

Continuations and Monodromy on Random Riemann Surfaces

André Galligo Adrien Poteaux *
Université de Nice (and INRIA)
Laboratoire de Mathématiques
Parc Valrose 06108 Nice cedex 02, France
galligo@unice.fr,
adrien.poteaux@sophia.inria.fr

ABSTRACT

Our main motivation is to analyze and improve factorization algorithms for bivariate polynomials in $\mathbb{C}[x, y]$, which proceed by continuation methods.

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 , that $\delta(0) \neq 0$ i.e. the corresponding fiber has d distinct points $\{y_1, \dots, y_d\}$. When we lift a loop $0 \in \gamma \subset \mathbb{C} - \Delta$ by a continuation method, we get d paths in X connecting $\{y_1, \dots, y_d\}$, 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 the loops turning around each point of Δ . Multiplying families of “consecutive” transpositions, we construct permutations then subgroups of the symmetric group. This allows us to establish and study experimentally some conjectures on the distribution of these transpositions then on transitivity of the generated subgroups.

These results provide interesting insights on the structure of such Riemann surfaces (or their union) and eventually can be used to develop fast algorithms.

Categories and Subject Descriptors

I.1.2 [Computing methodologies]: Symbolic and Algebraic Manipulations—*Algebraic Algorithms*

General Terms

Algorithms, Theory

Keywords

Random Riemann surface, Plane curve, Absolute Factor-

*Partially supported by the french Agence National de la Recherche, contract GECKO

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

SNC'09, August 3–5, 2009, Kyoto, Japan.

Copyright 2009 ACM 978-1-60558-664-9/09/08 ...\$10.00.

ization, Algebraic Geometry, Continuation methods, Monodromy, Symmetric group, Algorithms, Maple Code

1. INTRODUCTION

1.1 Factorization and topology

An important problem in Computer algebra is the factorization of approximate multivariate polynomials and the bivariate case captures its essential issues. See e.g. [3], [15, 16] or [5] and their bibliography. The reader can also consider [18] for an history of early algorithms. [1] was the first algorithmic paper using monodromy group action as developed below. The paper [14] considers point combinations, and an exponential search. The papers [26, 27, 25] discuss another interesting algorithm based on zero-sum identities.

A squarefree bivariate polynomial equation $f(x, y) = 0$ defines a reduced curve X in \mathbb{C}^2 . Then the closure of each connected component of $X - \text{Sing}(X)$ corresponds to an algebraic curve whose equation is an irreducible factor of f ; here $\text{Sing}()$ denotes the singular locus which consists at most in a finite number of points of X .

The condition can be analyzed further using a projection on a line. To simplify the discussion, assume that no irreducible component of X is a line, (this case can be treated separately), 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 A , π is d to 1. More precisely, $X - \pi^{-1}(A)$ is a d -covering of the line minus A ; moreover, it is the union of s connected such coverings $X_i - \pi^{-1}(A)$.

For x_0 not in A , the fiber $E = \pi^{-1}(x_0)$ consists of d distinct points, partitioned in s subsets E_i , E_i lying on $X_i - \pi^{-1}(A)$ for $1 \leq i \leq s$. Note that this partition of E characterizes the aimed factorization of f , as it defines it modulo $(x - x_0)$, and the factorization can be recovered via x -adic Hensel liftings.

1.2 Continuation or homotopy methods

A continuation method was proposed in [6]; 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 paper [30] was made the following important experimental observation (in the case of exact inputs, approxima-

tions with a great precision and with a slightly different monodromy action than the one considered here) which inspired our study: the partition of the fiber E can be recovered from only a few number of permutations of E corresponding to the monodromy action of random loops. Whereas, in theory as in [1], one needs to consider a set of representative of generators of the fundamental group which consists of a huge number of transpositions or other permutations.

