TORIC FACTORIZATION OF BIVARIATE POLYNOMIALS

MARTIN WEIMANN

Abstract. I prove here the existence of a deterministic algorithm that computes the rational factorization of bivariate polynomials generic at the toric infinity in small polynomial time with respect to the volume of the Newton polytope. When the input polynomial is sparse enough, the complexity improves that of the fast analoguous lifting and recombination algorithm developed by Chèze and Lecerf for dense polynomials. The proof uses residual criterions for algebraic osculation at the toric infinity, and combines cohomological properties of toric varieties with the irreducibility criterion of Ruppert.

Introduction

Rational factorization of bivariate polynomials is a central problem of Computational Algebra. Although there exist now fast algorithms, most of them consider the total degree as the main complexity indicator and use some hypothesis of genericity relatively to this invariant. In this note, I present an algorithm for a larger class of generic sparse polynomials, with now a small polynomial complexity with respect to the finer Newton polytope invariant. Geometrically, this corresponds to decomposing curves that are non degenerated at the toric infinity. One talks about toric factorization algorithms, the dense setting corresponding to the usual projective completion $\mathbb{P}^2$. Our approach generalizes to the sparse setting the fast lifting and recombination algorithm developed by Chèze and Lecerf [7], [2] for dense polynomials.

Main results. Let $f \in \mathbb{Q}[t_1, t_2]$ be a rational bivariate polynomial. We denote by N_f the Newton polytope of f, convex hull of the monomial exponents that appear in f. An exterior face of N_f is a one-dimensional face whose primitive inward normal vector has at least one negative coordinate. We introduce two hypothesis of genericity :

- (H_1) The Newton polytope N_f contains the elementary simplex.
- (H_2) The non monomial factors of the exterior facet polynomials of f are reduced.

Let $2 \leq \omega < 2,35$ be the matrix multiplication exponent. I prove here the following theorem:

Theorem 0.1. *There exists an algorithm that, given $f \in \mathbb{Q}[x, y]$ that obeys to (H_1) and (H_2) and given the rational factorization of the exterior facet polynomials of f, computes all the irreducible rational factors of f with $\mathcal{O}(\mathrm{Vol}(N_f)^\omega)$ arithmetic operations in $\mathbb{Q}$.*

Example 0.2. If $N_f = \mathrm{Conv}((0,0),(2,0),(0,2),(n,n))$ with $n >> 0$, the Chèze-Lecerf algorithm [2] requires one univariate factorization in degree $2n$ followed by $\mathcal{O}(n^{\omega+1})$ operations. My approach requires two univariate factorization in degree 2 followed by $\mathcal{O}(n^\omega)$ opérations.

Date: 11/03/2010.

Related results. In the year's 1980's, Lenstra et al. [8] obtain the first rational univariate factorization polynomial time algorithm based on their famous LLL algorithm of lattice basis reduction. In the same time, Kaltofen [6] succeeds in reducing multivariate to univariate factorization in polynomial time with respect to the total degree. Nevertheless, the first practical polynomial complexity algorithms for bivariate factorization of dense polynomials appear much latter, especially thanks to the works of Ruppert [9] and Gao [5] who introduce the logarithmic derivative method and linear algebra in the picture. Finally, Chèze and Lecerf [7], [2] obtain an optimal complexity for dense polynomials by combining Gao's point of view with the classical lifting and recombination scheme that consists in reducing bivariate to modular univariate factorization. For the sparse setting, Gao et al. obtain in [1] an exponential complexity algorithm that involves the combinatoric of the polytope. Toric geometry appears with our work with Elkadi and Galligo in [3], where we develop a semi-numerical probabilistic method based on toric interpolation criterions [10]. Latter on, I obtain in [11] a deterministic algorithm based on toric osculation criterions, from which is derived in [12] the first polynomial time algorithm for sparse polynomials that I present in this note.

