A Geometric-Numeric Algorithm for Absolute Factorization of Multivariate Polynomials[*]

Robert M. Corless[†] André Galligo[‡] Ilias S. Kotsireas[†§] Stephen M. Watt[†]

[†]The Ontario Research Centre for Computer Algebra
University of Western Ontario, London ON, N6A 5B7 Canada

[‡]Laboratoire de Mathématiques, Université de Nice-Sophia Antipolis,
Parc Valrose, Nice 06108 Cedex 2, France

[§]Department of Physics & Computing, Wilfrid Laurier University,
75 University Avenue West, Waterloo ON, N2L 3C5 Canada

ABSTRACT

In this paper, we propose a new semi-numerical algorithmic method for factoring multivariate polynomials absolutely. It is based on algebraic and geometric properties after reduction to the bivariate case in a generic system of coordinates. The method combines 4 tools: zero-sum relations at triplets of points, partial information on monodromy action, Newton interpolation on a structured grid, and a homotopy method. The algorithm relies on a probabilistic approach and uses numerical computations to propose a candidate factorization (with probability almost one) which is later validated.

1. INTRODUCTION

We provide a new semi-numerical probabilistic algorithmic method for solving the following problem: given a multivariate polynomial P of degree n with rational coefficients, is it possible to factor it absolutely as $P = P_1 \cdots P_s$ over $\mathbb{C}$? That is, decompose the curve $\mathcal{C}$ defined by P in the complex plane into irreducible components $\mathcal{C}_i$ defined by the irreducible factors of P. In other words, find a minimal extension $\mathbb{Q}[\alpha]$ of $\mathbb{Q}$ and an irreducible (on $\mathbb{C}$) factor of P in that extension.

Various algorithmic methods have been proposed to solve this problem which is called computation of an absolute factorization of the polynomial P. It has been studied by many authors, including recently by [5, 4, 16, 19, 15, 21], see also the review [10] and the book [25] for history and a large bibliography; this includes [2] and [8]. However, implementations in classical Computer Algebra systems like Maple or Mathematica or more specialized packages are not yet satisfactory. (Classical CA systems use an implementation of the so called "Single Extension Method".)

We adopt a semi-numerical approach, in which we first compute an approximation of the complex coefficients of the factors of P with high precision; then we construct, by rational approximation, an exact candidate factor of P together with an algebraic extension of $\mathbb{Q}$ containing the coefficient of that factor, then check by Euclidean division the fact that it is an exact factor.

Our approach also provides as a by-product an efficient guide for computing an approximate factorization of a polynomial known with a limited precision which is "near-by a composite polynomial". This procedure could be very helpful in applications.

Our algorithmic method can be seen as an improvement of several other algorithms: [16], [19], [21], [1], [3]. Indeed, we rely on ideas developed in these papers and we introduce new tools. The first and final steps of our algorithm are identical to those of [16], and the integration procedure (a marching algorithm) is similar to that of [3], so we will present them quickly and refer to these papers.

We use a collection of several tools including partial monodromy information as in [21], but the main tool is a new linear condition (see section 5) satisfied by the coordinates of the points in 3 fibers. This condition is a discrete analog of the zero sum condition on the second derivatives used in [19],[18], [5],[16]. We also adapt an idea exposed in [19]: several instances of this condition generate a matrix M with approximate entries and the analysis of its kernel provides a partition which leads to the desired factorization.

Although the input and output are polynomials with exact coefficients, the intermediate computations are made with

[*]Supported in part by EU contract IST 2001-35512, the Natural Sciences and Engineering Research Council of Canada, the Ontario Research and Development Challenge Fund, the ESPRIT Long Term Research project FRISCO, and Waterloo Maple Inc.

ISSAC 2002, July 7-10, 2002, Lille, France
©2000 ACM 1-58113-484-3/ 02/ 0007 $5.00

approximations of complex numbers by bigfloats whose precision is choosen by the user. We provide no complexity nor diophantine analysis. This is left as an open question.

This paper describes the results we presented in a poster at ISSAC'01. When writing this paper we received an interesting manuscript on decomposition of varieties [22] in which the authors independently discovered some of the ideas presented in our poster. See also the following papers of the same authors [23, 23].

In section 8, we describe the different steps of our method and in section 9 we illustrate them on a simple example: a bivariate polynomial of degree 9 irreducible on $\mathbb{Q}$.

2. REDUCTIONS AND STATEMENTS

2.1 Preparation

We first perform certain reductions on the input polynomial to get a monic square-free irreducible (over $\mathbb{Q}$) polynomial.

By using the Hilbert irreducibility theorem, we can reduce the problem to a bivariate polynomial. The basic idea is that, after generic sections $X_i = a_iX + b_iY + c_i$, an irreducible polynomial in $\mathbb{Q}[X_1, \cdots, X_\tau]$ becomes an irreducible polynomial in $\mathbb{Q}[X, Y]$. Moreover, if after such generic hyperplane sections, $\tilde{P}(X, Y) = P(a_1X + b_1Y + c_1, \cdots, a_\tau X + b_\tau Y + c_\tau)$ is reducible, then P is reducible and we can recover its factors from the factors of $\tilde{P}$ using Hensel lifting. An absolute factorization of $\tilde{P}$ lifts to an absolute factorization of P. This is described in several texts, see *e.g.* the book of Zippel [27]. We will therefore focus on bivariate irreducible (over $\mathbb{Z}$) polynomials $P \in \mathbb{Q}[X, Y]$.

We further consider "generic" affine change of coordinates in 2 variables

$$X = x + ay + b\ ;\ Y = y + c\ .$$

We will only consider properties $\mathcal{P}$ such that the set of changes of coordinates, for which $\mathcal{P}$ is not satisfied, is included in a strict algebraic subset V of $\mathbb{C}^3$. Then we say that a change of coordinates is **generic** for this property if (a, b, c) is not in V. For all "usual" applications, a change of coordinates whose coefficients (a, b, c) are decimal numbers provided by a pseudo-random function will almost surely be generic. So in practice, genericity is always easy to reach. We claim only that our algorithm proposes a good candidate decomposition to be checked and which will work with high probability.

We now recall a few simple results, see *e.g.* [16]. Let $P \in \mathbb{Q}[X, Y]$ with total degree n. After a change of coordinates $x \leftarrow X + \lambda Y$ and $y \leftarrow Y$, we get a new polynomial:

$$A_n(x, \lambda)y^n + \cdots + A_1(x, \lambda)y + A_0(x, \lambda),$$

where $A_i(x, \lambda)$ is a polynomial with $\deg_x(A_i) \leq n - i$ and $\deg_\lambda(A_i) \leq n$. As the total degree of P is n, the polynomial $A_n \in \mathbb{Q}[\lambda]$ is a non-zero polynomial and then, for all specializations of λ in $\mathbb{Q}$ except at most n, $A_n(\lambda) \neq 0$ and is in $\mathbb{Q}$. Simplifying, we get a new monic polynomial in $\mathbb{Q}[x, y]$: $y^n + a_{n-1}(x)y^{n-1} \cdots + a_0(x)$ with $\deg a_i(x) \leq n - i$ which we again call P.

LEMMA 2.1. *Let P be a polynomial $\mathbb{Q}[X, Y]$, monic in Y, of degree m, square-free and irreducible in $\mathbb{Q}[X, Y]$. Then there exists an extension $\mathbb{Q}[\alpha]$ of $\mathbb{Q}$ of degree s and a factorization $P = P_1 \cdots P_s$, with $m = ds$,*

$$P_i = Y^d + a_{m-1}(\alpha_i, X)Y^{d-1} + \cdots + a_0(\alpha_i, X)\ ,$$

where P_i is irreducible in $\mathbb{C}[X, Y]$, $a_k \in \mathbb{Q}[Z, X]$, $\deg_X(a_k) \leq d - k$ and where $\alpha_1, \cdots, \alpha_s$ are the different conjugates of α.

A consequence is that the factors have all the same degree.

2.2 Statements

Let P be a monic square-free polynomial in $\mathbb{Q}[X, Y]$, irreducible in $\mathbb{Q}[X, Y]$ as above.

- **Exact problem**

1 Find a simple extension $\mathbb{Q}[\alpha]$ of $\mathbb{Q}$ represented by an univariate irreducible monic polynomial $q(t)$ such that: $\mathbb{Q}[\alpha] = \mathbb{Q}[t]/q(t)$. Let $\alpha_1, \cdots, \alpha_s$ be the different conjugates of $\alpha = \alpha_1$.

2 Find polynomials $P_1 \cdots P_s$, with

$$P_i = Y^d + a_{d-1}(\alpha_i, X)Y^{d-1} + \cdots + a_0(\alpha_i, X),$$

such that P_i divides P.

Geometrically, if $\mathcal{C}$ (resp. $\mathcal{C}_i$) denotes the zero-set of P (resp. P_i), this means that $\mathcal{C}$ is the union of its irreducible components $\mathcal{C}_i$, for $i = 1 \ldots k$.

Moreover removing the singular locus of $\mathcal{C}$, the $\mathcal{C}_i$ are the connected components of $\mathcal{C}$.

- **Approximate Problem**

Find polynomials $P_1 \cdots P_s$, with

$$P_i = Y^d + a^i_{d-1}(X)Y^{d-1} + \cdots + a^i_0(X),$$

such that with a "very good" approximation ΔP:

$$P + \Delta P = P_1 \cdots P_s.$$

2.3 Reduction to the approximate problem

The exact problem reduces to the approximate problem as follows.

We want to find exact coefficients for the candidate exact factors from the coefficients of the polynomials P_i together with a polynomial defining the conjugates. We follow the treatment of [16]. Let us write

$$P_i = \sum_{k,l} a^{(i)}_{k,l} X^k Y^l.$$

For each (k, l) corresponding to a non-zero numbers $a^{(i)}_{k,l}$, we consider the univariate polynomial

$$R_{k,l}(Z) = \prod_{i=1}^{s} (Z - a^{(i)}_{k,l}).$$

As the factors P_i are conjugate, these polynomials $R_{k,l}$ have rational coefficients. The polynomial $R_{k,l}$ defines the extension for the coefficients of $X^k Y^l$ in $P_1, \cdots, P_s$. In fact, as $R_{k,l}$ is not an exact polynomial, we compute a good rational approximation for each coefficient of $R_{k,l}$. We can use the function *bestapprox* of the system PARI-GP [13]. Then we keep the square-free part of $R_{k,l}$.

For each non-zero coefficient, we have a polynomial defining an extension. We compute a common extension K defined by a polynomial T. Finally we express a factor in this extension and test if the remainder of the exact division between P and the factor is 0.

3. MONODROMY

3.1 Definition

We first recall classic facts which can be found in any introductory textbook on Algebraic Geometry (see *e.g.* [12] or [26]).

We consider a polynomial $P(x, y)$ whose degree in y equals its total degree n (so it is monic in y). Denote its zero-set by $\mathcal{C}$, which is a curve in $\mathbb{C}^2$; we denote by ϕ the projection of $\mathcal{C}$ on the x-axis. The curve $\mathcal{C}$ is a ramified covering of degree n of $\mathbb{C}$. Let Δ be the discriminant locus of ϕ, i.e. the set of abscissas of the ramification points, defined by the resultant in y of P and P'_y.