As above, denote by X the curve in \mathbb{C}^2 defined by $f(x, y) = 0$, by π its projection on the x -axis and choose a generic (i.e. random) fiber $E = \pi^{-1}(x_0)$ in X which has d points. To simplify the notations, we let $x_0 = 0$. We denote by $\Delta \in \mathbb{C}$ the discriminant locus of π . 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 is composite: $f = f_1 \dots f_s$, 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 to recover the factorization of f (see e.g. [8, 31, 3]). Monodromy also plays an important role in the factorization algorithms presented in [14, 24, 30, 31, 3, 4, 19].

1.3 A generic model

In [13], 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 $f = f_1 \dots f_s$ such that the curves $X_i = f_i^{-1}(0)$ are all smooth and intersect transversally in double points (nodes). A “generic” change of coordinates, allows to suppose that f is monic in y of degree d and total degree d and that the projections of the critical points on the x -axis are all distinct. As the X_i are smooth and cut transversally, 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).

Moreover as in [31], a method presented in [13] determined the targeted partition of the fiber E by following the roots in y above a small number of (random) loops in the x -axis.

Our aim is to analyze further and improve that approach; the 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. [32] and [8].

1.4 Organization

The paper is organized as follows. In section 2 the monodromy action is first presented in our particular setting; then an algorithmic approach and a Maple implementation for its computation are described. In section 3, our choices for the implementation of the continuation procedure are exposed. In section 4, we first recorded classical and recent results on the distribution of the roots of random polynomials useful for our purpose then we propose some conjectures on combinatorial aspects directly related to our problem; we also indicate the heuristical reasoning which guided their formulation. In section 5, we present a methodology and some experiments to support our conjectures and approach of the problem. In section 6 we report experiments showing the robustness of the studied strategy of factorization with respect to small perturbations of the input data. Finally we

conclude discussing on potential extensions of our geometric model.

2. MONODROMY GROUP

In this section, we keep the previous notations and describe algorithmically our main tool, the monodromy group, its representation and its calculation. A previous implementation can be found in the package `algcurses` of Maple (see also [8]), that our work aims to improve.

2.1 Our setting

The discriminant locus Δ of f is the zero-set of $\text{Res}_y(f, f'_y)$, it contains simple points which are the projections of the turning points of X i.e. points with a vertical tangent and multiple points which are projections of the singularities of X i.e. the solutions of $f = f'_y = f'_x = 0$.

To define the monodromy, first select a base point $x = a$ e.g. $a = 0$ in the complex x -plane minus the discriminant locus. Let E be the fiber of p 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, \dots, y_d) . This ordering of the d y -values labels the 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, \dots, y_d) is then analytically continued along 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, \dots, y_d) , but ordered differently: $(y_{\sigma_\alpha(1)}, y_{\sigma_\alpha(2)}, \dots, y_{\sigma_\alpha(d)})$, where σ_α is a permutation acting on the set of labels $\{1, 2, \dots, d\}$. We will say that the permutation σ_α is attached to the path γ_α . Note that for different choices of γ_α , we obtain different permutations.

Here are some typical situations. If $x = \alpha$ is a turning point, 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 model, we 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. For $d = 10$ that means considering 90 discriminant points and organizing 90 paths in a limited portion of the complex plane. The Maple package called `algcurses[monodromy]` described in [8] 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 `algcurses[monodromy]` in our setting. In order to see how fibers are permuted, we have to follow paths homotopic to the one showed in the next figure 1.

