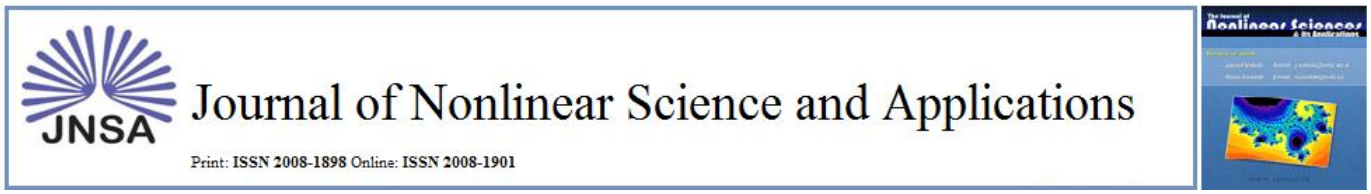
Available online at www.tjnsa.com
J. Nonlinear Sci. Appl. 5 (2012), 426–438
Research Article



An algorithm for solving zero-dimensional parametric systems of polynomial homogeneous equations

Ali Ayad*, Ali Fares, Youssef Ayyad

Équipe Algèbre et Combinatoire, EDST, Faculté des sciences - Section 1, Université libanaise, Hadath, Liban.

Dedicated to George A Anastassiou on the occasion of his sixtieth birthday

Communicated by Professor Yong-Zhuo Chen

Abstract

This paper presents a new algorithm for solving zero-dimensional parametric systems of polynomial homogeneous equations. This algorithm is based on the computation of what we call parametric U-resultants. The parameters space, i.e., the set of values of the parameters is decomposed into a finite number of constructible sets. The solutions of the input polynomial system are given uniformly in each constructible set by Polynomial Univariate Representations. The complexity of this algorithm is single exponential in the number n of the unknowns and the number r of the parameters.

Keywords: Symbolic computation, complexity analysis, theory of resultants, algebraic polynomial systems, parametric systems, Rational Univariate Representation, parametric Gaussian elimination.
2010 MSC: Primary 11Y16, 08A40, 11R09; Secondary 12D05, 15A06.

1. Introduction

A parametric system of polynomial homogeneous equations is a finite set of multivariate homogeneous polynomials $f_1, \ldots, f_k \in \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$ (in the variables $X_0, \ldots, X_n$) with polynomial coefficients in the variables $u = (u_1, \ldots, u_r)$ (the parameters) over the field $\mathbb{Q}$ of rational numbers, i.e., an infinite collection of algebraic systems of polynomial homogeneous equations in $X_0, \ldots, X_n$ parametrized by a finite number of variables called parameters. Parameters take values from the space $\mathcal{P} = \overline{\mathbb{Q}}^r$ which we call the parameters space, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. In the sequel, let us adopt the following notation: for

*Corresponding author
Email addresses: ayadali99100@hotmail.com (Ali Ayad), alikfares@yahoo.fr (Ali Fares), ayyadyoussef@hotmail.com (Youssef Ayyad)

Received 2011-1-14

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, i.e., $g^{(a)} = g(a_1, \ldots, a_r, X_0, \ldots, X_n)$.

In this paper, we are interested in solving zero-dimensional parametric systems of polynomial homogeneous equations, i.e., systems with finite number of solutions in the n-dimensional projective space $P^n(\overline{\mathbb{Q}})$. Solving such a system returns to determine the values of the parameters in $\mathcal{P}$ for which the associated polynomial systems have solutions in $P^n(\overline{\mathbb{Q}})$ (we call them consistent systems). However, when the system is consistent, it is sometimes necessary to describe the set of its solutions uniformly in these values of the parameters (see below).

Such parametric polynomial systems come from real-life problems as geometric [12, 25], optimization [41] and interpolation [35, 36, 15] ones, or physical problems [27, 33, 11], chemical reactions [10, 11, 15] and robots [16, 6, 35, 36].

In the literature, there are different algorithms for solving such parametric systems. They differ by the way that solutions are represented and by their complexity bounds. Grigoriev and Vorobjov [19] (also Montes [30]) give algorithms for solving zero-dimensional parametric polynomial systems which are based on the computation of parametric Gröbner bases [3]. They compute a partition of $\mathcal{P}$ into a finite number of constructible sets and for each set W of them, they compute polynomials $G_1, \ldots, G_s \in \mathbb{Q}(u_1, \ldots, u_r)[X_0, \ldots, X_n]$ which satisfy the following properties:

- The rational coefficients of $G_1, \ldots, G_s$ in $\mathbb{Q}(u_1, \ldots, u_r)$ are well-defined in W.
- For any $a \in W$, the set $\{G_1^{(a)}, \ldots, G_s^{(a)}\} \subset \overline{\mathbb{Q}}[X_0, \ldots, X_n]$ is the reduced Gröbner basis of the ideal spanned by $f_1^{(a)}, \ldots, f_k^{(a)}$ in $\overline{\mathbb{Q}}[X_0, \ldots, X_n]$ w.r.t. a certain fixed monomial order on $X_0, \ldots, X_n$.

If d is an upper bound on the degrees of $f_1, \ldots, f_k$ w.r.t. $X_0, \ldots, X_n$, the complexity bound of the algorithm of [19] is $d^{O(n^2 r)}$. Note that it is well-known [29] that in the non-parametric case, the lower bound of the complexity of computing Gröbner bases for polynomial ideals of positive dimension (i.e., with infinite number of solutions) is double-exponential in n.

Parametric geometric resolutions of zero-dimensional parametric polynomial systems are given by Giusti et. al. [13, 12, 14], Heintz et. al. [22] and Schost [36, 35]. The complexity bound in these papers is $d^{O(nr)}$. Gao et. al. [11], Wang [39], Dahan and Schost [37, 9] describe algorithms based on the computation of parametric triangular sets. The discriminant varieties for zero-dimensional parametric polynomial systems are introduced and computed by Lazard and Rouillier [26] with single exponential time in n and r [31]. Dynamic evaluation [32] are also used for solving parametric polynomial systems. Most of these algorithms suffer from the fact that they cannot compute solutions for all specializations of the parameters (if they exist), i.e., there is no partition of the parameters space $\mathcal{P}$ and solutions are computed uniformly just for a subset of $\mathcal{P}$.

In this paper, we give a new algorithm for solving zero-dimensional parametric systems of polynomial homogeneous equations. For a parametric system $(f_1, \ldots, f_k)$ (with the above notations), we focus on the subset $\mathcal{W}$ of the parameters space $\mathcal{P}$ formed by the values $a \in \mathcal{P}$ such that the associated system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ is zero-dimensional and does not have solutions at infinity (i.e., solutions for which $X_0 = 0$). The algorithm will describe uniformly the multiset of the multiplicities of the system which is defined by:

Definition 1.1. Let $\{g_1, \ldots, g_k\} \subset \mathbb{Q}[X_0, \ldots, X_n]$ be a zero-dimensional homogeneous system with solutions $\xi_1, \ldots, \xi_s \in P^n(\overline{\mathbb{Q}})$. The multiset of the multiplicities (MM) of this system is the multiset $(mult(\xi_1), \ldots, mult(\xi_s)) \in \mathbb{N}^s$ where $mult(\xi)$ is the multiplicity of ξ as a solution of the system (there is no order on the integers of this multiset).

