Записки научных
семинаров ПОМИ
Том 387, 2011 г.

A. Ayad

COMPLEXITY OF SOLVING PARAMETRIC POLYNOMIAL SYSTEMS

Abstract. We present three algorithms in this paper: the first algorithm solves zero-dimensional parametric homogeneous polynomial systems with single exponential time in the number n of the unknowns, it decomposes the parameters space into a finite number of constructible sets and computes the finite number of solutions by parametric rational representations uniformly in each constructible set. The second algorithm factorizes absolutely multivariate parametric polynomials with single exponential time in n and in the degree upper bound d of the factorized polynomials. The third algorithm decomposes the algebraic varieties defined by parametric polynomial systems of positive dimension into absolutely irreducible components uniformly in the values of the parameters. The complexity bound of this algorithm is double-exponential in n. On the other hand, the complexity lower bound of the problem of resolution of parametric polynomial systems is double-exponential in n.

Introduction

The simulation of many physical problems [44, 57, 21], chemical reactions [18, 21, 25], optimization [70], interpolation [59, 60, 25], robots [26, 13, 59, 60], and geometric problems [22, 42] yield to parametric systems of polynomial equations. A parametric system of polynomial homogeneous equations is a finite family of multivariate homogeneous polynomials $f_1, \ldots, f_k \in F[u_1, \ldots, u_r][X_0, \ldots, X_n]$ (in the variables $X_0, \ldots, X_n$) with polynomial coefficients in the variables $u = (u_1, \ldots, u_r)$ (the parameters) over a ground field F, 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. Some of these problems can be solved simply by determining the values of the parameters in an algebraic closure $\overline{F}$ of F for which the associated polynomial equation systems are consistent or not. However, when the system is consistent, it is sometimes

Key words and phrases: Symbolic computation, complexity analysis, parametric polynomials, parametric polynomial systems, Rational Univariate Representation, theory of resultants, polynomial factorization, algebraic varieties, irreducible components.

necessary to describe the set of its solutions uniformly in these values of the parameters (see below). The parameters take values from the space $\mathcal{P} := \overline{F}^r$ which is called the parameters space.

0.1. History

Different algorithms are intended for the resolution of parametric systems of polynomial equations. Heintz [32] exhibits an algorithm for the quantifier elimination problem in the theory of algebraically closed fields involving an algorithm that solves parametric linear systems by a parametrization of the Gaussian elimination procedure. Sit [63, 64] presented also algorithms for parametric linear systems. Grigoriev [28] presents an algorithm for the resolution of parametric systems of univariate polynomials by the computation of greatest common divisors of a family of univariate polynomials with parametric coefficients. Grigoriev and Vorobjov [29] and Montes [52] give algorithms for zero-dimensional parametric polynomial systems which are based on parametric Gröbner bases. If d is an upper bound on the degrees of $f_1, \ldots, f_k$, the complexity bound of the algorithm of [29] is $d^{O(n^2 r)}$. Weispfenning [69, 70] computes comprehensive Gröbner bases for parametric polynomial systems of positive dimension but with no complexity analysis of this computation.

Parametric geometric resolutions for zero-dimensional parametric polynomial systems are given by Giusti et. al. [23, 22, 24], Heintz et. al. [31], and Schost [60, 59]. The complexity bound in these papers is $d^{O(nr)}$. Gao et. al. [21], Wang [68], Dahan and Schost [61, 15] 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 [43] with single exponential time in n and r [54]. Dynamic evaluation [53] can be used for solving polynomial systems.

We also study in this paper the problem of factorization of multivariate polynomials. This problem is one of the principal problems in algebra and symbolic computation. It goes back to Newton, Gauss, Fermat, Kronecker, Hensel, and others. Berlekamp [4, 5] describes an algorithm for the factorization of univariate polynomials over a finite field. The first polynomial-time algorithm which factorises univariate polynomials with rational coefficients is realised by Lenstra, Lenstra and Lovasz (the LLL algorithm), it is based on the computation of minimal vectors of lattices [48]. Based on this algorithm and the Hensel lemma, Grigoriev and Chistov [11, 8, 27] present a polynomial-time algorithm which factorises

multivariate polynomials with coefficients in a field which is a finite extension of a purely transcendental extension of its prime subfield. In the same year, Kaltofen [34, 35, 37] describes a deterministic polynomial-time algorithm of reductions from multivariate to univariate integral polynomial factorization. Many other mathematicians worked on this problem like Zassenhaus [72], Niederreiter [56], von zur Gathen [67, 66], Lenstra [49, 50], Shoup [36], Gao [19, 20], Lecerf [7], and others.

These two topics are strongly related (see below for the parametric case and [8, 9, 27] for the nonparametric case).

0.2. Preliminaries

Let $F = H(T_1, \ldots, T_l)[\eta]$ be a finite extension of purely transcendental extension of its prime subfield H, where $H = \mathbf{Q}$ if $\mathrm{char}(F) = 0$ and $H \supseteq \mathbf{F}_p$ is a finite extension of sufficiently large cardinality[1] if $\mathrm{char}(F) = p > 0$ is a prime number. The variables $T_1, \ldots, T_l$ are algebraically independent over H, η is algebraic, separable over the field $H(T_1, \ldots, T_l)$ with a minimal polynomial $\phi \in H(T_1, \ldots, T_l)[Z]$. Let $(f_1, \ldots, f_k) \subset F[u_1, \ldots, u_r][X_0, \ldots, X_n]$ be a parametric system of homogeneous polynomial equations. In the whole our algorithm below we suppose that these polynomials are coded by dense representations, i.e., we represent all their monomials up to a certain degree, including those which are zeroes.

For any polynomial $f \in F[u_1, \ldots, u_r][X_0, \ldots, X_n]$, we denote by $l(f)$ the binary length of f which is the maximum of the binary lengths of the coefficients of f in H.

For any rational function $h \in F(u_1, \ldots, u_r)$, the degree of h w.r.t. $u_1, \ldots, u_r$, denoted by $\deg_{u_1,\ldots,u_r}(h)$, is the maximum of the degrees of its numerator and its denominator w.r.t. $u_1, \ldots, u_r$.

We suppose that we have the following bounds:

$$\deg_{T_1,\ldots,T_l,Z}(\phi) \leq d_1, \quad l(\phi) \leq M_1$$

and for any $1 \leq j \leq k$,

$$\begin{aligned} &\deg_{T_1,\ldots,T_l}(f_j) \leq d_2, \qquad \deg_{X_0,\ldots,X_n}(f_j) \leq d, \\ &\deg_{u_1,\ldots,u_r}(f_j) \leq \delta, \qquad l(f_j) \leq M_2. \end{aligned}$$

[1] the cardinal of H depends only on the degrees of the input polynomials of our algorithms

For a polynomial $g \in F(u_1,\ldots,u_r)[X_0,X_1,\ldots,X_n]$ and a value $a = (a_1,\ldots,a_r) \in \mathcal{P}$ of the parameters, we denote by $g^{(a)}$ the polynomial of $\overline{F}[X_0,X_1,\ldots,X_n]$ which is obtained by specialization of $u_1,\ldots,u_r$ by a in the coefficients of g if their denominators do not vanish on a ($\overline{F}$ is an algebraic closure of F). We denote by $V^{(a)}$ the projective variety of $P^n(\overline{F})$ defined by the polynomials $f_1^{(a)},\ldots,f_k^{(a)} \in \overline{F}[X_0,\ldots,X_n]$.

We associate to the system $(f_1,\ldots,f_k)$ the subset $\mathcal{U}$ of the parameters space $\mathcal{P}$ which is constructed by the values $a \in \mathcal{P}$ such that the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ is zero-dimensional and does not have solutions at infinity, i.e., the variety $V^{(a)}$ is a finite subset of $P^n(\overline{F})$ and $V^{(a)} \cap V(X_0) = \varnothing$.

Definition 0.1. *Let $a \in \mathcal{P}$ be such that the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ has a finite number of solutions $\xi_1,\ldots,\xi_s \in P^n(\overline{F})$. The multiset of the multiplicities of this system is the multiset* $(\mathrm{mult}(\xi_1),\ldots,\mathrm{mult}(\xi_s)) \in \mathbb{N}^s$ *where* $\mathrm{mult}(\xi)$ *is the multiplicity of ξ as a solution of the system (the integers of this multiset are not ordered).*

Effective generic points. We recall now the definition of effective generic points (see page 1840 of [8] and also [71, 55, 39, 9, 27]) of non empty irreducible projective varieties. Let $W \subset P^n(\overline{F})$ be a non empty projective variety which is defined and irreducible over F. We denote by $F[W]$ the coordinate ring of W and by $F(W)$ the field of rational functions over W which is the subfield of the fraction field of $F[W]$ formed by the fractions $\frac{g}{h}$ where g and h are homogeneous polynomials in $F[X_0,X_1,\ldots,X_n]$ of the same degree and $h \notin I(W)$ (i.e., h does not vanish identically on W). Let $m = \mathrm{codim}\,(W)$ and $t_1,\ldots,t_{n-m}$ be a transcendence basis of $F(W)$ over F.

An effective generic point [71, 55, 39, 9, 8, 27] of W is defined by the following field isomorphism:

$$\begin{aligned}\tau : F(t_1,\ldots,t_{n-m})[\theta] \\ \longrightarrow F\left(\frac{X_{j_1}}{X_s},\ldots,\frac{X_{j_{n-m}}}{X_s},\left(\frac{X_0}{X_s}\right)^{p^\nu},\ldots,\left(\frac{X_n}{X_s}\right)^{p^\nu}\right) \subseteq F(W) \quad (1)\end{aligned}$$

which is given by the following items:

- An integer $0 \le s \le n$ 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 $1 \le i \le n-m$ with the convention that $p^\nu = 1$ if $\mathrm{char}(F) = 0$ and $\nu \ge 0$ if $\mathrm{char}(F) = p > 0$.

- 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 [9, 8, 27]) if $\mathrm{char}(F) = 0$ and $\alpha_i \in H$ where $H \supseteq \mathbf{F}_p$ is a finite extension of sufficiently large cardinality if $\mathrm{char}(F) = p > 0$.
- The minimal polynomial $\Phi(Z) \in F(t_1, \ldots, t_{n-m})[Z]$ of θ over the field $F(t_1, \ldots, t_{n-m})$. This polynomial has to be separable.
- For each $1 \leq i \leq n$, a polynomial $B_i \in F(t_1, \ldots, t_{n-m})[\theta]$ such that

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

We recall here Lemma 2.7 of [27] which characterizes the elements of the ideal $I(W) \subset F[X_0, \ldots, X_n]$:

Lemma 0.2. *Let W be a non empty projective variety which is defined and irreducible over F. Suppose that we have an effective generic point of W defined as above by (1). Let $\psi \in F[X_0, \ldots, X_n]$ be a homogeneous polynomial. Then ψ vanishes identically on W (i.e., $\psi \in I(W)$) if and only if $\psi^{p^\nu}\left(\frac{X_0}{X_s}, \frac{X_1}{X_s}, \ldots, \frac{X_n}{X_s}\right) = 0$ in the field $F(t_1, \ldots, t_{n-m})[\theta]$ by using the field isomorphism τ^{-1}.*

0.3. Main results

In this paper, we cover all values of the parameters, i.e., we give finite partitions of the parameters space into constructible sets and we describe the solutions of the associated polynomial systems on each constructible set by rational univariate representations (rur [58]) for zero-dimensional systems and by effective generic points for systems of positive dimension (see below). We note that the computational model used within all the algorithms in this paper is the Turing machine model.

