International Mathematical Forum, 5, 2010, no. 7, 333 - 353

A Survey on the Complexity of Solving Algebraic Systems

Ali Ayad

CEA LIST, Software Safety Laboratory
Point Courrier 94, Gif-sur-Yvette, F-91191 France
ali.ayad@cea.fr, ayadali99100@hotmail.com
and
IRMAR, Campus de Beaulieu
Université Rennes 1, 35042, Rennes, France

Abstract

This paper presents a lecture on existing algorithms for solving polynomial systems with their complexity analysis from our experiments on the subject. It is based on our studies of the complexity of solving parametric polynomial systems. It is intended to be useful to two groups of people: those who wish to know what work has been done and those who would like to do work in the field. It contains an extensive bibliography to assist readers in exploring the field in more depth. The paper provides different methods and techniques used for representing solutions of algebraic systems that include Rational Univariate Representations (RUR), Gröbner bases, etc.

Mathematics Subject Classification: 11Y16, 03D15 68W30 14C05 13P10 34A34

Keywords: Symbolic computations, Complexity analysis, Algebraic polynomial systems, Parametric systems, Rational Univariate Representations, Gröbner bases, Triangular sets, irreducible components

1 Introduction

Solving algebraic systems of polynomial equations over a given field is a classical and fundamental problem in algebraic geometry and the symbolic computation domain. Algebraic systems arise in a number of symbolic and scientific applications in computer algebra, robotics [36, 15, 71, 72], geometry [32, 57], physical problems [56, 69, 25], and chemical reactions [24, 25, 35]

This paper is a survey on the complexity of algorithms for solving polynomial systems. It is divided into two parts: The first part (Section 2) deals with existing algorithms in the non-parametric case which in turn is divided into two subsections: Section 2.1 is dedicated to zero-dimensional systems, Section 2.2 to systems of positive dimension. The second part (Section 3) is devoted to algorithms for solving parametric polynomial systems. Is is also divided into several subsections: parametric linear systems (Section 3.1), parametric univariate equations (Section 3.2), zero-dimensional parametric polynomial systems (Section 3.3), parametric polynomial systems of positive dimension (Section 3.4), real solutions of parametric polynomial systems (Section 3.5) and a parametrization [1] of the Chistov-Grigoryev algorithm [11, 39, 10] (Section 3.6).

2 Solving non-parametric algebraic systems

Let K be a global field. An algebraic system (AS for abbreviation) of polynomial equations over K is a finite set of multivariate polynomials $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$ with coefficients in K. For the complexity analysis aims, we suppose that the degrees of $f_1, \ldots, f_k$ w.r.t. $X_1, \ldots, X_n$ are less than an integer d. Solving such a system returns to compute the common zeros of $f_1, \ldots, f_k$ in $\overline{K}^n$ where $\overline{K}$ is an algebraic closure of K. Natural questions arise:

1. How can we represent solutions of an AS ?
2. How much is hard to compute such representations of solutions ?

For the moment, one can answer the first question by showing three simple examples:

Example 2.1 *Let the following linear system:*

$$\begin{cases} X + 2Y - Z - 3 &= 0 \\ X - Y - 4Z + 9 &= 0 \\ Y + Z - 4 &= 0 \end{cases}$$

By the Gaussian elimination algorithm, it is easy to prove that this system has infinite number of solutions which are given by the following equalities (where t is a parameter):

$$\begin{cases} X &= 3t - 5 \\ Y &= -t + 4 \\ Z &= t \end{cases}$$

We can generalize this representation for non-linear systems:

Example 2.2 *Let the following non-linear system:*

$$\begin{cases} XYZ^2 - XY + 1 &= 0 \\ -X^2Y + X - 1 &= 0 \\ X^2 + Z + 1 &= 0 \end{cases}$$

This system is equivalent to the following system (by the computation of a Gröbner basis [7, 15] of the polynomial ideal spanned by the three polynomials with respect to the lexicographical order):

$$\begin{cases} Z^4 + Z^3 - Z^2 - Z + 1 &= 0 \\ Y + Z^3 + Z^2 - 1 &= 0 \\ X - Z^3 - 2Z^2 + 1 &= 0 \end{cases}$$

The last system has zero dimension, i.e., it has a finite number of solutions. These solutions are given by the following representation which is called Polynomial Univariate representation (PUR) [70]:

$$\theta^4 + \theta^3 - \theta^2 - \theta + 1 = 0, \quad \begin{cases} X &= \theta^3 + 2\theta^2 - 1 \\ Y &= -\theta^3 - \theta^2 + 1 \\ Z &= \theta \end{cases}$$

Example 2.3 *Let the following non-linear system:*

$$\begin{cases} X^2 + XY + Y - 1 &= 0 \\ -X^2 + Y^2 + 2X - 1 &= 0 \\ -3X + Y + 4Z + 3 &= 0 \end{cases}$$

This system has positive dimension, i.e., it has infinite number of solutions. Solving it returns to decompose its algebraic variety (i.e., its solutions set) into two irreducible components V_1 (dimension 0) and V_2 (dimension 1) which are defined by:

$$V_1 : \begin{cases} X + 1 &= 0 \\ -X + Z &= 0 \\ -X + Y + 1 &= 0 \end{cases}$$

$$V_2 : \begin{cases} X + Y - 1 &= 0 \\ Y + Z &= 0 \end{cases}$$

Solutions of the system in V_1 or in V_2 can easily represented by PURs as in Examples 2.1 and 2.2.

Algebraic varieties are fondamental objects in algebraic geometry, their decomposition into simple objects (i.e., discrete finite sets as in Example 2.2 or irreducible components as in Examples 2.1 and 2.3) reduces them and facilitates their manipulation for geometric computations.

The second question relies on the complexity analysis of algorithms that compute representations of solutions of polynomial systems. We will return to this question in detail when we consider complexity aspects of existing algorithms in the next sections.

