with $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$, and we assume the following technical condition: $\{\pi_j(\mathrm{N}(g_k))\}_{k \neq j}$ is essential for $j = 1, \ldots, n$ (this is satisfied in our setting). Then we have the two following theorems:

Theorem 2 ([DGS])**.** *For $1 \leq i \leq n$ let $g_i \in \mathbb{Z}[x_1, \ldots, x_n]$ such that*

$$\#V(g_1, \ldots, g_n) = \mathrm{MV}_n(\mathrm{N}(g_1), \ldots, \mathrm{N}(g_n)) \geq 1.$$

Then for $1 > \varepsilon > 0$

$$1 - \Delta_{\mathrm{r}}(\mathbf{g}; \varepsilon) \leq \frac{\mathbf{2}}{\varepsilon} \sum_{\mathbf{i,j=1}}^{\mathbf{n}} \frac{\mathrm{MV}_{\mathbf{n-1}}\left(\pi_{\mathbf{j}}(\mathrm{N}(\mathbf{g_k})) : \mathbf{k} \neq \mathbf{i}\right)}{\mathrm{MV}_{\mathbf{n}}(\mathrm{N}(\mathbf{g_1}), \ldots, \mathrm{N}(\mathbf{g_n}))} \log |\mathbf{g_i}|.$$

Theorem 3 ([DGS])**.** *Let $Q_1, \ldots, Q_n \subset \mathbb{R}^n$ be a family of convex integral polytopes such that $\mathrm{MV}_n(Q_1, \ldots, Q_n) \geq 1$. Let $\lambda : \mathbb{N} \to \mathbb{N}^n$ such that $\lim_{m \to \infty} \lambda(m) = \infty$, and, for each $m \geq 1$, let $g_{m,1}, \ldots, g_{m,n} \in \mathbb{Z}[x_1, \ldots, x_n]$ be a system of polynomials such that $\mathrm{N}(g_{m,k}) \subset \lambda_k(m) Q_k$,*

$$\#V\left(g_{m,1}, \ldots, g_{m,n}\right) = \left(\prod_{k=1}^{n} \lambda(m)_k\right) \cdot \mathrm{MV}_n(Q_1, \ldots, Q_n)$$

and $\log|g_{m,k}| = o(\lambda(m)_k)$. *Then, for any* $0 \leq \alpha_j < \beta_j < 2\pi$, $j = 1, \ldots, n$, *we have:*

$$\lim_{m\to\infty} \frac{\#\Big\{k : \alpha_j \leq \theta_{k,j} < \beta_j \,\forall j = 1, \ldots, n\Big\}}{\#V\big(g_{m,1}, \ldots, g_{m,n}\big)} = \frac{\prod_{j=1}^{n}(\beta_j - \alpha_j)}{(2\pi)^n}. \tag{2}$$

Figure 4 provides an illustration in Maple for the discriminant locus of a random bivariate polynomial of degree 20.

4.2. **A challenging problem.** An ambitious problem is to describe, when d goes to infinity, the asymptotic distribution in the symmetric group S_d of the $d(d-1)$ transpositions associated to the $d(d-1)$ turning points of a random Riemann surface X defined by a polynomial f(x,y) with random uniform coefficients.

In this paper we do not aim to solve this question, but to provide insights and prepare a further treatment of the subject. We will relate it to other results and auxiliary constructions, explain our intuition, and develop code in order to proceed to preliminary experiments and observations; then we will formulate two conjectures.

4.3. **A construction relying on critical points and transpositions.** As recalled above, when d goes to infinity, the critical points of f concentrate uniformly on the torus, equal to the product of unit circles, which is parametrized by two angles ϕ and ψ modulo 2π: the arguments of (x, y) in $\mathbb{C}^2$.

We divide the complex $x-$axis, considered as a real plane, into $d-1$ sectors of equal angles $2\pi/d - 1$; this gives a number of sectors about the square root of the number of points of the discriminant. Then, as a consequence of the results on the distribution of roots, there are about d discriminant points in each such sector. The corresponding critical points have a distribution of arguments of $y-$coordinates which tends to become uniform as d increases. Moreover, by the radius discrepancy results, most (and at least half) of the critical points are in a thin annulus around the torus for a large enough d. Call A this subset of critical points and A_1 its projection on the $x-$axis. A_1 is a subset of the discriminant locus lying in a thin annulus around the unit circle and containing most of the discriminant points.

We now order the elements of A_1 by increasing argument; therefore the corresponding critical points are also ordered. Then we join the consecutive points of A_1 (with respect to this ordering) and obtain a continuous real curve C homeomorphic to the unit circle.

As above, we denote by π the projection of the random Riemann surface X onto the x-axis (viewed as a real plane). We also order by increasing argument the d distinct points of the fiber of π above any point of C which is not a discriminant point.

The real curve $B_1 := \pi^{-1}(C)$ can be viewed as a "branched" braid in $\mathbb{C}^2 = \mathbb{R}^4$. Its branching points are critical points of X. Because of the radius discrepancy results, it lies near the product of the two unit circles, i.e. a torus, denoted by T.

Projecting the braid B_1 on the torus T, we obtain a new braid B lying on the torus having *a priori* more branching points. In order to draw a plane representation of that braid, we represent the two unit circles by two segments $(0, 2\pi)$ with identified extremities. Figure 7 is a sketch of a portion of such a B with 3 branching points.

