

Lifting and Recombination Techniques for Absolute Factorization

Guillaume Chèze

Grégoire Lecerf

Laboratoire de Mathématiques
Université de Nice Sophia-Antipolis
Parc Valrose
06108 Nice Cedex 2, France

Laboratoire de Mathématiques
Université de Versailles
45, avenue des États-Unis
78035 Versailles, France

Guillaume.Cheze@math.unice.fr

Gregoire.Lecerf@math.uvsq.fr

Abstract

In the vein of recent algorithmic results on polynomial factorization based on lifting and recombination techniques, we propose a new faster method for computing the absolute factorization of a bivariate polynomial. The complexity of our probabilistic algorithm is subquadratic in the dense size of the input polynomial, with respect to its total degree. In addition, we present a deterministic version only with soft quadratic worst case complexity.

Motivations and Related Works. All along this text, F denotes the polynomial we want to factor: this is a polynomial in two variables x and y over a commutative field \mathbb{K} ; its total degree is denoted by d . Under Hypothesis (C) \mathbb{K} has characteristic 0 or at least $d(d-1)+1$, we present new faster probabilistic and deterministic algorithms for computing the *absolute factorization* of F , that is the irreducible factorization over the algebraic closure $\bar{\mathbb{K}}$ of \mathbb{K} .

In the middle of the eighties, several authors designed the first polynomial time algorithms: Chistov, Duval, Dvornicich, Grigoriev, Kaltofen, Trager and Traverso. The motivations were mainly arising from *symbolic integration* and *polynomial system solving*.

From the nineties, other authors proposed different strategies based on topology and monodromy theory for computing approximate and exact factorizations in the special case when $\mathbb{K} = \mathbb{Q}$: Bajaj, Canny, Garrity, Warren, Galligo, Rupprecht, Corless, Kotsireas, Watt, Sommese, Verschelde, Wampler and Chèze (cited in chronological order). In this case, absolute factorization corresponds to the decomposition of the smooth locus of an equidimensional algebraic set into path connected components, which is an important ingredient for solving problems arising from kinematics, as exemplified in [7].

Another strategy has been investigated by Cormier, Singer, Trager and Ulmer: they have shown that the absolute factorization can be computed from the *minimal differential operator* associated to F .

Our new algorithms are less connected to these techniques but originate in [5, 6], that contain an efficient absolute irreducibility test, based on arithmetic alone. Roughly speaking, the test is formulated in terms of the existence of a closed differential 1-form having F as denominator. This test has been turned into a probabilistic factorization algorithm by Gao [3]: the absolute factorization reduces to the computation of a vector space of closed differential 1-forms. It is worth mentioning that Gao's algorithm computes both rational and absolute factorizations at the same time within $\tilde{O}(d^5)$ operations in \mathbb{K} .

On the other hand, improving the rational factorization algorithms of [1], a new *lifting and recombination* scheme has been proposed in [4]: the precision of the lifting is deduced from Ruppert's theorem and the recombination problem reduces to solving a linear system. Our main contribution here is to adapt this method in a way to deal efficiently with absolute factorization. Yet this adaptation is not straightforward: we had to design a new lifting device based on Paterson and Stockmeyer's evaluation rule and new formulae for recovering the factors from a basis of solutions of the linear system. For this task, we use some classical tools due to Rothstein, Trager, Lazard and Rioboo, which were primarily designed for symbolic integration.

Main Complexity Results. We now present our main complexity results in terms of the *computation tree* model. For the sake of simplicity, we assume that F is irreducible. This irreducibility assumption is

not restrictive since one can always use the algorithm presented in [4] to factor F over \mathbb{K} . The absolute irreducible factors of F will be denoted by F_1, \dots, F_r .