Unfortunately, for a large number of discriminant points, some paths automatically generated by the Maple command `algcurses[monodromy]`, with option `showpaths`, are not correct. As shown for instance in figure 2 which corresponds to a random polynomial of degree 10. One can see that the paths are crossing each other, and that some paths are crossing the circles when they should not do so (see [8, section 3.5]). We got this picture using Maple 9.5, with 10 and 20

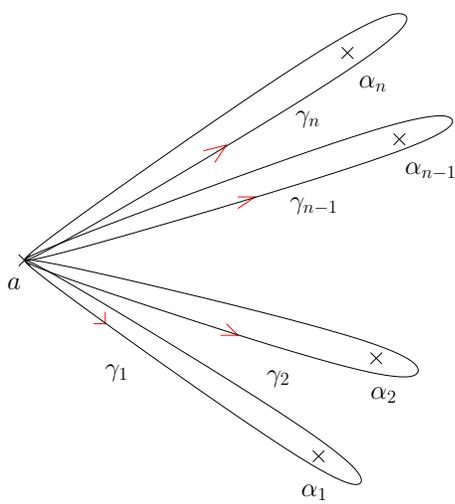


Figure 1: Paths encircling one point of the discriminant

Digits. The same computation with 30 or 40 Digits leads to better paths (in the sense that some errors do not appear), but still false ones.

To avoid this kind of bad behaviour, we rely on algorithms described in the second author thesis [21, 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 [20], and more details were provided in [21].

Our method is a “compute fibers and connect” one. 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:

- *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 1 in $\mathbb{C} \setminus \{\alpha_1, \dots, \alpha_n\}$. 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 [20] is not fully correct: one can create counter examples. To resolve the matter, an algorithm which computes the needed paths was developed in [21, 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 that are constituted only of segments \mathcal{T} and arc of circles centered on a critical point α_k and linking two connected edges of the tree \mathcal{T} (see [20, section 3.1] for more details). Thus, our aim is to know which sequence of edges of \mathcal{T} we have to follow, and in which sense

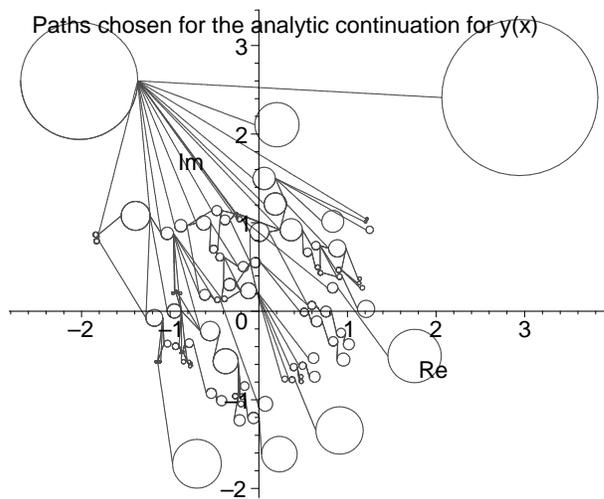


Figure 2: Paths followed by the algcurves [monodromy] Maple command for a polynomial of degree 10

we must go around each critical point we have to circle. The approach we give in [21, 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.

Considering the path γ_l , we search a path homotopic to $[a, \alpha_l]$ in $\mathbb{C} \setminus \{\alpha_1, \dots, \alpha_n\}$.

- Let $a_0 = a, a_1, \dots, a_{s-1}, a_s$ denote the successive intersection points between $[a, \alpha_l]$ and \mathcal{T} , ordered according to their apparition 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} .

- So, 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 sense computed, 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 explicit them but they are all given in [21].

- *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 [20]