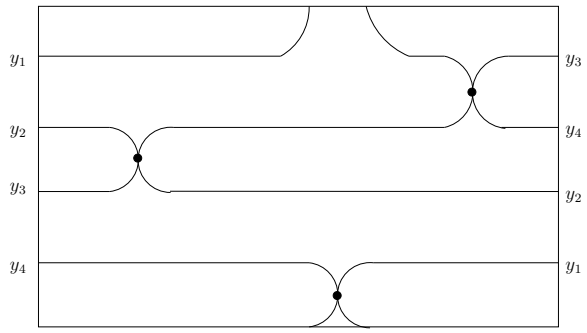


FIGURE 7. A portion of a branched braid

4.4. **Heuristics.**

Claim 1. *The number of additional branching points (created by the projection of B_1 on T) is small.*

The intuitions motivating this claim are the following : geometrically, this expectation is related to the proximity of the braid B_1 to the torus T; algebraically this could be analyzed as a small number of real solutions of some system of polynomial equations with bounded degrees and coefficients.

The interest of such a claim is that the branching points of B exchange consecutive points of the fibers of π (ordered by the argument of their second coordinate y), as shown on Figure 7, because B lies on a 2-dimensional torus.

So the claim would imply that most points of A_1, i.e. projection on the $x-$axis of branching points of B_1, are branching points of B; hence correspond to exchange of consecutive points of the fibers of π. In other words, most points of A, i.e. projection on the $x-$axis of points of A_1, are attached to neighbor transpositions $(i, i+1)$, with the natural identification $d+1 = 1$.

Moreover, the index i should also be uniformly distributed. Indeed, by our previous result, the projections on the torus of the critical points of the Riemann surface tend to be uniformly distributed; hence, the arguments of the second coordinate y (which correspond to the index i) tend to be uniformly distributed.

4.5. **First conjecture.** We formulate the following conjecture, based on the previous construction and heuristic reasoning:

Conjecture 1. *The limit distribution of the sequence of transpositions attached to the discriminant points of f (ordered by increased arguments) is that of uniformly distributed consecutive pairs $(i, i+1)$ in S_d, (with $d+1 = 1$).*

Note that this claim is asymptotic; and we only checked on examples a weak form of this conjecture.
For small and medium values of d, one should restrict the sequence to the discriminant points very near to the unit circle and expect a combination (a blending) between the uniform transpositions distribution and the uniform neighbor transpositions distribution. In that case, the distribution with the slowest transition (here the neighbor transpositions) bounds the time needed to reach transitivity (with a high probability).

5. Groups generated by random products of transpositions

5.1. **Statistics on the symmetric group.** In a recent joint work of the first author with L. Miclo [GM] was investigated the transition to transitivity of subgroups of the symmetric group S_d generated by K products of n transpositions as d tends to infinity. More precisely, two events were considered: "the subgroup is transitive", this means that the only orbit is the whole set $\{1, ..., d\}$ and a weaker event "the subgroup has no fixed point". When n increases, the second event happens "just" before and is easier to analyze.

Sharp transitions and so-called cut-off phenomena (see [Dia96]) have been proved in the case of transpositions (i, j) where i and j are uniformly chosen among the integers $[1..d]$ at "time" $n = \frac{d \ln(d)}{2K}$. The number of transpositions in a product is viewed as a number of time steps in a process.

The case of uniformly distributed neighbor transpositions $(i, i + 1)$ was also considered both theoretically and experimentally. However, only results on the weaker event "the subgroup has no fixed point" were proved with a sharp transition at "time" $n = \alpha d$ for $K = \beta \ln(d)$, where α and β are related via an invertible function $\beta(\alpha) = \int_0^1 exp(-2\alpha(1 - \cos(2\pi s))ds$, e.g. when $\beta = 2$ then approximately $\alpha = 0.3$. Hence the transition to the non existence of fixed points occurs about time $n = 0.3\, d$ for a subgroup generated by $K = 2\, \ln(d)$ products. The simulations indicate that the transition to transitivity appears approximately at twice this time, i.e. about time $n = 0.6\, d$

Several experiments were performed with the computer algebra system Maple, using the package `group` which provides facilities to represent permutations, compute products of permutations, generate subgroups and compute orbits. Maple also has a command `rand(1..d)()` which allows to produce sequences of integers between 1 and d almost following a uniform distribution. The average values of 100 (independent) runs were taken as an empirical estimation of the targeted probability. Figure 8 pictures interpolating probability curves with the number n of transpositions in the products in the abscissa (but renormalized with the unit equal to $0.3d$). The

two (almost coinciding) leftmost curves correspond to products of uniform transpositions and express that the transitions of the two events happen almost simultaneously. The two rightmost curves correspond to products of uniform neighbor transpositions. The rightmost curve corresponds to the transition to transitivity of products of neighbor transpositions; we remark that with respect to the other 3 curves a factor 2 in the abscissa shows up. Note that the figure indicates that for $n \geq d$ the empirical probability to get a transitive subgroup is greater than 0.95. The (asymptotic) behavior of the 3 curves at the left side is well understood and predicted by theorems. This is not yet the case for the rightmost curve.