2.1 Solving zero-dimensional algebraic systems

The elimination theory is the oldest theory that is used to solve polynomial systems by eliminating unknown variables: one by one [77] or all at once [14, 44, 12, 18, 23, 80, 67]. It reduces an AS to an equivalent one more easy to solve by successive evaluations of polynomials (for triangular systems [3, 73, 17]) or/and by computing roots of univariate polynomials (see Example 2.2). This theory includes the well-known Gaussian elimination procedure and the theory of resultants. It goes back to Kronecker (see e.g. [65]) and Macaulay [61]: For any $1 \leq i \leq k$, let $\tilde{f}_i$ to be the homogenization of f_i by introducing a new variable X_0. If the system $\tilde{f}_1 = \cdots = \tilde{f}_n = 0$ is zero-dimensional then one can compute a homogeneous polynomial $R \in K[U_0, \ldots, U_n]$ (where $U_0, \ldots, U_n$ are new variables), called the U-resultant of the system, such that there is a bijective correspondence between the solutions of the system in the n-dimensional projective space $P^n(\overline{K})$ (with their multiplicities) and the linear forms factors of R, i.e., for each linear form $L = \xi_0 U_0 + \cdots + \xi_n U_n$ factor of R in $\overline{K}[U_0, \ldots, U_n]$, the point $(\xi_0 : \cdots : \xi_n) \in P^n(\overline{K})$ is a solution of the system, its multiplicity is equal to that of L as a factor of R (see [61, 77, 53, 39, 9]). If $k = n$, Macaulay has associated to the system $\tilde{f}_1 = \cdots = \tilde{f}_n = 0$ a polynomial $\tilde{R}$ (in the coefficients of $\tilde{f}_1, \ldots, \tilde{f}_n$), called the resultant of the system, such that $\tilde{R} = 0$ if and only if the system has solutions in $P^n(\overline{K})$. This is a generalization of the Sylvester resultant of two univariate polynomials.

A double-exponential complexity bound d^{2^n} is known in Kronecker's works for solving zero-dimensional polynomial systems (see e.g., Collins [14] and Heintz [44]). Lazard [53] has described a method for computing U-resultant of zero-dimensional systems of homogeneous equations that is based on the reduction of matrices. Its complexity is of order $d^{O(n)}$, being polynomial in the number of solutions.

When the ground field K is a finite extension of purely transcendental extension of its prime field, Chistov and Grigoryev [11, 39, 10] have published an algorithm which combines the computation of the U-resultant of the system $\tilde{f}_1 = \cdots = \tilde{f}_k = 0$ with the primitive element theorem (Shape Lemma) [29, 50, 2] to decompose the finite set of the solutions of the system into a finite number of classes $\mathcal{C}_1, \ldots, \mathcal{C}_s$ such that for each class $\mathcal{C}$ among them, the algorithm computes univariate polynomials $\phi, B_0, \ldots, B_n \in K[Z]$ (where Z is a new variable), an integer j_0, $0 \leq j_0 \leq n$ and a power p^ν of the characteritic p of K which satisfy the following properties:

- ϕ is separable and irreducible over K.
- The equation $X_{j_0} = 0$ has no solutions in $\mathcal{C}$.
- A Polynomial Univariate Representation (PUR) of the elements of $\mathcal{C}$ is

given by

$$\phi(\theta) = 0, \quad \begin{cases} \left(\frac{X_0}{X_{j_0}}\right)^{p^\nu} & = B_0(\theta) \\ & \vdots \\ \left(\frac{X_n}{X_{j_0}}\right)^{p^\nu} & = B_n(\theta) \end{cases}$$

This reads as follows: for each solution $(\xi_0 : \cdots : \xi_n) \in P^n(\overline{K})$ of the system in $\mathcal{C}$, the fractions $\left(\frac{\xi_j}{\xi_{j_0}}\right)$ are obtained by the computation of the roots of ϕ in $\overline{K}$ and by an algorithm for extracting p^ν-th roots of elements from $\overline{K}$. In particular, the cardinal of $\mathcal{C}$ is equal to the degree of ϕ.

The complexity of this algorithm is $pd^{O(n)}$, being polynomial in its outputs. This kind of representations of solutions has been early obtained by Kronecker (see e.g. [65]) and has been known later by RUR (Rational Univariate Representation) [70] (see also [8, 68, 2, 6]). In contrary to PURs, in RURs the above polynomials $B_0, \ldots, B_n$ are in fact rational functions in Z. If K has characteristic zero or strictly positive under some conditions, the algorithm of [70] has complexity $d^{O(n)}$, being polynomial in the number of solutions of the system.

When the input polynomials are represented by Straight-line programs [50], probabilistic geometric algorithms exist in [30, 31, 46] with polynomial complexities. These algorithms compute geometric resolutions that give also rational univariate representations of the solutions.

In 1965, Bruno Buchberger (see e.g. [7]) has invented Gröbner bases which transform an input polynomial system into a triangular one. They form a generalization of the Gaussian elimination algorithm to non-linear systems and the euclidean algorithm to multivariate polynomials [54, 13]. A good overview of Gröbner bases and their applications can be found in the books of Cox et. al. [15, 16]. The complexity of computing Gröbner bases of zero-dimensional polynomial ideals is $d^{O(n)}$, being polynomial in the size of the polynomials which define the input ideal [54, 51, 22]. This bound is improved later in [43] and it becomes polynomial in $\max\{S, D^n\}$ where S is the size of the inputs polynomials which are given by dense representation and D is the arithmetic mean value of their degrees.

Algorithms for reducing an arbitrary zero-dimensional AS to a finite set of triangular systems are described in [55, 3] and in [78] for characteristic sets.

Linear algebra are also used to solve zero-dimensional polynomial systems by manipulating linear algebra methods in the finite K-algebra $A = K[X_1, \ldots, X_n]/(f_1, \ldots, f_k)$ in order to describe the set of solutions of the system: a simple way is to compute the eigen values of all the endomorphisms Φ_{X_i} of the algbra A $(1 \leq i \leq n)$, where Φ_{X_i} is the multiplication operator by X_i in A. Then zeros of the system are obtained by evaluating the polynomials

$f_1, \ldots, f_k$ on $(\lambda_1, \ldots, \lambda_n)$ where λ_i is an eigen value of Φ_{X_i} by the fact that for any $f \in K[X_1, \ldots, X_n]$, the eigen values of Φ_f are the $f(\xi)$ where ξ is a solution of the system. The complexity of this method is very large. There are other methods which compute eigen vectors of the endomorphisms of multiplication in A (see [4, 63, 16, 19]).