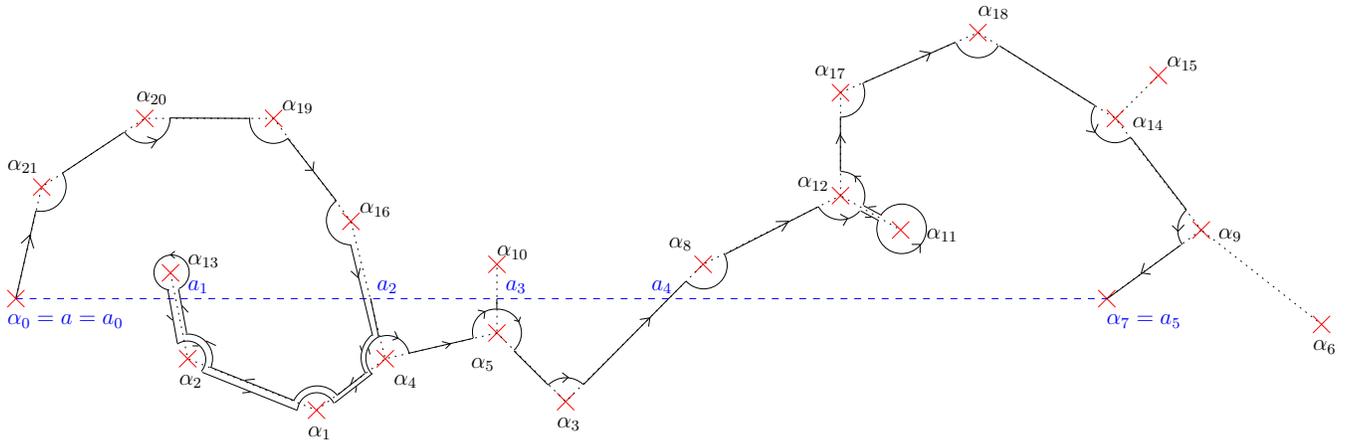


Figure 3: Path in the tree homotopic to $[a, \alpha_7]$ in $\mathbb{C} \setminus \{\alpha_1, \dots, \alpha_n\}$

and improved in [21] (the modular part of the algorithm is also described in [22, 23]). All details of our monodromy algorithm can be found in [20] and [21].

3. ANALYTIC CONTINUATIONS

3.1 Analytic Continuation Process

Following [8, section 3.6], we perform analytic continuation using first derivative order. From our combinatorics analysis (see section 4), 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.

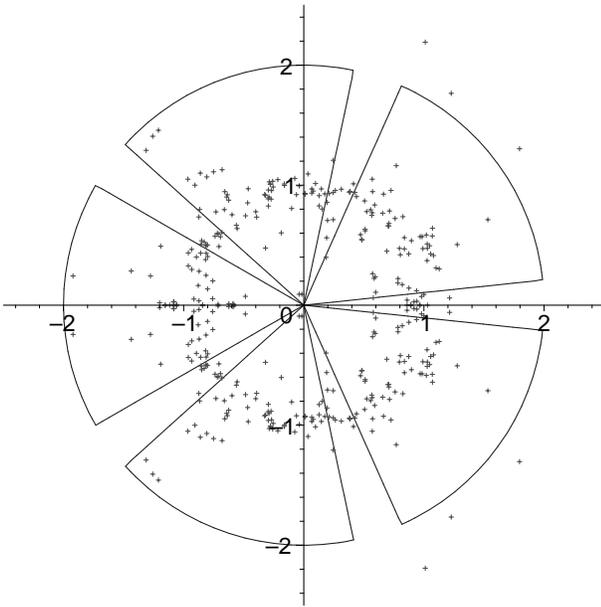


Figure 4: Paths and discriminant points for a curve of degree 20

Our Maple algorithm to make 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 from 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} .

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 point are different, we made experiments to get informations on how works our analytic continuation process; practical observations confirmed our natural intuition. The two following pictures illustrate our observations. We considered a polynomial F defined as the product of two random polynomials F_1 and F_2 . Figure 5 represents the analytic continuation process along a path which is close to a root of $\text{Res}_y(F_1, F_1'_y)$, whereas figure 6 represents the same for a root of $\text{Res}_y(F_1, F_2)$. 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 need 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 seems 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, as shown in the following table (the indicated times are for 3 loops for each polynomial).

