Factoring polynomials using singularities

Martin Weimann

RISC

24/11/2011

Motivations and results

Motivation

- $\mathbb{K}$ a field.
- $F \in \mathbb{K}[x, y]$ a square-free polynomial.
- $\mathcal{C} \subset \mathbb{P}^2$ the projective curve defined by F.

Question : What are the relations between the resolution of singularities of $\mathcal{C}$ and the factorization of F ?

Adjoints Polynomials

Definition : $H \in \mathbb{K}[x, y]$ is an **adjoint polynomial** of F if it vanishes with order at least

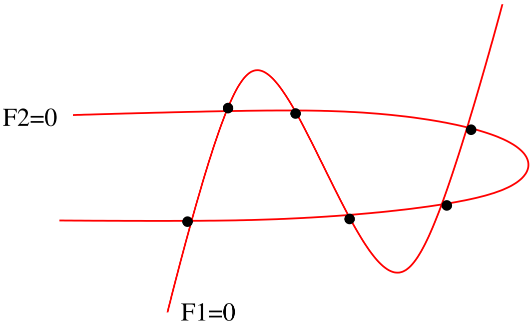
$$ord_p(H) \geq ord_p(F) - 1,$$

at each singular point p of $\mathcal{C}$ (including infinitely near ones).

- $Adj^n(F) \subset \mathbb{K}[x, y]$ generated by adjoints of degree $\leq n$.
- $\mathcal{A}^n(F) \subset \mathbb{K}[y]$ generated by mod (x) adjoints of degree $\leq n$.

Example of a degree 5 curve (I)

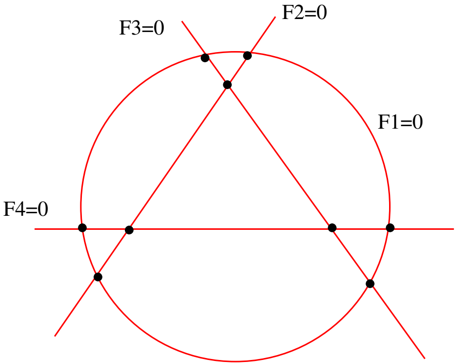
A cubic union a conic



$$
\begin{aligned}
Adj^1(F) &= 0 \\
Adj^2(F) &= \langle F_2 \rangle \\
Adj^3(F) &= \langle F_1, F_2, xF_2, yF_2 \rangle \\
\mathcal{A}^3(F) &= \langle F_1(0,y), F_2(0,y), yF_2(0,y) \rangle
\end{aligned}
$$

Examples of a degree 5 curve (II)

A conic union three lines



$$
\begin{aligned}
Adj^1(F) &= 0 \\
Adj^2(F) &= 0 \\
Adj^3(F) &= \langle F_2 F_3 F_4 \rangle.
\end{aligned}
$$

Main result

Suppose $F(0, y)$ monic squarefree of degree $d = deg(F)$.

Theorem 1 *Given the factorization of $F(0, y)$ over $\mathbb{K}$ and given a basis of $\mathcal{A}^{d-2}(F)$, one computes the rational factorization of F within $\mathcal{O}(d^\omega)$ arithmetic operations over $\mathbb{K}$.*

Remark The actual complexity for factoring bivariate polynomials belongs to $\mathcal{O}(d^{\omega+1})$ (Lecerf et al., 2007).

Recombinations using adjoint polynomials

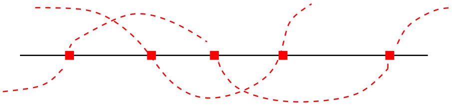
We assume for simplicity that $\mathbb{K}$ is algebraically closed.

The recombination problem

$$\begin{cases} F(x,y) = F_1(x,y)\cdots F_s(x,y) \\ F(0,y) = (y-\alpha_1)\cdots(y-\alpha_d). \end{cases}$$

Recombinations : Determine the vectors $\mu_i = (\mu_{ij}) \in \{0,1\}^d$ induced by relations

$$F_i(0,y) = \prod_{j=1}^{d} (y-\alpha_j)^{\mu_{ij}}, \quad i = 1,\ldots,s.$$



$$\Longrightarrow \quad \begin{cases} \mu_1 = (1,0,1,0,1) \\ \mu_2 = (0,1,0,1,0) \end{cases}$$

Degree d-2 adjoints mod (x) $\iff$ Recombinations

Linearization of recombinations : Determine equations and compute the reduced echelon basis of the vector subspace

$$W := \langle \mu_1, \ldots, \mu_s \rangle \subset \mathbb{K}^d.$$

Theorem 2 *One has an exact sequence of $\mathbb{K}$-vector spaces*

$$0 \longrightarrow W \longrightarrow \mathbb{K}^d \xrightarrow{A} \mathcal{A}^{d-2}(F)^v \longrightarrow 0$$

where

$$A = \left(\frac{H(\alpha)}{\partial_y F(0,\alpha)} \right)_{F(0,\alpha)=0,\ H \in \mathcal{A}^{d-2}(F)}$$

"Computing degree $d-2$ adjoint polynomials modulo (x) and solving recombinations are two equivalent problems."