Let x_0 be on the x-axis outside of Δ. Consider a loop $\gamma : [0, 1] \to \mathbb{C} - \Delta$ which is smooth with $\gamma(0) = \gamma(1) = x_0$. Following the roots of $P(\gamma(t), y)$ on top of the loop γ in $C - \Delta$, we get a permutation of the fiber $\phi^{-1}(x_0)$. This permutation depends only on the homotopy class of the loop γ.

This construction defines the group morphism called monodromy:

$$\pi_1(\mathbb{C} - \Delta) \to \mathcal{S}_n.$$

Here $\pi_1(-)$ denotes the first homotopy group.

3.2 Connectedness results

When P is irreducible over the complex field, the action on the fiber is transitive. That is any two points y_i and y_j of the fiber $\phi^{-1}(x_0)$ can be exchanged following a continuous path on the curve on top of some loop γ. This result also expresses the connectedness of the subspace formed by the curve $\mathcal{C}$ minus the ramification points.

We illustrate this claim with a very simple example. We take $P = y^2 - x$ and $x_0 = 1$. We have two roots $y_1 = 1$ and $y_2 = -1$. If we follow the circle $x(t) = e^{2i\pi t}$ $(0 \leq t \leq 1)$, we can parameterize the roots by $y_1(t) = e^{i\pi t}$ and $y_2(t) = -e^{i\pi t}$. After a round the two roots are exchanged.

If $\mathcal{C}$ is a smooth curve of degree n, then for a generic projection, its discriminant has $n(n-1)$ points. A loop around each of them generates one of the $\frac{n(n-1)}{2}$ transposition of the n points of a smooth fiber. To give an idea of the combinatorial explosion, for $n = 100$, there are about 10^4 points in the discriminant and about 10^{158} permutations of the fiber.

In fact there is a much stronger connectedness result which is a consequence of a theorem of M. Harris. The theorem says that if we perform a **generic** change of coordinates before taking the projection, then not only the action of the monodromy group is transitive but any permutation of the point of the fiber $\phi^{-1}(x_0)$ can be obtained by following a continuous path on the curve on top of some loop γ. We state the following theorem (also used in [16]) which can be deduced from Harris's result by methods from Algebraic Geometry related to properties of genericity. A complete proof is given in [22].

THEOREM 3.1. *Let P be a monic square-free polynomial in $\mathbb{Q}[X, Y]$ which admits (in an extension $\mathbb{Q}[\alpha]$ of $\mathbb{Q}$) a factorization $P = P_1 \cdots P_s$ with $n_i := deg(P_i)$. As above, we consider the plane curve $\mathcal{C}$ defined by P and its s irreducible components $\mathcal{C}_i$, that we project on the x-axis after a generic change of coordinates. Then the first homotopy group of the complement of the discriminant locus acts on a smooth fiber as the product of the symmetry groups $\mathcal{S}_{n_1} \times \mathcal{S}_{n_2} \times \ldots \times \mathcal{S}_{n_s}$.*

4. EFFECT OF A PERTURBATION

To simplify the exposition, we first consider the simple case when P has two factors $P = P_1 P_2$ with $\deg P_1 = n_1$, $\deg P_2 = n_2$ hence $\mathcal{C}$ has 2 smooth irreducible components that we project on the x-axis after a generic change of coordinates. Each of them has a monodromy action. We can relate the monodromy of $\mathcal{C}$ and the monodromies of the $\mathcal{C}_i$. As $\mathrm{D}iscr(P, y) = \mathrm{R}es(P, P'_y, y)$, we have:

$$\mathrm{D}iscr(P, y) = \mathrm{D}iscr(P_1, y)\mathrm{D}iscr(P_2, y)\mathrm{R}es(P_1, P_2, y)^2.$$

Denote by Δ, Δ_1, Δ_2, $\mathcal{R}$ the corresponding zero-sets. $\mathcal{R}$ is formed by the intersection points of the two components. By genericity and smoothness, we have the following disjoint union:

$$\Delta = \Delta_1 \cup \Delta_2 \cup \mathcal{R}.$$

As we are in the smooth case, turning around one of the points in $\mathcal{R}$ induces the identity on a smooth fiber, whereas turning around one of the points in $\Delta_1 \cup \Delta_2$ exchanges two points in a smooth fiber. So the monodromy action $\pi_1(C - \Delta) \to \mathcal{S}_n$ is the product of the two monodromy actions:

$$\pi_1(C - \Delta) \to \mathcal{S}_{n_1} \times \mathcal{S}_{n_2} \to \mathcal{S}_n.$$

4.1 A simple case

By a general small perturbation of P into $P + \Delta P$, the set $\mathcal{R}$ of double points gives rise to a set of "clusters" formed by couples of near points. Thus the first homotopy group of the complementary of the discriminant locus increases.

If a loop γ separates the two points of such a cluster, then the corresponding permutation of the smooth fiber connects the two components. This is the geometric translation that a generic perturbation of a composite P becomes an irreducible polynomial in $\mathbb{C}[x, y]$.

Example:

The polynomial equation $P = y^2 - x^2 = (y - x)(y + x)$ defines two lines, thus $\Delta_1 \cup \Delta_2$ is empty and $\mathcal{R} = \{0\}$. Consider a perturbation $\Delta P = \epsilon^2 << 1$ so $P + \Delta P = y^2 - x^2 + \epsilon^2$ is the equation of a hyperbola. Then the discriminant locus of the projection of this hyperbola on the x axis is a "cluster" formed by the two points $\{-\epsilon, +\epsilon\}$ in the x axis.