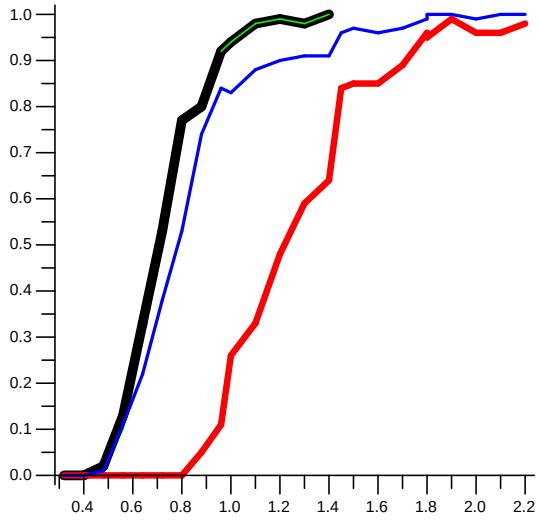


FIGURE 8. *Transitions for uniform and neighbor transpositions.*

So we formulate the following conjecture.

Conjecture 2. *As d tends to infinity, there is a sharp transition to transitivity of the subgroups of S_d generated by $K = 2\ln(d)$ products at "time" about $O(d)$ uniform neighbor transpositions $(i, i+1)$, with $d+1 = 1$.*

Let us note that in [GM], subgroups generated by a smaller number K of products of consecutive pairs were also considered: they present a slower transition to transitivity, at time n of the order of $d^{(1+2/K)}$. E.g. for $d = 50$, the simulations show that if $K = 4$, then for $n > 200$ one obtains a transitive subgroup with a probability almost equal to 1.

Finally, we remark that these transitions are observable via continuation methods as indicated below and that these considerations could be useful for the aimed factorization strategy.

5.2. **Estimated monodromy via K large loops.** Consider a large loop Γ on the x-axis (considered as a real plane) starting and ending at 0, and

encircling n discriminant points of f. Γ is homotopic to the concatenation of n loops γ_l, each encircling a discriminant point. The n discriminant points are ordered by increasing argument, therefore the permutation p_Γ attached to Γ is the product of the n transpositions attached to the γ_l.

Now, we define Γ to be formed by two rays starting and ending at 0 and by a portion of a circle of radius 2 encompassing an angle $\frac{2\pi}{m}$. So we can expect that Γ encircles about $\frac{d(d-1)}{m}$ discriminant points of f. The important observation is that we do not need to compute explicitly those points.

Then, if the previous conjectures are correct, the permutation p_Γ is the product of about $\frac{d(d-1)}{m}$ transpositions; moreover, we can also assume that these transpositions are uniformly distributed, in the sense described above.

Finally, we choose K and $n = \frac{d(d-1)}{m}$ as indicated in the previous subsection (i.e. K about $2\ln(d)$ and m bigger than K but smaller than d). Then we consider K such large loops Γ_k with $k = 1 \cdots K$, the K attached permutations p_k, and the subgroup G generated by these K permutations.

Putting together the two conjectures, we get the following corollary:

Corollary 1 (of the two conjectures)**.** *G is a transitive subgroup of the symmetric group.*

Example: For $d = 50$, $\ln(d)$ is about 4, so we can choose $K = 8$ and n about 125, i.e. the angles of the Γ_k are at least $(2\pi)/20$ (hence rather small). But as we remarked above, we can also choose a smaller K, here for $d = 50$, we can choose $K = 4$ and n about 300, i.e. the angles of the Γ_k should be about $(2\pi)/6$.

6. Experiments and Examples

6.1. **Methodology to test conjecture 1.** In order to check experimentally the validity of our first conjecture, we cannot follow precisely the procedure we described in our sketched proof; we need to adapt it to the actual possibility of our prototype implementation. What we did was to check a weaker claim: when passing from one discriminant point to a close one (in the sense of the Euclidean distance), only nearby points (in the sense of the Euclidean distance) of the fiber are exchanged. We observed in our examples that this happens very frequently and in general the exchange does not involve the points of the fiber which were just exchanged.

We consider examples of degrees from 7 to 10 whose complex coefficients are randomly generated using the Maple command `rand(-100,100)()` and performed on them the complete analysis. The corresponding data are provided on the second author's website.

As we cannot reproduce here voluminous data, we will only present the first coefficients of the polynomial and the first three elements in the list of the 42 corresponding discriminants points and fibers above them.

$F := (43+28I)x^2y^3+(9-62I)x^2y+(97-24I)x^2y^2+(-83+79I)x^4y^2+(39-82I)xy^4+94x+(-45+70I)x^4y+(90+67I)xy^3+(96-74I)x^5y+(-11+61I)x^4y^3+\cdots$

The random command in Maple produces integers, but this is generic enough to illustrate significant generic behavior, since the sample space already contains about 10 000 elements.

Here are some discriminant points and the corresponding fibers with their double points

-1.173 - 0.2706 I	-1.077 - 0.2767 I	-0.9366 - 0.4639 I
-1.121- 0.1015 I	-1.043 - 0.064 I	-0.2625 + 0.885 I
-0.3743 + 1.147 I	-0.322 + 1.081 I	0.1326 - 2.336 I
-0.2701 - 3.039 I	-0.272 - 2.813 I	0.38 - 1.489 I
-0.1134 - 1.086 I	0.7956 - 0.406 I	0.73 + 1.485 I
1.053 + 1.524 I	0.973 + 1.461 I	0.9217 - 0.349 I
0.6184 - 0.4864 I	0.1362 - 0.8096 I	-0.599 - 0.1382 I
0.6184 - 0.4864 I	0.1362 - 0.8096 I	-0.599 - 0.1383 I

It is hard to see the continuation just from these data, but even in this very simple low degree example the branching does not connect far away points. Of course, as our experimentations are using low degrees examples, these observations deserve a much more extensive study to be experimentally confirmed.