By definition, the F_i all belong to $\overline{\mathbb{K}}[x, y]$ but, from a computational point of view, a more precise description of the algebraic extensions of \mathbb{K} containing the F_i is necessary. It is well-known that there exists:

- A separable algebraic extension \mathbb{F} of \mathbb{K} of degree r ;
- A polynomial $F \in \mathbb{F}[x, y]$ of total degree d/r such that:

$$\{F_1, \dots, F_r\} = \{\chi(F) \mid \chi: \mathbb{F} \hookrightarrow \overline{\mathbb{K}}\},$$

where χ runs along all the embeddings of \mathbb{F} in $\overline{\mathbb{K}}$ that induce the identity on \mathbb{K} .

In practice, the extension \mathbb{F} will be represented by a quotient $\mathbb{F} = \mathbb{K}[z]/(q(z))$, where q is a monic separable irreducible polynomial in $\mathbb{K}[z]$ of degree r .

According to these definitions, our main complexity results are summarized in the following theorems.

Theorem. [2] *Under Hypothesis (C), if F is irreducible then its absolute factorization can be computed within $\tilde{O}(d^4)$ arithmetic operations in \mathbb{K} .*

For the sake of precision, we express our probabilistic algorithm in terms of the existence of families of computation trees so that, if the cardinality of \mathbb{K} is infinite, almost all the trees are executable and compute suitable results. For convenience, we write $\mathcal{A}(P) := \{a \in \mathbb{K}^n \mid P(a) \neq 0\}$, for any polynomial $P \in \overline{\mathbb{K}}[x_1, \dots, x_n]$. The constant $\omega \leq 3$ represents a feasible matrix multiplication exponent.

Theorem. [2] *There exists a family of computation trees over \mathbb{K} parametrized by*

$$(u, v, a, c_1, \dots, c_d) \in \mathbb{K}^{d+3}$$

such that: for any irreducible polynomial $F \in \mathbb{K}[x, y]$, such that Hypothesis (C) holds, any executable tree of the family computes F . The maximum of the costs of the trees of the family belongs to $\tilde{O}(d^{(\omega+3)/2})$.

In addition, there exists a nonzero polynomial $P \in \mathbb{K}[U]$ of degree at most d such that, for any $u \in \mathcal{A}(P)$, there exists a nonzero polynomial $Q_u \in \mathbb{K}[V]$ of degree at most $d(d-1)$ such that, for any $v \in \mathcal{A}(Q_u)$, there exists a nonzero polynomial $R_{u,v} \in \mathbb{K}[A]$ of degree at most $d(d-1)$ such that, for any $a \in \mathcal{A}(R_{u,v})$, there exists a nonzero polynomial $S_{u,v,a} \in \mathbb{K}[C_{1:d}]$ of total degree at most $d(d-1)/2$ such that, for any $c_{1:d} \in \mathcal{A}(S_{u,v,a})$, the tree corresponding to $(u, v, a, c_1, \dots, c_d)$ is executable on F .

Compared to [3], our new algorithm gains in solving a linear system in d unknowns instead of $2d(d+1)$.

References :

- [1] A. Bostan, G. Lecerf, B. Salvy, É. Schost, and B. Wiebelt; *Complexity issues in bivariate polynomial factorization*, in Proceedings of ISSAC 2004, pages 42–49. ACM, 2004.
- [2] G. Chèze and G. Lecerf; *Lifting and recombination techniques for absolute factorization*, Manuscript, 2004.
- [3] S. Gao; *Factoring multivariate polynomials via partial differential equations*, Math. Comp., 72(242):801–822, 2003.
- [4] G. Lecerf; *Sharp precision in Hensel lifting for bivariate polynomial factorization*, manuscript, Université de Versailles Saint-Quentin-en-Yvelines, 2004.
- [5] W. M. Ruppert; *Reduzibilität ebener Kurven*, J. Reine Angew. Math., 369:167–191, 1986.
- [6] W. M. Ruppert; *Reducibility of polynomials $f(x, y)$ modulo p* , J. Number Theory, 77(1):62–70, 1999.
- [7] A. J. Sommese, J. Verschelde, and C. W. Wampler; *Advances in polynomial continuation for solving problems in kinematics*, ASME Journal of Mechanical Design, 126(2):262-268, 2004.