Then the algorithm computes a finite partition of the set $\mathcal{W}$ into constructible sets such that for each set W of them, the MM and the number of solutions of the associated systems are constant in W and their

solutions are represented by Polynomial Univariate Representations (PUR [34]) as follows: the algorithm computes parametric univariate polynomials $\chi, \psi_1, \ldots, \psi_n \in \mathbb{Q}(u_1, \ldots, u_r)[Z]$ (Z is a new variable) which satisfy the following properties:

- The rational coefficients of $\chi, \psi_1, \ldots, \psi_n$ in $\mathbb{Q}(u_1, \ldots, u_r)$ are well-defined on W.
- For any $a \in W$, the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ are given by the following polynomial univariate representation:

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \frac{X_1}{X_0} &= \psi_1^{(a)}(\theta) \\ &\vdots \\ \frac{X_n}{X_0} &= \psi_n^{(a)}(\theta) \end{cases}$$

This reads as follows: each root θ of $\chi^{(a)}$ defines a solution of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ by evaluating the polynomials $\psi_1^{(a)}, \ldots, \psi_n^{(a)} \in \overline{\mathbb{Q}}[Z]$ on θ. In particular, the constant number of solutions of the system in W is given by the degree of χ w.r.t. Z. This gives a reduction method from the problem of solving multivariate polynomial systems to that of univariate polynomials.

In addition, the number of the elements of the partition, the degrees of $\chi, \psi_1, \ldots, \psi_n$ w.r.t. u and their binary lengths are single exponential in n and r. The total complexity and the total binary complexity of this algorithm are also single exponential in n and r (see Theorem 5.3 below for more details).

The paper is organized as follow. Section 2 presents some usefull complexity analysis of intermediate algorithms which will be used in the main algorithm of the paper. This includes a method for computing U-resultants for zero-dimensional polynomial systems, algorithms for computing uniformly the rank of a parametric matrix and multiplicities of parametric univariate polynomials. Section 3 introduces the notion of parametric U-resultants for parametric polynomial systems. Section 4 computes uniformly the MM of parametric polynomial systems by reducing the problem to the computation of the multiplicities of parametric univariate polynomials. The computation of parametric PUR is done in Section 5 by a parametric version of the Shape lemma.

2. Preliminaries

2.1. U-resultant

U-resultants was studied first by Kronecker and Van der Waerden [38] and after by Lazard [23, 24] and others. Here we show the definition of the U-resultants for zero-dimensional polynomial systems with a method from [24, 17] to compute them.

Definition 2.1. Let $g = \{g_1, \ldots, g_k\} \subset \mathbb{Q}[X_0, \ldots, X_n]$ be a zero-dimensional system of homogeneous equations. The U-resultant of g is a homogeneous polynomial $R \in \mathbb{Q}[U_0, \ldots, U_n]$ (where $U_0, \ldots, U_n$ are new variables) which satisfies the following property: R factorizes in the form:

$$R = \prod_i L_i \quad \text{where} \quad L_i = \sum_{0 \le j \le n} \xi_j^{(i)} U_j \quad \text{and} \quad \xi_j^{(i)} \in \overline{\mathbb{Q}},$$

and each $(\xi_0^{(i)} : \cdots : \xi_n^{(i)}) \in P^n(\overline{\mathbb{Q}})$ is a solution of the system g whose multiplicity is equal to that of L_i as a factor of R. Thus the number of the solutions of g (counted with their multiplicities) is equal to the degree of R.

Macaulay matrix:. In this paragraph, we give a way to distinguish zero-dimensional systems and to compute their associated U-resultants. Let $g = \{g_1, \ldots, g_k\} \subset \mathbb{Q}[X_0, \ldots, X_n]$ be a system (not necessary zero-dimensional) of homogeneous equations of degrees $D_1, \ldots, D_k$ such that $d \geq D_1 \geq \cdots \geq D_k$ for some integer d and let

$$\mathcal{D} = D_1 + \sum_{2 \leq i \leq n} (D_i - 1) \leq nd.$$

We introduce the linear form $g_{k+1} = U_0X_0 + \cdots + U_nX_n \in \mathbb{Q}(U_0, \ldots, U_n)[X_0, \ldots, X_n]$ and we denote by B_i (respectively B) the vector space of homogeneous polynomials in $\mathbb{Q}(U_0, \ldots, U_n)[X_0, \ldots, X_n]$ of degrees $\mathcal{D} - D_i$ (respectively $\mathcal{D}$) for all $1 \leq i \leq k+1$ where $D_{k+1} = 1$. Consider the $\mathbb{Q}(U_0, \ldots, U_n)$-linear map $\Psi : B_1 \oplus \cdots \oplus B_{k+1} \longrightarrow B$ defined by:

$$\Psi(h_1, \ldots, h_{k+1}) = \sum_{1 \leq i \leq k+1} h_i g_i \quad \text{for any} \quad (h_1, \ldots, h_{k+1}) \in B_1 \oplus \cdots \oplus B_{k+1}.$$

We denote by $\mathcal{M}$ the associated $N \times \left(\sum_{1 \leq i \leq k+1} N_i \right)$ matrix of Ψ in the monomials of $B_1, \ldots, B_{k+1}, B$ where $N_i := \dim(B_i) = \binom{n+\mathcal{D}-D_i}{n}$, $1 \leq i \leq k+1$ and $N = \dim(B) = \binom{n+\mathcal{D}}{n}$. $\mathcal{M}$ is called the Macaulay matrix of the system g. We write $\mathcal{M}$ in the form:

$$\mathcal{M} = \mathcal{M}(U_0, \ldots, U_n) = (\mathcal{M}_1 \quad \mathcal{M}_2)$$

where $\mathcal{M}_2$ is constructed by the last N_{k+1} columns of $\mathcal{M}$ with linear form entries over $\mathbb{Q}$ in the variables $U_0, \ldots, U_n$ and $\mathcal{M}_1$ has its entries in $\mathbb{Q}$.

We recall the basic result of Lazard's works (see Theorem 4.1, Theorem 5.1 and Theorem 7.1 of [24], see also [23] and Theorem 2.2 of [17]) in the following theorem:

Theorem 2.2. *Under the above notations,*

- *The system g has zero dimension if and only if the rank of its associated Macaulay matrix $\mathcal{M}$ is equal to N, i.e., $rk(\mathcal{M}) = N$.*
- *When g is a zero-dimensional system, the ideal generated by the N minors of $\mathcal{M}$ is a principal ideal of $\mathbb{Q}[U_0, \ldots, U_n]$. The generator $R \in \mathbb{Q}[U_0, \ldots, U_n]$ of this ideal is the U-resultant of the system g. In addition, the degree of R is equal to $N - rk(\mathcal{M}_1)$.*
- *R coincides with any nonzero N minor of $\mathcal{M}$ which contains $rk(\mathcal{M}_1)$ columns of $\mathcal{M}_1$.*

2.2. Parametric Gaussian elimination

In this subsection, we give an improved presentation of a parametrization of the well-known Gaussian algorithm with a study on the bounds of the outputs of the algorithm and a complete complexity analysis.

Let A be a parametric $n \times n$ matrix with entries in $\mathbb{Q}[u_1, \ldots, u_r]$ with degrees bounded by an integer δ and binary lengths (i.e., the maximum of the binary lengths of their coefficients in $\mathbb{Q}$) less than an integer M. Our goal is to study the dependancy of the rank of the system from different values of the parameters. The set $\{det(A) \neq 0\} \subset \mathcal{P}$ defines the locus in the parameters space $\mathcal{P}$ where A has maximal rank, i.e., $rk(A) = n$ (where $det(A) \in \mathbb{Q}[u_1, \ldots, u_r]$ is the determinant of A).

The parametrization of the Gaussian elimination procedure consists of performing ordinary Gaussian algorithm and separating steps where pivot Gaussian elements are nonzeros. The main theorem of this subsection is the following one:

Theorem 2.3. *There is an algorithm, called the parametric Gaussian algorithm which for a parametric $n \times n$ matrix A (with the above notations), products a partition of the parameters space $\mathcal{P}$ into $(n+1)$ constructible sets $\mathcal{U}_i$ $(0 \leq i \leq n)$ which satisfy the following property:*

- *The rank of A is constant in each $\mathcal{U}_i$ and is equal to i, this means that for any $a \in \mathcal{U}_i$, $rk(A^{(a)}) = i$, where $A^{(a)}$ is the matrix obtained from A by specialization of its entries on a.*

The degrees of the equations and inequations which define $\mathcal{U}_i$ w.r.t. u are bounded by $n\delta$. Their binary lengths are less than nM. The total complexity of the algorithm is $(n\delta)^{O(r)}$ operations in $\mathbb{Q}$ and the total binary complexity is $M(n\delta)^{O(r)}$.

Proof. The algorithm constructs a set of couples $(C^{(i)}, A^{(i)})$, $0 \leq i \leq n$ where $C^{(0)} = \mathcal{P}$, $A^{(0)} = A$ and $C^{(i)}$ $(1 \leq i \leq n)$ is a constructible subset of $\mathcal{P}$ given by its equations and inequations and $A^{(i)} = \left(A^{(i)}_{s,t}\right)_{1\leq s,t\leq n}$ is a $n \times n$ matrix with coefficients in $\mathbb{Q}[u_1, \ldots, u_r]$ obtained from A by linear row transformations and permutations. This matrix has the form:

$$A^{(i)} = \begin{pmatrix} A^{(i)}_{1,1} & \ldots & \ldots & \ldots & \ldots & \ldots & A^{(i)}_{1,n} \\ 0 & A^{(i)}_{2,2} & \ldots & \ldots & \ldots & \ldots & A^{(i)}_{2,n} \\ \vdots & 0 & \ddots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & 0 & A^{(i)}_{i,i} & \ldots & \ldots & A^{(i)}_{i,n} \\ \vdots & \vdots & \vdots & 0 & A^{(i)}_{i+1,i+1} & \ldots & A^{(i)}_{i+1,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & A^{(i)}_{n,i+1} & \ldots & A^{(i)}_{n,n} \end{pmatrix}$$

such that for all $a \in C^{(i)}$,

$$A^{(i)}_{1,1}(a) \neq 0, \ldots, A^{(i)}_{i,i}(a) \neq 0.$$

We do this construction by induction on i. We suppose that at the i-th step, $C^{(i)}$ is defined by equations and inequations of the form $g = 0$ and $h \neq 0$ where $g, h \in \mathbb{Q}[u_1, \ldots, u_r]$ satisfy the following bounds:

- The degrees of g, h and $A^{(i)}_{s,t}$ $(1 \leq s, t \leq n)$ w.r.t. u are bounded by $i\delta$;
- The binary lengths of g, h and $A^{(i)}_{s,t}$ $(1 \leq s, t \leq n)$ are less than $i(M + 1)$.

The $(i + 1)$-th step consists to do the following:

- If $A^{(i)}_{i+1,i+1} \in \mathbb{Q}[u_1, \ldots, u_r]$ is linearly dependent of the polynomials g, we exchange the $(i + 1)$-th row of $A^{(i)}$ by the $(i + 2)$-th row and we test again if $A^{(i)}_{i+2,i+1}$ is linearly dependent of g and so on. Each test corresponds to solve a linear system with at most i unknowns and $\binom{r+i\delta}{r} \leq (i\delta)^r$ equations with coefficients in $\mathbb{Q}$. This resolution can be done with $(i\delta)^{O(r)}$ operations in $\mathbb{Q}$ [28]. Each of these operations is done on elements of binary lengths less than $i(M+1)$. Then each test is done by $(i\delta)^{O(r)}$ operations in $\mathbb{Q}$. Its binary complexity is bounded by $M(i\delta)^{O(r)}$.
- If all the polynomials $A^{(i)}_{s,t}$, $s \geq i+1$, $t \geq i+1$ (even after exchange of columns) are linearly dependent of the polynomials g then $A^{(i)}_{s,t}(a) = 0$ for all $a \in C^{(i)}$. In this case, the algorithm stops and does not consider the next couple $(C^{(i+1)}, A^{(i+1)})$. The number of tests to do is equal to $(n - i)^2$. They are done by $n^2(i\delta)^{O(r)}$ operations in $\mathbb{Q}$ and with binary complexity bounded by $n^2M(i\delta)^{O(r)}$.
- If there exist $s_0 \geq i+1$, $t_0 \geq i+1$ such that $A^{(i)}_{s_0,t_0}$ is linearly independent of the polynomials g then we take $C^{(i+1)} = C^{(i)} \cap \{A^{(i)}_{s_0,t_0} \neq 0\}$. After exchange of rows and columns, we put $A^{(i)}_{s_0,t_0}$ in the position $(i+1, i+1)$ and we apply the ordinary linear transformations on the rows $i+2, \ldots, n$ of the obtained matrix. This will make zeros the entries below $A^{(i)}_{s_0,t_0}$ (we say that $A^{(i)}_{s_0,t_0}$ is the parametric Gauss pivot,

i.e., $A^{(i)}_{s_0,t_0}(a) \neq 0$ for all $a \in C^{(i+1)}$). Then $A^{(i+1)}$ is the obtained matrix which verifies the following property: $A^{(i+1)}_{i+1,i+1} = A^{(i)}_{s_0,t_0}$ does not vanish on $C^{(i+1)}$.

By Bareiss's method (see e.g., [2, 1]), the polynomials $A^{(i+1)}_{s,t} \in \mathbb{Q}[u_1, \ldots, u_r]$ are $(i+1)\times(i+1)$ minors of the matrix A and are given by the formula:

$$A^{(i+1)}_{s,t} = \det \begin{pmatrix} A_{1,1} & \ldots & A_{1,i} & A_{1,t} \\ \vdots & & \vdots & \vdots \\ A_{i,1} & \ldots & A_{i,i} & A_{i,t} \\ A_{s,1} & \ldots & A_{s,i} & A_{s,t} \end{pmatrix}$$

This proves the above induction bounds on the degrees of $A^{(i+1)}_{s,t}$ w.r.t. u and on their binary lengths.

The total complexity of the algorithm is deduced from the above bounds by the fact that there is at most n steps in the algorithm. □

2.3. Multiplicities of roots of parametric univariate polynomials

Let $G \in \mathbb{Q}[u_1, \ldots, u_r][Z]$ be a parametric univariate polynomial of degree bounded by an integer d (resp. δ) w.r.t. Z (resp. u) and binary length less than an integer M. Because that the multiplicities of the roots of G are given by the degree of the greatest common divisor (GCD) of the successive derivatives of G w.r.t. Z, we will begin by recalling an algorithm given by Grigoriev [18] in 1989 which computes uniformly the GCD of a finite set of parametric univariate polynomials as follows:

Lemma 2.4. *Let $\{h_1, \ldots, h_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][Z]$ be a set of parametric univariate polynomials of degrees bounded by d (resp. δ) w.r.t. Z (resp. u) and binary lengths less than M. There is an algorithm which decomposes the parameters space $\mathcal{P}$ into at most $k(\delta+d)^{O(r)}$ constructible sets such that for each set V among them, the algorithm computes a parametric univariate polynomial $h \in \mathbb{Q}[u_1, \ldots, u_r][Z]$ with the following properties:*

- *The degree of h w.r.t. $u_1, \ldots, u_r, Z$ is bounded by $(\delta + d)^{O(1)}$.*
- *The binary length of h is less than $(M + r)(\delta + d)^{O(1)}$.*
- *For any $a \in V$, the polynomial $h^{(a)} \in \overline{\mathbb{Q}}[Z]$ is the GCD of the set $\{h_1^{(a)}, \ldots, h_k^{(a)}\} \subset \overline{\mathbb{Q}}[Z]$.*

The number of arithmetic operations of this algorithm is bounded by $k^{O(1)}(\delta + d)^{O(r)}$ over $\mathbb{Q}$. Its binary complexity is bounded by $(kM)^{O(1)}(\delta + d)^{O(r)}$.

Proof. See Lemma 1 of [18]. □

Thus the generic computation of the multiset of the multiplicities of the roots of G is done in the following theorem:

Theorem 2.5. *Let G be a parametric univariate polynomial with the above notations. There is an algorithm which decomposes the parameters space $\mathcal{P}$ into at most $(\delta + d)^{O(r)}$ constructible sets such that for each set $\mathcal{V}$ among them, the algorithm computes a vector $s = (s_1, \ldots, s_h) \in \mathbb{N}^h$ such that for any $a \in \mathcal{V}$, the vector s is the multiset of the multiplicities of the roots of the polynomial $G^{(a)} \in \overline{\mathbb{Q}}[Z]$. The number of arithmetic operations of this algorithm is bounded by $(\delta + d)^{O(r)}$ over $\mathbb{Q}$. Its binary complexity is bounded by $M^{O(1)}(\delta + d)^{O(r)}$.*

Proof. For any $1 \leq j \leq \deg_Z(G) \leq d$, the algorithm of Lemma 2.4 computes a parametric GCD of the set $\{G, G', \ldots, G^{(j)}\} \subset \mathbb{Q}[u_1, \ldots, u_r][Z]$ of successive derivatives of G w.r.t. Z. This algorithm presents this GCD in the form:

$$A_{j,m}Z^m + A_{j,m-1}Z^{m-1} + \cdots + A_{j,0} \in \mathbb{Q}[u_1, \ldots, u_r][Z]$$

such that $\deg_{u_1,\ldots,u_r}(A_{j,t}) \leq (\delta+d)^{O(1)}$ for all $0 \leq t \leq m \leq d-j$. The degree of $\mathrm{GCD}(G, G', \ldots, G^{(j)})$ for all $1 \leq j \leq d$ determines the multiset of the multiplicities of the roots of G. The following constructible sets

$$\mathcal{V}_{j,t} := \{A_{j,t} *_{j,t} 0\} \subset \mathcal{P}$$

(where $*_{j,t} \in \{=, \neq\}$) form a partition of $\mathcal{P}$ such that the multiset of the multiplicities of the roots of G is constant on each one among them. The complexity bounds of the algorithm are deduced from those of the algorithm of Lemma 2.4. □

3. Parametric U-resultant

Let $f = \{f_1, \ldots, f_k\} \subset \mathbb{Q}[u_1, \ldots, u_r][X_0, \ldots, X_n]$ be a parametric system of polynomial homogeneous equations of degrees respectively $D_1, \ldots, D_k$ w.r.t. $X_0, \ldots, X_n$. In this section, we conserve the same notations of Section 2.1. In addition, for the complexity analysis aims, we suppose that the degrees of $f_1, \ldots, f_k$ w.r.t. u are bounded by an integer δ and their binary lengths are less than an integer M.

Definition 3.1. A parametric U-resultant of the system f is a couple (W, R) where W is a constructible subset of $\mathcal{P}$ and $R \in \mathbb{Q}[u_1, \ldots, u_r, U_0, \ldots, U_n]$ which satisfy the following property:

- For any $a \in W$, $R^{(a)}$ is the U-resultant for the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$.

The following lemma shows that there is a finite number of parametric U-resultants which cover all values of the parameters in the set $\mathcal{W}$:

Lemma 3.2. *There is an algorithm which computes at most N parametric U-resultants $(\mathcal{A}_1, R_1), \ldots, (\mathcal{A}_N, R_N)$ of the system f satisfying the following properties:*

- *The constructible sets $\mathcal{A}_1, \ldots, \mathcal{A}_N$ form a partition of $\mathcal{W}$.*
- *Each polynomial R_i is homogeneous in $U_0, \ldots, U_n$ of degree $N-i \leq N$. Moreover, $\deg_u R_i \leq i\delta \leq N\delta$, and its binary length is less than $iM \leq NM$.*

The number of arithmetic operations of this algorithm is $(N\delta)^{O(r)}$ in $\mathbb{Q}$ and its binary complexity is $M^{O(1)}(N\delta)^{O(r)}$.

Proof. The algorithm is given by the following steps:

- Compute the Macaulay matrix $\mathcal{M} = \mathcal{M}(u_1, \ldots, u_r, U_0, \ldots, U_n) = (\mathcal{M}_1 \quad \mathcal{M}_2)$ associated to the system f as it is defined in Section 2.1 where in this case $\mathcal{M}_1$ has entries in $\mathbb{Q}[u_1, \ldots, u_r]$.
- Apply the algorithm of Theorem 2.3 to $\mathcal{M}$. It computes a constructible set $\mathcal{A}$ where the rank of $\mathcal{M}$ is maximal, i.e., for all $a \in \mathcal{A}$, $rk(\mathcal{M}^{(a)}) = N$. By Theorem 2.2, $\mathcal{A}$ is the set of values $a \in \mathcal{P}$ where the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ has a finite number of solutions in $P^n(\overline{\mathbb{Q}})$.
  Theorem 2.3 also decomposes $\mathcal{P}$ into N constructible sets $\mathcal{U}_i$ such that the rank of $\mathcal{M}_1$ is constant in each $\mathcal{U}_i$ and is equal to i.
- By the third item of Theorem 2.2, for each $\mathcal{U}_i$, compute R_i as a N minor of $\mathcal{M}$ containing i columns of $\mathcal{M}_1$. Let $\Delta_i = \deg_{U_0,\ldots,U_n} R_i = N - i$ and $I_i \in \mathbb{Q}[u_1, \ldots, u_r]$ the coefficient of $U_0^{\Delta_i}$ in R_i. The constructible sets
  $$\mathcal{A}_i = \mathcal{U}_i \cap \mathcal{A} \cap \{I_i \neq 0\}$$
  satisfy the lemma. The inequation $I_i \neq 0$ ensures that no zero solutions are allowed at infinity according to the definition of $\mathcal{W}$.

The complexity bound of the algorithm follows from Theorem 2.3 (see also p. 24-25 of [7] and p .14-15 of [18]). □

4. Constant MMs

In this section, we fix a parametric U-resultant $(\mathcal{A}_i, R_i)$ from Lemma 3.2. We will compute a partition of $\mathcal{A}_i$ into constructible sets, each of them with a generic mutilset of the multiplicities of the system f (see Lemma 4.3 below). First, we will use a result from [8]:

Lemma 4.1. *Let N be an integer. One can construct vectors $b_1, \ldots, b_{N^2n} \in \mathbb{Q}^n$ pairwise distinct with the following property : for any pairwise distinct elements $\beta_1, \ldots, \beta_n \in \mathbb{Q}^n$, there exists $1 \leq p \leq N^2n$ such that*

$$< \beta_i, b_p > \neq < \beta_j, b_p > \quad \text{for all } i \neq j \tag{4.1}$$

where the operator $< ., . >$ is the euclidean inner product in $\mathbb{Q}^n$.

Proof. By Proposition 1, 2 and 3 of [8]. □

We apply Lemma 4.1 on the integer N defined in Section 2.1. For each $1 \leq j \leq n$, we consider $n \times n$ matrices $B_1, ..., B_{N^2n}$ with coefficients in $\mathbb{Q}$ such that the j-th row of B_p is b_p for all $1 \leq p \leq N^2n$. We introduce the polynomials

$$Q_j = R_i(U_0, 0, \ldots, 0, U_j, 0, \ldots, 0) \in \mathbb{Q}[u_1, \ldots, u_r, U_0, U_j] \tag{4.2}$$

and

$$G_j(Z) = Q_j(Z, -1) \in \mathbb{Q}[u_1, \ldots, u_r][Z] \tag{4.3}$$

where Z is a new variable.

The following lemma links the solutions of the systems $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ to the roots of the polynomials $G_1^{(a)}, \ldots, G_n^{(a)} \in \overline{\mathbb{Q}}[Z]$ (for all $a \in \mathcal{A}_i$).

Lemma 4.2. *Let $a \in \mathcal{A}_i$ and $\xi = (\xi_0 : \cdots : \xi_n) \in P^n(\overline{\mathbb{Q}})$. For any $1 \leq j \leq n$, there exists a matrix B_p among $B_1, ..., B_{N^2n}$ with the following property : If ξ is a solution of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ of multiplicity μ then after the linear transformation $V = B_pU$ where $U = (U_0, \ldots, U_n)$ and $V = (V_0, \ldots, V_n)$ are new variables one has*

$$\left(\frac{\xi_j}{\xi_0}\right) \quad \text{is a root of} \quad G_j^{(a)} \in \overline{\mathbb{Q}}[Z] \quad \text{of multiplicity } \mu.$$

Proof. Definition 3.1, Theorem 2.2 and Formula (4.3) prove that $\left(\frac{\xi_j}{\xi_0}\right)$ is a root of $G_j^{(a)}$ of multiplicity $\geq \mu$. If $\zeta = (\zeta_0 : \cdots : \zeta_n) \in P^n(\overline{\mathbb{Q}})$ is another solution of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ distinct from ξ, we have

$$\left(\frac{\xi_j}{\xi_0}\right) \neq \left(\frac{\zeta_j}{\zeta_0}\right)$$

by the definition of the linear transformation B_p and by Formula (4.1) of Lemma 4.1. Thus the multiplicity of $\left(\frac{\xi_j}{\xi_0}\right)$ as a root of $G_j^{(a)}$ is exactly μ. □

Lemma 4.3. *There is an algorithm which decomposes $\mathcal{A}_i$ into at most $(N\delta)^{O(nr)}$ constructible sets $\mathcal{B}$ such that for each $\mathcal{B}$, it computes a multiset $s = (s_1, \ldots, s_h) \in \mathbb{N}^h$ which fulfills the following property:*

- *For any $a \in \mathcal{B}$, s is the multiset of the multiplicities of the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$.*

The number of arithmetic operations of this algorithm is $(N\delta)^{O(r)}$ over $\mathbb{Q}$ and its binary complexity is $M^{O(1)}(N\delta)^{O(r)}$.

Proof. Let us consider the parametric univariate polynomials $G_1, \ldots, G_n \in \mathbb{Q}[u_1, \ldots, u_r][Z]$ defined by Formula (4.3). First by Lemma 4.2, we take the matrix B_{p_1} associated to G_1 and we put the linear transformation $V = B_{p_1}U$ in Formula (4.2). Second we apply the algorithm from Theorem 2.5 to the new G_1 obtained by (4.3) after the linear change of variables. This algorithm computes a finite partition of $\mathcal{A}_i$ into constructible sets W_{q_1} each of them with a constant multiset $s^{(1)} = (s_1^{(1)}, \ldots, s_{h_1}^{(1)}) \in \mathbb{N}^{h_1}$ of the multiplicities of the roots of G_1. Again after another linear transformation defined by a matrix B_{p_2} associated to G_2 by Lemma 4.2, we apply the algorithm from Theorem 2.5 to the new G_2 which decomposes each W_{q_1} into a finite number of constructible sets W_{q_1,q_2} each of them with a constant multiset $s^{(2)} = (s_1^{(2)}, \ldots, s_{h_2}^{(2)}) \in \mathbb{N}^{h_2}$ of the multiplicities of the roots of G_2 and so on. Finally, we get constructible sets $\mathcal{B} = W_{q_1,\ldots,q_n}$ that form a finite partition of $\mathcal{A}_i$. For each $\mathcal{B}$, we associate an integer $h = \min(h_1, \ldots, h_n)$ and a multiset $s = (s_1, \ldots, s_h)$ where $s_j = \min(s_j^{(1)}, \ldots, s_j^{(n)})$ for all $1 \leq j \leq h$ which satisfies the lemma. The complexity bounds follow from those of Theorem 2.5 by simple computations taking into account the bounds on R_i from Lemma 3.2. □

5. Parametric polynomial univariate representations

In this section, we fix a constructible set $\mathcal{B} \subset \mathcal{A}_i$ from Lemma 4.3 where $(\mathcal{A}_i, R_i)$ is a parametric U-resultant of the parametric system $f_1 = \cdots = f_k = 0$ by Lemma 3.2. Let $K = \mathbb{Q}(u_1, \ldots, u_r)$ be the field of rational functions in the parameters and for any $1 \leq j \leq n$, let λ_j be a root of the polynomial G_j (defined by (4.3)) in $\overline{K}$ with minimal polynomial being a divisor of G_j in $K[Z]$. The following lemma is a parametrization of the Shape lemma:

Lemma 5.1. *Under the above notations and hypotheses, there is an algorithm which computes a primitive element θ of the extension $E = K[\lambda_1, \ldots, \lambda_n]$ over K with its minimal polynomial $\chi \in K[Z]$. In addition, the degree of χ w.r.t. u is bounded by $\delta N^{O(n)}$. Its binary length is less than $rMN^{O(n)}$. The number of operations in $\mathbb{Q}$ of the algorithm is bounded by $\delta^{O(r)}N^{O(nr)}$. Its binary complexity is less than $M^{O(1)}\delta^{O(r)}N^{O(nr)}$.*

Proof. By induction on j, we construct a primitive element θ_j for each finite and separable extension $E_j = K[\lambda_1, \ldots, \lambda_j]$ over K with its minimal polynomial $\chi_j \in K[Z]$.

- For $j = 1$, we compute $\chi_1 \in K[Z]$ a monic irreducible factor of G_1 in $K[Z]$ such that λ_1 is a root of χ_1 by the algorithm of factorization of multivariate polynomials from [4] (see also [17]), i.e, χ_1 is the minimal polynomial of λ_1 over K. Lemma 1.3 of [4] proves that the degree of χ_1 w.r.t. u is bounded by $\delta N^{O(1)}$ and its binary length is less than $rMN^{O(1)}$. In addition, the factorization of G_1 is done by $(\delta N)^{O(r)}$ operations in $\mathbb{Q}$ and by $M^{O(1)}(\delta N)^{O(r)}$ binary operations (see [4]).

- We suppose that at the step $j-1$ of the induction, a primitive element θ_{j-1} of the extension $E_{j-1} = K[\lambda_1, \ldots, \lambda_{j-1}]$ over K is given with its minimal polynomial $\chi_{j-1} \in K[Z]$ such that the degree of χ_{j-1} w.r.t. u is bounded by $\delta N^{O(j)}$ and its binary length is less than $rMN^{O(j)}$.

  Again by the factorization algorithm of [4], we compute $h_j \in E_{j-1}[Z]$ a monic irreducible factor of G_j such that λ_j is a root of h_j, i.e, h_j is the minimal polynomial of λ_j over E_{j-1}. Again Lemma 1.3 of [4] gives the same bounds on h_j as above for χ_1. Then the extension

  $$E_j = K[\lambda_1, \ldots, \lambda_j] = E_{j-1}[\lambda_j] = K[\theta_{j-1}, \lambda_j]$$

  is a finite and separable extension over K of degree less or equal than N. We fix N arbitrary elements $0 = c_1, \ldots, c_N \in \mathbb{Q}$ pairwise distinct and we consider the N elements $\theta_{j-1} + c_1\lambda_j, \ \ldots \ , \theta_{j-1} + c_N\lambda_j$ of E_j. The theorem of primitive elements ensures that there is an element $\theta_j = \theta_{j-1} + c\lambda_j$ among them which is a primitive element of the extension E_j over K.

  In order to compute the minimal polynomial χ_j of θ_j over K, we express the powers of θ_j in the basis $\theta_{j-1}^{\alpha}\lambda_j^{\beta}$, $0 \leq \alpha < \deg_Z(\chi_{j-1})$, $0 \leq \beta < \deg_Z(h_j)$ of E_j over K. The coefficients of χ_j form a non-trivial

solution of a certain homogeneous linear system with coefficients in K (if this system does not have any non-trivial solution then the algorithm takes another element c among $c_1, \ldots, c_N$). It is a system of order $\deg_Z(\chi_{j-1}) \times \deg_Z(h_j) = \deg_Z(\chi_j) \leq N$, the degrees of its entries w.r.t. u are bounded by $\delta N^{O(j)}$ and their binary lengths are less than $rMN^{O(j)}$ using the hypotheses of the induction. Then by Cramer's formulas, we get the same bounds on the degrees and the binary lengths of the coefficients of χ_j. The resolution of these systems (for all $c \in \{c_1, \ldots, c_N\}$) is done by $\delta^{O(r)}N^{O(jr)}$ operations in $\mathbb{Q}$ and $M\delta^{O(r)}N^{O(jr)}$ binary operations [28].

To finish the proof of the lemma, we take $\theta = \theta_n$ and $\chi = \chi_n \in K[Z]$, then $E_n = K[\lambda_1, \ldots, \lambda_n] = K[\theta] = E$. □

Lemma 5.2. *We can compute polynomials $\psi_1, \ldots, \psi_n \in K[Z]$ of degrees $< N$ such that for all $1 \leq j \leq n$,*

$$\lambda_j = \psi_j(\theta)$$

where θ is the primitive element of the extension E over K from Lemma 5.1. In addition, the degrees of $\psi_1, \ldots, \psi_n$ w.r.t. u are bounded by $\delta N^{O(n)}$ and their binary lengths are less than $rMN^{O(n)}$. Their computation costs $\delta^{O(r)}N^{O(nr)}$ operations in $\mathbb{Q}$ and $M\delta^{O(r)}N^{O(nr)}$ binary operations.

Proof. The computation of $\psi_1, \ldots, \psi_n$ is done by induction on j as follows:

- For $j = 1$, one takes $\lambda_1 = \theta_1$.
- We suppose that at the step $j-1$ of the induction, $\lambda_1, \ldots \lambda_{j-1}$ are expressed as polynomial functions of θ_{j-1} with coefficients in K of degrees w.r.t. u bounded by $\delta N^{O(j)}$. Since $\theta_j = \theta_{j-1} + c\lambda_j$ (by the proof of Lemma 5.1), we express the powers of θ_j in the basis $\theta_{j-1}^{\alpha}\lambda_j^{\beta}$, $0 \leq \alpha < \deg_Z(\chi_{j-1})$, $0 \leq \beta < \deg_Z(h_j)$ of E_j over K.

  Again as in the proof Lemma 5.1, in order to express θ_{j-1} and λ_j as linear combination of the powers of θ_j with coefficients in K, it suffices to solve some linear system of order less than N. By Cramer's formulas, we get the bounds on the degree and the binary length of this expression of λ_j. By substitution of the expression of θ_{j-1} in those of $\lambda_1, \ldots \lambda_{j-1}$, we get the expressions of $\lambda_1, \ldots \lambda_{j-1}$ as linear combinations of the powers of θ_j with coefficients in K.

  The resolution of these systems is done by $\delta^{O(r)}N^{O(jr)}$ operations in $\mathbb{Q}$ and $M\delta^{O(r)}N^{O(jr)}$.

□

We can now summarize the main result of the paper in the following theorem:

Theorem 5.3. *There is an algorithm which for a parametric homogeneous polynomial system $f_1 = \cdots = f_k = 0$ (with the above notations) decomposes the associated subset $\mathcal{W}$ of $\mathcal{P}$ into at most $(\delta d)^{O(n^2r^2)}$ constructible sets such that for each set W among them, we have the following properties:*

- *The multisets of the multiplicities and the number of the solutions of the associated systems are constant in W and they are computed by the algorithm.*
- *The algorithm computes polynomials $\chi, \psi_1, \ldots, \psi_n \in \mathbb{Q}(u_1, \ldots, u_r)[Z]$ such that each value $a \in W$ satisfies:*
  - *The denominators of the coefficients of $\chi, \psi_1, \ldots, \psi_n$ do not vanish on a.*
  - *A parametric PUR of the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ is given by*

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \frac{X_1}{X_0} &= \psi_1^{(a)}(\theta) \\ &\vdots \\ \frac{X_n}{X_0} &= \psi_n^{(a)}(\theta) \end{cases}$$

– *The degrees of $\chi, \psi_1, \ldots, \psi_n$ w.r.t. u is bounded by $\delta^{O(r)} d^{O(n^2 r)}$ and their binary lengths do not exceed $M\delta^{O(r)} d^{O(n^2 r)}$.*

The number of arithmetic operations of the algorithm is $\delta^{O(r^2)} d^{O(n^2 r^2)}$ and its binary complexity is $M^{O(1)} \delta^{O(r^2)} d^{O(n^2 r^2)}$.

Proof. Let $\psi \in \mathbb{Q}[u_1, \ldots, u_r]$ be the lowest common multiple of the denominators of the coefficients of the polynomials $\chi, \psi_1, \ldots, \psi_n$ of Lemmas 5.1 and 5.2. We take the constructible set $P_1 = \mathcal{B} \cap \{\psi = 0\} \subset \mathcal{P}$. For all $a \in \mathcal{B} \setminus P_1$, the solutions of the associated system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ are given by the equations of Lemma 5.2 using Lemma 4.2.

Let T_1 be the variety defined by the equation $\psi = 0$ and the equations which define $\mathcal{B}$, we apply the algorithm of solving (non parametric) algebraic systems [5, 17, 4] (see Theorem 2.4 of [17] or Theorem 2.1 of [4]) which computes each irreducible component S_1 of codimension m of T_1 by an effective generic point defined by the following field isomorphism:

$$\mathbb{Q}(t_1, \ldots, t_{r-m})[\mu] \cong \mathbb{Q}(S_1) \tag{5.1}$$

where $t_1, \ldots, t_{r-m}$ are algebraically independent over $\mathbb{Q}$ and μ is separable over the field $\mathbb{Q}(t_1, \ldots, t_{r-m})$ with a minimal polynomial $\Phi \in \mathbb{Q}(t_1, \ldots, t_{r-m})[Z]$. This algorithm expresses each variable u_i as an element of $\mathbb{Q}(t_1, \ldots, t_{r-m})[\mu]$. By substitution of these expressions in the polynomials $G_j \in \mathbb{Q}[u_1, \ldots, u_r][Z]$, we get polynomials $g_j \in \mathbb{Q}(t_1, \ldots, t_{r-m})[\mu][Z]$.
By the same procedure as above (see Lemmas 5.1 and 5.2), we compute a primitive element $\theta^{(1)}$ of the extension $K'[\lambda_1, \ldots, \lambda_n]$ over K' with its minimal polynomial $\chi \in K'[Z]$ where $K' = \mathbb{Q}(t_1, \ldots, t_{r-m})[\theta]$ and λ_j is a root of $g_j \in K'[Z]$ in $\overline{K'}$.

Then we have again a parametric representation of the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ for all $a \in S_1 \setminus P_2$ where $P_2 = S_1 \cap \{\psi^{(1)} = 0\} \subset \overline{\mathbb{Q}}^r$ and $\psi^{(1)}$ is a suitable polynomial in $\mathbb{Q}[t_1, \ldots, t_{r-m}]$. We apply again the same procedure to the variety P_2, the algorithm stops after at most r steps because at each step the dimension decreases ($\dim(P_2) = \dim(S_1) - 1 = r - m - 1$). The bounds on the degrees and the total complexity are given by Lemmas 5.1 and 5.2 and those of Theorem 2.4 of [17] or Theorem 2.1 of [4]. □

Example 5.4. The following parametric system of non-homogeneous equations describes the position of the arm of a simple robot [16, 35, 36]:

$$\begin{cases} X_1 + X_2 &= u \\ X_3 + X_4 &= v \\ X_1^2 + X_3^2 &= 1 \\ X_2^2 + X_4^2 &= 1 \end{cases}$$

The variables u and v are the parameters, the unknowns are the variables $X_1, \ldots, X_4$. The algorithm decomposes the set $\mathcal{W} \subset \mathbb{C}^2$ of values of the parameters for which the associated systems are zero-dimensional into 3 constructible sets W_1, W_2, W_3, pairwise disjoint such that for each of them, a corresponding PUR of the solutions is given as follows:

$$W_1 = \{u \neq 0, u^2 + v^2 \neq 0\}, \quad \theta^2 - \frac{-u^4 + 4u^2 - u^2v^2}{u^2 + v^2} = 0, \quad \begin{cases} X_1 &= \frac{v}{2u}\theta + \frac{u}{2} \\ X_2 &= -\frac{v}{2u}\theta + \frac{u}{2} \\ X_3 &= -\frac{1}{2}\theta + \frac{3v}{2} \\ X_4 &= \frac{1}{2}\theta + \frac{v}{2} \end{cases}$$

$$W_2 = \{u \neq 0, u^2 + v^2 = 0\}, \quad \text{no solutions;}$$

$$W_3 = \{u = 0, v \neq 0\}, \quad \theta^2 + \frac{v^2}{4} - 1 = 0, \quad \begin{cases} X_1 &= \theta \\ X_2 &= -\theta \\ X_3 &= \frac{v}{2} \\ X_4 &= \frac{v}{2} \end{cases}$$

Note that $\mathbb{C}^2 \setminus \mathcal{W} = \{(0,0)\}$ and the associated system has positive dimension. Its solutions are also given by a PUR representation with an extra parameter t which takes arbitrary values in $\mathbb{C}$.

$$\theta^2 + t^2 - 1 = 0, \quad \begin{cases} X_1 &= \theta \\ X_2 &= -\theta \\ X_3 &= -t \\ X_4 &= t. \end{cases}$$

6. Conclusion

In this paper, we have described a new algorithm for solving zero-dimensional parametric systems of polynomial homogeneous equations. We have introduced the notion of parametric U-resultant, this is a generic way to compute U-resultants for zero-dimensional polynomial systems. The algorithm decomposes the parameters space into a finite number of constructible sets. For each one of them, a parametric Polynomial Univariate Representation is given which reduces the problem to that of solving univariate polynomials. We have also presented a parametrization of some intermediate algorithms for particular problems useful in the main algorithm. Despite the approach used here is new, the complexity bound of the algorithm is relatively analogue to that of previous algorithms on the subject. Note that if $r = \binom{n+d}{n}$ (i.e., each coefficient of the polynomials $f_1, \ldots, f_k$ is a parameter) and $d = n$, Grigoryev [20] has constructed a double-exponential (in n) number of MMs, i.e., a double-exponential number of elements of a partition of the parameters space. This gives a double-exponential lower bound on the complexity of solving parametric zero-dimensional polynomial systems.