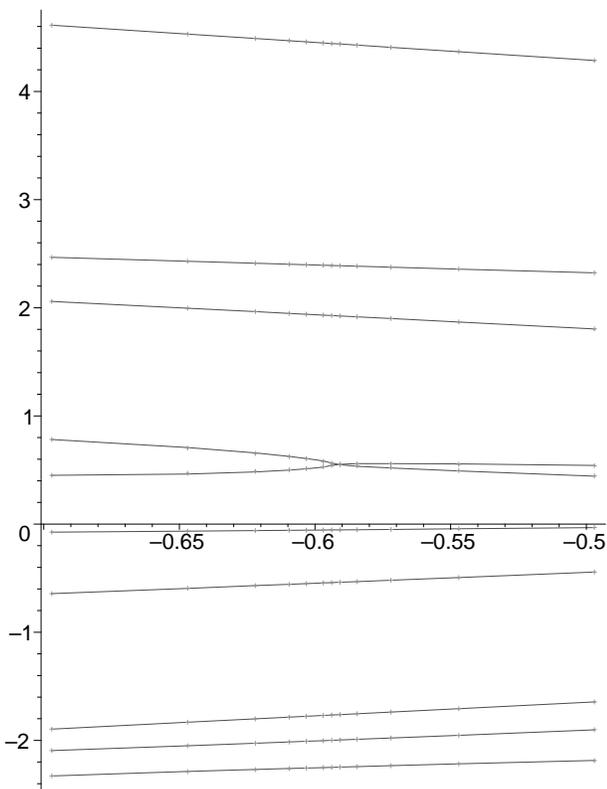


Figure 5: Intermediary steps for a turning point

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. COMBINATORICS

Roots of random univariate polynomials have been studied by many authors, and important results were achieved e.g. by Kac [17], Edelman-Kostan [10] in the real case, or by Erdos-Turan [11] in the complex case. This was generalized by Shub-Smale [29] and their coworkers, to the multivariate real case, by Zelditch-Schiffmann [28] and their coworkers, and also by Bilu [2] in the complex case. Let us also quote a recent joint work of the first author with C. d’Andrea and M. Sombra [7] which focused on effective bounds. Here are the results we will refer to in the following.

THEOREM 1 (ERDOS-TURAN [11]). *Let P be a degree d univariate polynomial in $\mathbb{C}[x]$ and denote by M a measure of the size of its coefficients. When d goes to infinity, if $M = o(d)$, then the roots of P concentrate uniformly on the unit circle of \mathbb{C} .*

THEOREM 2 ([7], SEE ALSO [2]). *For a bivariate polynomial $f(x, y)$, under the same kind of limited growth condition of the coefficients of f , but with a provisional technical assumption that f has integer coefficients, it also holds for the discriminant of f that its roots concentrate uniformly on the unit circle of \mathbb{C} . Moreover the critical points of f , with respect to the x -projection,*

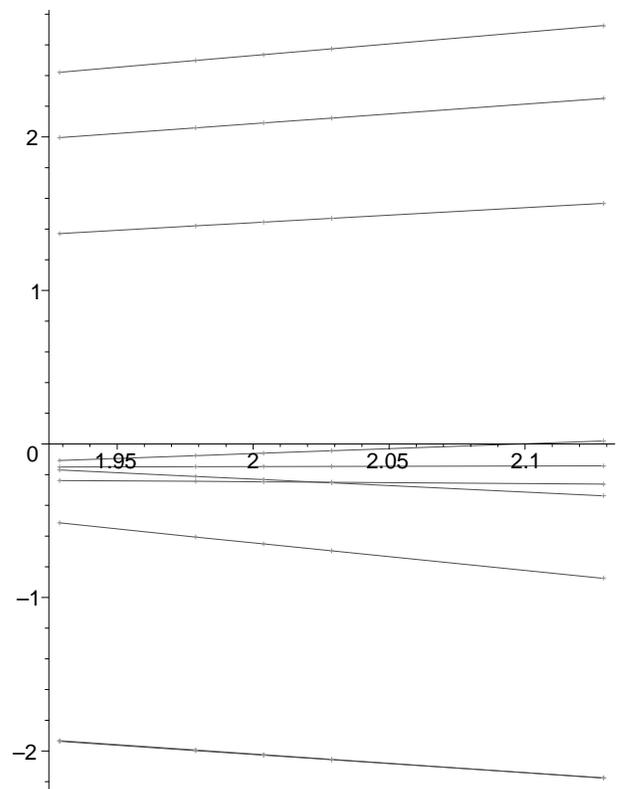


Figure 6: Intermediary steps for an intersection point

concentrate uniformly on the product of the two unit circles in \mathbb{C}^2 .

