Toric factorization of polynomials

Martin Weimann

University of Barcelona

Mega 2009

Introduction (I)

Main Problem : Given $f \in \mathbb{K}[x, y]$ defined over a field of characteristic zero, compute the irreducible factorization of f over a given algebraic extension $\mathbb{K} \subset \mathbb{L}$.

Introduction (II)

A classical approach : The Recombination-Lifting Scheme

1. Generic change of coordinates,
2. Factorize $[f]$ in $\mathbb{L}[x]/(x^k)[y]$ for some $k \geq 0$,
3. Detect and lift the factorizations that can be lifted.

• $k = 3 \Rightarrow$ Probabilistic algorithm, exponential complexity, efficient up to degree $d = 200$ (Chèze-Galligo-Rupprecht).

• $k = d + 1 \Rightarrow$ Deterministic algorithm, $< d^4$ operations in $\mathbb{L}$ (Lecerf, using Gao).

• $k = 2d \Rightarrow$ Deterministic algorithm using linear algebra, $< d^4$ operations in $\mathbb{L}$ (Chèze-Lecerf, Gao).

Introduction (III)

Objective : Avoid the change of coordinates in order to take advantage of the geometry of the Newton polytope N_f of f.

$\mathbb{L}$-factorization using geometry of N_f

$$\Longleftrightarrow$$

Decomposition of the curve $C \subset X$ of f in the toric compactification X of $\operatorname{Spec} \mathbb{L}[x^{\pm 1}, y^{\pm 1}]$ associated to N_f

We will talk about toric factorization algorithms.

Introduction (IV)

Simplification hypothesis : $\{(0,0),(1,0),(0,1)\} \subset N_f$.

So X toric completion of $\mathbb{L}^2 := \operatorname{Spec} \mathbb{L}[x,y]$. Denote by

$$\partial X = D_1 + \cdots + D_r$$

the boundary $X \setminus \mathbb{L}^2$. Then $D_i \leftrightarrow i^{th}$ exterior face of N_f, and

"Restriction of C to a finite infinitesimal neighborhood of D_i"

$$\Longleftrightarrow$$

"Coefficients of f with monomial exponents close to the i^{th}-face".

Example : Suppose $N_f = \operatorname{Conv}\{(0,0),(4,0),(0,2),(4,2)\}$. Then $X = \mathbb{P}^1 \times \mathbb{P}^1$, $\partial X = D_1 + D_2$, $\deg(C \cdot D_1) = 4$ and $\deg(C \cdot D_2) = 2$.

Main strategy

These observations motivate the following sketch of algorithm scheme :

1. Consider the curve C of f in the toric completion X.
2. Choose a Cartier divisor $D \geq \partial X$.
3. Compute the restriction $\gamma \in \mathrm{Ca}(D)$ of C to D.
4. Detect and keep the Cartier divisors $0 \leq \gamma' \leq \gamma$ that can be lifted to X.
5. Repeat the process with a "bigger" D up to recover the $\mathbb{L}$-decomposition of C.

- Step 4 ?
- Step 5 ?

Algebraic Osculation

Theorem 1 (-) *Let X be a smooth projective completion of $\mathbb{L}^2$ with SNC boundary, and let $D \geq \partial X$. There is an explicit residual pairing*

$$\langle \cdot \, , \, \cdot \rangle_D : \mathrm{Ca}_{\mathbb{L}}(D) \oplus H^0(X, \Omega^2_X(D)) \to \mathbb{L}$$

such that γ lifts to X iff $\langle \gamma \, , \, \cdot \rangle_D \equiv 0$. The lifting is unique up to rational equivalence.

Sketch of proof

Since $X \setminus |D| \simeq \mathbb{L}^2$, we deduce a decomposition

$$\mathrm{Pic}(D) \simeq \mathrm{Pic}(X) \oplus H^1(\mathcal{O}_D).$$

Serre Vanishing Theorem and X rational $\Rightarrow \gamma$ lifts iff some $\beta = \beta(\gamma) = 0$ in $H^2(\mathcal{O}_X(-D))$. Serre duality gives

$$H^2(\mathcal{O}_X(-D)) \otimes H^0(\Omega^2_X(D)) \xrightarrow{(\cdot,\cdot)} H^2(\Omega^2_X) \overset{Tr}{\simeq} \mathbb{L},$$

where Tr is the trace map. Then

$$\langle \gamma, \Psi \rangle_D := Tr(\beta, \Psi)$$

has the desired properties. Dolbeault resolution and residue currents $\Rightarrow \mathbb{L}$-pairing $=$ explicit sum of Grothendieck residues. □

An explicit formula

Suppose $D = \sum(k_i + 1)D_i$ and that $\gamma \in \mathrm{Ca}(D)$ is given by

$$[g_i] \in \frac{\mathbb{L}[x_i]}{(x_i^{k_i+1})}[y_i], \quad i = 1, \ldots, r.$$

If $g_i(0) \neq 0$, we have the explicit lifting condition : γ lifts iff

$$\sum_{i=1}^{r} \mathrm{coeff}_{(a_{im}, b_{im})}\, log_0(g_i) = 0$$

for all lattice points m in the interior of the polytope of D, with some explicit $(a_{im}, b_{im}) \in \mathbb{Z}^2 \setminus \{0\}$, $0 \leq a_{im} \leq k_i$.

The Reiss relation

Example : Suppose $X = \mathbb{P}^2$, $D = 3\mathbb{P}^1$ and $\gamma = \{\prod_p (y - \phi_p) = 0\}$, with $\phi_p \in \mathbb{L}[x]/(x^3)$. Then, there is only one lifting conditions, namely

$$\langle \gamma \, , \, \cdot \rangle_D \equiv 0 \iff \sum_p \phi_p''(0) = 0.$$

This is the classical Reiss relation, used in the CGR algorithm.

Application to polynomial factorization

We suppose now that

$$D := \mathrm{div}_\infty(f) + \partial X.$$

and we denote by γ the restriction to D of the curve $C \subset X$ of f.

Theorem 2 (-) *Let Q be a Minkowski-summand of N_f. There exists q a factor of f with $N_q = Q$ if and only if there exists $0 \leq \gamma' \leq \gamma$ such that*

1. $\langle \gamma', \cdot \rangle_D \equiv 0$
2. $\deg(\gamma' \cdot D_i) = \mathrm{Card}(Q^{(i)} \cap \mathbb{Z}^2) - 1, \quad i = 1, \ldots, r.$

We can compute q from γ' by solving an explicit $N \times N$ system of $\mathbb{L}$-affine equations, with $N = \mathrm{Card}(Q \cap \mathbb{N}^2) - 1$.

Sketch of proof

Denote by $i :\to X$ the inclusion.

$\Rightarrow$ The Cartier divisor $\gamma' := i^*(\mathrm{div}_0(q))$ has the desired properties.

$\Leftarrow$ By Thm 1, $\langle \gamma', \cdot \rangle_D \equiv 0 \Rightarrow \gamma'$ lifts to some $C' \in \mathrm{Ca}(X)$.
By (2), $H^1(\mathcal{O}_X(C' - D)) = 0$ and we can choose $C' \geq 0$.

If $0 \leq C_0 \leq C'$ is irreducible and not contained in C, then

$$
\begin{aligned}
i^*(C_0) \leq i^*(C) \quad &\Rightarrow \quad \deg(C_0 \cdot C) \geq \deg(C_0 \cdot D) \\
&\Rightarrow \quad \deg(C_0 \cdot \partial X) \leq 0 \\
&\Rightarrow \quad C_0 = 0.
\end{aligned}
$$

So $C' \leq C$. This gives a $\mathbb{L}$-factor q of f, and $N_q = Q$ by the degree conditions (2) imposed to γ'.
We can compute q from γ' since $H^0(\mathcal{O}_X(C' - D)) = 0$, and residue theory $\Rightarrow$ explicit formula. $\square$

A sketch of algorithm

Corollary. *The factorization of f can be computed from :*

1. *The Minkovski-sums decompositions of N_f.*
2. *The factorization of r univariate polynomials*

$$[f_i] \in \frac{\mathbb{L}[x_i]}{(x_i^{k_i+1})}[y_i], \ \deg[f_i] = l_i, \quad i = 1, \ldots, r$$

   with r the number of exterior faces of N_f, $l_1, \ldots, l_r$ their lattice lenghts and $k_1, \ldots, k_r$ their lattice distance to 0.
3. *The lifting-tests for each choice $\gamma' \leq \gamma$ induced by 1 and 2.*

The complexity of the algorithm obeys to

- $l_1 + \ldots + l_r \leq \deg(f)$ *(with equality $\Leftrightarrow$ N_f regular)*
- $\sum_{i=1}^{r} k_i l_i = 2\,\mathrm{Vol}(N_f)$.
- *Lifting-test for a* $\gamma' \iff \leq \mathrm{Card}(N_f \cap \mathbb{N}^{*2})$ *vanishing-sums.*

A remark

Morally, Thm 1 + Thm 2 $\Longleftrightarrow$ Toric Hensel lifting. Our algorithm fully takes advantage of the Ostrowski conditions

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

In particular, f irreducible over $\mathbb{K}$ $\Rightarrow$ irreducible $\mathbb{L}$-factors have same Newton polytope $\Rightarrow$ reduce (drastically) the number of choices $\gamma' \leq \gamma$.

What we gained ? A (small) example

Example 1. Suppose $N_f = \mathrm{Conv}\{(0,0),(4,0),(0,2),(4,2)\}$ and f irr. over $\mathbb{K}$. Then

1. Projective approach ($f \in \mathcal{O}_{\mathbb{P}^2}(6)$, $D = 7\mathbb{P}^1$) : Factorize

$$[f] \in \frac{\mathbb{L}[x]}{(x^7)}[y], \;\; \deg[f] = 6$$

   and test ≤ 21 vanishing-sums for each of the $\leq 20 = C_3^6$ possible recombinations.

2. Toric approach ($f \in \mathcal{O}_{\mathbb{P}^1 \times \mathbb{P}^1}(4,2)$, $D = 5D_1 + 3D_2$) : Factorize

$$[f_1] \in \frac{\mathbb{L}[x_1]}{(x_1^3)}[y_1], \deg[f_1] = 4 \;\text{ and }\; [f_2] \in \frac{\mathbb{L}[x_2]}{(x_2^5)}[y_2], \deg[f_2] = 2,$$

   and test ≤ 8 vanishing-sums for each of the $\leq 12 = C_2^4 \times C_1^2$ possible recombinations.

What we gained ? A second (small) example

Example 2. Suppose $N_f = \mathrm{Conv}\{(0,0),(6,0),(0,4)\}$. Then

1. Projective approach : Factorize

$$[f] \in \frac{\mathbb{L}[x]}{(x^7)}[y], \ \deg[f] = 6$$

   and test ≤ 21 vanishing-sums for each of the $\leq C_3^6 = 20$ possible recombinations.

2. Toric approach : Factorize

$$[f_1] \in \frac{\mathbb{L}[x_1]}{(x_1^{13})}[y_1], \ \deg[f_1] = 2$$

   and test ≤ 19 vanishing-sums for each of the $\leq C_1^2 = 2$ possible recombinations.

Using Linear Algebra

Two main problems in Theorem 2.

1. If using numerical calculous, when does a sum vanish ?
2. Need to compute Mink. decompositions of N_f.
3. Number of recombinations remains “exponential”.

Use linear algebra in order to replace :

1. Zero-sums by zero linear combinations
2. Recombinations by computation of a vector space basis.

(permits to use LLL, Chèze, Gao, Lecerf,...).

A toric version of the Chèze-Lecerf algorithm (I)

Hypothesis : The subscheme $\Gamma := C \cdot \partial X$ is reduced ($\iff$ exterior facet polynomials of f are square free over $\mathbb{L}$).

Notations : For any $D \geq \partial X$, $i : D \to X$, we let

$$\gamma = \sum_{p \in |\Gamma|} \gamma_p$$

the irreducible decomposition of $\gamma := i^*(C)$. Then we define the $\mathbb{L}$-vector space

$$L_C(D) := \{\mu \in \mathbb{L}^{|\Gamma|},\ \langle \gamma_\mu, \cdot \rangle_D \equiv 0\},$$

where $\mu = (\mu_p)_{p \in |\Gamma|}$, $\gamma_\mu := \sum \mu_p \gamma_p$.

A toric version of the Chèze-Lecerf algorithm (II)

Theorem 3 (-) *Let* $C = C_1 + \cdots + C_s$ *be the irreducible decomposition of* C *(over* $\mathbb{L}$*). Then* $\dim L_C(D) \geq s$*, and*

$$D \geq 2\,\mathrm{div}_\infty(f) \Longrightarrow \dim L_C(D) = s.$$

In that case, $i^*(C_j) = \gamma_{\mu_j}$ *where* $(\mu_1, \ldots, \mu_s)$ *is the reduced echelon basis of* $L_C(D)$*.*

Sketch of proof

- Easy : $\langle \mu_1, \ldots, \mu_s \rangle \subset L_C(D)$, dim s for all D.
- Suppose now $D = 2\,\mathrm{div}_\infty(f)$ and let $\mu \in L_C(D)$. Then,

1. γ_μ lifts and there exists $\omega \in H^0(\Omega^1_X(\log(-K_X)) \otimes \mathcal{O}_X(C))$,
   - $i^*(\omega)_p = \mu_p i^*(df/f)_p \ \ \forall\ p \in |\Gamma|$;
   - $i^*(d\omega) = 0 \in H^0(\Omega^2_X(2C - K_X) \otimes \mathcal{O}_D)$.
2. Using $D \simeq 2C$, we obtain

$$d\omega \in H^0(\Omega^2_X(2C - D)) \Rightarrow \omega = \frac{c}{f^2}\frac{dx \wedge dy}{xy} \Rightarrow d\omega = 0.$$

3. By a (variant of) a theorem of Ruppert, we deduce that

$$\omega = \sum_{j=1}^{s} c_j df_j/f_j + a_1 dx/x + a_2 dy/y,\ \ c_j \in \mathbb{L}.$$

4. We deduce that $\mu = c_1\mu_1 + \cdots + c_s\mu_s$. □

Further comments

1. By Theorem 2, we can compute the reduced echelon basis of $L_C(D)$ (so the factorizaton of f) without using a precision greater than $\mathrm{div}_\infty(f)$.
2. Theorem 1 is valid in a non toric completion of $\mathrm{Spec}\,\mathbb{L}[x, y]$ $\Longrightarrow$ One might improve the algorithms when C has (non toric) singularities along the boundary ∂X !
3. Better choices of D ?
4. $\mathrm{Char}\,\mathbb{K} \neq 0$?

Thank you !

(Especially for those who missed their plane to follow my talk)