The paper is organized in three main sections. Section 1 presents an algorithm which for a parametric polynomial system of homogeneous equations $(f_1, \ldots, f_k)$, computes a finite partition of the associated set $\mathcal{U}$ into constructible sets $\mathcal{A}$ such that for each set $\mathcal{A}$, the multisets of the multiplicities and the number of the solutions of the associated systems are constant in $\mathcal{A}$ and they are computed by the algorithm. The algorithm computes univariate polynomials $\Phi, \psi_1, \ldots, \psi_n \in F(u_1, \ldots, u_r)[Z]$ which satisfy the following properties: for any $a \in \mathcal{A}$, the denominators of the coefficients of $\Phi, \psi_1, \ldots, \psi_n$ do not vanish on a and the solutions of the

system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ are given by the following parametric polynomial representation:

$$\Phi^{(a)}(\theta) = 0, \qquad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} & = & \psi_1^{(a)}(\theta) \\ & \vdots & \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_n}} & = & \psi_n^{(a)}(\theta) \end{cases}$$

where for all $1 \leq j \leq n$, $p^{\nu_j} = 1$ if $\mathrm{char}(F) = 0$ and $\nu_j \geq 0$ if $\mathrm{char}(F) = p > 0$. The number of the elements of the partition is at most $(\delta d d_1)^{O(n^2 r^2)}$. The degrees of $\Phi, \psi_1, \ldots, \psi_n$ w.r.t. $u_1, \ldots, u_r$ and $T_1, \ldots, T_l$ are bounded by $d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$, their binary lengths do not exceed $(M_1 + M_2) l d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$. The total complexity of this algorithm does not exceed $(\delta d_2)^{O(r^2 l)} (d d_1)^{O(n^2 r^2 l)}$ and its binary complexity does not exceed $(p M_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (d d_1)^{O(n^2 r^2 l)}$ (see Theorem 1.9 for more details). These bounds are relatively analogy to those of Grigoriev and Vorobjov [29] and Montes [52] (parametric Gröbner bases), Schost [59, 60] (Newton-Hensel operator) and Lazard-Rouillier [43] (discriminant varieties). The method used in this paper is new but the complexity bound is the same as in the mentioned papers. The algorithm is based on the computation of parametric U-resultants (see Sec. 1).

Section 2 is devoted to the absolute factorization of parametric multivariate polynomials. We give an algorithm which for a parametric polynomial $f \in F[u_1, \ldots, u_r][X_0, X_1, \ldots, X_n]$ (where each coefficient is a parameter, i.e., $r = (d+1)^{n+1}$), computes a finite partition of the parameters space $\mathcal{P}$ into constructible sets $\mathcal{V}$ such that the absolute factorization of f is given uniformly in each constructible set $\mathcal{V}$, i.e., the algorithm computes s polynomials $G_1, \ldots, G_s \in F(C, u_1, \ldots, u_r)[X_0, \ldots, X_n]$, $s \leq d$ and a polynomial $\chi \in F(u)[C]$ where C is a new variable satisfying the following: for any $a \in \mathcal{V}$, there exists $c \in \overline{F}$ being a root of $\chi^{(a)} \in \overline{F}[C]$ such that the denominators of the coefficients of χ and G_j do not vanish on a and (c, a), respectively, and the absolute factorization of $f^{(a)}$ is given by

$$f^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c,a)}, \quad G_j^{(c,a)} \quad \text{is absolutely irreducible.}$$

The number of the elements of the partition is at most $d^{O(n r^2 d^2)}$. Moreover, $\deg_C(G_j), \deg_C(\chi) \leq d^{O(d)}$, $\deg_u(G_j), \deg_u(\chi) \leq d^{O(r d^2)}$. The total

complexity of the algorithm does not exceed $d^{O(nr^2d^3)}$ and its binary complexity does not exceed $p^{O(1)}d^{O(nr^2d^3)}$ (see Theorem 2.14 for more details). This algorithm is based on a parametric version of Hensel's lemma and an algorithm of quantifier elimination in the theory of algebraically closed field [10] in order to reduce the problem of finding absolute irreducible factors to the problem of representing solutions of zero-dimensional parametric polynomial systems. This algorithm is a review and a completion of that of 2004 [1].

Example 0.3. Let the following parametric multivariate polynomial

$$f = (u^2 + v)x^2 + uxy + vx + uy + v \in \mathbb{Q}[u, v][x, y],$$

where x and y are two variables, u and v are the parameters. The algorithm decomposes the parameters space in the form:

$$\mathbb{C}^2 = \mathcal{V}_1 \sqcup \mathcal{V}_2 \sqcup \mathcal{V}_3,$$

where $\mathcal{V}_1 = \{u^2+v = 0\}$. For any $(a, b) \in \mathcal{V}_1$ we get the following absolute factorization:

$$f^{(a,b)} = (x + 1)(ay + b).$$

$\mathcal{V}_2 = \{u^2 + v \neq 0, u \neq 0\}$. For any $(a, b) \in \mathcal{V}_2$, $f^{(a,b)}$ is absolutely irreducible.

$\mathcal{V}_3 = \{u = 0, v \neq 0\}$. For any $(a, b) \in \mathcal{V}_3$, there exists c a cubic primitive root of the unity (in this case $\chi = C^3 - 1$) which satisfies the following

$$f^{(a,b)} = b(x - c)(x - c^2).$$

In Sec. 3, we study the resolution of parametric homogeneous polynomial systems of positive dimension. We present an algorithm which for a parametric homogeneous polynomial system $(f_1, \ldots, f_k)$ computes a finite partition of $\mathcal{P}$ into constructible sets $\mathcal{F}$ such that the absolutely irreducible components of the projective varieties defined by $f_1, \ldots, f_k$ are given uniformly in each constructible set $\mathcal{F}$, i.e., for any $a \in \mathcal{F}$, the number of the absolutely irreducible components $W_1^{(a)}, \ldots, W_L^{(a)}$ of the projective variety $V^{(a)}$ defined above is constant (i.e., L is independent of a). For each absolutely irreducible component $W^{(a)}$ among $W_1^{(a)}, \ldots, W_L^{(a)}$ 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 such that $W^{(a)}$ is represented by a *parametric representative system* and by a *parametric effective generic point* in the following sense:

Parametric representative system

The algorithm computes polynomials

$$\psi_1, \ldots, \psi_N \in F(C, u_1, \ldots, u_r)[Y_0, \ldots, Y_n]$$

homogeneous in $Y_0, \ldots, Y_n$ and a univariate polynomial

$$\chi \in F(u_1, \ldots, u_r)[C].$$

For any $a \in \mathcal{F}$, there exists $c \in \overline{F}$, a root of $\chi^{(a)} \in \overline{F}[C]$ such that the denominators of the coefficients of χ and $\psi_1, \ldots \psi_N$ do not vanish on a and (c, a), respectively, and the homogeneous polynomials $\psi_1^{(c,a)}, \ldots, \psi_N^{(c,a)} \in \overline{F}[Y_0, \ldots, Y_n]$ define the component $W^{(a)}$, i.e.,

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

Parametric effective generic point

The algorithm computes polynomials

$$\Phi, B_1, \ldots, B_n \in F(C, u_1, \ldots, u_r)(t_1, \ldots, t_{n-m})[Z]$$

and a rational function $\theta = \sum_{0 \le j \le n} \alpha_j \frac{Y_j}{Y_0}$. For any $a \in \mathcal{F}$, there exists $c \in \overline{F}$, a root of $\chi^{(a)}$ such that the denominators of the coefficients of $\Phi, B_1, \ldots, B_n$ do not vanish on (c, a) and the following properties hold:

- $W^{(a)} \cap V(Y_0) = \varnothing$.
- The rational functions

  $$t_1 = \frac{Y_1}{Y_0}, \ldots, t_{n-m} = \frac{Y_{n-m}}{Y_0}$$

  over $W^{(a)}$ form a transcendence basis of $\overline{F}(W^{(a)})$ over $\overline{F}$.
- An effective generic point of $W^{(a)}$ is defined by the following univariate representation:

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

where $p^\nu = 1$ if $\mathrm{char}(F) = 0$ and $\nu \geq 0$ if $\mathrm{char}(F) = p > 0$. The degrees of the coefficients of $\psi_1, \ldots, \psi_N$ and $B_1, \ldots, B_n$ and their binary lengths are single exponential in n, r and d. However, those of the coefficients of χ and Φ are double exponential in n and single exponential in r and d. The number of the elements of this partition and the total complexity of this algorithm are double exponential in n (see Theorem 3.5 and Corollary 3.6 for more details). We know that the lower bound complexity of the problem of solving zero-dimensional parametric polynomial systems is double-exponential in n [30] (when $r = \binom{n+d}{n}$, i.e., each coefficient of the polynomials is a parameter), the above bound for solving parametric polynomial systems of positive dimension is thus close to the exact bound. Our algorithm is a parametrization of that of Grigoriev [27]. It decomposes the parameters space by induction on the codimension of the absolutely irreducible components.

In the literature, there is no study of the complexity bound of the determination of the absolutely irreducible components of varieties defined by parametric polynomial systems of positive dimension. We recall that there is no analysis of the complexity bound of the algorithms given in [69, 70, 21, 68, 61, 15].

We note that if the input parametric polynomial system $f_1 = \cdots = f_k = 0$ is represented by a straight-line program, then by the works of Lecerf [46, 48] and Jeronimo, Sabia [33], the complexity of the equidimensional decomposition of varieties is single exponential with probabilistic algorithms.

Example 0.4. 1. Return to Example 0.3 and consider the hypersurface $V = V(f)$ defined by the parametric polynomial $f = (u^2 + v)x^2 + uxy + vx + uy + v$. The parameters space is decomposed into four constructible sets $\mathcal{F}_1 = \mathcal{V}_1 \setminus \{(0,0)\}$, $\mathcal{F}_2 = \mathcal{V}_2$, $\mathcal{F}_3 = \mathcal{V}_3$, and $\mathcal{F}_4 = \{(0,0)\}$ where $\mathcal{V}_1, \mathcal{V}_2$ and $\mathcal{V}_3$ are defined in Example 0.3.