The fiber defined by P on top of $x_0 = 1$ is the pair of points $M_1 = (1, -1)$ and $M_2 = (1, 1)$. The fiber defined by $P + \Delta P$ on top of $x_0 = 1$ is the couple of points $N_1 = (1, -\sqrt{1 + \epsilon^2})$ and $N_2 = (1, \sqrt{1 + \epsilon^2})$. N_1 and N_2 are small perturbations of M_1 and M_2, but they are now exchanged if we follow a loop from $x_0 = 1$ passing through the cluster. Indeed in the complex setting the hyperbola is irreducible and thus remains connected even if we remove a finite number of points. However if we consider only loops which remain far away from the cluster, the two points of the fiber can never be exchanged. This expresses the geometric fact: with a "rough" scaling the hyperbola looks like two lines.

Metric analysis

We see we need a metric analysis to understand the perturbation. For example, for $n = 100$, with the hypothesis that the 3 loci $\mathrm{D}iscr(P_1, y)$, $\mathrm{D}iscr(P_2, y)$, and $\mathrm{R}es(P_1, P_2, y)$ have only simple roots, using Ostrowski's inequalities [14], a relative precision on the coefficients of 10^{-12} generates small enough clusters and "leaves room" in the x plane to draw loops avoiding the clusters using a marching algorithm (we will later describe this procedure in section 6).

4.2 General case

In the general case, the geometric situation can be more intricate because the components can be singular and also can intersect on singular points. Then a generic projection cannot separate the different discriminant locus of the components. Nevertheless, we can rely on the theorem stated in the previous section for the description of the monodromy action in an exact setting. But we will have to deal with an approximate setting.

By a general perturbation of P, the intersection points of two (or several) components may give rise to more complicated clusters of points. In the most extreme case it could be a cluster of $\deg(P)$ points. Ostrowski's inequalities can handle that case and provide sharp estimates, hence the previous analysis can be generalized along the same lines. However the required precision may become huge.

Therefore there are two main strategies of computation. Either we perform (as a preprocessing step) a geometric analysis of the singularities, identify and locate them, then try to avoid them (or take advantage of their knowledge if we can). Or we perform computations with very high precision (floating point with thousands of digits) with the expectation that the clusters remain very small and that the path we will construct by our marching algorithm does not cross a cluster. Such an expectation will almost surely produce errors which can be difficult to detect and correct.

5. A SIMPLE CONSERVATION LAW

We consider, as above, the restriction ψ of a generic projection ϕ of a curve $\mathcal{C}$ on top of the complement of the discriminant locus Δ. Then $\psi : \pi^{-1}(\mathbb{C} - \Delta) \to \mathbb{C} - \Delta$ is a finite covering.

We will present a new "conservation law". When we consider the inverse image of a grid by π, it allows us to characterize the subsets of points of a fiber belonging to an irreducible (over $\mathbb{C}$) component of $\mathcal{C}$.

5.1 Triplets and zero-sum relations

For an arbitrary polynomial $P \in \mathbb{C}[x, y]$ monic in y of degree n and of total degree n, consider 3 points $a, b, c \in \mathbb{C}$ and denote by $Z(a)$ the zeros of $P(a, y)$, similarly for b and c:

$$Z(a) = \{a_1, a_2, \ldots, a_n\}$$

$$Z(b) = \{b_1, b_2, \ldots, b_n\}$$

$$Z(c) = \{c_1, c_2, \ldots, c_n\}$$

We will refere to this geometric situation by saying that $Z(a), Z(b), Z(c)$ are the fibers on top of the points a, b, c.

PROPOSITION 5.1. *For any fixed ordering of the roots, define the (weighted) sums of roots:*

$$\mathcal{U}_1 = (a - b)c_1 + (b - c)a_1 + (c - a)b_1$$
$$\vdots$$
$$\mathcal{U}_n = (a - b)c_n + (b - c)a_n + (c - a)b_n$$

Then we have:

$$\mathcal{U}_1 + \mathcal{U}_2 + \ldots + \mathcal{U}_n = 0.$$

Proof: This is trivial if two of the 3 points are equal, so let suppose that the 3 points $a, b, c \in \mathbb{C}$ are distinct. As $P \in \mathbb{C}[x, y]$ is monic and has its degree in y equal its total degree, it can be written:

$$P(x, y) = y^n + (Ax + B)y^{n-1} + Q(x, y)$$

A and B are two rational numbers and $Q(x, y)$ has only terms of degree in y smaller than $n - 1$.

Replacing x successively by a, b, c and applying the first Viete formula for the sum of the roots, we get:

$$-\sum a_i = Aa{+}B \; ; \; -\sum b_i = Ab{+}B \; ; \; -\sum c_i = Ac{+}B \; .$$

Thus $(a - b)\sum c_i + (b - c)\sum a_i + (c - a)\sum b_i = 0$.

Remark 1: This result can be generalized to more than 3 points, but we do not need this generalization in the sequel.

Remark 2: If we let $b - a = c - a = 2\epsilon$, divide by ϵ^3 and take the limit when ϵ goes to 0, then $\mathcal{U}_i$ is changed into the second derivative of the implicit function defined by $P(x, y) = 0$ near by the points (a, a_i). So we recover the criteria discussed in [19],[18], [5],[16].

5.2 Path following on a grid

We consider the inverse image by ψ of a path λ in $\mathbb{C} - \Delta$ connecting 3 distinct points a, b, c. We first index the points in the fiber $Z(a) = \psi^{-1}(a)$ on top of a, that we denote by a_i, then we deduce the indices of the points of the two other fibers $Z(b)$ and $Z(c)$ by path following in the covering

$\phi^{-1}(\mathbb{C} - \Delta)$, we denote them by b_i and c_i. There is no ambiguity once we have choosen a path in $\phi^{-1}(\mathbb{C} - \Delta)$.