6.2. **Large loops.** Here, we can take random polynomials of higher degrees, since we do not perform anymore the complete analysis but only computations of few permutations via analytic continuations along large loops.

Consider a degree 20 random polynomial: it has 380 discriminant points depicted in Figure 4; they are essentially contained in an annulus around the unit circle. We also consider the 5 large loops Γ_k, $k = 1 \cdots 5$, each of them encircles an angle of $\frac{\Pi}{3}$ and hence contains about a sixth of the 380 discriminant points i.e. about $60 = 3.d$ of these points (see figure 4). Following our conjectures, we expect that the corresponding 5 permutations generate a transitive group. This is indeed the case.

7. Application to factorization

We also tested our approach with the following strategy for computing an absolute factorization of a polynomial $P \in \mathbb{Q}[x, y]$ of degree d which is a product of random polynomials.

(1) Compute (approximately) the roots $y_1, ..., y_n$ of $P(0, y)$,
(2) Determine the partition of $\{y_1, ..., y_n\}$ to be induced by the factorization of P, here it is given by the orbits of the estimated generators.
(3) Form the univariate factorization $P(0, y) = Q_1(y)...Q_s(y)$.
(4) Perform Hensel liftings, with respect to x, to find the factors.

7.1. **Maple computations.** We present the sequence of Maple command lines we used, the reader can find the file `analyticcontinuation.mpl` on the second author's website:

We begin with the product of two random polynomials of degree 10:

```
> read "analyticcontinuation.mpl":
> r:=rand(-100..100):
> c:=proc() r()+r()*I end:
> F1:=randpoly([x,y],'dense',degree=10,coeffs=c):
> F2:=randpoly([x,y],'dense',degree=10,coeffs=c):
> F:=expand(F1*F2):
> res:=allturns(F,x,y):
```

```
// make the analytic continuation
> G:=groupe(res):
// define the group generated by the 3 permutations
> group[orbit](G,1);
           {1, 3, 4, 6, 7, 9, 11, 14, 16, 18}
> group[orbit](G,2);
         {2, 5, 8, 10, 12, 13, 15, 17, 19, 20}
```

We have the same behavior when we increase the degree:

```
> F1:=randpoly([x,y],'dense',degree=20,coeffs=c):
> F2:=randpoly([x,y],'dense',degree=20,coeffs=c):
> F:=expand(F1*F2):
> G:=groupe(allturns(F,x,y)):
> group[orbit](G,1);
{1, 3, 4, 5, 7, 8, 10, 12, 13, 19, 20, 21, 25,
 26, 30, 32, 33, 36, 37, 40}
> group[orbit](G,2);
{2, 6, 9, 11, 14, 15, 16, 17, 18, 22, 23, 24,
 27, 28, 29, 31, 34, 35, 38, 39}
```

Finally, our algorithm can recover several small factors:

```
> F1:=randpoly([x,y],'dense',degree=2,coeffs=c):
> F2:=randpoly([x,y],'dense',degree=3,coeffs=c):
> F3:=randpoly([x,y],'dense',degree=4,coeffs=c):
> F4:=randpoly([x,y],'dense',degree=5,coeffs=c):
> F5:=randpoly([x,y],'dense',degree=6,coeffs=c):
> F:=expand(F1*F2*F3*F4*F5):
> G:=groupe(allturns(F,x,y)):
> group[orbit](G,1);
     {1, 11, 16, 19, 20}
> group[orbit](G,2);
       {2, 6, 10, 17}
> group[orbit](G,3);
    {3, 5, 8, 9, 12, 13}
> group[orbit](G,4);
         {4, 15}
> group[orbit](G,7);
       {7, 14, 18}
```

In these three examples, we only used 3 loops, each of them making an angle of $\frac{\Pi}{3}$.

7.2. **Approximate coefficients.** If the data are given within some approximation, our approach still applies to get the elements of the fiber which belongs to the same factor. This good behavior is not a surprise as we are in a generic (random) setting; it is illustrated by the following examples.

We consider several polynomials of degree 20, defined as the product of 2 to 5 random polynomials, to which we add another random polynomial representing noise: it is the sum of 4 random monomials with small coefficients. In table 1, we indicate, for each approximate polynomial considered,

Exact factors involved	Size of coefficients	Results
2 factors of degree 10	10^4	ϵ Factors found 10^{-1} 10 & 10 10^0 20
3 factors of degree 7, 7 and 6	10^3	ϵ Factors found 10^{-2} 7 & 7 & 6 10^{-1} 14 & 6 10^0 20
4 factors of degree 3, 4, 6 and 7	10^4	ϵ Factors found 10^1 7 & 6 & 4 & 3 10^2 17 & 3 10^3 20
5 factors of degree 2, 3, 4, 5 and 6	10^5	ϵ Factors found 10^0 6 & 5 & 4 & 3 & 2 10^1 9 & 6 & 5 10^2 15 & 5 10^3 20