For any $(a,b) \in \mathcal{F}_1$, the hypersurface $V^{(a,b)}$ admits two absolutely irreducible components W_1 and W_2 which are defined, respectively, by the polynomials $x+1$ and $ay+b$, i.e., the parametric polynomial $x+1$ (respectively, $uy+v$) forms a parametric representative system for W_1 (respectively, W_2). A parametric effective generic point of W_1 (respectively, W_2) is given by the equations $x = -1$ and $y = t$ (respectively, $x = t$ and $y = \frac{-v}{u}$, $u \neq 0$ on $\mathcal{F}_1$) where t is a parameter.

For $(a,b) \in \mathcal{F}_2$, we have only one absolutely irreducible component W because $f^{(a,b)}$ is absolutely irreducible. The set $\{f\}$ is a parametric representative system for W. A parametric effective generic point of W

is given by the equations $x = t$ and $y = -\frac{(u^2+v)t^2+vt+v}{u(t+1)}$ ($u \neq 0$ on $\mathcal{F}_2$) where $t \neq -1$ is a parameter.

For any $(a, b) \in \mathcal{F}_3$, the hypersurface $V^{(a,b)}$ admits two absolutely irreducible components W_1 and W_2 which are defined, respectively, by the polynomials $x - c$ and $x - c^2$ where c is a cubic primitive root of the unity, i.e., the parametric polynomial $x - c \in \mathbb{Q}(c, u, v)(x, y)$ (respectively, $x - c^2 \in \mathbb{Q}(c, u, v)(x, y)$) forms a parametric representative system for W_1 (respectively, W_2) for $\chi = C^3 - 1 \in \mathbb{Q}(u, v)[C]$ which is the polynomial that defines the field extension of $\mathbb{Q}(u, v)$ of the definition of W_1 and W_2. A parametric effective generic point of W_1 (respectively, W_2) is given by the equations $x = c$ and $y = t$ (respectively, $x = c^2$ and $y = t$) where t is a parameter.

For $(0, 0) \in \mathcal{F}_4$, $V^{(0,0)} = \mathbb{C}^2$. A parametric representative system is given by the zero polynomial and a parametric effective generic point is defined by the equations $x = t_1, y = t_2$ where t_1 and t_2 are parameters.

2. Consider the following parametric polynomial system which appears in [6, 69, 21]:

$$\begin{cases} x_4 - u_4 + u_2 = 0 \\ x_4 + x_3 + x_2 + x_1 - u_4 - u_3 - u_1 = 0 \\ x_3x_4 + x_1x_4 + x_2x_3 + x_1x_3 - u_1u_4 - u_1u_3 - u_3u_4 = 0 \\ x_1x_3x_4 - u_1u_3u_4 = 0 \end{cases}$$

where $u_1, \ldots, u_4$ are the parameters and the variables $x_1, \ldots, x_4$ are the unknowns of the system. The algorithm decomposes the parameters space $\mathbb{C}^4$ into three constructible sets $\mathcal{F}_1$, $\mathcal{F}_2$, and $\mathcal{F}_3$ which satisfy the following:

$\mathcal{F}_1 = \{u_2 - u_4 \neq 0\}$, $\quad \theta^3 - \alpha\theta^2 + \beta\theta - u_1u_3u_4 = 0$,

$$\begin{cases} x_1 = -\frac{1}{u_2-u_4}\theta^2 + \frac{\alpha}{u_2-u_4}\theta - \frac{\beta}{u_2-u_4} \\ x_2 = \frac{1}{u_2-u_4}\theta^2 - \frac{\alpha'}{u_2-u_4}\theta + \frac{\beta'}{u_2-u_4} \\ x_3 = \theta \\ x_4 = u_4 - u_2 \end{cases}$$

$\mathcal{F}_2 = \{u_2 - u_4 = 0,\ u_1u_3u_4 \neq 0\}$, $\quad$ no solutions;

$$\mathcal{F}_3 = \{u_2 - u_4 = 0,\ u_1u_3u_4 = 0\}, \quad \theta^2 - (u_1^2 + u_3^2 + u_4^2 - 2\beta) = 0,$$

$$\begin{cases} x_1 = -\frac{1}{2}\theta - t + \frac{\alpha}{2} \\ x_2 = t \\ x_3 = \frac{1}{2}\theta + \frac{\alpha}{2} \\ x_4 = 0, \end{cases}$$

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 $\beta' = u_1u_2 + u_1u_3 + u_2u_3 - u_2u_4 + u_2^2$.

Note that for any specialization $(a_1, \ldots, a_4)$ of the parameters in $\mathcal{F}_1$, the associated system admits 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 $(a_1, \ldots, a_4) \in \mathcal{F}_3$, the associated system has dimension 1.

1. Solving zero-dimensional parametric homogeneous polynomial systems

Suppose that we have a parametric system of polynomial homogeneous equations $f_1 = \cdots = f_k = 0$ where $f_1, \ldots, f_k \in F[u_1, \ldots, u_r][X_0, \ldots, X_n]$ are coded by dense representation of degrees $D_1, \ldots, D_k \leq d$, respectively (w.r.t. $X_0, \ldots, X_n$). In this section, we are interested in the set $\mathcal{U}$ associated with the system which is defined in the introduction. The basic tool of this section is the computation of the resultants of the systems $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ ($a \in \mathcal{P}$) uniformly in the values a of the parameters. We introduce the notion of parametric U-resultant where $U = (U_0, \ldots, U_n)$ are new variables algebraically independent over the field $F(u_1, \ldots, u_r, X_0, \ldots, X_n)$. Each parametric U-resultant R is a polynomial of $F[u_1, \ldots, u_r, U_0, \ldots, U_n]$ homogeneous in $U_0, \ldots, U_n$, associated with a constructible subset W of $\mathcal{P}$ such that for any $a \in W$, $R^{(a)} \in \overline{F}[U_0, \ldots, U_n]$ is the U-resultant of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ (see Sec. 1.1). When a parametric U-resultant (W, R) is calculated, we reduce R to parametric univariate polynomials (by suitable specializations of the variables $U_0, \ldots, U_n$) which allows us by a calculation of parametric greatest common divisors to find the multiset of the multiplicities of the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ uniformly in the values $a \in W$ of the parameters (see Sec. 1.2). The description of the solution set of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ is given by parametric rational univariate representations using parametric shape lemma (see Sec. 1.3).

1.1. Parametric U-resultant

Lazard [40, 41] generalised the notion of resultant for overdetermined polynomial systems, we discuss here the concept of U-resultant which was studied by Kronecker and Van der Waerden [41]. We follow the constructions of Lazard's work [41] (see also [27]). We suppose that $d \geq D_1 \geq \cdots \geq D_k$ and let

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

We introduce the linear form

$$f_{k+1} = U_0 X_0 + \cdots + U_n X_n \in F(u_1, \ldots, u_r, U_0, \ldots, U_n)[X_0, \ldots, X_n]$$

and the spaces B_i (respectively, B) of homogeneous polynomials in $F(u_1, \ldots, u_r, U_0, \ldots, U_n)[X_0, \ldots, X_n]$ of degrees $\mathcal{D} - D_i$ (respectively, $\mathcal{D}$) for all $1 \leq i \leq k+1$ where $D_{k+1} = 1$. Consider the $F(u_1, \ldots, u_r, U_0, \ldots, U_n)$-linear map $\Psi : B_1 \oplus \cdots \oplus B_{k+1} \longrightarrow B$ defined by:

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

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 $N = \dim(B) = \binom{n+\mathcal{D}}{n}$. We write $\mathcal{M}$ in the form:

$$\mathcal{M} = \mathcal{M}(u_1, \ldots, u_r, U_0, \ldots, U_n) = (\mathcal{M}_1 \quad \mathcal{M}_2),$$

where $\mathcal{M}_2$ is constructed by the last N_{k+1} columns of $\mathcal{M}$ with linear form entries over F in the variables $U_0, \ldots, U_n$ and $\mathcal{M}_1$ has its entries in $F[u_1, \ldots, u_r]$. We recall the basic result of Lazard's works (see Theorem 4.1 and Theorem 7.1 of [41], see also [40] and Theorem 2.2 of [27]) in the following theorem:

Theorem 1.1. (1) *Let $a = (a_1, \ldots a_r) \in \mathcal{P}$, the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ has a finite number of solutions in $P^n(\overline{F})$ if and only if $\mathrm{rk}(\mathcal{M}^{(a)}) = N$ where $\mathcal{M}^{(a)} := \mathcal{M}(a_1, \ldots a_r, U_0, \ldots U_n)$ has its coefficients in the field $\overline{F}(U_0, \ldots, U_n)$.*

(2) *For any $a \in \mathcal{U}$, the ideal generated by the N minors of $\mathcal{M}^{(a)}$ is a principal ideal which is generated by their greatest common divisor $R_a \in \overline{F}[U_0, \ldots, U_n]$ of degree $N - \mathrm{rk}(\mathcal{M}_1^{(a)})$.*

(3) *For any $a \in \mathcal{U}$, the homogeneous polynomial $R_a \in \overline{F}[U_0, \ldots, U_n]$ factorizes in the form:*

$$R_a = \prod_i L_i, \quad \text{where} \quad L_i = \sum_{0 \le j \le n} \xi_j^{(i)} U_j \quad \text{with} \quad \xi_j^{(i)} \in \overline{F},$$

and each $(\xi_0^{(i)} : \cdots : \xi_n^{(i)}) \in P^n(\overline{F})$ is a solution of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$, its multiplicity is equal to that of L_i as a factor of R_a. The number of the solutions of the system (counted with their multiplicities) is equal to $\deg_{U_0, \ldots U_n}(R_a)$.

Definition 1.2. *For any $a \in \mathcal{U}$, the polynomial $R_a \in \overline{F}[U_0, \ldots, U_n]$ of Theorem 1.1 is called the U-resultant of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$.*

The computation of U-resultants is based on the following lemma (see [41, Theorem 5.1]).

Lemma 1.3. *For any $a \in \mathcal{U}$, the U-resultant R_a coincides with any nonzero N minor of $\mathcal{M}^{(a)}$ which contains $\mathrm{rk}(\mathcal{M}_1^{(a)})$ columns of $\mathcal{M}_1^{(a)}$.*

Definition 1.4. *A parametric U-resultant of the system $f_1 = \cdots = f_k = 0$ is a couple (W, R) where W is a constructible subset of $\mathcal{P}$ and $R \in F[u_1, \ldots, u_r, U_0, \ldots, U_n]$ which satisfy the following property:*

For any $a \in W$, $R^{(a)}$ is the U-resultant of 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 $\mathcal{U}$.

Lemma 1.5. *There is an algorithm which computes at most N parametric U-resultants $(W_1, R_1), \ldots, (W_N, R_N)$ of the system $f_1 = \cdots = f_k = 0$ satisfying the following properties:*

(a) *The constructible sets $W_1, \ldots, W_N$ form a partition of $\mathcal{U}$.*

(b) *Each R_i is homogeneous in $U_0, \ldots, U_n$ of degree $N - i \le N$. Moreover, $\deg_u R_i \le i\delta \le N\delta$, $\deg_{T_1, \ldots, T_l} R_i \le i d_1 d_2 \le N d_1 d_2$, and $l(R_i) \le i d_1 M_1 M_2 \le N d_1 M_1 M_2$.*

The number of arithmetic operations of this algorithm is $(N\delta d_1 d_2)^{O(rl)}$ *in* H *and its binary complexity is* $(M_1 M_2)^{O(1)}(N\delta d_1 d_2)^{O(rl)}$.