Then we form the linear combinations:

$$\mathcal{U}_i = (a-b)c_i + (b-c)a_i + (c-a)b_i.$$

Claim:

With the same kind of genericity argument used in [16] we can generalize theorem 3.1, see [22],

After a random affine change of coordinates, if $a, b, c \in \mathbb{C}$ are chosen randomly, then a partial sum of the $\mathcal{U}_i$ is zero iff it corresponds to an irreducible (over $\mathbb{C}$) factor of the polynomial P.

Here "corresponds" means that the points a_i indexed by the subset J of indices i of the partial sum, are exactly the intersection points of the fiber $Z(a)$ with an union of irreducible components of the curve defined by P.

Conservation law:

Now, let $a, b, c, d, e, ...$ be $\nu > 3$ nodes in $\mathbb{C} - \Delta$. We choose (see below) a path, or a tree of paths, in $\mathbb{C} - \Delta$ to connect them. So we can index the points in the fiber $Z(a)$ and deduce the indexing of the points of the other fibers by path following.

Then, the zero sum relation for a triplet a, b, c indexed by a subset J (and corresponding to a factor of P) gives rise to a zero sum relation indexed by the same J for any choices of a triplet among the ν elements. This is what we may call a "conservation law".

Therefore, if we are able to perform simultaneous path continuation algorithm on the finite covering defined by $\mathcal{C}$, we can collect and combine many instances of the criteria. They will allow efficient and robust detection of the irreducible components of $\mathcal{C}$.

5.3 Factors in an exact setting

We use the previous properties to compute (exactly in $\mathbb{C}$) the factors (over $\mathbb{C}$) of a polynomial P.

The previous steps provide us with a structured grid of points on the zero set $\mathcal{C}$ of P. We denote them by $M_j^k = (x^k, y_j^k)$ for $(1 \leq j \leq n)$. To each triplet of points among the x_k, indexed by (k_1, k_2, k_3), and to each integer j we associate the complex number $\mathcal{U}_j^{(k_1,k_2,k_3)}$.

We collect all these numbers in a matrix $\mathcal{M}$ of dimension $n \times N$, where $N \geq n$ is the number of triplets (to be choosen later).

We know that each factor of P generates a zero sum of $\mathcal{U}_j^{(k_1,k_2,k_3)}$ with j belonging to the same subset of $\{1, ..., n\}$ for every index (k_1, k_2, k_3). This means that to such a factor is attached an element in the kernel of $\mathcal{M}$ whose entries are either 0 or 1. We can show that, by genericity, this condition is necessary and sufficient.

So we get a partition of the fiber $f^{-l}(xo)$ into p subsets. Extending this partition along the grid, we get p sub grids. By interpolation, using Vandermonde matrices emanating from each of the p grids, we can recover polynomials monic in y and test that they are indeed the desired factors of P.

5.4 Factors in an approximate setting

We follow the same procedure with approximate data, and retain the notations $M_j^k = (x^k, y_j^k)$, $\mathcal{U}_j^{(k_1,k_2,k_3)}$ and $\mathcal{M}$.

In this model of computation, zero sums are only approximately zero, and the consideration of the kernel of $\mathcal{M}$ is replaced by that of the approximate kernel computed by SVD (Singular Value Decomposition). We choose x^k well apart in $\mathbb{C} - \Delta$ in order to stabilize the computation. We choose N great enough (say $2n$) in order to ease the computation by diminishing the dimension of the approximate kernel.

The recognition of the desired vectors in the approximate kernel, is efficient because they are of a special form (their entries are either 0 or 1) and because for $N = 2n$, genericaly they will generate the kernel.

The idea of making a matrix of zero relations (not exactly the same relations as ours) and consider such vectors in the kernel was considered in [19].

6. A MARCHING ALGORITHM

We use an adaptation of the algorithm in [3].

6.1 Numerical Parameterization

In [3] we find a method for the numerical parameterization of a path $(x(s), y(s))$ in the curve defined by $P(x, y) = 0$, together with a heuristic for choosing directions on the path that keep the path away from potential ramification points of nearby factorable curves. We here adapt that method for the computation of loops γ.

As in [3] we differentiate with respect to the parameter s to find the equations: $P_x\dot{x} + P_y\dot{y} = 0$. If $P_y \neq 0$, then $\dot{y} = -\dot{x}P_x/P_y$. Choosing a complex time parameter $s = e^{i\theta}x$ gives

$$\dot{y} = -e^{i\theta}\frac{P_x(x(s), y(s))}{P_y(x(s), y(s))}\,. \qquad (1)$$

We see that, unlike the joint parameter case in [3], once the loop γ in x has been specified, then y is locally fixed by the uniqueness theorem for the solution of initial value problems, and that θ plays no role. Hereafter let $\theta = 0$.

6.2 Heuristic on the condition number

Now we consider a smooth fiber $y_0^1, \ldots, y_0^n$ on top of a point x_0 in the x axis and the n paths on top of a path $x = \gamma(t)$ starting from x_0. The condition number of each piece $y^j(t)$ of the curve is $\alpha = 1/\sqrt{|p_y(\gamma(t), y^j(t))|}$ (a simple derivation from the result of [3]). However, we wish to avoid ramification points on all leaves of the curve. Therefore we define the *condition number* α as

$$\alpha = \sum_{j=1}^{n} \frac{1}{\sqrt{|p_y(\gamma(t), y^j(t))|}}\,. \qquad (2)$$

We wish to choose the geometry of the loop γ so as to avoid regions of large condition number. As in [3], differentiation of α leads to a derivative expression for $\dot{\alpha}$, which can be monitored locally in the construction of the loop. Control-theoretic techniques can thus be used to choose the loop to avoid regions of large α.