1. The toric lifting and recombination scheme

1.1. **The toric setting.** Let X be the toric surface defined by the normal fan of N_f. By hypothesis (H_1), the surface X is a completion of the affine plane $\mathbb{C}^2$, whose boundary (the toric infinity) $\partial X := X \setminus \mathbb{C}^2$ is a union of irreducible toric divisors that are one-to-one with the exterior facets of N_f. Let C be the Zariski closure to X of the affine curve of f. For D an effective Cartier divisor with support $|\partial X|$, the schematic intersection $\gamma_C := C \cap D$ admits the irreducible decomposition over $\mathbb{Q}$

$$\gamma_C = \bigcup_{P \in \mathcal{P}} \gamma_P,$$

indexed by the set of the non monomial irreducible rational factors of all of the exterior facet polynomials of f, and where γ_P corresponds to lifting P to a local equation of C modulo the local equation of D. The γ_P's have disjoint supports by (H_2). The lifting and recombination problem consists in choosing a suitable D (lifting precision) in order to deduce the decomposition of γ_C induced by that of C (recombination).

1.2. **Lifting and recombinations.** Let us consider D as a subscheme of X and the γ_P's as Cartier divisors of D. Let V be the vector space over $\mathbb{Q}$ free generated by the γ_P's. We want to compute the subspace $W \subset V$ generated by the restrictions to D of the rational components of C. To this aim, we introduce the intermediary subspace $W \subset V(D) \subset V$ generated by all the elements of V that are restriction to D of divisors on X. The following theorem gives an upper bound for the necessary lifting precision.

Theorem 1.1. *Let D_∞ be the polar divisor of the rational function of X induced by f^2. There is equality $W = V(D)$ as soon as $D \geq D_\infty$.*

Proof. We refer to [12] for the proof. The main part consists in associating to $\gamma \in V(D)$ a rational 1-form $\phi(\gamma)$ with polar divisor bounded by $C + \partial X$, and whose restriction to D is

closed. If now $D \geq D_\infty$, some vanishing cohomology property holds and $\phi(\gamma)$ is forced to be closed. Then, a theorem of Ruppert [9] combined with a Galois theory argument imply that $\phi(\gamma)$ is $\mathbb{Q}$-linear combination of the logarithmic derivatives of the rational factors of f. It follows easily that $\gamma \in W$. □

There remains to determine an explicit system of equations that gives the vector subspace $V(D) \subset V$. When a Cartier divisor of D extends to a Cartier divisor of X ?

Theorem 1.2. *There exists an explicit residual pairing*

$$\langle \cdot, \cdot \rangle_D : \mathrm{Div}(D) \otimes \mathbb{C} \times H^0(X, \Omega^2_X(D)) \to \mathbb{C}$$

such that $\gamma \in \mathrm{Div}(D)$ *extends to* X *if and only if* $\langle \gamma, \cdot \rangle_D \equiv 0$.

Proof. We refer to [11] for the proof. The main difficulty is to make explicit such a pairing. Roughly speaking, the linear form $\langle \gamma, \cdot \rangle_D$ sends a rational 2-form $\omega \in H^0(X, \Omega^2_X(D))$ to the sum of residues of a primitive of ω along a local analytic lifting curve of γ. In some sense, this result is a converse to the classical residue theorem. □

Example 1.3. Suppose $X = \mathbb{P}^2$ and $D \simeq 3\mathbb{P}^1$ with affine equation $x^3 = 0$. Let $\gamma \in \mathrm{Div}(D)$, given by a finite collection of truncated implicit functions $\phi_p \in \mathbb{C}[[x]]/(x^3)$, $p \in |D|$. We obtain $h^0(\Omega_{\mathbb{P}^2}(3)) = 1$ and the unique lifting condition is given by the classical Reiss relation $\sum_p \phi_p''(0) = 0$ that is used in many probabilistic algorithms for dense factorization (*e.g* [4]).

Corollary 1.4. *We have* $W = \ker(A)$ *for some explicit rational matrix* A *that only depends on* $C \cap D_\infty$, *and which is indexed by* $\mathcal{P}$ *and by the set* M *of interior lattice points of* $2N_f$.

Proof. This follows from theorems 1.1 and 1.2 combined with the wellknown isomorphism

$$H^0(X, \Omega^2_X(D_\infty)) \simeq \bigoplus_{m \in M} \mathbb{C}\, t^m \frac{dt_1 \wedge dt_2}{t_1 t_2}.$$

The matrix A is rational since both the γ_P's and the pairing $\langle \cdot, \cdot \rangle_D$ are defined over $\mathbb{Q}$. □

Example 1.5. If $f(x, y)$ is a generic dense polynomial of degree d, corollary 1.4 says that we can deduce the factorization of f from its factorization modulo (x^{2d}) by solving a linear system of $(d-1)(d-2)/2$ equations and $\leq d$ unknowns. We recover a theorem of Lecerf.

