REDUCIBLE FIBERS OF POLYNOMIALS

ARNAUD BODIN

Abstract. We give an algorithm to find reducible fibers of a bivariate polynomial.

1. Ruppert's equation, Gao's theorem

Let $\mathbb{F}$ be any field of characteristic p. Let $f \in \mathbb{F}[x,y]$. The aim of this note is to give a method to find the values c for which $f-c$ is reducible based on results of W. Ruppert and S. Gao, [Ru], [Ga].

We consider the following equation :

$$\frac{\partial}{\partial y}\left(\frac{g}{f-c}\right) = \frac{\partial}{\partial x}\left(\frac{h}{f-c}\right), \tag{1}$$

where $g,h \in \mathbb{F}[x,y]$ are unknows and $f \in \mathbb{F}[x,y]$, $c \in \mathbb{F}$ are given data. This equation can be "linearized" to the equivalent equation:

$$(f-c)\cdot\left(\frac{\partial g}{\partial y} - \frac{\partial h}{\partial x}\right) = g\cdot\frac{\partial f}{\partial y} - h\cdot\frac{\partial f}{\partial x}. \tag{2}$$

Notice that this equation is linear in the coefficient of g and h.

The *bidegree* of a polynomial g is $\deg g = (\deg_x g, \deg_y g)$. Let (m,n) be the bidgree of f. We impose the following restrictions:

$$\deg g \leqslant (m-1,n), \qquad \deg h \leqslant (m,n-1). \tag{3}$$

The relation $\deg g \leqslant (m-1,n)$ means $\deg_x g \leqslant m-1$ and $\deg_y g \leqslant n$. Note that relations (3) define a finite dimensional vector space for the coefficients of g and h.

We suppose that f is not constant and that for all $c \in \mathbb{F}$, $\gcd(f-c, \frac{\partial f}{\partial x}) = 1$. Then for each g there is at most one h that satisfies (2) and (3). We define

$$G = \{g \in \mathbb{F}[x,y] \mid (2) \text{ and } (3) \text{ holds for some } h \in \mathbb{F}[x,y]\}.$$

G is a finite dimensional vector space and is at least one dimensional because $g = \frac{\partial f}{\partial x} \in G$ (for $h = \frac{\partial f}{\partial y}$).

Date: September 27, 2005.

Theorem 1.1 (Ruppert,Gao)**.** *Let $\mathbb{F}$ be a field of characteristic p and $f \in \mathbb{F}[x, y]$ of bidegree (m, n), $c \in \mathbb{F}$ with $\gcd(f - c, \frac{\partial f}{\partial x}) = 1$. If $p = 0$ or if $p > (2m - 1)n$ then the number of irreducible factors of $f - c$ is equal to the dimension of G.*

2. Finding reducible fibers

We apply this theorem to find reducible fibers of a polynomial $f \in \mathbb{F}[x, y]$, that is to say find the values $c \in \mathbb{F}$ such that $f - c$ has more than one irreducible factor. The hypothesis $\gcd(f - c, \frac{\partial f}{\partial x}) = 1$ implies that $f - c$ is reduced (i.e. do not have a repeated factor), by Stein factorization theorem this implies that the polynomial f is non-composite, that is to say not all fibers are reducible.

The method is has follows. Considers equation (2) where c, g, h are unknowns. This provides a linear system of equations in the coefficients of g and h with a parameter c. The vector space of solution has always the same dimension, excepted for a finite number of values. Theses values can be easily detected, for example after a Gauss reduction of the linear system. Then by theorem 1.1 these values are the values c such that $f - c$ is reducible.

We give below some examples and its implementation in the library `reduc.lib` for Singular, [Sing].

Example 2.1. Let $f(x, y) = x + y(x - 1)(x - 2) \in \mathbb{F}[x, y]$.

```
LIB "reduc.lib";
ring r = 0, (x,y,c), dp;
poly f = x+y*(x-1)*(x-2);
reducible(f);
> Reducible fibers f-c corresponds to the roots of c2-1
```

Then $f - 1$ and $f - 2$ are reducible.

Example 2.2. Let $q = xy + 1$, $p = xq + 1$ and $f(x, y) = 3yp^3 + 3p^2q - 5pq - q \in \mathbb{C}[x, y]$ be the Briançon polynomial.

```
LIB "reduc.lib";
ring r = 0, (x,y,c), dp;
poly q = xy+1;
poly p = x*q+1;
poly f = 3*y*p^3+3*p^2*q-5*p*q-q;
reducible(f);
```

The result is:

```
> Reducible fibers f-c corresponds to the roots of 1
```

This shows that there is no reducible fibers (as the root of the polynomial 1).

Example 2.3. We can have parameters and non-zero characteristic. Let $f_s(x,y) = x + y(x-1)(x-2)(x-s) \in \mathbb{F}_7[x,y]$.

```
LIB "reduc.lib";
ring r = (7,s), (x,y,c), dp;
poly f = x+y*(x-1)*(x-2)*(x-s);
reducible(f);
> Reducible fibers f-c corresponds to the roots of
> c3+(-s-3)*c2+(3s+2)*c+(-2s)
```

After factorization we find that reducible fibers are for the value $c = 1, c = 2, c = s$.

References

[Ga] S. Gao, Factoring multivariate polynomials via partial differential equations. Math. Comp. 72 (2003), 801–822.

[Ru] W. Ruppert. Reducibility of polynomials $f(x,y)$ modulo p. J. Number Theory 77 (1999), 62–70.

[Sing] G.-M. Greuel, G. Pfister, H. Schönemann. SINGULAR: a computer algebra system for polynomial computations. Centre for computer algebra, university of Kaiserslautern, 2001, http://www.singular.uni-kl.de.

Laboratoire Paul Painlevé, Mathématiques, Université de Lille 1, 59655 Villeneuve d'Ascq, France.

E-mail address: Arnaud.Bodin@math.univ-lille1.fr