2.2 Solving algebraic systems of positive dimension

When the system $f_1 = \cdots = f_k = 0$ has positive dimension, its resolution returns to decompose the algebraic variety $V = V(f_1, \ldots, f_k) \subset \overline{K}^n$ into its irreducible components and to give computational methods to represent these components. Algebraically, this returns to the primary decomposition of the ideal I spanned by $f_1, \ldots, f_k$.

In 1983, Chistov and Grigoryev [11, 10, 39] have described an effective algorithm which decomposes an arbitrary projective variety (e.g., the variety $\tilde{V} = V(\tilde{f}_1, \ldots, \tilde{f}_k) \subset P^n(\overline{K})$ defined by the homegenous polynomials of Section 2.1) into its irreducible components when K is a finite extension of purely transcendental extension of its prime field. Each component W is given by the two following ways:

- An effective generic point (see [83, 66, 52, 11, 10, 39] and below).
- A finite set of homogeneous polynomials that define W.

The algorithm computes the codimension m of W with a transcendental basis $t_1, \ldots, t_{n-m}$ of $K(W)$ over K where $K(W)$ is the field of rational functions over W. An effective generic point of W is defined by the following fields isomorphism:

$$\tau : K(t_1, \ldots, t_{n-m})[\theta] \longrightarrow K\Big(\frac{X_{j_1}}{X_s}, \ldots, \frac{X_{j_{n-m}}}{X_s}, \Big(\frac{X_0}{X_s}\Big)^{p^\nu}, \ldots, \Big(\frac{X_n}{X_s}\Big)^{p^\nu}\Big) \subseteq K(W) \tag{1}$$

which is given by the following items:

- An integer $0 \leq s \leq n$ which is selected in such a way that the variety W is not contained in the hyperplane defined by the equation $X_s = 0$.
- The elements X_j/X_s are rational functions over W. In addition, $\tau(t_i) = X_{j_i}/X_s$ for $1 \leq i \leq n-m$ with the convention that $p^\nu = 1$ if $char(K) = 0$ and $\nu \geq 0$ if $char(K) = p > 0$.
- A linear combination $\theta = \alpha_1 X_{j_1}/X_s + \cdots + \alpha_{n-m} X_{j_{n-m}}/X_s$ where $\alpha_i \in \mathbb{Z}$ and $0 \leq \alpha_i \leq \deg(W)$ (see [11, 10, 39]) if $char(K) = 0$ and $\alpha_i \in H$ where $H \supseteq \mathbf{F}_p$ is a finite extension of sufficiently large cardinality if $char(K) = p > 0$.

- The minimal polynomial $\phi(Z) \in K(t_1, \ldots, t_{n-m})[Z]$ of θ over the field $K(t_1, \ldots, t_{n-m})$. This polynomial has to be separable.
- For each $1 \leq i \leq n$, a polynomial $B_i \in K(t_1, \ldots, t_{n-m})[\theta]$ such that

$$\tau^{-1}\Big((X_i/X_s)^{p^\nu}\Big) = B_i.$$

  This gives a rational univariate representation of the elements of W similar to that of zero-dimensional polynomial systems of Section 2.1 but with extra parameters $t_1, \ldots, t_{n-m}$ to represent the infinite number of solutions of the system in W (see Examples 2.1 and 2.3). In fact, when $\tilde{V}$ has dimension zero (in this case $m = n$), we find again the RUR of Section 2.1.

In addition, the algorithm computes bounds on the degrees and the binary lengths of the output polynomials. It is based on a polynomial algorithm for factoring multivariate polynomials over K [11, 10, 39]. Its complexity is polynomial in d^{n^2}.

Geometric resolutions of polynomial systems of positive dimension are given by Giusti et. al. [31, 33]. They include a rational univariate respresentation of the solutions as above in Chistov-Grigoryev algorithm.

Dynamic evaluation [65] are also used for solving algebraic systems of polynomial equations.

In 1988, Gianni et. al. [27] have used Gröbner bases and quotient ideals of the polynomial ring $K[X_1, \ldots, X_n]$ to compute a primary decomposition of the ideal $I =< f_1, \ldots, f_k >$ (see also [15, 19]). The factorization of the polynomials $f_1, \ldots, f_k$, combined with the Buchberger's algorithm give also a decomposition of the variety V [37, 38]. Note that it is well-known [62] that the lower bound of the complexity of computing Gröbner bases for polynomial ideals of positive dimension is double-exponential in n.

In 1990, Giusti and Heintz [28] have described a well-parallelizable algorithm for decomposing the variety V into equidimensional components and irreducible components. The sequential complexity of their algorithm is $k^5 d^{O(n^2)}$. Later in 1993 [29], they give another well-parallelizable algorithm which computes the dimension, the geometric degree and the isolated points of V in polynomial sequential time in the size of the outputs. In 1999, Elkadi and Mourrain [20] have proposed also a probabilistic algorithm based on the Bezoutian matrices with the same complexity bound.

In 2000, Lecerf [59, 60] has presented an algorithm which computes a geometric resolution for each equidimensional component of V with polynomial complexity in kd^n. In 2002, Jeronimo and Sabia [47] have also proposed a probabilistic algorithm which represents each equidimensional component of V by a set of $(n+1)$ polynomials of degrees $\leq d^n$. These polynomials are coded by straight-line programs with polynomial lengths in kd^n.

Sommese et. al. [76] have given a numeric algorithm for decomposing V into irreducible components. For each component W, a finite subset of W of cardinal equal to the geometric degree of W and a finite family of polynomials which defines W are computed by the algorithm. In particular, the algorithm gives the set of isolated points of V.

