Bivariate factorization using Newton polytope

Martin WEIMANN

RISC - Linz

24/11/2011

Motivations and results

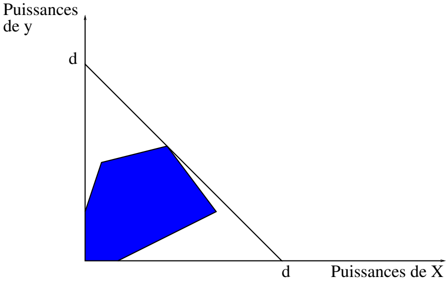
Objective : Factoring bivariate polynomials over a number field in polynomial time in the volume of the Newton polytope.

The Newton polytope

Let $f \in \mathbb{K}[x, y]$ be a bivariate polynomial, $f(x, y) = \sum_{(i,j)\in\mathbb{N}^2} c_{ij} x^i y^j$.

The **Newton polytope** of f is the convex hull of its exponents :

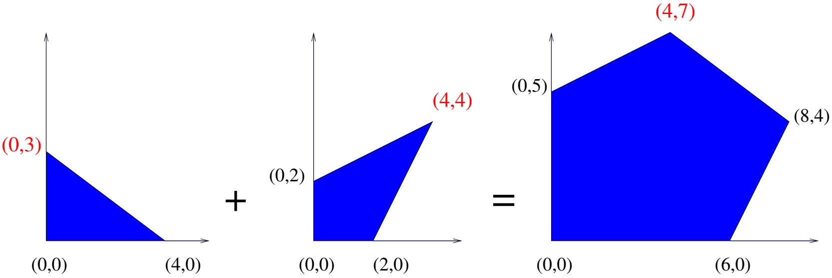
$$N_f = \mathrm{Conv}((i, j) \in \mathbb{N}^2,\ c_{ij} \neq 0).$$



For a fixed degree, many possible polytopes $\Longrightarrow$ better complexity indicator.

Ostrowski's theorem : $N_{f_1 f_2} = N_{f_1} + N_{f_2}$

- $f_1 = 1 - 2x^4 + \mathbf{y^3} - xy$
- $f_2 = 3 - x^2 + xy^2 - 2\mathbf{x^4y^4} + y^2$
- $f_1 f_2 = 3 + 2x^6 + 4x^8y^4 - 2\mathbf{x^4y^7} + y^5 + \cdots$



$$N_{f_1 f_2} = N_{f_1} + N_{f_2}$$

Factorization, the case of dense polynomials

The **lifting and recombinations** scheme :

1. Factorization in $\mathbb{K}[[x]]/(x^k)[y]$ (with good coordinates).
2. Recombination of modular factors.
3. Factorization in $\mathbb{K}[x,y]$.

• **k=3 :** Algo probabilistic, exponential complexity
(Chèze-Galligo-Rupprecht).

• **k=2d :** Algo deterministic. Complexity $\mathcal{O}(d^{\omega+1})$ with $\omega \approx 2.34$
(Ruppert, Gao, Belabas-Van Hoeij et al., Lecerf, etc).

Problem : Does not take into account the Newton polytope.

Main result

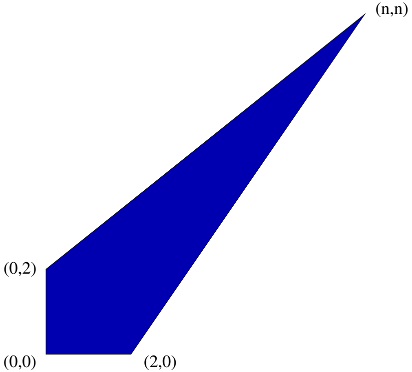
Definition : We say that f is **non degenerated** if $0 \in \mathrm{N}_f$ and if the exterior facet polynomials are separable.

Theorem 1 ***(W., J. of Complexity)*** *One can factorize non degenerated bivariate polynomials over a number field in time* $\mathcal{O}(\mathrm{Vol}(\mathrm{N}_f)^{\omega})$ *modulo the exterior facets factorization.*

Generalizes the algorithms of Lecerf and Chèze-Lecerf to the case generic/polytope. Advantages :

- Univariate factorization (much) faster.
- For a fixed volume, there exist arbitrarily high degrees.