We simply use the Maple `dsolve` command with the numeric option, which implements an improved version of the NODES package [20].

7. COMBINATION OF TOOLS

We now combine the tools presented in sections 3 and 5 to obtain a powerful factoring algorithm.

7.1 Size of the matrix

The partial information provided by the monodromy is taken into account for diminishing considerably the size of the matrix $\mathcal{M}$. Indeed, we were able to group the n elements of each fiber into m blocks ($m \ll n$).

$$\{1, ..., n\} = \bigcup_{\ell=1}^{m} I_\ell.$$

All the fiber points associated to a block I_l belong to the same irreducible component. We can therefore replace the matrix $\mathcal{M}$ by a new matrix $\mathcal{N}$ of dimensions $m \times N$ whose entries are given by:

$$\mathcal{N}_\ell^i = \sum_{j \in I_\ell} \mathcal{U}_j^i.$$

7.2 Precision

Because of the genericity hypothesis, any zero sum should correspond to a factor a fortiori for N simultaneous zero sums. We consider a rectangular matrix $\mathcal{N}$ of dimensions $m \times N$ with $N = 2m$. Then the probability is very small that the kernel of $\mathcal{N}$ or even its approximate kernel contains any other element besides the ones generated by the zero sums.

A perturbation of $P + \Delta P$ of P produces a perturbation of the same order of magnitude on the y coordinates of a smooth fiber on top of a point x_1 far enough from the discriminant locus of the projection of the curve on the x axis if x_1 is not too big (say $|x_1| < 10$). So the induced perturbation on the entries of $\mathcal{N}$ is less than $10n$ the same order of magnitude. It is easy to handle by SVD computations and recover an approximate kernel, without high precision computation.

8. ALGORITHM, THE DIFFERENT STEPS

1) Reduction to a bivariate polynomial P, irreducible over $\mathbb{Q}$, monic in y of degree n and in generic coordinates. P defines a plane curve which projects on the x-axis. Choice of a base point out of the discriminant locus (say $x_0 = 0$), approximate computation of the corresponding fiber $Z(0) = \{y_1^0, ..., y_n^0\}$.

2) Use the marching algorithm to compute two different paths joining x_0 and infinity which avoid the discriminant locus and put together form a (big) loop γ. By path following, compute the monodromy action along γ on the fiber $Z(0)$. This defines a first partition of $Z(0)$ hence of $\{1, \ldots, n\}$ into m subsets.

3) Choose s points $\{a^1, \ldots, a^k\}$ on γ, compute their fibers $\{Z(a^1), \ldots, Z(a^k)\}$ and index them coherently with $Z(0)$ by following (continuously) the roots of P on top of γ.

4) Consider N triplets $\{T_1, \ldots, T_N\}$ made by taking points in $\{0, a^1, \ldots, a^k\}$. Compute the corresponding numbers $\mathcal{U}_1^{T_1}$, $\ldots$, $\mathcal{U}_n^{T_N}$ and form the matrix $\mathcal{N}$ as in the previous section.

5) Compute a set of generators of the kernel K of $\mathcal{N}$. Recognize all the generators such that their entries are only either 0 or 1. They define the aimed partition of $Z(a)$: the partition induced by the intersection with each irreducible component. Extend by path following (thanks to the coherent indexing of the fibers) this partition to the other fibers $\{Z(a^1), \ldots, Z(a^k)\}$. Consider the set of subgrids each corresponding to a same irreducible component.

6) Interpolate on each of these subgrids to get the approximate absolute factors $P_1, \ldots, P_s$ of P.

7) Compute a suitable representation of the aimed extension of $\mathbb{Q}$, recognize the exact coefficients of P_1 in this extension and check by exact division the divisibility.

9. AN EXAMPLE

We consider the following polynomial of degree 9 with integer coefficients which is irreducible over $\mathbb{Q}$. We use this simple example to better explain some steps of our algorithm by providing a (hopefully) clear illustration.

$$P = -3x^9 + 8x^6y^3 - 5x^3y^6 + y^9 - 4x^7y+$$
$$3x^4y^4 - 8x^7 + 8x^6y - x^5y^2 + 6x^4y^3 - 10x^3y^4$$
$$+x^2y^5 + 3y^7 - 3x^5y + 3x^4y^2 - 5x^3y^3 + 4x^2y^4$$
$$+3y^6 - 4x^5 + 5x^4y - 11x^3y^2 + 5x^2y^3 + 4xy^4$$
$$+3y^5 - x^4 - 16x^3y - x^2y^2 + 8xy^3 + 6y^4 - 10x^3$$
$$-16x^2y + 4xy^2 + 8y^3 - 20x^2 + 3y^2 - 16x + 7y - 3.$$

This polynomial is monic in y. For sake of clarity, we do not perform any change of coordinates,

We first compute the fiber on top of $x = 0$. With Maple we get via [fsolve(subs($x = 0, P$)$, y$, complex)]

$$Z_0 = [-1.1277696 - .50994583I, -1.1277696 + .50994583I,$$
$$-.16451672 - 1.0398063I, -.16451672 + 1.0398063I,$$
$$.24753138 - 1.6184039I, .24753138 + 1.6184039I,$$
$$.32903345, .88023822 - 1.1084581I, .88023822 + 1.1084581I]$$

We see that the roots are well separated. Following our algorithm (see the previous section) we should now find a path in the x complex plane avoiding the points of the discriminant of P. It happens that in this example the axis of pure imaginary points, $x = ti$ with t real, is far away from the discriminant locus. So we can choose to follow by continuity these 9 roots of P when x remains on that axis.