3 Solving parametric algebraic systems

Let K be a global field. A parametric algebraic system of polynomial equations over K is a finite set of multivariate polynomials $F_1, \ldots, F_k \in K[u_1, \ldots, u_r][X_1, \ldots, X_n]$ with polynomial coefficients in the variables $u = (u_1, \ldots, u_r)$ (the parameters) over K. For the complexity analysis aims, we suppose that the degrees of $F_1, \ldots, F_k$ w.r.t. $X_1, \ldots, X_n$ are less than d. Solving such a system returns to determine the values of the parameters in the parameters space $\mathcal{P} = \overline{K}^r$ for which the associated polynomial systems have solutions in $\overline{K}^n$ (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 Example 3.1 and Section 3.6). In the sequel, let us adopt the following notation: for a polynomial $g \in K(u_1, \ldots, u_r)[X_0, \ldots, X_n]$ and a value $a = (a_1, \ldots, a_r) \in \mathcal{P}$ of the parameters, we denote by $g^{(a)}$ the polynomial of $\overline{K}[X_1, \ldots, X_n]$ which is obtained by specialization of u by a in the coefficients of g if their denominators do not vanish on a, i.e., $g^{(a)} = g(a_1, \ldots, a_r, X_1, \ldots, X_n)$.

Parametric polynomial systems come from real-life problems as geometric [32, 57], optimization [81] and interpolation [71, 72, 35] ones, or physical problems [56, 69, 25], chemical reactions [24, 25, 35] and robots [36, 15, 71, 72]. 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.

Example 3.1 *Consider the following parametric polynomial system from [7, 79, 25]:*

$$\begin{cases} X_4 - u_4 + u_2 = 0 \\ X_4 + X_3 + X_2 + X_1 - u_4 - u_3 - u_1 = 0 \\ X_3X_4 + X_1X_4 + X_2X_3 + X_1X_3 - u_1u_4 - u_1u_3 - u_3u_4 = 0 \\ X_1X_3X_4 - u_1u_3u_4 = 0 \end{cases}$$

In Section 3.6, we will see that one can decompose $\mathbb{C}^4$ into three contructible sets $\mathcal{V}_1$, $\mathcal{V}_2$ and $\mathcal{V}_3$ given with their associated parametric Polynomial Univari-

ate Representations as follows:

$$\begin{cases} \mathcal{V}_1 = \{u_2 - u_4 \neq 0\}, \\ \theta^3 - \alpha\theta^2 + \beta\theta - u_1u_3u_4 = 0, \\ X_1 = -\frac{1}{u_2-u_4}\theta^2 + \frac{\alpha}{u_2-u_4}\theta - \frac{\beta}{u_2-u_4} \\ X_2 = \frac{1}{u_2-u_4}\theta^2 - \frac{\alpha'}{u_2-u_4}\theta + \frac{\beta'}{u_2-u_4} \\ X_3 = \theta \\ X_4 = u_4 - u_2 \end{cases}$$

$$\mathcal{V}_2 = \{u_2 - u_4 = 0,\ u_1u_3u_4 \neq 0\}, \quad \textit{no solutions.}$$

$$\begin{cases} \mathcal{V}_3 = \{u_2 - u_4 = 0,\ u_1u_3u_4 = 0\}, \\ \theta^2 - (u_1^2 + u_3^2 + u_4^2 - 2\beta) = 0, \\ X_1 = -\frac{1}{2}\theta - t + \frac{\alpha}{2} \\ X_2 = t \\ X_3 = \frac{1}{2}\theta + \frac{\alpha}{2} \\ X_4 = 0 \end{cases}$$

where $\alpha = u_1 + u_3 + u_4$, $\beta = u_1u_4 + u_1u_3 + u_3u_4$, $\alpha' = u_1 + u_2 + u_3$ *and* $\beta' = u_1u_2 + u_1u_3 + u_2u_3 - u_2u_4 + u_2^2$.
Remark that for any specialization $(a_1, \ldots, a_4)$ *of the parameters in* $\mathcal{V}_1$, *the associated system has three solutions which correspond to the three roots* a_1, a_3 *and* a_4 *of the equation* $\theta^3 - \alpha\theta^2 + \beta\theta - u_1u_3u_4 = 0$. *For* $(a_1, \ldots, a_4) \in \mathcal{V}_3$, *the associated system has dimension 1.*

3.1 Solving parametric linear systems

Let us begin by the case of parametric systems of linear equations i.e. when F_i has degree 1 w.r.t. $X_1, \ldots, X_n$ for all $1 \leq i \leq k$.

In 1983, Heintz [44] has parametrized the Gaussian elimination algorithm for solving linear systems (see also p. 24-25 of [12], p .14-15 of [40] and [5]). Its complexity is polynomial in n and exponential in r (see [44]). Later W. Sit [74, 75] has given another algorithm based on the computation of Gröbner bases. These algorithms decompose $\mathcal{P}$ into a finite number of constructible sets such that for each set $\mathcal{V}$ among them, they compute $(s+1)$ vectors $Z_0, Z_1, \ldots, Z_s \in K(u_1, \ldots, u_r)^n$ where Z_0 is a generic particular solution the input parametric linear system and $\{Z_1, \ldots, Z_s\}$ is a generic basis of the solution space of the associated parametric homogeneous system i.e., for all $a \in \mathcal{V}$, we have:

- The denominators of the entries of $Z_0, Z_1, \ldots, Z_s$ don't vanish on a.
- $Z_0^{(a)}$ is a particular solution of the linear system specialized on a and the set $\{Z_1^{(a)}, \ldots, Z_s^{(a)}\}$ is a basis of the associated homogeneous linear system.

3.2 Solving systems of parametric univariate polynomial equations

When $n = 1$, Grigoryev (see Lemma 1 of [40]) has introduced an algorithm for solving parametric univariate polynomial equations by the construction of generic greatest common divisors (GCD) for finite set of parametric univariate polynomials. The complexity of this algorithm is polynomial in k and d and exponential in r. In Chapter 1 of [6], there is a parametrization of the well-known euclidean algorithm. These two algorithms decompose $\mathcal{P}$ into a finite number of constructible sets pairwise disjoint. For each set $\mathcal{V}$ among them, they compute a parametric polynomial $g \in K[u_1, \ldots, u_r][X_1]$ which satisfies the following property:

- For any $a \in \mathcal{V}$, the polynomial $g^{(a)} \in \overline{K}[X_1]$ is a GCD of $F_1^{(a)}, \ldots, F_k^{(a)} \in \overline{K}[X_1]$.