References

[1] S. Basu, R. Pollack, M-F. Roy, *Algorithms in real algebraic geometry*, Springer, New York, 2003. 2.2

[2] B. Buchberger, G. E. Collins, R. Loos, R. Albrecht, *Computer Algebra: Symbolic and Algebraic Computation*, Wien, Springer, 1983. 2.2

[3] B. Buchberger, *Gröbner Bases: An algorithmic method in polynomial ideal theory*, in Multidimensional System Theory (N.K.Bose et al.,Eds), Reidel, Dordrecht (1985), 374-383. 1

[4] A.L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math., **34**(4) (1986), 1838-1882. 5, 5, 5

[5] A.L. Chistov, D. Grigoriev, *Subexponential-time solving systems of algebraic equations*, I and II, LOMI Preprint, Leningrad, 1983, E-9-83, E-10-83. 5

[6] D. Cox, J. Little, D. O'shea, *Ideals, Varieties and Algorithms*, Second Edition, Springer 1997. 1

[7] A. Chistov, D. Grigoriev, *Complexity of quantifier elimination in the theory of algebraically closed fields*, LNCS, **176** (1984), 17-31. 3

[8] A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde Matrices, NP-Completeness, and Transversal Subspaces*, Foundations of Computational Mathematics **3**(4) (2003), 421-427. 4, 4

[9] X. Dahan, E. Schost, *Sharp estimates for triangular sets*, Proceedings ISSAC 2004. 1

[10] K. Gatermann, X. Bincan, *Existence of 3 Positive Solutions of Systems from Chemistry*, July 2003. 1

[11] X-S. Gao, S-C. Chou, *Solving parametric algebraic systems*, ISSAC 1992, California USA, 335-341. 1

[12] M. Giusti, E. Schost, *Solving some overdetermined polynomial systems*, Proc. of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), 1-8 (electronic), ACM, New York, 1999. 1

[13] M. Giusti, J. Heintz, K. Hagele, J.E. Morais, L.M. Pardo, J.l. Montana, *Lower bounds for diophantine approximations*, J. of Pure and Applied Algebra, **117, 118** (1997), 277-317. 1

[14] M. Giusti, G. Lecerf, B. Salvy, *A Gröbner free alternative for polynomial system solving*, Journal of Complexity, **17** (1) (2001), 154-211. 1

[15] M.-J. Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso, A. Zanoni, *Parametric*, Report Research, The FRISCO Consortium, 2000. 1

[16] M.-J. Gonzalez-Lopez, T. Recio, *The ROMIN inverse geometric model and the dynamic evaluation method*, In "Computer Algebra in Industry, Problem Solving in Practice", Edited by Arjeh M. Cohen, Wiley, (1991), 117- 141. 1, 5.4

[17] D. Grigoriev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations*, J. Sov. Math., **34** (4) (1986), 1762-1803. 2.1, 2.1, 5, 5, 5

[18] D. Grigoriev, *Complexity of quantifier elimination in the theory of ordinary differential equations*, Lecture Notes Computer Science, **378** (1989), 11-25. 2.3, 2.3, 3

[19] D. Grigoriev, N. Vorobjov, *Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute*, Proc. ACM Intern. Conf. Symb and Algebraic Computations, Scotland, (2000), 137-145. 1
[20] D. Grigoriev, *Constructing double-exponential number of vectors of multiplicities of solutions of polynomial systems*, In Contemporary Math., AMS, **286** (2001), 115-120. 6
[21] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. **24** (3) (1983), 239-277.
[22] J. Heintz, T. Krick, S. Puddu, J. Sabia and A. Waissbein, *Deformation Techniques for efficient polynomial equation solving*, Journal of Complexity, **16** (2000), 70-109. 1
[23] D. Lazard, *Algèbre linéaire sur $k[X_1, \ldots, X_n]$ et élimination*, Bull. Soc. Math. France, **105** (1977), 165-190.
[24] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theo. Comput, Sci, **15** (1981), 77-110. 2.1, 2.1
2.1, 2.1
[25] D. Lazard, *On the specification for solvers of polynomial systems*, 5th Asian Symposium on Computers Mathematics -ASCM 2001, Matsuyama, Japan. Lecture Notes Series in Computing, **9**, World Scientific, (2001), 66-75. 1
[26] D. Lazard, F. Rouillier, *Solving parametric polynomial systems*, Journal of Symbolic Computation, **42** (6) (2007), 636-667. 1
[27] D. Lazard, *Resolution of polynomial systems*, Computers Mathematics. Proceedings of the Fourth Asian Symposium (ASCM 2000). Xiao-Shan Gao, Dongming Wang ed. World Scientific (2000), 1-8. 1
[28] G. Matera, J.M.T. Torres, *The Space Complexity of Elimination Theory: Upper bounds*, Foundations of Computational Mathematics, FOCM'97, Springer Verlag, 1997, 267-276. 2.2, 5
[29] E.W. Mayr and A.R. Meyer. *The Complexity of the Word Problems for Commutative Semigroups and Polynomial Ideals*. Advances in Mathematics, **46** (1982), 305-329. 1
[30] A. Montes, *A new algorithm for discussing Gröbner basis with parameters*, J. of Symb. Comp., **33** (2002), 183-208. 1
[31] G. Moroz, *Complexity of the Resolution of Parametric Systems of Equations and Inequations*, ISSAC, Genova, Italy, 2006. 1
[32] T. Mora, *Solving Polynomial Equation Systems I, The Kronecker-Duval Philosophy*, Encyclopedia of Mathematics and its Applications 88, Cambridge University Press (2003). 1
[33] K. Rimey, *A System of Polynomial Equations and a Solution by an Unusual Method*, SIGSAM Bulletin, **18** (1) (1984), 30-32. 1
[34] F. Rouillier, *Solving zero-dimensional polynomial systems through the rational univariate representation*, Appl. Alg. in Eng. Comm. Comput., **9** (5) (1999), 433-461. 1
[35] E. Schost, *Computing Parametric Geometric Resolutions*, Applicable Algebra in Engineering, Communication and Computing **13** (5) (2003), 349-393.
[36] E. Schost, *Sur la résolution des systèmes polynomiaux à paramètres*, Thèse de doctorat, École polytechnique, décembre 2000. 1, 5.4
[37] E. Schost, *Complexity results for triangular sets*, Journal of Symbolic Computation **36** (3-4) (2003), 555-594. 1, 5.4
[38] B.L. Van Der Waerden, *Modern algebra*, Vol 2, 1950. 1
[39] D. Wang, *Elimination Practice Software Tools and Applications*, World Scientific Pub Co Inc, 2004. 2.1
[40] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Computation, **14** (1991), 1-29.
[41] V. Weispfenning, *Solving parametric polynomial equations and inequalities by symbolic algorithms*, MIP-9504, Universitat Passau, Januar 1995, in Proc. of the workshop "Computer Algebra in Science and Engineering", Bielefed, August 1994, World Scientific, (1995), 163-179. 1