Therefore we just have to substitute $x = ti$ and follow the 9 roots on top of the 2 paths $t \geq 0$ and $t \leq 0$, then compare the 9 asymptotic values of y/t when t goes to + or - infinity. By composition this gives us a permutation corresponding to the monodromy along the $x = ti$ axis. As the 9 roots remain well separated when we move x along this axis, this marching algorithm can be done safely. Once we have done that, we get a first partition of Z_0 into 5 classes:

$$\{-.16451672 - 1.0398063I\},$$

$$\{-.16451672 + 1.0398063I\},$$

$$\{.32903345\},$$

$$\{-1.1277696 + .50994583I,$$

$$.24753138 - 1.6184039I, .88023822 + 1.1084581I\},$$

$$\{-1.1277696 - .50994583I,$$

$$.24753138 + 1.6184039I, .88023822 - 1.1084581I\}.$$

So with our notations: $n = 9$ and $m = 5$. Now we should consider $N = 10$ triples of values of x. For that we compute the roots of P in several points of the $x = ti$ axis and relate them by continuity: for i from 1 to 30 we do

$$Z[i] := [fsolve(subs(x = 0.1iI, P), y, complex)];$$

Then take $T_1 = [0.1, 1.2, 1.9]$, and similarly for the other triplets T_k. For instance for the roots indexed by 1 on top of T_1 we get the 3 values:

$$y_1^{0.1} = -.1707524204 - 1.095846439I,$$

$$y_1^{1.2} = -.3590843406 + 1.306993679I,$$

$$y_1^{1.9} = -.8595156610 + 1.136938773I.$$

So we can form the linear combination:

$$\mathcal{U}_1^{T_1} = (0.1 - 1.2)(-.8595156610 + 1.136938773I)$$

$$+(1.2 - 1.9)(-.1707524204 - 1.095846439I)$$

$$+(1.9 - .1)(-.3590843406 + 1.306993679I)$$

$$= .4186421079 + 1.869048479I.$$

Then we compute $\mathcal{U}_2^{T_1}$, ..., $\mathcal{U}_9^{T_1}$. So we get the first line of the matrix $\mathcal{N}$.

Similarly we compute all the entries of the matrix $\mathcal{N}$ (with 10 lines) and compute its approximate kernel.

It is generated by the 3 vectors $V1 = (1, 1, 1, 0, 0)$, $V2 = (0, 0, 0, 1, 0)$, $V3 = (0, 0, 0, 0, 1)$. This indicates the partition of the fiber by the irreducible components into 3 classes. So P should factorize into a product of three polynomials of degree 3.

Now we follow each of the 3 classes of this last partition along $x = ti$ axis, and interpolate on these grid. So we get three polynomials with approximate coefficients that we denote by $P1$, $P2$, $P3$:

$$P1 = y^3 - .682327xy - .5344287x^3 - 1.36465x + y - .36465$$

$$P2 = y^3 + (.341163 - 1.1615414I)xy-$$

$$-(2.2327856 + .79255199I)x^3$$

$$+(.68232780 - 2.3230828I)x + y + 1.6823278 - 2.3230828I$$

$$P3 = y^3 + (.341163 + 1.16154I)xy-$$

$$-(2.2327856 - .79255199I)x^3$$

$$+(.68232780 + 2.3230828I)x + y + 1.6823278 + 2.3230828I.$$

We first check that the product is approximately P. This is true here up to 10^{-8}. Then we compute a polynomial q whose roots are the 3 coefficients of xy:

$$q = (t + .68232780)(t - .34116390 + 1.1615414I)$$

$$(t - .34116390 - 1.1615414I);$$

$$= t^3 + 1.0000000 - .2757127510^{-10}I + 1.0000000t + 10^{-9}It$$

We recognize a good approximation of the irreducible polynomial $t^3 + t + 1$ whose first root we denote by u.

Then $u = -.6823278038$, $u^2 = .4655712318$. And we get:

$$P1 := y^3 + uxy + (u^2 - 1)x^3 + 2ux + y + 2u + 1.$$

And we can check by exact division (with coefficients in $\mathbb{Q}[t]/(t^3 + t + 1)$) that P is a multiple of $P1$.

10. CONCLUSION

The current algorithms for absolute factorization in Computer Algebra systems are limited in their range of applicability. They can hardly treat bivariate polynomials of medium degrees. In this paper, we have presented a new algorithm for computing an absolute factorization of bivariate rational polynomials. It relies on geometric properties of a generic projection of the corresponding complex plane curve $\mathcal{C}$ on the x axis and it also uses approximate computations with big floats. It is designed to improve several other algorithms and notably the one described in [16] which works very efficiently for polynomials of medium degrees. So our challenge is to factorize over $\mathbb{C}$ polynomials of degree 100 or more.

From an algorithmic point of view, the needed genericity is easily achieved with probability almost one, by performing affine linear change of coordinates whose coefficients are provided by a standard function "random" available on any computer. One drawback is that after that operation the representation in a monomial basis of a polynomial becomes dense. However this difficulty can be bypassed by using a straight line program representation. Another, more serious, is that such translations may be ill-conditioned.

In order to perform numerical marching (also called homotopy) algorithms, we were obliged to represent complex numbers by big floats approximations. This induces a very serious difficulty. Indeed a general small perturbation of a composite curve is an irreducible one, so following a smooth path in the x axis, we can jump undiscernibly from the approximation of one irreducible component to the approximation of another irreducible component. The only way we see to bypass this difficulty of following such undesirable connecting paths is to choose path far away from the clusters (or constellations) of points resulting from the perturbation of multiple points of the discriminant locus. We proposed two strategies, either rely on a prior geometric study of the possible singularities which can appear in the considered curve, or use really big floats which is time and memory consuming. In a future work, we intend to analyze further how these strategies can be developed and combined in order to get an efficient and reliable algorithm which can factorize all the polynomials of high degrees.

