Advances in Applied Mathematics 45 (2010) 607–623

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

On factoring parametric multivariate polynomials

Ali Ayad [a,b,*,1]

[a] CEA LIST, Software Safety Laboratory, Point Courrier 94, Gif-sur-Yvette, F-91191 France
[b] IRMAR, Campus de Beaulieu, Université Rennes 1, 35042, Rennes, France

ARTICLE INFO

Article history:
Received 23 June 2009
Revised 28 March 2010
Accepted 30 March 2010
Available online 26 May 2010

MSC:
11Y16
68W30
11C08
12D05
14C05

Keywords:
Symbolic computations
Complexity analysis
Polynomial absolute factorization
Irreducible polynomials
Parametric polynomials
Algebraic polynomial systems
Parametric systems

ABSTRACT

This paper presents a new algorithm for the absolute factorization of parametric multivariate polynomials over the field of rational numbers. This algorithm decomposes the parameters space into a finite number of constructible sets. The absolutely irreducible factors of the input parametric polynomial are given uniformly in each constructible set. The algorithm is based on a parametric version of Hensel's lemma and an algorithm for quantifier elimination in the theory of algebraically closed field in order to reduce the problem of finding absolute irreducible factors to that of representing solutions of zero-dimensional parametric polynomial systems. The complexity of this algorithm is single exponential in the number n of the variables of the input polynomial, its degree d w.r.t. these variables and the number r of the parameters.

1. Introduction

A polynomial with coefficients in a field K is said to be absolutely irreducible if it is irreducible over an algebraic closure $\overline{K}$ of K, this is equivalent to that it is irreducible over all algebraic extensions of K. Its absolute factorization is its unique decomposition into a product of absolutely irreducible factors.

* Address for correspondence: CEA LIST, Software Safety Laboratory, Point Courrier 94, Gif-sur-Yvette, F-91191 France.
E-mail address: ayadali99100@hotmail.com.

[1] We gratefully thank Professor Dimitri Grigoriev for his help in the redaction of this paper, and more generally for his suggestions about the approach presented here.

0196-8858/$ – see front matter
doi:10.1016/j.aam.2010.03.006

A parametric multivariate polynomial is a polynomial $F \in \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$ whose polynomial coefficients (over $\mathbb{Q}$) in the variables $u = (u_1, \ldots, u_r)$ (the parameters). In this paper, we suppose that the parameters are algebraically independent over $\mathbb{Q}$, therefore all coefficients of parametric multivariate polynomials are algebraically independent over $\mathbb{Q}$ (see the second paragraph of Section 3.4 for the general case).

The main goal of the paper is to compute the absolute factorization of a parametric multivariate polynomial F uniformly for different values of the parameters in the set $\mathcal{P} = \overline{\mathbb{Q}}^r$ which we call the parameters space (see below and Example 1.6). In the sequel, let us adopt the following notation: for a polynomial $g \in \mathbb{Q}(u_1, \ldots, u_r)[X_0, \ldots, X_n]$ and a value $a = (a_1, \ldots, a_r) \in \mathcal{P}$ of the parameters, we denote by $g^{(a)}$ the polynomial of $\overline{\mathbb{Q}}[X_0, \ldots, X_n]$ which is obtained by specialization of u by a in the coefficients of g if their denominators do not vanish on a.

Definition 1.1. A Parametric Absolutely Irreducible Factor (PAIF) of a parametric multivariate polynomial $F \in \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$ is a 3-tuple (W, ϕ, G) where W is a constructible subset of $\mathcal{P}$, $\phi \in \mathbb{Q}(u)[C]$ (C is a new variable) and $G \in \mathbb{Q}(C, u_1, \ldots, u_r)[X_0, \ldots, X_n]$ is a parametric multivariate polynomial with rational coefficients in C and $u_1, \ldots, u_r$. This 3-tuple does satisfy the following properties:

- All rational functions coefficients of ϕ in $\mathbb{Q}(u)$ are well-defined on W.
- For any $a \in W$, there exists $c \in \overline{\mathbb{Q}}$, a root of $\phi^{(a)} \in \overline{\mathbb{Q}}[C]$ such that the denominators of the coefficients of G do not vanish on (c, a) and $G^{(c,a)}$ is an absolutely irreducible factor of $F^{(a)}$.

Remark 1.2. Recall that in symbolic computation, the absolute factorization of a polynomial over a ground field K requires also to compute a primitive extension $K[\alpha]$ of K (represented by the minimal polynomial of α over K) that contains all coefficients of all the absolutely irreducible factors of the polynomial to be factored. For this reason, PAIFs contain a polynomial ϕ which defines parametrically the algebraic extension of $\overline{\mathbb{Q}}$ where the coefficients of G belong to, i.e., for any $a \in W$, there exists $c \in \overline{\mathbb{Q}}$ such that $G^{(c,a)} \in \overline{\mathbb{Q}}(c)[X_0, \ldots, X_n]$ and the minimal polynomial of c over $\overline{\mathbb{Q}}$ is a divisor of $\phi^{(a)}$ in $\overline{\mathbb{Q}}[C]$.

Definition 1.3. A Parametric Absolute Factorization (PAF) of a parametric multivariate polynomial $F \in \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$ is a tuple $(W, \phi, G_1, \ldots, G_s)$ where s is a given integer, W is a constructible subset of $\mathcal{P}$, $\phi \in \mathbb{Q}(u)[C]$ and for all $1 \leqslant j \leqslant s$, $G_j \in \mathbb{Q}(C, u_1, \ldots, u_r)[X_0, \ldots, X_n]$ is a parametric multivariate polynomial with rational coefficients in C and $u_1, \ldots, u_r$. This tuple does satisfy the following properties:

- All rational functions coefficients of ϕ in $\mathbb{Q}(u)$ are well-defined on W.
- For any $a \in W$, there exists $c \in \overline{\mathbb{Q}}$, a root of $\phi^{(a)} \in \overline{\mathbb{Q}}[C]$ such that for all $1 \leqslant j \leqslant s$, the denominators of the coefficients of G_j do not vanish on (c, a) and

$$F^{(a)} = G_1^{(c,a)} \cdots G_s^{(c,a)}$$

is the absolute factorization of $F^{(a)}$.

Remark 1.4. Let $(W, \phi, G_1, \ldots, G_s)$ be a PAF of a parametric multivariate polynomial $F \in \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$. Then $G_1, \ldots, G_s$ are the unique polynomials in $\mathbb{Q}(C, u_1, \ldots, u_r)[X_0, \ldots, X_n]$ such that for all $1 \leqslant j \leqslant s$, (W, ϕ, G_j) is a PAIF of F (for fixed W and ϕ). Therefore, the number of absolutely irreducible factors of F is constant in W.

The main theorem of the paper ensures that we can cover all values of the parameters as follows: