Décomposition Irreductible de Courbes

André Galligo and David Rupprecht

Université de Nice-Sophia Antipolis, France

Journées : Courbes, surfaces et visibilité

10 et 11 Dcembre 2001 ; IHP (Paris).

Introduction

- In [Galligo, Watt 1997] and [Rupprecht 2001] an algorithmic method for computing absolute factorization of multivariate polynomials.

  An implementation has shown that it is very efficient for medium degrees (about 60).

- The computation of irreducible branches of maximal dimension of an algebraic subvariety of $\mathbb{C}^p$ is a generalization.

  For sake of simplicity we limit ourselves to the case of curves in $\mathbb{C}^7$.

- The output we provide consists of

  - extensions of $\mathbb{Q}$ and

  - adapted representations for irreducible branches with coefficients in these extensions .

- This is an alternative to : projection + factorization.

The decomposition algorithm is divided into several steps.

1 A generic change of coordinates and computation of a generic plane section of the curve $\mathscr{C}$.

2 A combinatorial procedure (Zero sums search) computes the partition induced on the plane section by the irreducible components of $\mathscr{C}$.

3 An adapted Newton-Hensel liftings to get approximations of the factors of the equation of a generic projection of $\mathscr{C}$.

4 Construction of candidates

- for the equation of a generic projection of $\mathscr{C}$ and
- for its absolute factorization.

5 Test of the validity of these candidates.

Preliminaries

Genericity and Galois group action

We consider changes of coordinates with coefficients in $\mathbb{Q}$ of the form:

$X = x + ay + b_1 z^{(1)} + \ldots + b_\tau z^{(\tau)}$; $Y = y + c_1 z^{(1)} + \ldots + b_\tau z^{(\tau)}$.

Genericity is obtained by taking random coefficients.

Lemma 0.1 *Let P be a monic square-free polynomial in $\mathbb{Q}[X,Y]$ irreducible in $\mathbb{Q}[X,Y]$.*
There exists an extension $\mathbb{Q}[\alpha]$ of $\mathbb{Q}$ and a factorization $P = P_1 \cdots P_s$, with

$$P_i = Y^m + c_{m-1}(\alpha_i, X)Y^{m-1} + \cdots + c_0(\alpha_i, X),$$

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

The numbers b_i

Let P be a monic square-free polynomial in $\mathbb{Q}[X,Y]$ of degree n.
For $x_0 \in \mathbb{Q}$, generic,

- the roots $y_1, \cdots, y_n$ of $P(x_0, Y)$ are distinct
- the curve defined by P is smooth at the points (x_0, y_i)
- there exist analytic functions $\varphi_i(X)$ in the neighborhood of x_0 (for $i = 1, \cdots, n$) such that

$$\begin{cases} \varphi_i(x_0) = y_i \\ P(X, \varphi_i(X)) = 0. \end{cases}$$

$$\varphi_i(X) = y_i + a_i(X - x_0) + b_i(X - x_0)^2 + \cdots.$$

- Then

$$\sum b_i = 0.$$

Lemma 0.2 *:*
If P has no factor of degree 1, then for almost all values of x_0, the b_i are all non-zero and different.

Theorem 0.3 *Let Q be a polynomial of degree n. Consider $P(x, y, \lambda) = Q(x + \lambda y, y)$.*
Then for almost all specializations (x_0, λ_0) of (x, λ), the sum

$$\sum_{i \in J} b_i, \quad J \subsetneq \{1, \cdots, n\}$$

vanishes if only if it corresponds to some union of roots of a family of factors of P.

Zero sums search

We have an implementation of an efficient algorithm. On a small PC it takes :
- less than a second for n about 30 and
- less than a minute for n about 70.

Decomposition Algorithm for the reduced case

Output:

A candidate decomposition consists of:

1 the number m of irreducible components $\mathscr{C}_u$ of $\mathscr{C}$ over $\mathbb{Q}$, and the degrees n_u of the $\mathscr{C}_u$,

so $n = \sum n_u$ is the degree of the curve $\mathscr{C}$,

2 for each u,

- the number m_u of irreducible components $\mathscr{C}_k$ of $\mathscr{C}_u$ over $\mathbb{Q}$, and the common degrees p_u of the $\mathscr{C}_k$,

  so $n_u = m_u.p_u$
- an extension K_u of $\mathbb{Q}$ defined by a univariate polynomial q_u of degree m_u
- $h_u(x, y)$, absolutely irreducible with coefficients in K_u of degree p_u. $h_u(x, y)$ is a factor of a polynomial $P_u(x, y)$ with coefficients in $\mathbb{Q}$ and of degree n_u,

3 $P(x, y) = P_1(x, y)P_2(x, y)....P_m(x, y) \in I$,

4 for each u, a test showing that the ideal generated by I and $P_u(x, y)$ defines a variety of dimension 1 .

Algorithm for the non reduced case

Simplified Input:

- An ideal I generated by polynomials in $\tau+2$ variables defining a curve $\mathscr{C}$ with only one component over $\mathbb{Q}$.
- $\{x = 0\}$ is a generic plane section . $J = I|_{x=0}$, is $\mathbb{Q}$ primary (i.e. J defines a set of conjugated multiple points.

  The intersection $J \cap \mathbb{Q}[y]$ is generated by $p(y)^e$ with $p(y)$ $\mathbb{Q}$-irreducible, $e > 1$ and $\nu := deg(p) > 1$.

Output:

A candidate decomposition of the curve $\mathscr{C}$:

- The degree n of $\mathscr{C}$, the number m of irreducible components $\mathscr{C}_k$ of $\mathscr{C}$ over $\mathbb{C}$, and the common degree δ and multiplicity μ of each $\mathscr{C}_k$. $n = m\mu\delta$, $\nu = m\delta$.
- A simple extension field K of $\mathbb{Q}$ of degree m .

  A polynomial $h(x, y)$ absolutely irreducible with coefficients in K, of degree δ.
- A polynomial $P(x, y)$ with coefficients in $\mathbb{Q}$ of degree $m\delta$, multiple of $h(x, y)$ and such that $P(0, y) = p(y)$
- A test showing that $P(x, y)^e$ belongs to I.

Deflation procedure for the equations of a generic section

$\diamondsuit$ We start with a set of generators $(f_1, ..., f_s)$ of J defining a set of generators of the regular local ring $\mathcal{M}$.
We consider the following algorithm, $\mathcal{A}$, which proceeds by completion (via 4 rules) of two families $\mathcal{F}$ and $\mathcal{G}$.
When $\mathcal{A}$ starts $\mathcal{G}$ is empty and $\mathcal{F}$ contains the localizations (denoted by $\theta_1, ..., \theta_s$) of the $f_1, ..., f_s$ in $\mathcal{M}$.

1 Compute the order o of an element θ of $\mathcal{F}$, then form a partial derivative θ_a of order $o-1$ of θ.

2 If the order of θ_a is greater than 1, then put θ_a in $\mathcal{F}$.

3 If the order of θ_a is 1 and if its initial form is linearly independent of the initial forms of the element already in $\mathcal{G}$ then put θ_a in $\mathcal{G}$.

4 If the order of θ_a is 1 but if its initial form is linearly dependent of the initial forms of the element of $\mathcal{G}$ then compute (by a linear combination between θ_a and the elements of $\mathcal{G}$) a new element γ_a, if $\gamma_a \neq 0$ its initial form has order greater than 1, put γ_a in $\mathcal{F}$.

Now, the analysis procedure keeps the record of a sequence of computations followed by algorithm $\mathcal{A}$

Example:
$J = (f = y^3 + 7z^2y - zy^3 + y^4, g = y^2 - zy + z^3)$
localized at $(0,0)$. $\tau = 1$
The order of f is 3 , so we compute the second derivatives:
$f_3 = f_{yy} = 6y - 6yz + 12y^2$ and put f_3 in $\mathcal{G}$,
then $f_4 = f_{zz} = 14y$.
As the initial form of f_3 is proportional to the initial form of f_3, we compute the zero linear combination
$f_5 = 7f_3 - 3f_4 = -42yz + 84y^2$ and we put it in $\mathcal{F}$.
Now we choose a new derivative of an element in $\mathcal{F}$, e.g. $f_5 = f_{zy} = 14z - 3y^2$, its initial form is independent of that of f_3. So we put f_5 in $\mathcal{G}$.
Algorithm $\mathcal{A}$ stops.

The procedure keeps the record of the sequence of computations:
$f_3 = f_{yy}$; $f_5 = f_{zy}$
which contains only derivations and we forget the zero linear combination which was useless for this sequence.

$\diamondsuit$ The algebraic complexity of such pattern of sequences of computations can be studied and bounded. See the PhD thesis of G. Lecerf.

Flat deformation

As the section $x=0$ generic, the local scheme defined by I near by M_1 is a flat deformation along the x-axis of the one defined by J.
So a zero linear combination with coefficient in the field $\mathbb{C}$, extends to one with coefficients in $\mathbb{C}\{x\}$.

$\diamondsuit$ As we are able to lift any zero linear combinations between the initial forms to new element of the ideal I, we obtain an algorithm for computing, locally near by the generic section, a set of generators of the radical of I. So we are ready for computing Taylor expansions along the curve.

Example: Let us consider the two following polynomials.

$$F := -z^5x^3 + 2z^5x^2 - z^5x + z^3yx^2 - 2z^3yx$$
$$+z^3y + z^2x^2 - 2z^2x + z^2 - yx + z + 2y$$

and

$$G := z^6x^6 - 3z^6x^5 + 3z^6x^4 - 3z^4yx^5 - z^6x^3 + 9z^4yx^4$$
$$-9z^4yx^3 + 3z^2y^2x^4 + 3z^4yx^2 - 9z^2y^2x^3$$
$$+9z^2y^2x^2 - y^3x^3 - 3z^2y^2x - z^2x^3 + 3y^3x^2$$
$$+3z^2x^2 - 3y^3x - z^2x + y^3 + yx^2 - z^2 - zx - 3yx + z + 2y.$$

They define a multiple curve in $\mathbb{C}^3$ and $x = 0$ is a generic section.
We get

$$f(y,z) := F(0,y,z) = 2y + z + z^2 + z^3 y$$

and

$$g(y,z) := G(0,y,z) = 2y + z - z^2 + y^3.$$

So f and g vanish at $(0,0)$ and the smallest sequence of computation providing a set of generators of the corresponding maximal ideal is:
$h = f - g$ then $h'_z = 4z + 3z^2 y$.
We deform the zero linear combination into
$H := (1-x)F - G$ then

$$H'_z = -6z^5x^6 + 18z^5x^5 - 18z^5x^4 + 12z^3yx^5 + 6z^5x^3 + 5z^4x^4 - 36z^3yx^4 - 15z^4x^3$$
$$+36z^3yx^3 - 6zy^2x^4 + 15z^4x^2 - 12z^3yx^2 - 3z^2yx^3 + 18zy^2x^3 - 5z^4x + 9z^2yx^2$$
$$-18zy^2x^2 - 9z^2yx + 6zy^2x + 3z^2y - 4zx + 4z.$$

So G and H'_z define locally the reduced curve associate to the given curve.

Other steps

Now, we can follow the steps of the decomposition algorithm for the reduced case.
I.e. for the step 2, we compute numerically the roots y_i of p. Each root y_i corresponds to only one point M_i of the considered generic plane section of the curve $\mathscr{C}$. We compute numerically the corresponding coordinate $z_i^{(j)}$ of M_i, this can be done by solving numerically the equations of the reduced scheme.
By genericity, the point M_i is a smooth point, so one can apply the implicit function theorem to get the Taylor expansions of y and $z^{(j)}$ on the curve near by M_i. This can be done via the procedure explained in the previous subsection. Get

$$y = y_i + a_i x + b_i x^2 + \ldots \ \ and \ \ z^{(j)} = z_i^{(j)} + a_i^j x + b_i^j x^2 + .. \ (1 \leq j \leq \tau)$$

and collect the coefficients b_i.