Proof. We consider the Macaulay matrix $\mathcal{M}$ associated with the system $f_1 = \cdots = f_k = 0$ which is defined above. The parametric Gaussian elimination procedure (see [32] and [2, Theorem 2.4.1]) calculates a constructible set W where the rank of $\mathcal{M}$ is maximal, i.e., for all $a \in W$, $rk(\mathcal{M}^{(a)}) = N$. By Theorem 1.1, W is the set of $a \in \mathcal{P}$ where the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ admits a finite number of solutions in $P^n(\overline{F})$. This procedure also decomposes $\mathcal{P}$ into N constructible sets $\mathcal{U}_i$ such that the rank of $\mathcal{M}_1$ is constant over each $\mathcal{U}_i$ and equal to i.

For each $\mathcal{U}_i$, we get R_i as a N minor of $\mathcal{M}$ which contains i columns of $\mathcal{M}_1$ (by Lemma 1.3). Let $\Delta_i = \deg_{U_0,\ldots,U_n} R_i = N - i$ and $I_i \in F[u_1,\ldots,u_r]$ the coefficient of $U_0^{\Delta_i}$ in R_i. The constructible sets

$$W_i = \mathcal{U}_i \cap W \cap \{I_i \neq 0\}$$

satisfy the lemma. The inequation $I_i \neq 0$ ensures that no zero is allowed at infinity according to the definition of $\mathcal{U}$. The complexity bound follows from [32] (see also [10, p. 24–25 and [28, p. 14–15]). □

1.2. Constant multisets of the multiplicities

We fix a parametric U-resultant (W_i, R_i) from Lemma 1.5. Let $N \geq d^n$ be an integer. By Propositions 1, 2, and 3 of [12], one can construct vectors $b_1,\ldots,b_{N^2n} \in F^n$, pairwise distinct with the following property: for any pariwise distinct elements $\beta_1,\ldots,\beta_n \in F^n$, there exists $1 \leq t \leq N^2 n$ such that

$$\langle \beta_i, b_t \rangle \neq \langle \beta_j, b_t \rangle \text{ for all } i \neq j, \tag{2}$$

where $\langle .\,,.\rangle$ is the euclidean inner product in F^n. For each $1 \leq j \leq n$, we consider $n \times n$ matrices $B_1,\ldots,B_{N^2n}$ with coefficients in F such that the jth row of B_t is b_t for all $1 \leq t \leq N^2 n$. We introduce the polynomials

$$Q_j := R_i(U_0, 0,\ldots,0,U_j,0,\ldots,0) \in F[u_1,\ldots,u_r,U_0,U_j] \tag{3}$$

and

$$G_j(Z^{p^{\nu_j}}) = Q_j(Z,-1) \in F[u_1,\ldots,u_r][Z], \tag{4}$$

where Z is a new variable and p^{ν_j} is a maximal power of Z. The following lemma links the solutions of the systems $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ to the roots of the polynomials $G_1^{(a)},\ldots,G_n^{(a)} \in \overline{F}[Z]$ (for any $a \in W_i$).

Lemma 1.6. *Let $a \in W_i$ and $\xi = (\xi_0 : \cdots : \xi_n) \in P^n(\overline{F})$. For any $1 \leq j \leq n$, there exists a matrix B_t among $B_1, \ldots, B_{N^2 n}$ 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 $V = B_t U$ where $U = (U_0, \ldots, U_n)$ and $V = (V_0, \ldots, V_n)$ are new variables one has*

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

Proof. Definition 1.4, Theorem 1.1, and formula (4) prove that $\left(\frac{\xi_j}{\xi_0}\right)^{p^{\nu_j}}$ is a root of $G_j^{(a)}$ of multiplicity $\geq \mu$. If $\zeta = (\zeta_0 : \cdots : \zeta_n) \in P^n(\overline{F})$ is another solution of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ distinct from ξ, we have

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

by the definition of the linear transformation B_t and by formula (2). Thus the multiplicity of $\left(\frac{\xi_j}{\xi_0}\right)^{p^{\nu_j}}$ as a root of $G_j^{(a)}$ is exactly μ. □

Lemma 1.7. *There is an algorithm which decomposes W_i into at most $(N\delta)^{O(nr)}$ constructible sets $\mathcal{W}$ such that for each $\mathcal{W}$, it computes a multiset $s = (s_1, \ldots, s_h) \in \mathbb{N}^h$ which fulfills the following property: For any $a \in \mathcal{W}$, 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

$$(d_1 d_2)^{O(l)} (N\delta)^{O(r+l)} \quad \text{in} \quad H$$

and its binary complexity is $(M_1 M_2)^{O(1)} (d_1 d_2)^{O(l)} (N\delta)^{O(r+l)}$.

Proof. We consider the parametric univariate polynomials $G_1, \ldots, G_n \in F[u_1, \ldots, u_r][Z]$ defined by (4). By Lemma 1.6, there exists a matrix B_t associated to G_1, then we evaluate the linear transformation $V = B_t U$ in formula (3) and we apply the algorithm from Lemma 1 of [28] (see also Lemma 3.4.2 of [2]) to the new G_1 obtained by (4) (after the linear change of variables) which computes a finite partition of W_i into constructible sets W_{i,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 multiplicities of the roots of G_1. Again after another linear transformation

associated to G_2, we can decompose each W_{i,q_1} into a finite number of constructible sets W_{i,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 multiplicities of the roots of G_2 and so on. Finally, we get constructible sets $\mathcal{W} := W_{i,q_1,\ldots,q_n}$ that form a finite partition of W_i. For each $\mathcal{W}$, 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 bound follows from Lemma 1 of [28]. □

1.3. Parametric shape lemma

We fix a constructible set $\mathcal{W} \subset W_i$ of Lemma 1.7 where (W_i, R_i) is a parametric U-resultant of the parametric system $f_1 = \cdots = f_k = 0$ from Lemma 1.5. Let $K := F(u_1, \ldots, u_r)$ 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 $Q_j(Z, -1)$ (defined by (4)) in $\overline{K}$ such that $\lambda_j^{p^{\nu_j}}$ is separable over K with its minimal polynomial being a divisor of G_j in $K[Z]$.

Lemma 1.8. *We can compute polynomials $\chi, \psi_1, \ldots, \psi_n \in K[Z]$ of degrees $< N$ such that*

$$\chi(\theta) = 0, \quad \begin{cases} \lambda_1^{p^{\nu_1}} &= \psi_1(\theta) \\ &\vdots \\ \lambda_n^{p^{\nu_n}} &= \psi_n(\theta), \end{cases}$$

where χ is the minimal polynomial of θ over K. The degrees of $\chi, \psi_1, \ldots, \psi_n$ w.r.t. $u_1, \ldots, u_r$, and $T_1, \ldots, T_l$ are, respectively, bounded by $\delta(Nd_1)^{O(n)}$ and $d_2(Nd_1)^{O(n)}$. Their binary lengths are bounded by $(M_1 + M_2)rld_2(Nd_1)^{O(n)}$. This calculation costs $(\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$ operations in H and its binary complexity is $(pM_1M_2)^{O(1)}(\delta d_2)^{O(rl)}(Nd_1)^{O(nrl)}$.

Proof. By induction on j, we construct a primitive element θ_j for each finite and separable extension $E_j := K[\lambda_1^{p^{\nu_1}}, \ldots, \lambda_j^{p^{\nu_j}}]$ over K with its minimal polynomial $\chi_j \in K[Z]$. We take $\theta := \theta_n$ and $\chi := \chi_n \in K[Z]$ then $E_n = K[\lambda_1^{p^{\nu_1}}, \ldots, \lambda_n^{p^{\nu_n}}] = K[\theta]$. The computation of the coefficients of $\psi_1, \ldots, \psi_n$ is done by solving some linear systems over K of order $\leq N$ using Cramer's formulas (see Lemmas 3.5.1 and 3.5.2 of [2] for the description of these linear systems and the complete detailed proof of the Lemma). □

We can now summarize the main result of this section in the following theorem.

Theorem 1.9. *There is an algorithm that for a parametric homogeneous polynomial system $f_1 = \cdots = f_k = 0$ decomposes the associated subset $\mathcal{U}$ of $\mathcal{P}$ into at most $(\delta d d_1)^{O(n^2 r^2)}$ constructible sets $\mathcal{A}$ such that for each set $\mathcal{A}$, the multisets of the multiplicities of the solutions of the associated systems and their number are constant in $\mathcal{A}$ and they are computed by the algorithm. Moreover, it computes polynomials $\chi, \psi_1, \ldots, \psi_n \in F(u_1, \ldots, u_r)[Z]$ such that each value $a \in \mathcal{A}$ satisfies:*

- *The denominators of the coefficients of $\chi, \psi_1, \ldots, \psi_n$ do not vanish on a.*
- *A parametric representation of the solutions of the system $f_1^{(a)} = \cdots = f_k^{(a)} = 0$ is given by*

$$\chi^{(a)}(\theta) = 0, \quad \begin{cases} \left(\frac{X_1}{X_0}\right)^{p^{\nu_1}} &= \psi_1^{(a)}(\theta) \\ &\vdots \\ \left(\frac{X_n}{X_0}\right)^{p^{\nu_n}} &= \psi_n^{(a)}(\theta). \end{cases}$$

- *The degrees of $\chi, \psi_1, \ldots, \psi_n$ w.r.t. $u_1, \ldots, u_r$ and $T_1, \ldots, T_l$ are bounded by $d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$, their binary lengths do not exceed $(M_1 + M_2) l d_2 \delta^{O(r)} (d d_1)^{O(n^2 r)}$.*

The number of arithmetic operations of the algorithm is

$$(\delta d_2)^{O(r^2 l)} (d d_1)^{O(n^2 r^2 l)}$$

and its binary complexity is $(p M_1 M_2)^{O(1)} (\delta d_2)^{O(r^2 l)} (d d_1)^{O(n^2 r^2 l)}$.