TABLE 1. Factoring approximate polynomials

Exact factors involved	Size of coefficients	Results
2 factors of degree 14 and 6	10^4	ϵ Factors found 10^{-2} 14 & 6 10^{-1} 20
3 factors of degree 7, 7 and 6	10^3	ϵ Factors found 10^{-3} 7 & 7 & 6 10^{-2} 13 & 7 10^{-1} 20
4 factors of degree 3, 4, 6 and 7	10^4	ϵ Factors found 10^{-3} 7 & 6 & 4 & 3 10^{-2} 13 & 7 10^{-1} 20
5 factors of degree 2, 3, 4, 5 and 6	10^5	ϵ Factors found 10^{-1} 6 & 5 & 4 & 3 & 2 10^0 13 & 5 & 2 10^1 20

TABLE 2. Factoring dense noised polynomials

the size ϵ of the coefficient of the polynomial representing the noise, and the number (and degrees) of factors found by our algorithm.

In table 2, we consider dense noised polynomials: we perturbed each coefficient of the polynomial F.

As expected, our algorithm can detect perturbed factors. This good behavior is promising but it needs to be studied and evaluated further, depending on the perturbation. This will be the subject of a future work in continuation of [GvH07].

8. Traveling fast and randomness

Our aim is to contribute to the design of fast bivariate polynomial factorization algorithms. As explained in the introduction, we concentrate on absolute factorization which proceeds by Hensel liftings from a good guess of

the partition (induced by the factorization) of a smooth fiber. The determination of this partition is a bottleneck of the algorithm; it can be computed by a trace method (using LLL to determine zero-sums). Of course, it is much cheaper (since it can be done in $\tilde{O}(d^2)$ arithmetic operations, where the notation $\tilde{O}(\cdot)$ hides logarithmic factors) to check the vanishing of a candidate zero-sum than to determine it. Therefore, our aim is to provide a good guess.

As we are considering a dense input polynomial, a quadratic complexity is in $O(d^4)$; if we get a complexity in $\tilde{O}(d^3)$, we are sub-quadratic in the input (therefore already fast), and we are "very fast" (i.e. quasi optimal) if we get a soft linear complexity, i.e. $\tilde{O}(d^2)$. This is actually our target.

Our conjectures motivated by the above presented experiments and reasoning would imply, with a good probability, that $O(\log(d))$ large random loops (see section 3) suffice to generate a transitive subgroup of the monodromy group of each irreducible component; hence it is sufficient to deduce the researched partition of a smooth fiber. So we are led to analyze the continuation process on the d paths above such a large loop γ. It is a marching (i.e. a discretization) of each path in order to determine precisely its end point, avoiding jumping from one path to another one.

8.1. **Continuation and complexity.** Let us recall the general idea of the considered continuation methods. First, it chooses dynamically (i.e not in advance) N points on the loop γ say $0 = x_0, ..., x_i, ..., x_N = 0$. Then we connect the elements of the two fibers $\{y_{i,j}\}_j$ and $\{y_{i+1,j}\}_j$ above two successive points x_i and x_{i+1} pairwise, such that two connected elements correspond to values of the same continuation. The strategy is to use a prediction-correction scheme. At each step i, the choice of each pair relies on the computations at $(x_i, y_{i,j})$ of the two first derivatives of f, which determine the tangent to the curve at each point. Relying on a Runge-Kutta scheme of order 2, the distance between the segment above $[x_i, x_{i+1}]$ and the path is estimated through the computations of the second derivatives of f, because $|x_i - x_{i+1}|$ is assumed to be small. Figupre 9 illustrates the discretization process.

For a fixed x_i, each Newton step amounts to a fixed number of operations on the derivatives of a bivariate polynomial of degree d, instanced at x_i (this costs less than $O(d^2)$) and these operations should be done simultaneously on the d points of the fiber. The corresponding complexity is less than $\tilde{O}(d^2)$ arithmetic operations. This should be multiplied by the number N of steps, which gives a complexity of $\tilde{O}(d^2)N$ arithmetic operations. Hence, a soft linear complexity of the determination of the partition will be achieved if we can use a number N of discretization steps at most polynomial in $\log(d)$; and a sub-quadratic complexity if $N = \tilde{O}(d)$.

Such bounds are not valid in general, but we expect that they will be reached "generically" i.e. with a good probability when the data satisfy random hypothesis. However, the rigorous analysis of the situation is very complicated and we are not able to establish precise theorems for the moment. Here we will only provide insights that indicate that our target, which will be fulfilled if a logarithmic number of steps suffice, is credible.

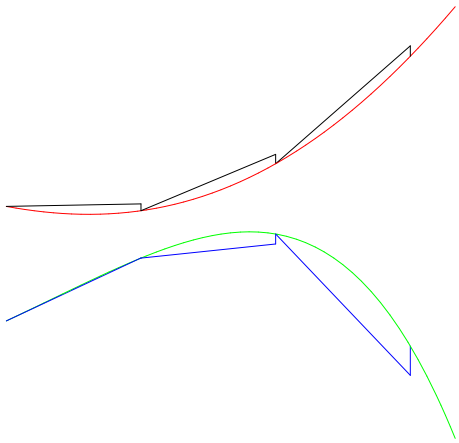


FIGURE 9. A partial analytic continuation following two leaves of the curve via a Runge-Kutta method.