3.3 Zero-dimensional case

Several algorithms are destinated to the resolution of zero-dimensional parametric polynomial systems. Among the tools and techniques used, one distinguishes the Newton-Hensel operator [71, 72, 45], the parametric Gröbner bases computation [41, 64], the parametric triangular sets [17, 73] and the discriminant varieties [58].

3.3.1 Parametric geometric resolution [71, 72, 45]

A Parametric geometric resolution of the system $(F_1, \ldots, F_k)$ is a description of the solutions by a parametric polynomial univariate representation as follows:

$$\phi(\theta) = 0, \quad \begin{cases} X_1 & = B_1(\theta) \\ & \vdots \\ X_n & = B_n(\theta) \end{cases}$$

where $\phi, B_1, \ldots, B_n \in K(u_1, \ldots, u_r)[Z]$.

In his PhD thesis, Schost [71, 72] has given a probabilistic algorithm for computing parametric geometric resolution of zero-dimensional parametric polynomial systems with complexity $d^{O(rn)}$. This algorithm computes also the equation of the hypersurface S subset of $\mathcal{P}$ where the specialization fails, i.e., $\forall a \in S$, at least one of the denominators of the coefficients of $\phi, B_1, \ldots, B_n$ vanishes on a. For $a \notin S$, the solutions of the system $F_1^{(a)} = \cdots = F_n^{(a)} = 0$ are obtained by a specialization of the parameters on a in the parametric geometric resolution. The degree of this equation is bounded by $d^{O(n)}$.

Note that an RUR from [70, 31, 30, 2] on the field $K(u_1, \ldots, u_r)$ gives a parametric geometric resolution.

3.3.2 Parametric Gröbner bases

Gröbner bases form a practical tool to solve algebraic sytems [7, 15, 21]. In 2000, Grigoryev and Vorobjov [41] (also Montes [64]) give algorithms for computing parametric Gröbner bases for zero-dimensional polynomial systems. They compute a partition of $\mathcal{P}$ into a finite number of constructible sets and for each set $\mathcal{V}$ among them, they compute polynomials $G_1, \ldots, G_s \in K(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ which satisfy the following properties:

- The rational coefficients of $G_1, \ldots, G_s$ in $K(u_1, \ldots, u_r)$ are well-defined in $\mathcal{V}$.
- For any $a \in \mathcal{V}$, the set $\{G_1^{(a)}, \ldots, G_s^{(a)}\} \subset \overline{K}[X_1, \ldots, X_n]$ is a reduced Gröbner basis of the ideal spanned by $F_1^{(a)}, \ldots, F_k^{(a)}$ in $\overline{K}[X_1, \ldots, X_n]$ w.r.t. a certain fixed monomial order on $X_1, \ldots, X_n$.
- The vector of the multiplicities of the system is constant in $\mathcal{V}$ and it is computed by the algorithm.

The complexity bound of the algorithm of [41] is $d^{O(n^2 r)}$ when the input polynomials are coded by dense representation. 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 [42] has constructed a double-exponential (in n) number of vector of multiplicities, 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.

3.3.3 Parametric triangular sets [17, 73]:

For $k = n$, there is a probabilistic algorithm in [17] which computes a parametric triangular set $\{T_1, \ldots, T_n\} \subset K(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ equivalent to the input system $(F_1, \ldots, F_n)$. The degrees of $T_1, \ldots, T_n$ w.r.t. $u_1, \ldots, u_r$ are bounded by $2d^{2n}$, however in [73], they were bounded by $d^{O(n^2)}$.

This algorithm computes also an hypersurface $S \subset \overline{K}^r$ defined by a polynomial of degree $\leq d^n$ such that $\forall a \notin S$, the denominators of the the coefficients of $T_1, \ldots, T_n$ don't vanish on a and $V(T_1^{(a)}, \ldots, T_n^{(a)}) = V(F_1^{(a)}, \ldots, F_n^{(a)})$. Its complexity is $d^{O(nr)}$, being polynomial in the size of the output.

3.3.4 Discriminant Varieties [58]

The discriminant variety is a generalization of the discriminant of a univariate polynomial and contains all those parameter values leading to non-generic solutions of the system.

Let π be the projection of $\overline{K}^{n+r}$ on the parameters space $\mathcal{P}$. A discriminant variety of the system $(F_1, \ldots, F_k)$ is a subvariety W of $\mathcal{P}$ such that for any open set U of $\mathcal{P} \setminus W$, the restriction of π on $\pi^{-1}(U) \cap V(F_1, \ldots, F_k)$ is an analytic covering of U.

The minimal discriminant variety of the system $(F_1, \ldots, F_k)$ is the intersection of all its discriminant varieties. Lazard and Rouillier [58] have proposed an efficient algorithm for computing minimal discriminant varieties. The degree of these varieties and the complexity of the algorithm are single exponential in n.

3.4 General case

This section covers the two cases: zero-dimensional and positive dimension.

3.4.1 Parametric geometric resolution [32]

Under some conditions on the system $(F_1, \ldots, F_k)$, the algebraic Zariski closure of the subset of $\mathcal{P}$ where associated systems are consistent (i.e. the consistent locus of the system) is an hypersurface of $\mathcal{P}$. A polynomial equation of minimal degree that defines this hypersurface is given in [32]. This is achieved by application of the geometric resolution method [31, 33] on the system $(F_1, \ldots, F_k)$. A description of a generic solution of the system is given by a RUR for values of the parameters in this hypersurface.