1.3. **Factors computation.** The restrictions $\gamma_1, \ldots, \gamma_s$ to D_∞ of the irreducible rational components $C_1, \ldots, C_s$ of C correspond (up to some permutation) to the unique reduced echelon basis of $W = \ker(A)$. Then, the osculation condition $C_j \cap D_\infty = \gamma_j$ uniquely determines the Newton polytope of the corresponding factor f_j of f and give sufficiently linear osculation conditions for computing f_j.

2. The algorithm

We deduce from the previous results a deterministic algorithm running in polynomial time with respect to $V := \mathrm{Vol}(N_f)$.

Input: $f \in \mathbb{Q}[t_1, t_2]$ satisfying hypothesis (H_1) and (H_2).

Output: The irreducible rational factors of f.

• *Step* 0*: Univariate factorization.* Compute the set $\mathcal{P}$ of non monomial irreducible rational factors of all the exterior facet polynomials of f.

• *Step* 1*: Lifting.* This is the γ_C computation. Lift each $P \in \mathcal{P}$ to a local equation of C modulo the local equation of D_∞. Complexity $\widetilde{\mathcal{O}}(V^2)$.

• *Step* 2*: Recombination.*
a) Build the matrix A. Complexity $\widetilde{\mathcal{O}}(V^2)$.
b) Compute the reduced echelon basis of $\ker(A)$. Complexity $\mathcal{O}(V\,\mathrm{Card}(\mathcal{P})^{\omega-1})$.

• *Step* 3*: Factors computation.* For each vector γ_j of the previous basis, compute the corresponding factor f_j of f by solving the linear system derived from the osculation conditions $C_j \cap D_\infty = \gamma_j$. Complexity $\mathcal{O}(V^\omega)$.

The algorithm is correct thanks to Theorem 1.2 and Corollary 1.4. The given complexities are deduced from those wellknown of the involved modular algorithms (Newton interation, basis computation, etc.) combined with the equality $\deg(C \cdot D_\infty) = \mathcal{O}(\mathrm{Vol}(N_f))$ and with the combinatorial restrictions $N_f = N_{f_1} + \cdots + N_{f_s}$ imposed by a theorem of Ostrowski. Theorem 1.1 follows. □

References

[1] F. Abu Salem, S. Gao, A.G.B. Lauder, *Factoring polynomials via polytopes*, proc. of ISSAC (2004).
[2] G. Chèze and G. Lecerf, *Lifting and recombination techniques for absolute factorization*, J. of Comp. 23 (2007), no. 3, pp. 380-420.
[3] M. Elkadi, A. Galligo, M. Weimann, *Towards Toric Absolute Factorization*, J. Symb. Comp. Vol. 44 (2009), no. 9, pp. 1194-1211.
[4] A. Galligo, D. Rupprecht, *Irreducible decomposition of curves*, J. Symb. Comp., 33 (2002), pp. 661-677.
[5] S. Gao, *Factoring multivariate polynomials via partial differential equations*, Math. Comp. 72 (2003), no. 242, pp. 801-822.
[6] E. Kaltofen, *A polynomial-time reduction from bivariate to univariate integral polynomial factorization*, Proc. 23rd Symp. Foundations of Comp. Sci. (1982), pp. 57-64.
[7] G. Lecerf, *Sharp precision in Hensel lifting for bivariate polynomial factorization*, Math. Comp. 75 (2006), no. 254, pp. 921-933.
[8] A.K. Lenstra, H.W. Lenstra, Jr. and L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261, no.2 (1982), pp. 515-534.
[9] W. Ruppert, *Reduzibilitat Ebener Kurven*, J. Reine Angew. Math. 369 (1986), pp.167-191.
[10] M. Weimann, *An interpolation theorem in toric varieties*, Ann. Inst. Four. 58 (2008), pp. 1371-1381.
[11] M. Weimann, *Algebraic osculation and factorization of sparse polynomials*, arXiv: 0904.0178v1.
[12] M. Weimann, *A lifting and recombination algorithm for rational factorization of sparse polynomials*, arXiv:0912.0895v1.

Martin Weimann, University of Barcelona, Gran Via, 585 08007 Barcelona.
E-mail address: weimann23@gmail.com