A characteristic example



- Chèze-Lecerf : $\mathbf{1}$ univariate factorization of degree $\mathbf{2n}$ and $\mathcal{O}(n^{\omega+1})$ operations.
- Theorem 1 : $\mathbf{2}$ univariate factorizations of degree $\mathbf{2}$ and $\mathcal{O}(n^{\omega})$ operations.

The algorithm

ALGORITHM

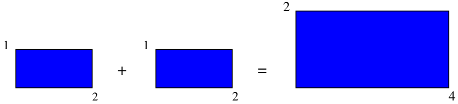
Input : $f \in \mathbb{K}[x, y]$ non degenerate.
Output : Irreducible rational factors of f.

- *Step* 1. Univariate facet factorization (black-box)
- *Step* 2. Hensel lifting (Newton iteration)
- *Step* 3. Recombination (linear algebra)
- *Step* 4. Factors computation (interpolation).

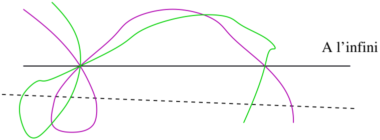
Step 3 ?

Geometry

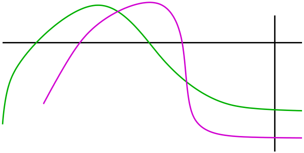
Example of bidegree $(4, 2)$



- **Classical approach** : we look at the curve of f in $\mathbb{P}^2$:



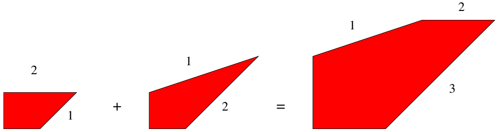
- **Toric approach** : we look at the curve of f in $\mathbb{P}^1 \times \mathbb{P}^1$.

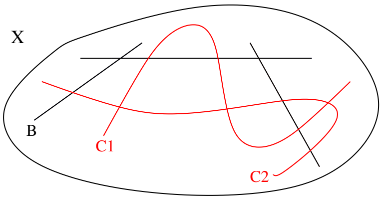


The general case : toric compactification

Let X be the **toric completion** of $\mathbb{K}^2$ defined by the polytope of f.

Intersection of the curve $C \subset X$ of f with the boundary $B = X \setminus \mathbb{K}^2$ given by exterior facet polynomials factorizations.





Recombinations

- Given :
  - $D \in \mathrm{Div}(X)$ effective with support B (lifting precision)
  - Local decomposition $C \cap D = \sum_{P \in \mathcal{P}} \gamma_P$ (lifted facet factorization).

- We want :
  - The decomposition $C \cap D = \gamma_1 + \cdots + \gamma_s$ induced by the irreducible decomposition $C = C_1 + \cdots + C_s$.

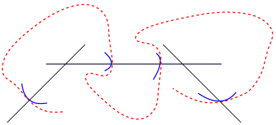
- We reduce to a problem of **linear algebra :**
  - Let $V \subset \mathrm{Div}(D) \otimes \mathbb{K}$ generated by the γ_P's.
  - Let $W \subset V$ generated by the γ_i's
  - Let $V(D) \subset V$ generated by the γ's restriction of divisors on X. One has :

$$W \subset V(D) \subset V$$

- **To solve** :
  - Equations of $V(D) \subset V$ (lifting conditions) ?
  - For which D we have $W = V(D)$ (sufficient precision) ?

A theorem on extensions of line bundles

Equations of $V(D) \subset V$ $\iff$ criterions of **algebraic osculation** on the boundary of X.



Theorem 2 (W.) *Let $D \subset X$ with support B. There is an exact sequence*

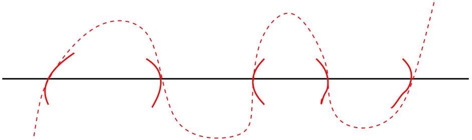
$$0 \to \mathrm{Pic}(X) \to \mathrm{Pic}(D) \xrightarrow{\alpha} H^0(X, \Omega^2_X(D))^v \to 0$$

where $\alpha(L)$ associates to ψ the sum of the residues of a primitive of ψ along the zeroes of a section of L.

Proof : Serre duality, Dolbeault cohomology, residue currents.

A simple example : the Reiss relation

Suppose $X = \mathbb{P}^2$ and $D \simeq 3\mathbb{P}^1$. Suppose $L \in \mathrm{Pic}(D)$ defined by $\phi_j \in \mathbb{K}[[x]]/(x^3)$, $j = 1, \dots, d$.



We have $h^0(\Omega^2_{\mathbb{P}^2}(3)) = 1$, so a unique extension condition. We obtain

$$L \text{ extends to } X \iff \sum_j \phi_j''(0) = 0.$$

We recover the **Reiss relation**.

The good lifting precision (choice of D)

Theorem 3 (W.) *If $D \geq 2\,\mathrm{div}_\infty(f)$, then $W = V(D)$.*

Proof. Logarithmic forms, toric cohomology, Gao-Ruppert's Theorem.

Corollary *Recombinations $\iff$ $\mathcal{O}(\mathrm{Vol}(\mathrm{N}_f))$ linear equations and r unknowns, r the number of facet factors.*

Proof. Thm 2, thm 3 and $h^0(\Omega^2_X(2C)) = \mathcal{O}(\mathrm{Vol}(\mathrm{N}_f))$.

Example. In the dense case, we recover a theorem of Lecerf :

$$\text{Factorization } \bmod(x^{2d}) \Longrightarrow \begin{cases} \text{recombination with linear algebra} \\ \mathcal{O}(d) \text{ unknowns}, \mathcal{O}(d^2) \text{ equations.} \end{cases}$$

Complexity

Complexity analysis

Let $\Delta := \mathrm{Vol}(\mathrm{N}_f)$.

1. Lifting : $\widetilde{\mathcal{O}}(d_i k_i)$ for the i-th facet, with d_i the degree, k_i the precision. We have

$$\sum k_i d_i = \sum k_i (C \cdot D_i) = C \cdot (\sum k_i D_i) = C \cdot D = 2C^2 = 4\Delta,$$

so a total of $\widetilde{\mathcal{O}}(\Delta)$ operations.

2. Recombinations. Linear system of $\mathcal{O}(\Delta)$ equations, r unknowns.

- Matrix computation : $\widetilde{\mathcal{O}}(\Delta^2)$ operations (arithmetic).
- Reduced echelon basis : $\mathcal{O}(\Delta r^{\omega-1}) \subset \mathcal{O}(\Delta^{\omega})$ operations.

3. Factors computation. Interpolation.

- Polytopes computation : negligeable.
- Factors : $\sum_i \mathcal{O}(\Delta_i^{\omega}) \subset \mathcal{O}(\Delta^{\omega})$ operations (Ostrowski's theorem).

$\square$

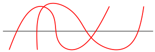
Improvements

- **In theory :** We conjecture a complexity $\widetilde{\mathcal{O}}(\Delta r^{\omega-1})$ (dense case : $\widetilde{\mathcal{O}}(d^{\omega+1})$, Lecerf et al.). Requires :
  - Better analysis of usual algorithm in the sparse case.
  - Fast toric interpolation "multi-charts".
- **In practice :**
  - Combine probabilistic (Hensel with small precision) and deterministic (high precision).
  - Use lazy calculus.
- **Bit-complexity :**
  - Control on the size of the coefficients.
  - Theoretical bound / arithmetic of toric varieties (using extended Newton polytope of Philipon, Sombra et al. ?).

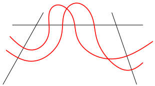
Conclusion

Perspectives

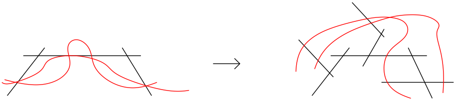
- Generic case w.r.t the degree : $\mathcal{O}(d^{\omega+1})$ (Lecerf, Van Hoeij,...)



- Generic case w.r.t the polytope : $\mathcal{O}(\Delta^{\omega})$ (Weimann).



- General case ? Study relations **singularities** and **factorization**.



More singularities $\Longrightarrow$ Faster factorization

An underlying open problem...

Let $X = \mathbb{A}^2 \cup B$ be a smooth compactification such that :

- B is a normal crossing union of rational curves.
- B intersects transversally the curve of C of f.

Find an effective divisor D supported on B **with size controlled by f** and such that

$$\begin{cases} H^1(\Omega^1_X(\log(B) \otimes \mathcal{O}_X(C - D)) = 0 \\ H^0(\Omega^2_X(B + 2C - D)) = 0. \end{cases}$$

- When X is toric, one can choose $D \in |2C|$.
- In general, things become more complicated...