3.4.2 Parametric Gröbner bases

Gröbner bases compute also consistent locus by eliminating the variables $X_1, \ldots, X_n$ [15]. For a parametric system $(F_1, \ldots, F_k)$, one proceeds in one of the following two ways:

- Compute a Gröbner basis of the ideal spanned by $F_1, \ldots, F_k$ in $K(u_1, \ldots, u_r)[X_1, \ldots, X_n]$ w.r.t. a certain monomial order on the monomials in $X_1, \ldots, X_n$.
- Compute a Gröbner basis of the ideal spanned by $F_1, \ldots, F_k$ in $K[u_1, \ldots, u_r, X_1, \ldots, X_n]$ w.r.t. a certain monomial order on the monomials in $u_1, \ldots, u_r, X_1, \ldots, X_n$.

By each one of these two strategies, we can compute a constructible subset of $\mathcal{P}$ where the specializations of the parameters give Gröbner bases of the specialized ideals [48, 26, 34, 35, 15, 49].

In 1991, Weispfenning has introduced the notion of comprehensive Gröbner bases [79, 81] which decompose $\mathcal{P}$ into constructible sets, each of them with a generic Gröbner basis. Thus, we are able to compute conditions on the parameters when the associated systems have no solutions, a finite number of solutions, have dimension s where s is an integer or the existence of real

solutions. Note that there is no complexity analysis for the construction of comprehensive Gröbner bases in [79, 81].

3.4.3 Parametric triangular and characteristic sets

For a parametric system of polynomial equations and inequations, Gao and Chou [25] have described the consistent locus of $\mathcal{P}$ by decomposing it into a finite number of constructible sets such that for each of them, they compute a parametric triangular set of polynomials which represents the generic solutions of the input system. In particular, the dimension of the input system is constant in each constructible set. Note that there is no complexity study of this computation in [25].

Implementations of methods based on the computation of characteristic sets are done in [78].

3.5 Real solutions of parametric systems

For a parametric univariate polynomial $F \in \mathbb{R}[u_1, \ldots, u_r][X]$, there is an algorithm in [82] which decomposes $\mathcal{P}$ into semi-algebraic sets such that the number of distinct real roots of F and their multiplicities are constant in each semi-algebraic set. There is no complexity bounds in [82].

Lazard has studied the number of real solutions of parametric systems of polynomial equalities and inequalities [57, 58, 56]. Gatermann [24] has given conditions on the parameters for which a special parametric system comming from chemistry has three positive real solutions.

3.6 Parametric PURs

In our PhD thesis [1], we have described an algorithm for decomposing algebraic varieties defined by parametric homogeneous equations into irreducible components uniformly in $\mathcal{P}$. This algorithm is a parametrization of that of Chistov-Grigoryev [11, 10, 39]. Let K be a finite extension of purely transcendental extension of its prime field and $\tilde{F}_1, \ldots, \tilde{F}_k \in K[u_1, \ldots, u_r][X_0, \ldots, X_n]$ be the homogeneous polynomials of $F_1, \ldots, F_k$. In [1], there is an algorithm which deomposes $\mathcal{P}$ into a finite number of constructible sets such that for each set $\mathcal{V}$ among them, the following properties hold:

- The number of absolutely irreducible components is constant in $\mathcal{V}$, i.e., for any $a, b \in \mathcal{V}$, the number of absolutely irreducible components of the variety $V(\tilde{F}_1^{(a)}, \ldots, \tilde{F}_k^{(a)})$ is equal to that of $V(\tilde{F}_1^{(b)}, \ldots, \tilde{F}_k^{(b)})$.
- For each absolutely irreducible components W of codimension m, the algorithm computes a basis $Y_0, \ldots, Y_n$ of the space of linear forms in

$X_0, \ldots, X_n$ with coefficients in H (where $H = \mathbb{Q}$ if $char(K) = 0$ and $H \supseteq \mathbf{F}_p$ is a finite extension of $\mathbf{F}_p$ if $char(K) = p > 0$) such that W is represented by a *parametric representative system* and by a *parametric effective generic point (parametric PUR)* as follows:

Parametric representative system:
The algorithm computes polynomials $\psi_1, \ldots, \psi_N \in K(C, u_1, \ldots, u_r)[Y_0, \ldots, Y_n]$ homogeneous in $Y_0, \ldots, Y_n$ and a polynomial $\chi \in K(u_1, \ldots, u_r)[C]$ (where C is a new variable). For each $a \in \mathcal{V}$, there exists $c \in \overline{K}$, a root of $\chi^{(a)} \in \overline{K}[C]$ such that the denominators of the coefficients of χ and ψ_j don't vanish on a and (c, a) respectively and the homogeneous polynomials $\psi_1^{(c,a)}, \ldots, \psi_N^{(c,a)} \in \overline{K}[Y_0, \ldots, Y_n]$ define the component W, i.e.,

$$W = V(\psi_1^{(c,a)}, \ldots, \psi_N^{(c,a)}) \subset P^n(\overline{K}).$$

Parametric PUR:
The algorithm computes polynomials $\phi, B_1, \ldots, B_n \in K(C, u_1, \ldots, u_r)(t_1, \ldots, t_{n-m})[Z]$ where $\{t_1, \ldots, t_{n-m}\}$ is a transcendence basis of $\overline{K}(W)$ over $\overline{K}$. For each $a \in \mathcal{V}$, there exists $c \in \overline{K}$, a root of $\chi^{(a)}$ such that the denominators of the coefficients of $\phi, B_1, \ldots, B_n$ don't vanish on (c, a) and a parametric Polynomial Univariate Representation of elements of W is given by:

$$\phi^{(c,a)}(t_1, \ldots, t_{n-m}, \theta) = 0, \begin{cases} \left(\frac{Y_1}{Y_0}\right)^{p^\nu} & = B_1^{(c,a)}(t_1, \ldots, t_{n-m}, \theta) \\ & \vdots \\ \left(\frac{Y_n}{Y_0}\right)^{p^\nu} & = B_n^{(c,a)}(t_1, \ldots, t_{n-m}, \theta) \end{cases}$$

where $p^\nu = 1$ if $char(K) = 0$ and $\nu \geq 0$ if $char(K) = p > 0$. The variety W is not contained in the hyperplane $V(Y_0) \subset P^n(\overline{K})$.