Proof. We continue the discussion started before the theorem and we consider the constructible set $P_1 = \mathcal{W} \cap \{\psi = 0\} \subset \mathcal{P}$ where $\psi \in F[u_1, \ldots, u_r]$ is the l.c.m. of the denominators of the coefficients of the polynomials $\chi, \psi_1, \ldots, \psi_n$ given by Lemma 1.8. For any $a \in \mathcal{W} \backslash P_1$, the solutions of the associated system are given by the equations of Lemma 1.8. For the variety T_1 defined by the equation $\{\psi = 0\}$ and the equations which define $\mathcal{W}$, we apply the algorithm of solving algebraic systems [9, 27, 8] (see Theorem 2.4 of [27] or Theorem 2.1 of [8]) which computes each irreducible component S_1 of codimension m of T_1 by an effective generic point defined by the following field isomorphism:

$$F(t_1, \ldots, t_{r-m})[\mu] \cong F(S_1) \tag{5}$$

where $t_1, \ldots, t_{r-m}$ are algebraically independent over F and μ is separable over the field $F(t_1, \ldots, t_{r-m})$ with a minimal polynomial $\Phi \in F(t_1, \ldots, t_{r-m})[Z]$. It expresses each variable u_i as an element of $F(t_1, \ldots, t_{r-m})[\mu]$. By substitution of these expressions in the polynomials $G_j \in F[u_1, \ldots, u_r][Z]$, we get polynomials $g_j \in F(t_1, \ldots, t_{r-m})[\mu][Z]$.

By the same procedure as above (see Lemma 1.8), we compute a primitive element $\theta^{(1)}$ of the extension $K'[\lambda_1^{p^{\nu_1}}, \ldots, \lambda_n^{p^{\nu_n}}]$ over K' with its minimal polynomial $\chi \in K'[Z]$ where $K' := F(t_1, \ldots, t_{r-m})[\theta]$ and $\lambda_j^{p^{\nu_j}}$ 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 $P_2 = S_1 \cap \{\psi^{(1)} = 0\} \subset \overline{F}^r$ and $\psi^{(1)}$ is a suitable polynomial in $F[t_1, \ldots, t_{r-m}]$. 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 bound are given by Lemma 1.8 and those of Theorem 2.4 of [27] or Theorem 2.1 of [8] (the complete discussion on the recursive computation of the complexity bound is given in details in Theorem 3.5.3 of [2]). □

2. Absolute factorization of parametric multivariate polynomials

Let f be a parametric polynomial in $F[u_1, \ldots, u_r][Z_0, \ldots, Z_n]$, in this section we are interested in the absolute factorization of the polynomials $f^{(a)} \in \overline{F}[Z_0, \ldots, Z_n]$ uniformly in the values $a \in \mathcal{P}$ of the parameters (see below).

We restrict our attention to the case when $F = H$ and each coefficient of f is a parameter, i.e., we can write f in the form:

$$f = \sum_{|I| \leq d} u_I Z^I,$$

where $I = (i_0, \ldots, i_n) \in \mathbb{N}^{n+1}$, $|I| = i_0 + \cdots + i_n$ is the norm of I and $Z^I = Z_0^{i_0} \cdots Z_n^{i_n}$. The variables $(u_I)_{|I| \leq d}$ are the parameters $u = (u_1, \ldots, u_r)$ of f.

We introduce the set $\overline{H}_d[Z_0, \ldots, Z_n] := \{h \in \overline{H}[Z_0, \ldots, Z_n], \deg(h) = d\}$ of polynomials of degrees exactly d in $Z_0, \ldots, Z_n$. There is a natural bijection between this set and the set

$$\mathcal{P} = \left(\overline{H}^{\binom{n+d}{n}} \setminus \{(0, \ldots, 0)\}\right) \times \overline{H}^{\binom{n+d}{n+1}},$$

which will be the parameters space. The first factor corresponds to the monomials of degrees d, the second factor corresponds to those of degrees strictly less than d.

The main tool of this section is the Hensel lemma (see Lemma 3.3). This lemma is applicable to polynomials $g \in F[X, Y_1, \ldots, Y_n]$ which satisfy the following two conditions:

(H1): $\mathrm{lc}_X(g) = 1$, i.e., g is monic w.r.t. X.

(H2): $g_0(X) := g(X, 0, \ldots, 0)$ is separable in $F[X]$.

2.1. Preparation to the Hensel lemma

For any $a \in \mathcal{P}$, the polynomials $f^{(a)} \in \overline{H}[Z_0, \ldots, Z_n]$ do not satisfy necessary the conditions $(H1)$ and $(H2)$. The following lemma overcomes this problem.

Lemma 2.1. *There is an algorithm which decomposes $\mathcal{P}$ into at most $d^{O(n)}$ constructible sets $\mathcal{W}$ such that for each set $\mathcal{W}$, there exists a linear transformation of variables $X, Y_1, \ldots, Y_n$ and the algorithm computes a polynomial $g \in H(u)[X, Y_1, \ldots, Y_n]$. For each specialization $a \in \mathcal{W}$ of the parameters, the denominators of the coefficients of g do not vanish on a and the polynomial $g^{(a)} \in \overline{H}[X, Y_1, \ldots, Y_n]$ fulfills the conditions (H1) and (H2). Moreover, $\deg_u(g) \leq 2d^2$, $\deg_X(g) \leq d$, $\deg_Y(g) \leq 2d^3$, and $l(g) = O(nd^3 \log_2(d))$. The complexity bound of the algorithm is $d^{O(n)}$.*

To prove this lemma we should give some notations and intermediate results. For each couple (a, T) where $a \in \mathcal{P}$ and T is a $(n+1) \times (n+1)$ matrix with coefficients in H, we associate the polynomial $g_{(a,T)} \in \overline{H}[X, Y_1, \ldots, Y_n]$ defined by

$$g_{(a,T)}(X, Y_1, \ldots, Y_n) = f^{(a)}(T(X, Y_1, \ldots, Y_n)).$$

Proposition 2.2. *One can produce explicitly a family $\{T_1, \ldots, T_{N_1}\}$ of nonsingular $(n+1) \times (n+1)$ matrices with entries in H. For each value $a \in \mathcal{P}$ (i.e., $f^{(a)} \in \overline{H}_d[Z_0, \ldots, Z_n]$), there exists $1 \leq i \leq N_1 = (d+1)^n$ such that the polynomial $g_{(a,T_i)}$ satisfies*

$$0 \neq \mathrm{lc}_X(g_{(a,T_i)}) \in \overline{H}.$$

Proof. Let $a=(a_I)_{|I|\leq d}\in\mathcal{P}$ and $T=\left(t_{i,j}\right)_{1\leq i,j\leq n+1}$ be a $(n+1)\times(n+1)$ matrix with indeterminate coefficients. Then

$$\begin{aligned} g_{(a,T)}(X,Y_1,\ldots,Y_n) &= \sum_{|I|\leq d} a_I\left(t_{1,1}X+t_{1,2}Y_1+\cdots+t_{1,n+1}Y_n\right)^{i_0} \\ &\quad\cdots\left(t_{n+1,1}X+t_{n+1,2}Y_1+\cdots+t_{n+1,n+1}Y_n\right)^{i_n} \\ &= \left(\sum_{i_0+\cdots+i_n=|I|=d} a_I t_{1,1}^{i_0}t_{2,1}^{i_1}\cdots t_{n+1,1}^{i_n}\right)X^d+G, \end{aligned}$$

where $\deg_X(G)<d$ and

$$\begin{aligned} 0\neq h &:= \mathrm{lc}_X(g_{(a,T)}) \\ &= \sum_{i_0+\cdots+i_n=|I|=d} a_I t_{1,1}^{i_0}t_{2,1}^{i_1}\cdots t_{n+1,1}^{i_n}\in\overline{H}[t_{1,1},t_{2,1},\ldots,t_{n+1,1}]; \end{aligned}$$

h is a homogeneous polynomial in $t_{1,1}$, $t_{2,1},\ldots,t_{n+1,1}$ of degree d. This polynomial is nonzero because $a\in\mathcal{P}$, i.e., at least one of the values a_I ($|I|=d$) is nonzero.

We fix $b_0,\ldots b_d\in H$, pairwise distinct (if $\mathrm{char}(H)=0$ one takes $b_i=i$ and if $\mathrm{char}(H)=p>0$, one takes $b_i\in\mathbb{F}_{p^m}$ where $p^{m-1}\leq d<p^m$). By Zippel–Schwartz lemma [66, 3], there exists $(t_{1,1},t_{2,1},\ldots,t_{n+1,1})\in\{b_0,\ldots b_d\}^{(n+1)}$ such that $h(t_{1,1},t_{2,1},\ldots,t_{n+1,1})\neq 0$. One can take $t_{1,1}=1$ because h is homogeneous. With the condition $\det(T)\neq 0$, we can take

$$\mathbf{T}=\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ t_{2,1} & 1 & 0 & \ldots & 0 \\ t_{3,1} & 0 & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ t_{n+1,1} & 0 & \ldots & 0 & 1 \end{pmatrix},$$

where all the coefficients of T are equal to zero except the first column and the main diagonal. This proves the proposition by taking $N_1=(d+1)^n$ (see also Proposition 2.1 of [1]). □

Proof of Lemma 2.1 For each matrix T_i ($1\leq i\leq N_1$) of Proposition 2.2, we consider

$$g_i:=g_{(u,T_i)}\in H[u][X,Y_1,\ldots,Y_n],\quad h_i:=\mathrm{lc}_X(g_i)\in H[u]$$

and the constructible set W_i defined by the following equations and inequations:

$$h_1 = 0, \ldots, h_{i-1} = 0, \quad h_i \neq 0.$$

These sets form a partition of $\mathcal{P}$. By division of g_i by its leading coefficient h_i, we get a polynomial in $H(u)[X, Y_1, \ldots, Y_n]$ which fulfills the condition (H1) for each specialization $a \in W_i$. For the condition (H2), we fix (W_i, g_i, h_i) and we associate to each integer $0 \leq t \leq \lfloor \frac{\log_2 d}{\log_2 p} \rfloor$ (where $\lfloor * \rfloor$ is the integer part of $*$) a polynomial $g_{i,t} \in H(u)[X, Y_1, \ldots, Y_n]$ defined by

$$\frac{1}{h_i} g_i(X, Y_1, \ldots, Y_n) = g_{i,t}(X^{p^t}, Y_1, \ldots, Y_n)$$

and the constructible set $W_{i,t}$ defined in W_i by the inequation

$$\frac{\partial}{\partial X}(g_{i,t}) \neq 0. \tag{6}$$

The sets $W_{i,t}$ form also a partition of $\mathcal{P}$. If $\mathrm{char}(H) = 0$, we obtain $W_i = W_{i,0}$ which is defined by (6) with the convention $0^0 = 1$. We fix now a set $W_{i,t}$ and we compute the following discriminant:

$$\mathrm{Dis} := \mathrm{Dis}\, c_X(g_{i,t}) = \mathrm{res}_X \left(g_{T_i,t}, \frac{\partial}{\partial X}(g_{i,t}) \right) \in H(u)[Y_1, \ldots, Y_n]$$

we have $\deg_Y(\mathrm{Dis}) \leq d(2dp^{-t} - 1) =: D_1$ and we consider the sets

$$W_{i,t}^{(1)} = \{a \in W_{i,t},\ 0 \equiv \mathrm{Dis}^{(a)} \in \overline{H}[Y_1, \ldots, Y_n]\},$$
$$W_{i,t}^{(2)} = \{a \in W_{i,t},\ 0 \neq \mathrm{Dis}^{(a)}\}$$

then

$$W_{i,t} = W_{i,t}^{(1)} \cup W_{i,t}^{(2)}.$$

We begin by decomposing $W_{i,t}^{(2)}$, we fix $b_0, \ldots, b_{D_1} \in H$ pairwise distinct (if $\mathrm{char}(F) = p > 0$, one takes $b_i \in \mathbb{F}_{p^m}$ where $p^{m-1} \leq D_1 < p^m$). For each $c^{(j)} = (c_1^{(j)}, \ldots, c_n^{(j)}) \in \{b_0, \ldots, b_{D_1}\}^n$ $(1 \leq j \leq N_2 = (D_1 + 1)^n)$, one calculates the polynomial

$$g_{i,t,j}(X, Y_1, \ldots, Y_n) = g_{i,t}(X, Y_1 + c_1^{(j)}, \ldots, Y_n + c_n^{(j)}) \in H(u)[X, Y_1, \ldots, Y_n]$$

and a subset $W_{i,t}^{(2,j)}$ of $W_{i,t}^{(2)}$ defined by the inequation $\mathrm{Dis}(c^{(j)}) \neq 0$. By Zippel–Schwartz lemma [66, 3] (see also Lemma 4.2.2 of [2]), one can choose the elements $c^{(j)}$ such that the sets $W_{i,t}^{(2,j)}$ form a partition of $W_{i,t}^{(2)}$ and then polynomials $g_{i,t,j}$ satisfy the condition (H2).