4.1 A challenging problem

We address an even more ambitious problem: when d goes to infinity, describe 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 defined by such a polynomial $f(x, y)$.

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 formulate some conjectures.

4.2 Relation between critical points and transpositions

As recalled above when d goes to infinity, the critical points of f concentrate uniformly on the product of unit circles which is parameterized by two angles ϕ and ψ modulo 2π , the arguments of (x, y) in \mathbb{C}^2 . We order the $d(d-1)$ discriminant points by their increasing arguments and join consecutive ones by as many segments of lines. We obtain a continuous real curve C homeomorphic to the unit circle and which tends to it when d goes to infinity.

Let, as above, π denote the projection of the random Riemann surface X onto the x -axis (a real plane). We also order by increasing arguments the d distinct points of the fiber of

π above the unique point a of C whose argument is 0, and should be near-by 1. The real curve $\pi^{-1}(C)$ in $\mathbb{C}^2 = \mathbb{R}^4$, can be viewed as a "branched" braid on a torus homeomorphic to $\mathbb{S}^1 \times \mathbb{S}^1$, where \mathbb{S}^1 denotes the unit circle. Representing the two \mathbb{S}^1 by two segments $(0, 2\pi)$ with identified extremities, the figure 7 sketches a portion with 3 turning points.

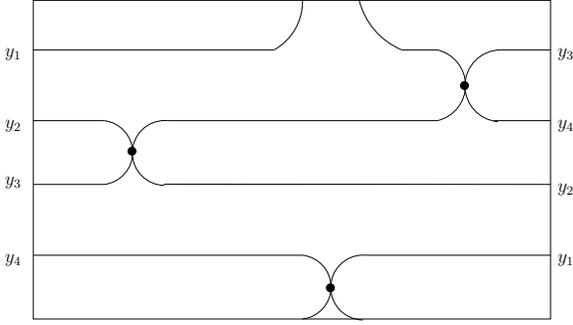


Figure 7: A portion of a branched braid

The branching points of that braid correspond to the critical points of f w.r.t. the x -projection. Heuristically and asymptotically, the limits of these branching points are distributed uniformly in the previous square. Of course, this claim needs to be formalized and rigorously proved. Nevertheless it indicates that asymptotically, as shown on the picture when the arguments ϕ_k of the discriminant points of f increase, the corresponding transpositions t_k are consecutive pairs i.e. of type $(i, i + 1)$ with $d + 1 = 1$. Indeed the only possible exchange at a critical point is with a direct neighbour. Moreover, as the critical points are uniformly distributed in the square, the index i which is directly related to the y coordinate of these points, should also be uniformly distributed. On the basis of this heuristic argumentation, we formulate the following:

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. For small and medium values of d , one can rather expect a blending of the two preceding distributions: uniform transpositions and uniform consecutive pairs. Another way for looking experimentally at this conjecture is to derive some consequences of it and try to check them on examples.

4.3 Products of transpositions

In a recent joint work with L. Miclo [12], the first author 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. A cut-off phenomenon (see [9]) was proved in the case of transpositions (i, j) where i and j are uniformly chosen among the integers $[1..d]$ at "time" $n = \frac{d \ln(d)}{2K}$. They also considered the case of uniformly distributed consecutive pairs (i, j) , but were only able to prove partial results and observe simulations; nevertheless, they posed 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 $K = \beta \ln(d)$ products of about $\alpha(\beta)d$ uniform consecutive pairs $(i, i + 1)$ with $d + 1 = 1$ and $\alpha(2) \leq 1$.*

Let us note that in [12], 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 can be observable via continuation methods as indicated below and that these considerations could be useful for the aimed factorization strategy.