In addition, the algorithm computes bounds on the degrees and the binary lengths of the output polynomials. It is based on algorithms for computing parametric GCDs (Section 3.2) and factoring parametric multivariate polynomials over K. Its complexity is double-exponential in n.

4 Conclusion

In this paper, we have presented an overview on the complexity of solving systems of polynomial equations. Different methods for representing solutions of polynomial systems (for different dimensions) are given with their complexity analysis for parametric and non-parametric polynomial systems. In anyway, this paper reflects our point of view on the problem and is not considered as

an exhaustive paper on the historic of the problem.

ACKNOWLEDGEMENTS. We gratefully thank Professor Dimitry Grigoryev for his help in the redaction of this paper, and more generally for his suggestions about the approach presented here.

References

[1] A. Ayad, *Complexité de la résolution des systèmes algébriques paramétriques*, PhD thesis, University of Rennes 1, France, 2006.

[2] M.E. Alonso, E. Becker, M.-F. Roy and T. Wormann, *Zeros, multiplicities and idempotents for zero-dimensional systems*, Algorithms in algebraic geometry and applications, 1996, 1 - 15.

[3] P. Aubry, D. Lazard and M. Moreno, *On the theories of triangular sets*, J. of Symbolic Computation, Special Issue on Polynomial Elimination, **28(1)** (1999), 105 - 124.

[4] W. Auzinger, W. and H. J. Stetter, *An elimination algorithm for the computation of all zeros of a system of multivariate polynomial equations*, In Proc. Intern. Conf. on Numerical Math., **86** of Int. Series of Numerical Math, Birkhuser Verlag (1988), 12 - 30.

[5] C. Ballarin and M. Kauers, *Solving Parametric Linear Systems: an Experiment with Constraint Algebraic Programming*, SIGSAM Bulletin, **38(2)** (2004), p. 33-46.

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

[7] 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.

[8] J. F. Canny, *Some algebraic and geometric computations in pspace*. Twentieth ACM Symp. on Theory of Computing (1988), 460 - 467.

[9] J. F. Canny and E. Kaltofen, Y.N. Lakshman, *Solving Systems of Nonlinear Polynomial Equations Faster*, ISSAC (1989), 121 - 128.

[10] A.L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time*, J. Sov. Math., **34**, No. 4 (1986), 1838 - 1882.

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

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

[13] A. M. Cohen, J. H. Davenport, A. J. P. Heck, *An overview of computer algebra*, In "Computer Algebra in Industry, Problem Solving in Practice", Edited by Arjeh M. Cohen, Wiley, 1991, 1 - 52.

[14] G.E. Collins, *Quantifier Elimination for the Elementary Theory of Real Closed Fields by Cylindrical Algebraic Decomposition*, Lect. Notes Comput. Sci. **33** (1975), 134 - 183.

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

[16] D. Cox, J. Little and D. O'shea, *Using Algebraic Geometry*, Springer, 1998.

[17] X. Dahan and E. Schost, *Sharp estimates for triangular sets*, Proceedings ISSAC, Santander, Spain, 2004, 103 - 110.

[18] J. Davenport and J. Heintz, *Real quantifier elimination is doubly exponential*, J. of Symbolic Computation, **5** (1988), 29 - 35.

[19] A. Dickenstein and L. Z. Emiris, *Solving Polynomial Equations, Foundations, Algorithms, and Applications*, Springer, 2005.

[20] M. Elkadi and B. Mourrain, *A new algorithm for the geometric decomposition of a variety*, Proceedings of the 1999 international symposium on Symbolic and algebraic computation, Canada, 1999, 9 - 16.

[21] J.C. Faugère, *A new efficient algorithm for computing Gröbner bases without reduction to zero (F5)*, Proceedings of the 2002 international symposium on Symbolic and algebraic computation, 2002, Lille, France, 75 - 83.

[22] J. C. Faugère , P. Gianni , D. Lazard and T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, Journal of Symbolic Computation, **16**, N. 4 (1993), 329 - 344.

[23] N. Fitchas, A. Galligo and J. Morgenstern, *Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields*, J. Pure Appl. Algebra **67**, No. 1 (1990), 1 - 14.

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

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

[26] P. Gianni, *Properties of Gröbner bases under specializations*, In Davenport, J.H., ed, EURO-CAL'87, New York, Springer, LNCS **378** (1987), 293 - 297.

[27] P. Gianni and B. Trager *Gröbner bases and primary decomposition in polynomial ideals*, Journal of Symbolic Computation, **6** (1988), 148 - 166.

[28] M. Giusti and J. Heintz, *Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles*, Effective methods in algebraic geometry (Castiglioncello, 1990), 169 - 194.

[29] M. Giusti and J. Heintz, *La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial*, in Computational Algebraic Geometry and Commutative Algebra, Symposia Mathematics (D. Eisenbud and L. Robbiano, Eds.), **34**, Cambridge Univ. Press, Cambridge, UK, 1993, 216 - 256.

[30] M. Giusti, J. Heintz, J. E. Morais and L. M. Pardo, *When Polynomial Equation Systems Can Be Solved Fast ?*, Actes de AAECC'11 (Paris 1995), Lecture Notes in Computer Science, Springer Verlag, **948** (1995), 205 - 231.

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

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

[33] M. Giusti, G. Lecerf and B. Salvy, *A Gröbner free alternative for polynomial system solving*, Journal of Complexity, **17**, No. 1 (2001), 154 - 211.

[34] M.-J. Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso and A. Zanoni, *Gröbner bases specialization through Hilbert functions: the homogeneous case*, ACM SIGSAM Bulletin, **34**, Issue 1 (2000), 1 - 8.

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

[36] M.-J. Gonzalez-Lopez and 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.

[37] H-G. Gräbe, *On Factorized Gröbner Bases*, In "Computer Algebra in Science and Engineering" (ed. Fleischer, Grabmeier, Hehl), World Scientific Singapore, 1995, 77 - 89.

[38] H-G. Gräbe, *Minimal Primary Decomposition and Factorized Gröbner Bases*, in J. AAECC, **8** (1997), 265 - 278.

[39] D. Grigoryev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations*, J. Sov. Math., **34**, No. 4 (1986), 1762 - 1803.