For decomposing $W_{i,t}^{(1)}$, one calculates the signed sub-resultant polynomial sequence

$$SR_{dp^{-t}}, SR_{dp^{-t}-1}, \ldots, SR_1, SR_0 \in K[X]$$

of $P := g_{i,t}$ and $Q := \frac{\partial}{\partial X}(g_{i,t}) \in K[X]$, where $K = H(u)[Y_1, \ldots, Y_n]$ by algorithm 8.22 of [3]. We write each SR_j in the form

$$SR_j = A_j^{(j)} X^j + \cdots + A_0^{(j)},$$

where $A_k^{(j)} \in K$. For each $1 \leq j \leq dp^{-t}$, we consider a constructible subset $W_{i,t}^{(1,j)}$ of $W_{i,t}^{(1)}$ defined by the following equations and inequation

$$A_1^{(1)} = 0, \ldots, A_{j-1}^{(j-1)} = 0, \quad A_j^{(j)} \neq 0.$$

By Corollary 8.55 of [3], for any $a \in W_{i,t}^{(1,j)}$, $SR_j^{(a)} \in \overline{H}[Y_1, \ldots, Y_n][X]$ is a g.c.d. of $P^{(a)}$ and $Q^{(a)}$ of degree j in X. Let Q_j and R_j be the pseudo-quotient and the pseudo-remainder, respectively, of the pseudo-division of $g_{i,t}$ by SR_j in $K[X]$. The polynomial Q_j fulfills the condition (H2) in $W_{i,t}^{(1,j)}$. The degree, length and complexity bounds are computed in Sec. 3 of [1], Lemma 4.2.1 and Corollary 4.2.5 of [2]. □

2.2.Hensel's lemma

Let $R_N := F[Y_1, \ldots, Y_n]/((Y_1, \ldots, Y_n)^N)$, where $1 \leq N < \infty$ and $R_\infty = F[Y_1, \ldots, Y_n]$. We recall here a version of the Hensel lemma [72, 8, 27, 66].

Lemma 2.3. *Let $N > 1$ and $g \in R_N[X]$ which is satisfying the conditions* (H1) *and* (H2) *(see above).*

Then for any decomposition of g_0 in the form $g_0 = g_0^{(1)} \cdots g_0^{(s)}$, where $g_0^{(1)}, \ldots, g_0^{(s)} \in F[X]$ are monic, the following holds:

For each multi-index $I = (i_1, \ldots, i_n)$, $|I| > N \geq 1$, there exist unique polynomials $g_I^{(1)}, \ldots, g_I^{(s)} \in F[X]$ which satisfy:

(i) $\deg(g_I^{(j)}) < \deg(g_0^{(j)})$, $|I| \geq 1$, $1 \leq j \leq s$.

(ii) *In the completion of* $R_N[X]$ *w.r.t.* $(Y_1,\ldots,Y_n)$ *i.e., the ring* $K[X][[Y_1,\ldots,Y_n]]$ *of formal power series in* $Y_1,\ldots,Y_n$ *over* $K[X]$ *(see* [17]*) one has the decomposition:*

$$g = G_1\cdots G_s, \quad \textit{where} \quad G_j = g_0^{(j)} + \sum_{|I|\geq 1} g_I^{(j)} Y^I, \quad 1\leq j\leq s.$$

Let us write g in the form: $g = g_0 + \sum_{|I|\geq 1} g_I Y^I$, where $g_I \in K[X]$ and $\deg(g_I) < \deg(g_0)$ for all $|I|\geq 1$ according to (H1). Under the hypotheses of the Hensel lemma (i.e., Lemma 2.3), the condition (ii) is equivalent to the equations

$$g_I = \sum_{1\leq j\leq s} g_0^{(1)}\cdots g_0^{(j-1)} g_I^{(j)} g_0^{(j+1)}\cdots g_0^{(s)} + V_I, \quad |I|\geq 1. \tag{7}$$

where $V_I \in F[X]$. The coefficients of $V_I \in F[X]$ are polynomial functions of those of the polynomials $g_J^{(1)},\ldots,g_J^{(s)}$ for all $|J|<|I|$. For example, for $s=2$, $V_I = \sum_{1\leq|J|<|I|} g_I^{(1)} g_{I-J}^{(2)}$.

Let $\mathcal{D} := \deg_X(g) = \deg(g_0)$. For fixed $|I|$, the coefficients of $g_I^{(1)},\ldots,g_I^{(s)}$ form a vector of $F^{\mathcal{D}}$ which is the unique solution of the linear system $Bx = b_I$ given by (7), where B is $\mathcal{D}\times\mathcal{D}$ matrix with entries that only depend on the coefficients of $g_0^{(1)},\ldots,g_0^{(s)}$ (B is nonsingular by unicity of $g_I^{(1)},\ldots,g_I^{(s)}$ in Lemma 2.3). The second term b_I depends on the coefficients of g_I and V_I. Note that in case $s=2$, we get $B = \mathrm{Sylv}(g_0^{(1)}, g_0^{(2)})$ is the well-known Sylvester matrix of $g_0^{(1)}$ and $g_0^{(2)}$.

Remark 2.4. In case $s=2$, we get $B = Sylv(g_0^{(1)}, g_0^{(2)})$ is the Sylvester matrix of $g_0^{(1)}$ and $g_0^{(2)}$.

Notations. For any $1\leq j\leq s$, let $k_j = \deg(g_0^{(j)})$, then $\mathcal{D} = \sum_j k_j$. We write

$$g_0^{(j)} = X^{k_j} + \sum_{0\leq i<k_j} \alpha_i^{(j)} X^i, \quad g_I^{(j)} = \sum_{0\leq i<k_j} \alpha_i^{(j,I)} X^i,$$

and

$$g_I = \sum_{0\leq i<\mathcal{D}} v_{i,I} X^i, \quad |I|\geq 1.$$

Theorem 2.5. *Under the hypotheses of Lemma 2.3 and the above notations, for any $|I| \geq 1$, the coefficients of $g_I^{(1)}, \ldots, g_I^{(s)}$ are rational functions of the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ and the coefficients of g and they are given by:*

$$\alpha_i^{(j,I)} = \frac{P_i^{(j,I)}}{(\det(B))^{2|I|-1}}, \quad 1 \leq j \leq s, \quad 0 \leq i < k_j.$$

where $P_i^{(j,I)}$ is a polynomial, its variables are the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ and those of g. Its coefficients are elements of H. Moreover,

(1) *The degrees w.r.t. the coefficients of $g_0^{(1)}, \ldots, g_0^{(s)}$ and those of g are bounded from above by*

$$\deg_{\alpha_i^{(j)}}(P_i^{(j,I)}) \leq (2|I|-1)(\mathcal{D}-1)(s-1),$$
$$\deg_{\alpha_i^{(j)}}(\det(B)) \leq (\mathcal{D}-1)(s-1),$$

and

$$\deg_{v_{i,I}}(P_i^{(j,I)}) \leq (2|I|-1)(s-1).$$

(2) *If $F = H$ and M is an upper bound of the binary length of g then that of $P_i^{(j,I)}$ is bounded by*

$$sM + (2|I|-1)(\mathcal{D}-1)(s-1).$$

Proof. By recurrence on $|I|$ and by using Cramer's formulas on the linear system $Bx = b_I$ defined above. □

2.3. Partition of the parameters space by the Hensel lemma

We fix a couple $(\mathcal{W}, g)$ of Lemma 2.1, for any $a \in \mathcal{W}$, the polynomial $g^{(a)}$ satisfies the conditions (H1) and (H2) of Lemma 2.3. Let $\mathcal{D} := \deg_X(g) \leq d$, $\deg_Y(g) \leq 2d^3$ (see Lemma 2.1) and we write g in the form:

$$g = X^{\mathcal{D}} + \sum_{0 \leq |I| \leq 2d^3, 0 \leq i < \mathcal{D}} v_{i,I} X^i Y^I = g_0 + \sum_{1 \leq |I| \leq 2d^3} g_I Y^I,$$

where $v_{i,I} \in H(u)$. Let $k = (k_1, \ldots, k_s) \in \mathbb{N}^s$ be a partition of $\mathcal{D}$, i.e., $\mathcal{D} = k_1 + \cdots + k_s$, $k_1 \geq \cdots \geq k_s$, we associate to this partition a subset U_k of $\mathcal{W}$ defined by

Definition 2.6. *U_k is the set of values $a \in \mathcal{W}$ of the parameters such that the polynomial $g^{(a)}$ fulfills the following condition:*

(H3)*: There exist monic polynomials $g_0^{(1)}, \ldots, g_0^{(s)} \in \overline{H}[X]$ which satisfy*

$$g_0^{(a)} = g_0^{(1)} \cdots g_0^{(s)}, \quad \deg(g_0^{(j)}) = k_j, \quad 1 \leq j \leq s$$

and such that by application of Lemma 2.3 one gets a factorization of $g^{(a)}$ in $\overline{H}[X, Y_1, \ldots, Y_n]$. In other words, the polynomials $G_j^{(a)}$ $(1 \leq j \leq s)$ given by Lemma 2.3 are in $\overline{H}[X, Y_1, \ldots, Y_n]$. The latter condition will be called the termination condition.

We write the rational functions $v_{i,I}$ (coefficients of g) in the form:

$$v_{i,I} = \frac{S_{i,I}}{R_{i,I}}, \quad \text{where} \quad S_{i,I}, R_{i,I} \in H[u]$$

and $R_{i,I}^{(a)} \neq 0$ for any $a \in \mathcal{W}$.