Illustrative example of a non-reduced curve

Equations of the curve $\mathscr{C}$

$$F := 2\,y^6\,x\,z - x^2\,y^4\,z^2 + 2\,x^4\,y^2\,z + 5\,y^{28}\,x^6 + 3\,y^{32}\,x^3 + y^{24}\,x^9 - 7\,y^{20}\,x^{12}$$
$$-11\,y^{16}\,x^{15} - 4\,y^{12}\,x^{18} + 6\,y^8\,x^{21} + 5\,y^4\,x^{24} + y^8\,z - y^8\,x - 2\,x^4\,y^4 + x^6\,z$$
$$+2\,y^6\,x^2\,z - 2\,y^7\,x\,z - x^6 - y^8 - y^{32} - x^{24} - 2\,x^3\,y^4 - 3\,y^{24}\,x^6$$
$$-2\,y^{28}\,x^3 + 2\,y^{20}\,x^9 + 5\,y^{16}\,x^{12} + 6\,y^{12}\,x^{15} - 2\,x^{18}\,y^8 - 4\,x^{21}\,y^4 + y^9$$
$$-x^7 + x^2\,y^4\,z^3 - 2\,x^4\,y^3\,z - x^3\,y^4\,z^2 + x^2\,y^5\,z^2 - 2\,x^4\,y^2\,z^2 + 2\,x^5\,y^2\,z$$
$$+y^{36} + x^{27} + 2\,x^3\,y^4\,z + 2\,y^5\,x^3 - 2\,y^6\,x\,z^2 + y\,x^6.$$

$$G := 2\,y^6\,x\,z - x^2\,y^4\,z^2 + 2\,x^4\,y^2\,z + 2\,x^4\,z^4 - 2\,x^3\,z^6 - x^2\,z^8 + 2\,x\,z^{10} + x^6\,z$$
$$-2\,x^4\,z^5 + 2\,x^5\,z^4 - 2\,y^{10}\,x\,z + y^{12} - 2\,x^6 + x^9 - y^8 + 3\,x^3\,y^8 + 3\,x^6\,y^4$$
$$-2\,x^3\,y^4 - x^7 + 2\,x^3\,z^6\,y + x^2\,z^8\,y - 2\,x^4\,z^6 + x^2\,z^9 - x^3\,z^8 - 2\,x\,z^{11}$$
$$+2\,x^2\,z^{10} - z^{12}\,x + z^{12}\,y + 2\,x^3\,z^7 + z^{13} - 4\,y^6\,x^4\,z + x^2\,y^8\,z^2$$
$$+x^5\,y^4\,z^2 - 2\,x^7\,y^2\,z - 2\,x^4\,z^4\,y - 2\,x\,z^{10}\,y - z^{12} + y\,x^6.$$

$$H := 2\,y^6\,x\,z - x^2\,y^4\,z^2 + 2\,x^4\,y^2\,z + 2\,x^4\,z^4 - 2\,x^3\,z^6 - x^2\,z^8 + 2\,x\,z^{10}$$
$$+y^8\,z - y^8\,x - 2\,x^4\,y^4 + x^6\,z + 2\,y^6\,x^2\,z - 2\,y^7\,x\,z - 2\,x^6$$
$$+x^9 - y^8 + x^6\,y^4 - 2\,x^3\,y^4 + y^9 - x^7 + x^2\,y^4\,z^3 - 2\,x^4\,z^4\,y^4$$
$$-2\,x^4\,y^3\,z - x^3\,y^4\,z^2 + x^2\,y^5\,z^2 - 2\,x^4\,y^2\,z^2 + 2\,x^5\,y^2\,z - z^{12} + 2\,x^3\,y^4\,z$$
$$+2\,x^3\,z^6\,y^4 - 2\,x\,z^{10}\,y^4 + x^2\,z^8\,y^4 - 2\,x^7\,z^4 + 2\,x^6\,z^6 + x^5\,z^8$$
$$-2\,x^4\,z^{10} + z^{12}\,y^4 + z^{12}\,x^3 + 2\,y^5\,x^3 - 2\,y^6\,x\,z^2 + y\,x^6.$$

G B computations for this example

This medium sized example was designed to better explain the ideas of our approach and illustrate the different steps of our algorithm. About the hardness of this example, we can say that a Groebner basis (in short G B) of I is not easy to compute.

The resultant of two of these polynomials is not easy to compute.

We did not succeed with several distributed implementations.

Description of a generic plane section

We consider the plane section $\{x = 2\}$, defined by the ideal J spanned by
$f = F(2, y, z)$, $g = G(2, y, z)$, $h = H(2, y, z)$ in $\mathbb{Q}[y, z]$.
* the gcd of the resultant (with respect to z) of g and h and of the resultant (with respect to z) of g and f is p1 p2 with

$$p_1 := y^4 + 7 \ \ ; \ \ p_2 := y^{12} + 16y^8 + 192y^4 + 512$$

then $J = J_1 \cap J_2$ with
$s_1 := z - 3 + y \ \ ; \ \ s_2 := 128z + y^{10} + 16y^6 + 128y^2$
* J_1 is generated by p_1 and s_1, it defines 4 simple points.
* The radical of J_2 is generated by p_2 and s_2. But J_2 is generated by $(p_2^2,\ p_2 s_2,\ s_2^2)$ therefore it defines 12 multiple points each of multiplicity 3 and order 2.