Another direction of investigation is to generalize our factorization algorithm into an algorithm for computing the irreducible (over $\mathbb{C}$) decomposition of space curves or more generally of positive dimensional schemes. One of the authors has already done some work in this direction in [6] and [7]. This was also investigated by many authors including [21].

11. ACKNOWLEDGEMENT

This work was initiated when the second author (A. Galligo) visited the University of Western Ontario (UWO) in London, Ontario (Canada) during the spring 2001 and held an Ontario Research Chair in Computer Algbera at the Ontario Research Centre for Computer Algebra. He would like to thank UWO and ORCCA for their hospitality.

12. REFERENCES

[1] Bajaj C. Canny J. Garrity R. Warren J. *Factoring rational polynomials over the complexes*, ISSAC'89 Proceedings, (1989), pp 81-90.

[2] Chistov, A.L. and Gregoriev D. Y. *Subexponential-time solving systems of algebraic equations* preprint (1983).

[3] Corless R.M. Giesbrecht M.W. Hoeij v.M. Kotsireas I.S. Watt S.M *Towards Factoring Bivariate Approximate Polynomials*, ISSAC'2001 Proceedings, London, Canada, July 2001, pp. 85-92.

[4] Duval D. *Absolute factorization of polynomials: a geometric approach*, SIAM J. Comput. 20 (1991), no. 1, pp. 1-21.

[5] Galligo, A. and Watt, S. *An absolute primality test for bivariate polynomials* Proc. Intern. Symp. on Symbolic and Algebraic Computation, 217-224, ACM Press (1997).

[6] Galligo, A. and Ruppecht, D. *Semi-Numerical Determination of Irreducible Branches of a Reduced Space Curve* Proc. Intern. Symp. on Symbolic and Algebraic Computation, 137-142, ACM Press (2001).

[7] Galligo, A. and Ruppecht, D. *Absolute irreducible decomposition of Curves* To appear in J. Symb. Comp.

[8] Heintz, J. and Sieveking, M. *Absolute primality of polynomials is decidable in random polynomial time in the number of variables* Proc. ICALP (1981), LNCS 115, pp. 16-28.

[9] Kaltofen E. *Fast parallel absolute irreducibility testing*, JSC vol 1, 1985, pp. 57–67.

[10] Kaltofen E. *Polynomial factorization 1987–1991.* LATIN'92 Proceedings, Sao Paulo, Brazil, 1992, pp. 294-313, Lecture Notes in Comput. Sci., 583, Springer, Berlin, 1992.

[11] Kaltofen E., *Effective Hilbert Irreducibility* Information and Control, 66, 123-137 (1985).

[12] Mumford D. *Introduction to Algebraic Geometry*, Cambridge Mass., Harvard University, 1955.

[13] PARI-GP http://www.parigp-home.de/

[14] Ostrowski A. M. *Solution of equations and systems of equations*, New York, Academic Press, 1960.

[15] Ragot, J. F. *Sur la factorisation absolue des polynomes*, PhD Thesis, Univ. Limoges, (1997).

[16] Ruppecht, D. *Semi-numerical absolute factorization of polynomials with integer coefficients* To appear in Journal of Symb. Comp. (2001).

[17] Ruppecht, D. *Elements pour un calcul approche et certifie : etude du PGCD et de la factorisation* PhD thesis, University of Nice, France, (2000), `http://www-math.unice.fr/~rupprech`

[18] Sasaki T. Suzuki M. Kolar M. Sasaki M. *Approximate factorization of multivariate polynomials and absolute irreducibility testing.* Japan J. Indust. Appl. Math. 8 (1991), no. 3, pp. 357-375.

[19] Sasaki T. *Approximate Multivariate Polynomial Factorization Based on Zero-Sum Relations* Proc. Intern. Symp. on Symbolic and Algebraic Computation, 284-291, ACM Press (2001).

[20] Shampine L.F. Corless R.M. *Initial Value Problems for ODEs in Problem Solving Environments* J. Comp. & App. Math. (2000) 125, pp. 31-40

[21] Sommese A.J. Verschelde J. and Wampler C.W. *Using Monodromy to Decompose Solution Sets of Polynomial Systems into Irreducible Components* Proc. of a NATO Conference in Eilat Israel, "Application of Algebraic Geometry to Coding Theory, Physics and Computation", pp. 297-315, Kluwer Academic Publishers, (2001).

[22] Sommese A.J. Verschelde J. and Wampler C.W. *Symmetric functions applied to decomposing solution sets of polynomial systems* preprint, november 2001.

[23] Sommese A.J., Verschelde J. and Wampler C.W. *Functions Applied to Decomposing Solution Sets of Polynomial Systems*, (2001), preprint available from `http://www.math.uic.edu/~jan`.

[24] Sommese A.J., Verschelde J. and Wampler C.W. *Numerical decomposition of the solution sets of polynomial systems into irreducible components,* SIAM Journal on Numerical Analysis, 38 (2001), 2022–2046.

[25] J. von zur Gathen and J. Gerhard *Modern Computer Algebra* Cambridge University Press, (1999).

[26] Walker R.J. *Algebraic curves*, Princeton University Press, 1950. Princeton mathematical series ; vol 13.

[27] Zippel, R. E. *Effective polynomial computation* Boston, Kluwer Academic Publishers, Kluwer international series in engineering and computer science vol 241 (1993)