The condition $g_0^{(a)} = g_0^{(1)} \cdots g_0^{(s)}$ is equivalent to:

$$S_{i,0}^{(a)} = R_{i,0}^{(a)} \sum_{0=l_0 \leq l_1 \leq \cdots \leq l_s = i} \prod_{1 \leq m \leq s} \alpha_{l_m - l_{m-1}}^{(m)}, \quad 0 \leq i < \mathcal{D}, \tag{8}$$

where $\alpha_{k_j}^{(j)} = 1$, $1 \leq j \leq s$ and the $\alpha_i^{(j)}$ are the coefficients of $g_0^{(j)}$ (as above).

The following theorem proves an equivalent condition to the termination condition.

Theorem 2.7. *The termination condition is equivalent to*

$$V_I = 0, \quad 2d^3 < |I| \leq 2sd^3,$$

where V_I is given by (7).

Proof. The proof is the same as Theorem 5.2 of [1]. □

Each $V_I \in H(\alpha_i^{(j)}, u)[X]$ depends only on polynomials $\{g_J^{(j)}\}_{|J|<|I|,\, 1 \leq j \leq s}$. We replace the coefficients of the polynomials $\{g_J^{(j)}\}_{1 \leq |J| \leq 2sd^3,\, 1 \leq j \leq s}$ in the new termination condition (Theorem 2.7) by their expressions given by Theorem 2.5, one gets polynomial equations in the form:

$$Q_i^{(I)} = 0, \quad 2d^3 < |I| \leq 2sd^3, \quad 0 \leq i \leq \mathcal{D} - 2, \tag{9}$$

where $Q_i^{(I)} \in H[\alpha_i^{(j)}, u]$, the $\alpha_i^{(j)}$ are the coefficients of $g_0^{(j)}$.

Corollary 2.8. *Let $k = (k_1, \ldots, k_s)$ be a partition of $\mathcal{D}$ where $s \geq 2$. Then the set U_k is the $\overline{H}$-realization in $\mathcal{W}$ of the following quantifier formula:*

$$\exists\ \alpha_i^{(j)}, \quad 1 \leq j \leq s, \quad 0 \leq i < k_j \quad \textit{which satisfy (8) and (9).} \tag{10}$$

Proof. By Theorem 2.7 and the above discussion. □

Lemma 2.9. *The number of equations in the formula (10) is*

$$N = (\mathcal{D}-1)\left(\binom{n+2sd^3}{n} - \binom{n+2d^3}{n}\right) + \mathcal{D} \leq d^{O(n)}.$$

The number of its quantifiers is $\mathcal{D} \leq d$, the degrees of its equations w.r.t. $\alpha_i^{(j)}$ are bounded by $D \leq 4d^6$. Their degrees w.r.t. u are bounded by $\delta \leq 8d^7$. The binary length of the coefficients of its equations in H is bounded by $\mathcal{M} = O(nd^6 \log_2(d))$ in the case $H = \mathbb{Q}$ ($\mathcal{M} = \log_2 p$ if $H = \mathbb{F}_p$).

Proof. By the bounds of Theorem 2.5. □

Lemma 2.10. *Let k be a partition of $\mathcal{D}$, then we can produce the following decomposition:*

$$U_k = \bigcup_{\beta}\left\{\bigwedge_{\alpha}(B_\alpha^{(\beta)} = 0) \wedge (C^{(\beta)} \neq 0)\right\}$$

such that for any α, β we have:

- $B_\alpha^{(\beta)}, C^{(\beta)} \in H[u_1, \ldots, u_r]$;
- $\deg_u(B_\alpha^{(\beta)}), l(B_\alpha^{(\beta)}) \leq d^{O(nrd^2)}$;
- $\deg_u(C^{(\beta)}), l(C^{(\beta)}) \leq d^{O(nd)}$;
- *The number of α and that of β are $\leq d^{O(nrd^2)}$.*

This decomposition costs $d^{O(nr^2d^3)}$ operations in H. Its binary complexity is bounded by $p^{O(1)}d^{O(nr^2d^3)}$.

Proof. By application of the quantifier elimination algorithm of Chistov–Grigoriev [10] on the formula (10) which defines U_k (Corollary 2.8) by taking into account the bounds of Lemma 2.9. □

The constructible sets U_k where the k's are the partitions of $\mathcal{D}$ do not form a partition of $\mathcal{W}$ and for any $a \in U_k$, the decomposition $g^{(a)} = G_1^{(a)} \cdots G_s^{(a)}$ given by the Hensel lemma is not an absolute factorization of $g^{(a)}$. To have a partition of $\mathcal{W}$ into constructible sets and an absolute factorization of $g^{(a)}$ uniformly in each of them, we introduce the following definition.

Definition 2.11. *One says that a partition $k' = (k'_1, \ldots, k'_h)$ of $\mathcal{D}$ is finer than another partition $k = (k_1, \ldots, k_s)$ of $\mathcal{D}$ if for all $1 \leq l \leq s$, $k_l = k'_{i_l} + k'_{i_l+1} \cdots + k'_{i_{l+1}-1}$ for certain $1 \leq i_1 < \cdots < i_s \leq h$.*

Proposition 2.12. *If k' is finer than k then $U_{k'} \subset U_k$.*

Proof. By definition 2.6. □

Lemma 2.13. *For each couple $(\mathcal{W}, g)$ of Lemma 2.1, the constructible set $\mathcal{W}$ decomposes in the form:*

$$\mathcal{W} = \bigcup_{k \in pt(\mathcal{D})} \mathcal{U}_k,$$

where $pt(\mathcal{D})$ is the set of the partitions of $\mathcal{D}$. For each set $\mathcal{U}_k$, there exist polynomials $G_1, \ldots, G_s \in H(C_1, \ldots, C_{\mathcal{D}}, u)[X, Y_1, \ldots, Y_n]$, where $C_1, \ldots, C_{\mathcal{D}}$ are new variables. For each specialization $a \in \mathcal{U}_k$ of the parameters, there exists $(c_1, \ldots, c_{\mathcal{D}}) \in \overline{H}^{\mathcal{D}}$ a solution of the algebraic system defined by (8) and (9) such that the denominators of the coefficients of G_j do not vanish on $(c_1, \ldots, c_{\mathcal{D}}, a)$ and the absolute factorization of $g^{(a)} \in \overline{H}[X, Y_1, \ldots, Y_n]$ is given by:

$$g^{(a)} = \prod_{1 \leq j \leq s} G_j^{(c_1, \ldots, c_{\mathcal{D}}, a)}, \quad G_j^{(c_1, \ldots, c_{\mathcal{D}}, a)} \text{ is absolutely irreducible.}$$

Proof. For each $k \in pt(\mathcal{D})$, one takes $\mathcal{U}_k = U_k \setminus \bigcup_{k' \neq k} U_{k'}$, the union ranges over all the partitions k' of $\mathcal{D}$ being finer than k. These sets form a partition of $\mathcal{W}$. The polynomials $G_1, \ldots, G_s$ are given by the Hensel lemma and Theorem 2.5 as rational functions in the parameters u and the coefficients $C_1, \ldots, C_{\mathcal{D}}$ of $g_0^{(1)}, \ldots, g_0^{(s)}$. □

In the sequel, we replace the variables $C_1, \ldots, C_{\mathcal{D}}$ of Lemma 2.13 by only one variable C and we show how to pass from the absolute factorization of $g^{(a)}$ (given by Lemma 2.13) to that of $f^{(a)}$ uniformly in the values

a of the parameters. This change is based on the algorithm of solving zero-dimensional parametric polynomial systems of Sec. 1 (Theorem 1.9).

We fix a constructible set $\mathcal{U}_k \subset \mathcal{W}$ given by Lemma 2.13 and we consider the parametric polynomial system S which is defined by Eqs. (8) and (9), the parameters of S are the variables $u = (u_1, \ldots, u_r)$, the unknowns are the variables $C_1, \ldots, C_{\mathcal{D}}$ which replace the variables $\alpha_i^{(j)}$ in these equations. For any $a \in \mathcal{U}_k$, the system $S^{(a)}$ (obtained after specialization of the parameters by a) admits a finite number of solutions which correspond to the permutations of the factors of $g_0^{(a)}$ (see Definition 2.6), i.e., by the fact that there is a bijective correspondance between the solutions of $S^{(a)}$ and the permutations of the factors of $g_0^{(a)}$.

We can now show the main result of this section in the following theorem.

Theorem 2.14. *There is an algorithm which decomposes the parameters space $\mathcal{P}$ into $d^{O(nr^2d^2)}$ constructible sets $\mathcal{V}$ such that for each $\mathcal{V}$, the algorithm computes polynomials $h_1, \ldots, h_s \in H(C,u)[Z_0, \ldots, Z_n]$ and a polynomial $\chi \in H(u)[C]$. For any $a \in \mathcal{V}$, there exists $c \in \overline{H}$, a root of $\chi^{(a)} \in \overline{H}[C]$ such that the denominators of the coefficients of χ and h_j do not vanish on a and (c,a), respectively, and the absolute factorization of $f^{(a)}$ is given by*

$$f^{(a)} = \prod_{1 \le j \le s} h_j^{(c,a)}, \quad h_j^{(c,a)} \text{ is absolutely irreducible.}$$

Moreover, $\deg_C(h_j)$, $\deg_C(\chi) \le d^{O(d)}$, $\deg_u(h_j)$, $\deg_u(\chi) \le d^{O(rd^2)}$. The number of arithmetic operations of the algorithm is $d^{O(nr^2d^3)}$ and its binary complexity is $p^{O(1)}d^{O(nr^2d^3)}$.

Proof. One applies the algorithm of Theorem 1.9 to the zero-dimensional parametric polynomial system S, we get a partition of $\mathcal{U}_k$ into $d^{O(r^2d^2)}$ constructible sets $\mathcal{V}$ such that for each set $\mathcal{V}$, the algorithm computes polynomials $\chi, \psi_1, \ldots, \psi_{\mathcal{D}} \in H(u)[C]$ which satisfy the following properties:

— The denominators of the coefficients of $\chi, \psi_1, \ldots, \psi_{\mathcal{D}}$ do not vanish on $a \in \mathcal{V}$.

— For each solution $(c_1, \ldots, c_{\mathcal{D}}) \in \overline{H}^{\mathcal{D}}$ of the system $S^{(a)}$, there exists

$c \in \overline{H}$, a root of $\chi^{(a)} \in \overline{H}[C]$ such that

$$\begin{cases} c_1 &= \psi_1^{(a)}(c) \\ &\vdots \\ c_{\mathcal{D}} &= \psi_{\mathcal{D}}^{(a)}(c) \end{cases}$$

— $\deg_C(\chi)$, $\deg_C(\psi_j) \leq d^{O(d)}$ and $\deg_u(\chi)$, $\deg_u(\psi_j) \leq d^{O(rd^2)}$.