4.4 Subgroup attached to K large loops

Consider a large loop Γ in the x -plane starting and ending at 0 and encircling n discriminant points of f . Γ is homotopic to the concatenation of n loops γ_i , each encircling a discriminant point. The n discriminant points are ordered by increasing arguments, therefore the permutation p_Γ attached to Γ is the product of the n transpositions attached to the γ_i .

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

Then, if the previous conjectures are correct, 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 precised above).

Finally, we consider not one but K such large loops Γ_k , the K attached permutations p_k , and the subgroup G generated by these K permutations. We choose K and $n = \frac{d(d-1)}{m}$ as indicated in the previous subsection.

CONJECTURE 3. *G is a transitive subgroup of the symmetric group.*

Example: For $d = 50$, $\ln(d)$ is about 4, 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 at least $(2\pi)/6$ hence not so small but feasible.

5. EXPERIMENTS ON EXAMPLES

5.1 Preliminary remark

Even if our approach improves previous algorithms, our implementation in Maple 11 is still a prototype one, and needs for instance 2 hours to perform the complete monodromy computation for all the 90 loops and discriminant points of a degree 10 random polynomial f . Thus, it is not yet realistic to perform this computation for much higher degrees.

However for these degrees, the distribution announced by Erdos-Turan theorem, of the roots in a generic fiber can be far from the asymptotic uniform distribution on the unit circle. The same is also true for the distribution of discriminant

points. Therefore, as we can see on figure 4, the difference between arguments is not yet a good approximation of the Euclidean distance between these points.

5.2 Methodology

So, 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. What we can do is to check a weaker claim, which seems natural: when passing from one discriminant point to a close one (in the sense of the Euclidean distance), only near by points (in the sense of the Euclidean distance) of the fibre are exchanged. Indeed as observed in our examples, this happens very frequently and in general the exchange does not involve the points of the fibre 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 (rather voluminous) data are provided in our website:

<http://www-sop.inria.fr/members/Adrien.Poteaux/>

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 discriminant points and fibers above them.

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

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.

5.3 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 , $k = 1 \dots 5$, each of them encircles an angle of $\frac{\pi}{3}$ and hence contains about just less than a sixth of the 380 discriminant points i.e. about $60 = 3.d$ of these points. Following our conjectures we expect that the corresponding 5 permutations generate a transitive group. This is indeed the case.

5.4 Factorization

We also tested our approach on the factorization problem. We present our results by giving the sequence of Maple command line we use to get the result (the reader can find the file `analyticcontinuation.mpl` on the second author's webpage):

We first begin by 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 behaviour by increasing 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 severable 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 $\frac{\pi}{3}$.

6. APPROXIMATE COEFFICIENTS

If the data is given within some approximation, our approach may still be applied to get the elements of the fiber which belongs to the same factor. This is illustrated by the following examples.

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

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

Table 1: Factoring approximate polynomials

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 behaviour 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 [13].

7. 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 behaviours 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 several conjectures and explained our intuition behind the phenomena we propose to investigate.

There are also different other directions of research. The main one is to investigate with the hypothesis of uniformity the link between exact and approximate factorization. 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 of deformations of higher order multiple points are more spread out.