Example

- Let $F(x,y) = y^5 - xy^3 - xy^2 - 3y^3 + 2xy + x^2 - 2y$. One computes

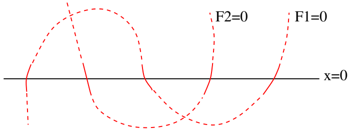
$$\begin{cases} F(0,y) = (y-2)(y-1)y(y+1)(y+2) \\ \mathcal{A}^{d-2}(F) = \langle y, y^2-1, y^3 \rangle \end{cases}$$

(e.g. using conductor in integral closure). One obtains

$$A = \frac{1}{24}\begin{pmatrix} 2 & -4 & 0 & 4 & -2 \\ 3 & 0 & 6 & 0 & 3 \\ -8 & -4 & 0 & 4 & 8 \end{pmatrix}.$$

- So $ker(A) = \langle (1,0,1,0,1), (0,1,0,1,0) \rangle$, solving recombinations :

$$F = F_1 F_2, \qquad F_1(0,y) = (y-2)y(y+2), \quad F_2(0,y) = (y-1)(y+1).$$



- There only remains to lift the induced modular factorization :

$$F(0,y) = F_1(0,y) \times F_2(0,y) \overset{Hensel}{\Longrightarrow} F(x,y) = (y^3 - 4y - x)(y^2 - 1 - x).$$

Algorithm and complexity follows

• **Recombinations :** Reduced echelon basis of the $d \times (d-s)$ matrix A of maximal rank over $\mathbb{K}$.

Requires $\mathcal{O}(d(d-s)^{\omega-1}) \subset \mathcal{O}(d^{\omega})$ operations.

• **Factorization :** Hensel lifting with precision $deg_x(F)+1$.

$$\begin{aligned} F(0,y) &= F_1(0,y)\cdots F_s(0,y) \\ \Longrightarrow F(x,y) &= F_1(x,y)\cdots F_s(x,y). \end{aligned}$$

Requires $\widetilde{\mathcal{O}}(d^2) \subset \mathcal{O}(d^{\omega})$ operations. $\square$

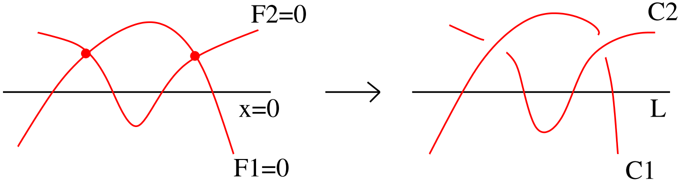
Proof of Theorem 2

One wants to prove the exact sequence

$$0 \longrightarrow W \longrightarrow \mathbb{K}^d \xrightarrow{A} \mathcal{A}^{d-2}(F)^v \longrightarrow 0$$

Disconnect the components

- $\pi : X \to \mathbb{P}^2$ the embeded resolution of singularities of $\mathcal{C}$
- C and L the strict transforms of $\mathcal{C}$ and $x = 0$.



- The irreducible factors of F are now one-to-one with the **connected** components $C_1, \ldots, C_s$ of C.

Reformulate the recombination problem

• The C_i's and the p_j's being **connected components** of C and $C \cap L$ one has :

$$\begin{array}{ccccccc} H^0(\mathcal{O}_C) & \simeq & H^0(\mathcal{O}_{C_1}) \oplus \cdots \oplus H^0(\mathcal{O}_{C_s}) & \simeq & \mathbb{K}^s & \simeq & W \\ H^0(\mathcal{O}_{C\cap L}) & \simeq & H^0(\mathcal{O}_{\{p_1\}}) \oplus \cdots \oplus H^0(\mathcal{O}_{\{p_n\}}) & \simeq & \mathbb{K}^d & & \end{array}$$

• One can identifiy the inclusion $0 \longrightarrow W \longrightarrow \mathbb{K}^d$ with the restriction map

$$0 \longrightarrow H^0(\mathcal{O}_C) \xrightarrow{\rho} H^0(\mathcal{O}_{C\cap L})$$

• One needs now to **compute the cokernel of** ρ**.**

The key result

Proposition 1 *One has an exact sequence*

$$0 \to H^0(\mathcal{O}_C) \xrightarrow{\rho} H^0(\mathcal{O}_{C\cap L}) \xrightarrow{R} H^0(\Omega_C(L))^v \longrightarrow H^0(\Omega_C)^v \to 0$$

where

$$R: \quad (\lambda_i)_i \quad \longmapsto \quad \Big(\Psi \mapsto \sum_{i=1}^{n} res_{p_i}(\lambda_i\Psi)\Big).$$

In particular, $\dim H^0(\Omega_C(L)) = g + d - s$*, with* g *the genus of* $\mathcal{C}$*.*