8.2. **Expected distance between paths.** In our setting, asymptotically and in average, the paths come close when the loop γ crosses the annulus R centered at the origin and delimited by the circles of radius $1 - O(d^{-2})$ and $1 + O(d^{-2})$, where the discriminant points tend to concentrate. Moreover, for a generic ξ in that area, the d roots of $f(\xi, y) = 0$ tend to concentrate uniformly on the unit circle of the y-complex plane.

To expect good bounds for N, we need better insights on the distributions of the roots of $f(\xi, y) = 0$ and on their two-point correlation. Let us assume that this distribution behaves like a uniform one; then, the expected minimum distance between two roots of $f(\xi, y) = 0$ is $O(d^{-2})$, while the average one is $O(d^{-1})$.

On the other hand, as there are less than d^2 discriminant points, the average angular distance between a generic point of the unit circle and the set of discriminant points is $O(d^{-2})$. Therefore, we may assume that if we choose a line passing by the origin with a random direction, then it remains at an expected distance $O(d^{-2})$ from the discriminant points when it crosses the annulus R.

Now, if a critical point (α, β) is a turning point, the equation of f can be approximated locally by a quadric $A \cdot (x - \alpha) + B \cdot (y - \beta)^2 = 0$, where $A = f'_x(\alpha, \beta)$ and $B = f''_{yy}(\alpha, \beta)$. The second derivative is in average $O(d)$ times bigger than the first one. As a point ξ of a random line near the projection α of this critical point satisfies (in average) $|\xi - \alpha| > O(d^{-2})$, the distance between the two roots near β and above ξ is in average $O(d^{-1.5})$.

While if a critical point (α, β) is a node, then the equation of f can be approximated locally by a quadric $A \cdot (x - \alpha)^2 = B \cdot (y - \beta)^2$ where $A = f''_{xx}(\alpha, \beta)$ and $B = f''_{yy}(\alpha, \beta)$. The two derivatives are in average of the same size up to a factor $O(1)$. As, again, a point ξ of a random line near the projection α of this critical point satisfies (in average) $|\xi - \alpha| > O(d^{-2})$, the distance between the two roots near β and above ξ is in average $O(d^{-2})$.

Summarizing, we see that when the loop γ crosses the annulus R, we can expect that two paths above γ do not come closer than $O(d^{-2})$. Therefore,

the next task is to force, during the marching, each segment of tangent approximating each path to remain in a tubular neighborhood of radius $O(d^{-2})$ around this path.

8.3. **Tubular neighborhood and discretization.** The Taylor expansion of the implicit function defined by f at a point (ξ, η) of the Riemann surface is given by $y - \eta = a \cdot (x - \xi) + b \cdot (x - \xi)^2 + O((x - \xi)^3)$ with $a = -\frac{f'_x(\xi,\eta)}{f'_y(\xi,\eta)}$ and $b = -\frac{f''_{xx}(\xi,\eta)+2af''_{xy}(\xi,\eta)+a^2f''_{yy}(\xi,\eta)}{2f'_y(\xi,\eta)}$.

Lemma 1. *When d tends to infinity, the expectation for the maximum of the distribution for quotients of d independent uniform variables in $[0, 1]$ is $O(d)$.*

Now let us assume that along the intersection of a random line issued form the origin and the annulus, the first and second derivatives evaluated at the fiber above x_i behave like uniform independent variables. As, in average, the first derivatives have the same magnitude of size and the second derivatives are $O(d)$ greater, we expect from the formulae recalled above that, in average, $a < O(d)$ and $b < O(d^2)$.

All these estimates are confirmed by several experiments we made in Maple on bivariate dense polynomials of degree 400. Moreover, in all our computations (restricted to points on the Riemann surface near the unit torus) we always had $a < O(d)$ and $b < O(d^2)$.

Since we chose $N = O(1)$, we have $|x_i - x_{i+1}| = O(d^{-2})$ in the intersection of the loop γ and the annulus. Using this in the Taylor expansion, this gives us a distance between the segment of tangent and the path of $|b(x_i - x_{i+1})^2| = O(d^{-2})$. This is the requested order of magnitude.

Remark 1. *Relying on the same kind of arguments, one can see that the average maximal bounds for coefficients of the following terms (of the Taylor expansion corresponding to the implicit function defined by f) increase by a factor $O(d)$ at each degree. However, since we have $|x_i - x_{i+1}| = O(d^{-2})$, the bound on the corresponding term is indeed multiplied by $O(1/d)$.*

Therefore this emphasizes our claim that the term $|b(x_i - x_{i+1})^2|$ estimates the distance between the tangent and the path. Moreover it also indicates that the process will benefit from higher degree Taylor expansion approximations.

8.4. **Turning around each discriminant point.** To answer a suggestion of the anonymous referee, the previous approach can be adapted to provide an alternative computation of the transposition attached to each discriminant point by the monodromy action. This would provide a "random" alternative to our "determinist" algorithm described in section 2.

Since the $O(d^2)$ discriminant points tend to concentrate uniformly on the unit circle, we expect the minimal distance between two of them to be greater than $O(d^{-4})$, moreover we can assume that there is no more than $O(d)$ elements in such a cluster. Therefore, for each discriminant point, we construct a loop γ turning around it and with a good probability to pass far enough from the other discriminant points. The idea is simple: we start from the origin and make a random small step to a new point Ω such that two near-by discriminant points are "frankly" not colinear with Ω. In the

worst cases among the $O(d^2)$ discriminant points, since the minimal distance between two such points is greater than $O(d^{-4})$, the angular distance between them from Ω is greater than $O(d^{-5})$.

Then, we consider a "thin" loop γ similar to the "large" loop considered in the previous subsections but formed by two random lines issued from Ω turning around a specific discriminant point α but passing at a distance greater than $O(d^{-5})$ to all discriminant points (including α). The picture will look like Figure 2.

Therefore, we can adapt the previous analysis replacing $O(d^{-2})$ by $O(d^{-5})$ in the distance to the discriminant points: this leads, for a critical point (α, β) and a point ξ of a random line near the projection α, to an average distance between the two roots near β and above ξ of $O(d^{-3})$ if (α, β) is a turning point, and $O(d^{-5})$ if it is a node.

Hence, during the marching (in the worst cases, but in average among the f and the loops γ), each segment of tangent approximating each path must remain in a tubular neighborhood of radius $O(d^{-5})$ while crossing the annulus R and approaching the "cluster" of discriminant points at a distance smaller say than $O(d^{-2})$ from the lines. We can bound by $O(d)$ the number of the points in this cluster. Since R has a thickness of $O(d^{-2})$, which is much bigger than $O(d \cdot d^{-5})$, we choose a priori $N = O(d)$ steps for crossing R: $N_1 = O(d)$ steps of length $O(d^{-5})$ near by these discriminant points and $N_2 = O(1)$ steps of length $O(d^{-2})$ elsewhere.

Now, near this cluster of discriminant points, the average value of f'_y is much smaller than the average values of the other derivatives, by about two orders of magnitude. This was not the case in the previous subsection where the roots of the resultants $\mathrm{Res}_y(f, f'_y)$ play randomly the same role.

Summarizing, if we choose a step length about $|x_i - x_{i+1}| = O(d^{-5})$ during $N_1 = O(d)$ steps, we expect to be safe.

9. Concluding Remarks

In this paper we presented an original approach towards factorization and approximate factorization of high degree polynomials: considering the special (but not uncommon) case of a product of polynomials with random coefficients of limited size. This hypothesis simplifies the geometry: in particular, the curves corresponding to the factors are smooth. But it also implies several nice behaviors for the distribution of the discriminant and critical points of these curves. This deserves to be studied further and to be used to develop a new class of algorithms. We already developed and presented some programs to analyze the situations. Our preliminary study and results show that the subject is rich and promising.

We formulated two conjectures and explained our intuition behind the phenomena we propose to investigate.

There are several other directions of research. The main one is to investigate, with the hypothesis of uniformity, quantitative relations between exact and approximate factorizations. The second one is to investigate how our approach can be continued even if the curves corresponding to the factor have higher singularities; indeed, one can expect that if a random large loop in the complex plane encircles the projection of these singularities without

meeting them, the combinatorial and algorithmic situation is roughly the same that the one considered here. However, the numerical phenomena of the perturbed situation are more complicated, since clusters resulting from deformations of higher order multiple points are more spread out.

Acknowledgments

The authors would like to thank the two anonymous referee for helpful comments. The second author also acknowledges the support of the European Union (PITN-GA-2008-214584 SAGA).

References

[BCGW93] C Bajaj, J Canny, T Garrity, and J Warren. Factoring rational polynomials over the complex numbers. *SIAM J. Comput.*, 22(2):318–331, 1993.

[Bil97] Y. Bilu. Limit distribution of small points on algebraic tori. *Duke Math J.*, 89:465–476, 1997.

[CG05] Guillaume Chèze and André Galligo. Four lectures on polynomial absolute factorization. In *Solving polynomial equations*, volume 14 of *Algorithms Comput. Math.*, pages 339–392. Springer, Berlin, 2005.

[CG06] Guillaume Chèze and André Galligo. From an approximate to an exact absolute polynomial factorization. *J. Symbolic Comput.*, 41(6):682–696, 2006.

[CGvH+01] R.M Corless, M.W. Giesbrecht, M. van Hoeij, I.S. Kotsireas, and S.M. Watt. Towards factoring bivariate approximate polynomials. In B. Mourrain, editor, *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (ISSAC 2001)*. ACM, 2001.

[CL07] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *Journal of Complexity*, 23(3):380–420, 2007.

[DGS] C. D'Andrea, A. Galligo, and M. Sombra. Resultants and distribution of solutions of systems of polynomial equations. Submitted to publication.

[Dia96] P. Diaconis. The cutoff phenomenon in finite Markov chains. *Proc. Nat. Acad. Sci. USA*, 93(4):1659–1664, 1996.

[DvH01] Bernard Deconinck and Mark van Hoeij. Computing Riemann matrices of algebraic curves. *PhysicaD*, 152:28–46, 2001.

[EK95] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc.*, 32:1–37, 1995.

[ET50] P. Erdös and P. Turán. On the distribution of roots of polynomials. *Ann. Math.*, 51:105–119, 1950.

[Gao03] Shuhong Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242):801–822 (electronic), 2003.