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

[41] D. Grigoryev and 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.

[42] D. Grigoryev, *Constructing double-exponential number of vectors of multiplicities of solutions of polynomial systems*, In Contemporary Math., AMS, 2001, **286**, 115 - 120.

[43] A. Hashemi and D. Lazard, *Sharper Complexity Bounds for Zero-dimensional Gröbner Bases and Polynomial System Solving*, Research report, INRIA, 2005.

[44] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. **24**, 3 (1983), 239 - 277.

[45] 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.

[46] J. Heintz, G. Matera and A. Waissbein, *On the Time-Space Complexity of Geometric Elimination Procedures*, Appl. Algebra Eng. Commun. Comput. **11**, No. 4 (2001), 239 - 296.

[47] G. Jeronimo and J. Sabia, *Effective equidimensional decomposition of affine varieties*, J. Pure Appl. Algebra, **169**, No. 2-3 (2002), 229 - 248.

[48] M. Kalkbrenner, *On the stability of Gröbner bases under specializaions*, J. of Symb. Comp., **24** (1997), 51 - 58.

[49] D. Kapur, *An Approach for Solving Systems of Parametric Polynomial Equations* , Principles and Practice of Constraint Programming, (eds. Saraswat and Van Hentenryck), MIT press, 1995.

[50] T. Krick and L.M. Pardo, *A computational method for diophantine approximation*, Algorithms in algebraic geometry and applications, Santander, 1994, 193 - 253.

[51] Y. N. Lakshman, *A single exponential bound on the complexity of computing Gröbner bases of zero dimensional ideals*, Effective methods in algebraic geometry, Progress in Mathematics, 94, Birkhiiuser Verlag, Basel, 1991, 227 - 234.

[52] S. Lang, Algebra, Addison-Wesley , 1993.

[53] D. Lazard, *Résolution des systèmes d'équations algébriques*, Theo. Comput, Sci, **15** (1981), 77 - 110.

[54] D. Lazard, *Gröbner-Bases, Gaussian elimination and resolution of systems of algebraic equations*, EUROCAL 1983, 146 - 156.

[55] D. Lazard, *Solving zero-dimensional algebraic systems*, Journal of Symbolic Computation, **13** (1992), 117 - 131.

[56] 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.

[57] 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.

[58] D. Lazard and F. Rouillier, *Solving parametric polynomial systems*, Research report, INRIA, SALSA project, 2004.

[59] G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions*, Proceedings of the 2000 international symposium on Symbolic and algebraic computation symbolic and algebraic computation, St. Andrews, Scotland, 2000, 209 - 216.

[60] G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers*, Journal of Complexity, **19**, Issue 4 (2003), 564 - 596.

[61] F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Tracts in Mathematics and Mathematical Physics. Cambridge University Press, 1916.

[62] 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.

[63] H.M. Moller and R. Tenberg, *Multivariate polynomial system solving using intersections of eigenspaces*, J. Symbolic Computation, **32** (2001), 513 - 531.

[64] A. Montes, *A new algorithm for discussing Gröbner basis with parameters*, J. of Symb. Comp., **33** (2002), 183 - 208.

[65] T. Mora, *Solving Polynomial Equation Systems I, The Kronecker-Duval Philosophy*, Encyclopedia of Mathematics and its Applications 88, Cambridge University Press (2003).

[66] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties*, Springer-Verlag, Berlin, Heidelberg, New York 1995.

[67] S. Puddu and J. Sabia,*An effective algorithm for quantifier elimination over algebraically closed fields using straight-line programs*, J. of Pure and Appl. Algebra, **129** (1997), 173 - 200.

[68] J. Renegar, *On the Computational Complexity and Geometry of the First-order Theory of the Reals: Parts I–III*, Journal of Symbolic Computation, **13** (1992), 255 - 352.

[69] K. Rimey, *A System of Polynomial Equations and a Solution by an Unusual Method*, SIGSAM Bulletin, **18(1)** (1984), 30 - 32.

[70] F. Rouillier, *Solving zero-dimensional polynomial systems through the rational univariate representation*, Appl. Alg. in Eng. Comm. Comput., **9(5)** (1999), 433 - 461.

[71] E. Schost, *Computing Parametric Geometric Resolutions*, Applicable Algebra in Engineering, Communication and Computing **13(5)** (2003), 349 - 393.

[72] E. Schost, *Sur la résolution des systèmes polynomiaux à paramètres*, Thèse de doctorat, École polytechnique, Décembre 2000.

[73] E. Schost, *Complexity results for triangular sets*, Journal of Symbolic Computation **36(3-4)** (2003), 555 - 594.

[74] W.Y. Sit, *A theory for parametric linear systems*, Proceedings of the 1991 international symposium on Symbolic and algebraic computation, Bonn, West Germany (1991), 112 - 121.

[75] W.Y. Sit, *An algorithm for solving parametric linear systems*, J. Symbolic Computation, **13** (1992), 353 - 394.

[76] A.J. Sommese, J. Verschelde, and C.W. Wampler, *Numerical decomposition of the solution sets of polynomial systems into irreducible components*, SIAM Journal on Numerical Analysis **38** (2001), 2022 - 2046.

[77] B.L. Van Der Waerden, *Modern algebra*, Vol. 2, 1950.

[78] D. Wang, *Elimination Practice Software Tools and Applications*, World Scientific Pub Co Inc, 2004.

[79] V. Weispfenning, *Comprehensive Gröbner bases*, J. Symbolic Computation, **14** (1991), 1 - 29.

[80] V. Weispfenning, *Quantifier Elimination for Real Algebra - the Cubic Case*, ISSAC, 1994, 258 - 263.

[81] 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.

[82] L. Yang, *Recent Advances on Determining the Number of Real Roots of Parametric Polynomials*, J. Symb. Comput. **28(1-2)**, 1999, 225 - 242.

[83] O. Zariski and P. Samuel, *Commutative Algebra*, vol. 1 (Springer-Verlag 1958) and vol. 2 (Springer-Verlag 1976).

Received: June, 2009