8. REFERENCES

- [1] C. Bajaj, J. Canny, T. Garrity, and J. Warren. Factoring rational polynomials over the complex numbers. *SIAM J. Comput.*, 22(2):318–331, 1993.
- [2] Y. Bilu. Limit distribution of small points on algebraic tori. *Duke Math J.*, 89:465–476, 1997.
- [3] G. Chèze and A. Galligo. Four lectures on polynomial absolute factorization. In *Solving polynomial equations*, volume 14 of *Algorithms Comput. Math.*, pages 339–392. Springer, Berlin, 2005.
- [4] G. Chèze and A. Galligo. From an approximate to an exact absolute polynomial factorization. *J. Symbolic Comput.*, 41(6):682–696, 2006.
- [5] G. Chèze and G. Lecerf. Lifting and recombination techniques for absolute factorization. *Journal of Complexity*, 23(3):380–420, 2007.
- [6] R. Corless, M. Giesbrecht, M. van Hoeij, I. Kotsireas, and S. 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.
- [7] C. D’Andrea, A. Galligo, and M. Sombra. Resultants and distribution of solutions of systems of polynomial equations. *Preprint*, 2009.
- [8] B. Deconinck and M. van Hoeij. Computing riemann matrices of algebraic curves. *PhysicaD*, 152:28–46, 2001.
- [9] P. Diaconis. The cutoff phenomenon in finite markov chains. *Proc. Nat. Acad. Sci. USA*, 93(4):1659–1664, 1996.
- [10] A. Edelman and E. Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc.*, 32:1–37, 1995.
- [11] P. Erdős and P. Turán. On the distribution of roots of polynomials. *Ann. Math.*, 51:105–119, 1950.
- [12] A. Galligo and L. Miclo. On the cut-off phenomenon for the transitivity of subgroups. *Preprint*, 2009.
- [13] A. Galligo and M. van Hoeij. Approximate bivariate factorization: a geometric viewpoint. In *SNC ’07: Proceedings of the 2007 international workshop on*

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

Table 2: Factoring dense noised polynomials

- Symbolic-numeric computation*, pages 1–10, New York, NY, USA, 2007. ACM.
- [14] A. Galligo and S. M. Watt. A numerical absolute primality test for bivariate polynomials. In W. Küchlin, editor, *ISSAC*, pages 217–224, Maui, USA, 1997. ACM.
- [15] S. Gao. Factoring multivariate polynomials via partial differential equations. *Math. Comp.*, 72(242):801–822 (electronic), 2003.
- [16] S. Gao, E. Kaltofen, J. May, Z. Yang, and L. 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.
- [17] M. Kac. On the average number of real roots of a random algebraic equation ii. *Proc. London Math. Soc.*, 50:390–408, 1948.
- [18] E. Kaltofen. Challenges of symbolic computation my favorite open problems. *JSC*, 29(6):891–919, 2000.
- [19] A. Leykin and F. Sottile. Galois groups of schubert problems via homotopy computation. *Mathematics of Computation*, 78:1749–1765, 2009.
- [20] A. 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.
- [21] A. 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.
- [22] A. Poteaux and M. 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.
- [23] A. Poteaux and M. Rybowicz. Good Reduction of Puiseux Series and Applications. In *Submitted to JSC*, 2009.
- [24] D. Rupprecht. *Elements de géométrie algébrique approchée: Etude du pgcd et de la factorisation*. PhD thesis, Univ. Nice Sophia Antipolis, 2000.
- [25] 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.
- [26] T. Sasaki, T. Saito, and T. Hilano. Analysis of approximate factorization algorithm. I. *Japan J. Indust. Appl. Math.*, 9(3):351–368, 1992.
- [27] T. Sasaki and M. Sasaki. A unified method for multivariate polynomial factorizations. *Japan J. Indust. Appl. Math.*, 10(1):21–39, 1993.
- [28] B. Shiffman and S. Zelditch. Random polynomials with prescribed newton polytope. *J. Amer. Math. Soc.*, 17:49–108, 2004.
- [29] 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.
- [30] A. Sommese, J. Verschelde, and C. 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.
- [31] A. Sommese, J. Verschelde, and C. Wampler. Symmetric functions applied to decomposing solution sets of polynomial systems. *SIAM J. Numer. Anal.*, 40(6):2026–2046, 2002.
- [32] C. Tretkoff and M. Tretkoff. Combinatorial Group Theory, Riemann Surfaces and Differential Equations. *Contemp. Math.*, 33:467–517, 1984.