[GKM+04] Shuhong Gao, Erich Kaltofen, John May, Zhengfeng Yang, and Lihong Zhi. Approximate factorization of multivariate polynomials via differential equations. In *ISSAC '04: Proceedings of the 2004 international symposium on Symbolic and algebraic computation*, pages 167–174, New York, NY, USA, 2004. ACM.

[GM] A. Galligo and L. Miclo. On the cut-off phenomenon for the transitivity of subgroups. Submitted to publication.

[GP09] André Galligo and Adrien Poteaux. Continuations and monodromy on random riemann surfaces. In *SNC '09: Proceedings of the 2009 conference on Symbolic numeric computation*, pages 115–124, New York, NY, USA, 2009. ACM.

[GvH07] Andre Galligo and Mark van Hoeij. Approximate bivariate factorization: a geometric viewpoint. In *SNC '07: Proceedings of the 2007 international workshop on Symbolic-numeric computation*, pages 1–10, New York, NY, USA, 2007. ACM.

[GW97] André Galligo and Stephen M. Watt. A numerical absolute primality test for bivariate polynomials. In Wolfgang Küchlin, editor, *ISSAC*, pages 217–224, Maui, USA, 1997. ACM.

[HN08] Christopher Hughes and A. Nikeghbali. The zeros of random polynomials cluster uniformly near the unit circle. *Compositio Mathematica*, 144:734–746, 2008.

[Kac48] M. Kac. On the average number of real roots of a random algebraic equation II. *Proc. London Math. Soc.*, 50:390–408, 1948.

[Kal00] E. Kaltofen. Challenges of symbolic computation: my favorite open problems. *JSC*, 29(6):891–919, 2000.

[LS09] Anton Leykin and Frank Sottile. Galois groups of Schubert problems via homotopy computation. *Mathematics of Computation*, 78:1749–1765, 2009.

[Pot07] Adrien Poteaux. Computing monodromy groups defined by plane algebraic curves. In *Proceedings of the 2007 International Workshop on Symbolic-numeric Computation*, pages 36–45, New-York, 2007. ACM.

[Pot08] Adrien Poteaux. *Calcul de développements de Puiseux et application au calcul de groupe de monodromie d'une courbe algébrique plane*. PhD thesis, Université de Limoges, 2008.

[PRa] Adrien Poteaux and Marc Rybowicz. Complexity Bounds for the rational Newton-Puiseux Algorithm over Finite Fields and Related Problems. Submitted to publication.

[PRb] Adrien Poteaux and Marc Rybowicz. Good Reduction of Puiseux Series and Applications. to appear in Journal of Symbolic Computation.

[PR08] Adrien Poteaux and Marc Rybowicz. Good Reduction of Puiseux Series and Complexity of the Newton-Puiseux Algorithm. In *Proceedings of the ISSAC '08 Conference*, pages 239–246, New-York, 2008. ACM.

[Rup00] David Rupprecht. *Elements de géométrie algébrique approchée: Etude du pgcd et de la factorisation*. PhD thesis, Univ. Nice Sophia Antipolis, 2000.

[Sas01] T. Sasaki. Approximate multivariate polynomial factorization based on zero-sum relations. In *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation (ISSAC 2001)*, pages 284–291. ACM, 2001.

[SS93a] Tateaki Sasaki and Mutsuko Sasaki. A unified method for multivariate polynomial factorizations. *Japan J. Indust. Appl. Math.*, 10(1):21–39, 1993.

[SS93b] M. Shub and S. Smale. Complexity of Bézout's theorem II: volumes and probabilities. In *Proceedings MEGA' 92 Vol. 109 of Progress in Mathematics*, pages 267–285, 1993.

[SSH92] Tateaki Sasaki, Tomokatsu Saito, and Teruhiko Hilano. Analysis of approximate factorization algorithm. I. *Japan J. Indust. Appl. Math.*, 9(3):351–368, 1992.

[SVW01] A.J. Sommese, J. Verschelde, and C.W. Wampler. Using monodromy to decompose solution sets of polynomial systems into irreducible components. In *Application of Algebraic Geometry to Coding Theory, Physics and Computation*, pages 297–315. Kluwer Academic Publishers, 2001. Proceedings of a NATO Conference, February 25 - March 1, 2001, Eilat, Israel.

[SVW02] A.J. Sommese, J. Verschelde, and C.W. Wampler. Symmetric functions applied to decomposing solution sets of polynomial systems. *SIAM J. Numer. Anal.*, 40(6):2026–2046, 2002.

[SZ04] B. Shiffman and S. Zelditch. Random polynomials with prescribed Newton polytope. *J. Amer. Math. Soc.*, 17:49–108, 2004.

[TT84] C. L. Tretkoff and M. D. Tretkoff. Combinatorial group theory, Riemann surfaces and differential equations. In *Contributions to group theory*, volume 33 of *Contemp. Math.*, pages 467–519. Amer. Math. Soc., Providence, RI, 1984.

Galligo: Université de Nice-Sophia Antipolis, Laboratoire de Mathématiques. Parc Valrose, 06108 Nice Cedex 02, France
E-mail address: galligo@unice.fr
URL: http://math1.unice.fr/~galligo/

Poteaux: UPMC, Univ Paris 06, INRIA, Paris-Rocquencourt center, SALSA Project, LIP6/CNRS UMR 7606 France
E-mail address: adrien.poteaux@lip6.fr
URL: http://www-salsa.lip6.fr/~poteaux/