The curve $\mathscr{C}$ decomposes over $\mathbb{Q}$ into:
$\mathscr{C}_1$ which is reduced of degree 4 and
$\mathscr{C}_2$ which is of multiplicity 3 and whose degree is $3 \times 12 = 36$.

Coefficients of Taylor expansions of $y(x)$ and $z(x)$

Near by the 4 simple points,it works as in the non-reduced case.

For the multiple points, we build new polynomials, such that, near by the 12 points, they locally define the reduced curve associated to $\mathscr{C}$.
This construction can be elaborated in the generic section on f, g, h then lifted to F, G, H.

As the 12 multiple points have order two, the derivatives with respect to y or z of the elements of J_2 still vanish at these 12 points.

$$GB(p_2^2, s_2^2, g_y, h_z) = (p_2, s_2)$$

So the variety associated to the ideal (g_y, h_z) consists of the 12 aimed reduced points.

By genericity, the equations $G_y(x, y, z)$ and $H_z(x, y, z)$ define a reduced curve near by our 12 points.
So we can compute the targeted Taylor expansions.

Zero sums analysis

We compute recursively the $12+4$ Taylor expansions (up to order 2) for y and z. Then the b_i.
For the 4 points defined by J_1. We easily check that the only zero sum is the trivial one. This implies that the curve $\mathscr{C}_1$ is absolutely irreducible.

A quick check on the sums among the 12 first numbers b_i provides a partition of the 12 points y_i into 3 classes of 4 points each, that we re-index $\{y_1, ..., y_4\}$, $\{y_5, ..., y_8\}$, $\{y_9, ..., y_{12}\}$. So the curve $\mathscr{C}_2$ decomposes into 3 absolutely irreducible triple components of degree 3×4.
This partition induces a factorization of p_2 into 3 factors p_{21}, p_{22}, p_{23}.
$p_{21} := (y - y_1)...(y - y_4)$ and so on.
$p_{21} = y^4 + 3.441277672$,
$p_{22} = y^4 + 6.279361164 + 10.45713023\, i$,
$p_{23} = y^4 + 6.279361164 - 10.45713023\, i$,
We recognize the 3 roots of

$$q(T) := T^3 + 16T^2 + 192T + 512.$$

Therefore, the triple components admit polynomial equations with coefficients in the splitting field of $q(T)$.

Product of Taylor expansions

By Newton-Hensel lifting we compute Taylor expansions $\phi_i(x)$ and $\psi_i(x)$ of y and z of degree 4 near by the 16 points.
Then we form the product $\prod_{i=13}^{16}(y-\phi_i(x))$. We easily recognize an approximation of :

$$P_1(x,y)=y^4+x^3-1.$$

Then we form the product $\prod_{i=1}^{12}(y-\phi_i(x))$. We easily recognize an approximation of :

$$P_2(x,y)=y^{12}+2x^3y^8+3x^6y^4+x^9$$

which admits the following $\mathbb{Q}[T]/q(T)$-irreducible factor P_{21} with coefficient in $\mathbb{Q}[T]/q(T)$:

$$P_{21}(x,y)=y^4+\frac{1}{8}Tx^3.$$

Dimension Test

In this example the equations of P_1 and P_2 are so simple that we can perform interactively a sequence of divisions, then discover that the irreducible components are monomial curves.

Conclusion

We proposed a decomposition algorithm which rely on numerical computation and on a random change of coordinates.

We have shown that we could take advantage of the large difference between the computational cost of elimination in 3 variables and elimination in 2 variables.

Most Groebner bases programs cannot solve a system of medium size polynomials in 3 variables when the associated scheme admits multiple components of positive dimension.

We believe that this geometric feature should be detected and then appropriate strategies of computations should be applied.

Our approach can be generalized to deal with multiple components of higher equidimensional varieties.

Furthermore one can address the problem of finding efficient irreducible decomposition of a general scheme not necessarily equidimensional nor reduced.