Proof : Uses Koszul resolution, Serre duality and the **residue theorem** that says that any rational 1-form Ψ on C satisfies

$$\sum_{p\in C_j} res_p(\Psi) = 0.$$

Relation with adjoint polynomials (and Theorem 2 follows)

- One has a commutative diagramm with vertical isomorphisms.

$$\begin{array}{ccccccccc}
H^0(\mathcal{O}_C) & \hookrightarrow & H^0(\mathcal{O}_{C\cap L}) & \to & H^0(\Omega_C(L))^v & \to & H^0(\Omega_C)^v & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
W & \hookrightarrow & \mathbb{K}^d & \to & Adj^{d-2}(F)^v & \stackrel{\beta}{\to} & Adj^{d-3}(F)^v & \to & 0
\end{array}$$

- The map β is dual of the "multiplication by x" map so that

$$ker(\beta) = \mathcal{A}^{d-2}(F)^v.$$

- The exact sequence

$$0 \to W \longrightarrow \mathbb{K}^d \xrightarrow{A} \mathcal{A}^{d-2}(F)^v \to 0$$

follows, the matrix A being computed from basic residue calculus. $\square$

Is $F(0, y)$ non square-free an opportunity ?

Just one example...

- Let $F(x,y) = y^5 - y^4 - xy^3 - y^3 + y^2 + x^2 + xy - x$. One has

$$F(0,y) = (y-1)^2 y^2 (y+1).$$

- The curve $\mathcal{C}$ has only 3 branches intersecting $x = 0$ (with 2 tangents) and recombinations only involve **3 unknowns instead of 5=deg (F)**.

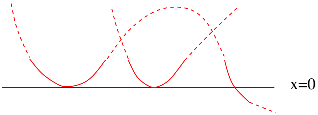
- Let

$$A := \left(res_\alpha \left[\frac{H(y)dy}{F(0,y)} \right] \right)_{F(0,\alpha)=0,\ H\in\mathcal{A}^{d-2}(F)}.$$

- One has $W = ker(A)$, but the residues now depend on higher derivatives :

$$res_1 \left[\frac{H(y)dy}{(y-1)^2 y^2 (y+1)} \right] = \frac{H'(1) - H(1)}{4}.$$

- One obtains here $\mathcal{A}^{d-2}(F) = \langle y-1, y^2, y^3 \rangle$ and $ker(A) = \langle (1,0,1), (0,1,0) \rangle$.



Conclusion

$$\textbf{Factorization} \quad \overset{\mathcal{O}(\mathbf{d}^\omega)}{\Longleftrightarrow} \quad \textbf{Adjoints mod (x)}$$

...So what ?

Hensel lifting *vs* adjoint polynomials

Via Hensel lifting : $\mathcal{O}(d^{\omega+1})$ (Lecerf, Belabas-Van Hoeij et al.)

1. Factorization modulo (x).
2. Factorization modulo (x^{2d}) *via* Hensel.
3. Linear system $d \times \mathcal{O}(d^2)$ over $\mathbb{K}$.
4. Factorization in $\mathbb{K}[x, y]$ *via* Hensel.

Via adjoint polynomials : $\mathcal{O}(d^{\omega})$ + computation of $\mathcal{A}^{d-2}(F)$.

1. Factorization modulo (x).
2. Adjoint polynomials modulo (x).
3. Linear system $d \times (d - s)$ over $\mathbb{K}$.
4. Factorization in $\mathbb{K}[x, y]$ *via* Hensel.

Factoring using adjoint polynomials ?

Question : Can we compute degree $d-2$ adjoints mod (x) faster than the actual $\mathcal{O}(d^{\omega+1})$ for factorization ?

Answer : Fast computation of all adjoint polynomials is enough since

$$\textbf{Adjoints} \overset{\mathcal{O}(\mathbf{gd}^{\omega-1})}{\Longrightarrow} \textbf{Adjoints mod (x)}$$

Not clear... One expects ***a priori*** the inclusions

$$\begin{aligned} \text{Factorization} \quad &\subset \quad \text{Desingularization (integral closure)} \\ &\subset \quad \text{Adjoints computation (conductor).} \end{aligned}$$

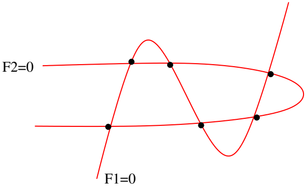
($\simeq$ Newton-Puiseux cost, $\widetilde{\mathcal{O}}(d^5 log(p))$ for $\mathbb{K} = \mathbb{F}_p$, Poteaux-Rybowitch).

Nevertheless...

Philosophy : The complexity of **"factoring using adjoints mod (x)"** is related to that of "discriminant-integral closure-conductor".

...Is this approach interesting for some particular cases ?

- $\mathcal{C}$ transversal union of smooth curves ?



- Few intersection points ? (extreme = d concurring lines)
- Symetry hypothesis ?
- ? ? ?

Thank you for your attention