We fix now a set $\mathcal{V}$ and we replace the expressions

$$\begin{cases} C_1 &= \psi_1(C) \\ &\vdots \\ C_{\mathcal{D}} &= \psi_{\mathcal{D}}(C) \end{cases}$$

in the coefficients of the polynomials $G_j \in H(C_1, \ldots, C_{\mathcal{D}}, u)[X, Y_1, \ldots, Y_n]$ of Lemma 2.13. One gets polynomials $g_j \in H(C, u)[X, Y_1, \ldots, Y_n]$ such that for any $a \in \mathcal{V}$, there exists $c \in \overline{H}$, a root of $\chi^{(a)} \in \overline{H}[C]$ and the absolute factorization of $g^{(a)}$ is given by:

$$g^{(a)} = \prod_{1 \leq j \leq s} g_j^{(c,a)}, \quad g_j^{(c,a)} \quad \text{is absolutely irreducible.}$$

To pass from absolute factorization of $g^{(a)}$ to that of $f^{(a)}$, one has to return to the form of the polynomial g which is given by the proof of Lemma 2.1. The complexity bound follows from Theorem 1.9, Lemmas 2.1 and 2.10. □

3. Solving parametric homogeneous polynomial systems of positive dimension

Let $f_1 = \cdots = f_k = 0$ be a parametric system of polynomial homogeneous equations $f_1, \ldots, f_k \in F[u_1, \ldots, u_r][X_0, \ldots, X_n]$ which are coded by dense representation with the notations and the bounds from Sec. 0.2. In this section, we are interested in the decomposition of the varieties $V^{(a)} := V(f_1^{(a)}, \ldots, f_k^{(a)}) \subset P^n(\overline{F})$ into absolutely irreducible components uniformly in the values $a \in \mathcal{P}$ of the parameters (see Theorem 3.5).

3.1. Trees of components

We recall here the notion of tree of components from [27] adjusted for the parametric case. For each $a \in \mathcal{P}$, we associate to the system

$f_1^{(a)} = \cdots = f_k^{(a)} = 0$ a tree of components, denoted by $T^{(a)}$, defined as follows:

The root of $T^{(a)}$ is the n-dimensional projective space $P^n(\overline{F})$ over $\overline{F}$. The level of a node v of this tree is the number of edges in branches going from the root to the node. The number of the levels of the tree $T^{(a)}$ is at most $n+1$. For any node of level m, denoted by v_m, we associate a projective variety $W_{v_m}^{(a)} \subset P^n(\overline{F})$, absolutely irreducible of codimension m (for $m = n+1$, one takes $W_{v_{n+1}}^{(a)} = \varnothing$). The construction of these varieties is based on the following lemma.

Lemma 3.1. *There is an algorithm which decomposes the parameters space $\mathcal{P}$ into a finite number of constructible sets. For each set $\mathcal{U}$ among them, it computes linear combinations $h_1, \ldots, h_{n+1}$ of $f_1, \ldots, f_k$ with coefficients in the field H such that any $a \in \mathcal{U}$ satisfies the following property:*

- *For any $1 \leq m \leq n+1$, the codimension of any absolutely irreducible component of the variety $V(h_1^{(a)}, \ldots, h_m^{(a)}) \subset P^n(\overline{F})$ which is not an absolutely irreducible component of $V^{(a)}$ is m. By consequence $V^{(a)} = V(h_1^{(a)}, \ldots, h_{n+1}^{(a)})$.*

Suppose for the moment that this lemma is proven and fix a constructible set $\mathcal{U}$ of the partition of $\mathcal{P}$ with the associated polynomials $h_1, \ldots, h_{n+1}$. We return to the construction of the trees $T^{(a)}$ for all $a \in \mathcal{U}$. Indeed, the sons of the root are the absolutely irreducible components of the hypersurface $V(h_1^{(a)})$ and for each node v_m of the tree, its sons are the absolutely irreducible components of the variety

$$\mathcal{W}_{v_m}^{(a)} := W_{v_m}^{(a)} \cap V(h_{m+1}^{(a)}). \tag{11}$$

One can distinguish two types of nodes of level not greater than n:

Definition 3.2. *A node v_m of the tree $T^{(a)}$ is called a node of the first type (i.e., v_m is a leaf of $T^{(a)}$) if the variety $W_{v_m}^{(a)}$ is an absolutely irreducible component of $V^{(a)}$ and v_m is called a node of the second type if $W_{v_m}^{(a)} \nsubseteq V^{(a)}$.*

Corollary 3.3. *For any $1 \leq m \leq n+1$, the absolutely irreducible components of the variety $V(h_1^{(a)}, \ldots, h_m^{(a)})$ are the varieties $W_{v_m}^{(a)}$ where v_m ranges over all the nodes of level m of $T^{(a)}$ and the varieties $W_{v_j}^{(a)}$ $(j < m)$ which are components of $V^{(a)}$ (i.e., the leaves v_j of $T^{(a)}$ of level $j < m$).*

Proof. By induction on m and by taking into account the above construction of the trees of components. □

Proposition 3.4. *For any $a \in \mathcal{U}$, all the absolutely irreducible components of $V^{(a)}$ appear in $T^{(a)}$, i.e., for each component W of $V^{(a)}$, of codimension m, there exists a leaf v_m of $T^{(a)}$ of level m such that $W = W_{v_m}^{(a)}$.*

Proof. One has $W \subset V^{(a)} \subset V(h_1^{(a)}, \ldots, h_m^{(a)})$, then W is contained in an absolutely irreducible component of $V(h_1^{(a)}, \ldots, h_m^{(a)})$, but $W \not\subseteq W_{v_j}^{(a)}$ for any leaf v_j of level $j < m$, then there is a node v_m of $T^{(a)}$ such that $W \subset W_{v_m}^{(a)}$ (Corollary 3.3), or $\dim W = \dim W_{v_m}^{(a)} = n - m$ thus $W = W_{v_m}^{(a)}$. □

In the sequel, we prove a result stronger than Lemma 3.1. Indeed, in the following theorem (main theorem of this section), we give a finer partition of the parameters space and we compute all the varieties $W_{v_m}^{(a)}$ for all nodes v_m of $T^{(a)}$ uniformly in each element of this partition.

Theorem 3.5. *There is an algorithm which for a parametric polynomial system $f_1 = \cdots = f_k = 0$ (which is given as in the introduction), partitions the parameters space into $k(\delta d d_1)^{r^3 d^{O(n^3)}}$ constructible sets such that for each set $\mathcal{F}$ among them, the following properties hold:*

— For any $1 \leq m \leq n+1$, the number of nodes of levels m is constant in $\mathcal{F}$, i.e., for any values $a, b \in \mathcal{F}$, the number of nodes v_m of the tree $T^{(a)}$ is equal to that of $T^{(b)}$.

— For each absolutely irreducible variety W_{v_m} 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 such that W_{v_m} is represented by a parametric representative system and by a parametric effective generic point in the following sense:

Parametric representative system

The algorithm computes polynomials

$$\psi_1, \ldots, \psi_N \in F(C, u_1, \ldots, u_r)[Y_0, \ldots, Y_n]$$

homogeneous in $Y_0, \ldots, Y_n$ of degrees $\leq d^{O(m)}$ and a polynomial $\chi \in F(u_1, \ldots, u_r)[C]$. For any $a \in \mathcal{F}$, there exists $c \in \overline{F}$, a root of $\chi^{(a)} \in \overline{F}[C]$ such that the denominators of the coefficients of χ and ψ_j do not vanish on a and (c, a), respectively, and the homogeneous polynomials $\psi_1^{(c,a)}, \ldots, \psi_N^{(c,a)} \in \overline{F}[Y_0, \ldots, Y_n]$ define the variety $W_{v_m}^{(a)}$, i.e.,

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

Moreover, the following bounds on the degrees and the binary lengths hold:

- $\deg_C(\psi_j) \leq \delta d^{O(n^3 d)}, \quad \deg_C(\chi) \leq \delta^{O(r^2)} d^{r^2 d^{O(n^3)}}$.
- $\deg_u(\psi_j) \leq \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_u(\chi) \leq \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.
- $\deg_{T_1,\ldots,T_l}(\psi_j) \leq d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$,
  $\deg_{T_1,\ldots,T_l}(\chi) \leq d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.
- $l(\psi_j) \leq (M_1 + M_2) d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$,
  $l(\chi) \leq (M_1 + M_2) d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.
- $N \leq d^{O(n^2)}$.

Parametric effective generic point:

- *The variety* $W_{v_m}^{(a)}$ *is not contained in the hyperplane* $V(Y_0) \subset P^n(\overline{F})$.
- *The rational functions* $t_1 = \frac{Y_1}{Y_0}, \ldots, t_{n-m} = \frac{Y_{n-m}}{Y_0}$ *over* $W_{v_m}^{(a)}$ *form a transcendence basis of* $\overline{F}(W_{v_m}^{(a)})$ *over* $\overline{F}$.
- *The algorithm computes polynomials*

$$\phi, B_1, \ldots, B_n \in F(C, u_1, \ldots, u_r)(t_1, \ldots, t_{n-m})[Z]$$

and a rational function $\theta = \sum_{0 \leq j \leq n} \alpha_j \frac{Y_j}{Y_0}$ *with* $0 \leq \alpha_j \leq \deg(W_{v_m}^{(a)}) \leq d^m$. *For any* $a \in \mathcal{F}$, *there exists* $c \in \overline{F}$, *a root of* $\chi^{(a)}$ *such that the denominators of the coefficients of* $\phi, B_1, \ldots, B_n$ *do not vanish on* (c, a) *and an effective generic point of* $W_{v_m}^{(a)}$ *is given by the following field isomorphism:*

$$\tau : \overline{F}\left(1, \left(\frac{Y_1}{Y_0}\right)^{p^\nu}, \ldots, \left(\frac{Y_n}{Y_0}\right)^{p^\nu}\right) \longrightarrow \overline{F}(t_1, \ldots, t_{n-m})[\theta]. \qquad (12)$$

This isomorphism is defined by the following univariate representation:

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

Moreover, the following bounds on the degrees and the binary lengths hold:

- $\deg_C(B_j) \leq \delta d^{O(n^3 d)}, \quad \deg_C(\phi) \leq \delta^{O(r^2)} d^{r^2 d^{O(n^3)}}$.
- $\deg_u(B_j) \leq \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}, \quad \deg_u(\phi) \leq \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.
- $\deg_{t_1,\ldots,t_{n-m}}(B_j), \deg_{t_1,\ldots,t_{n-m}}(\phi) \leq d^{O(n^3)}$.
- $\deg_{T_1,\ldots,T_l}(B_j) \leq d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$,
  $\deg_{T_1,\ldots,T_l}(\phi) \leq d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.
- $\deg_Z(B_j) < \deg_Z(\phi) \leq d^{O(m)}$ *et* $p^\nu \leq d^{O(m)}$.
- $l(B_j) \leq (M_1 + M_2) d_2 \delta^{O(r^2)} d^{O(n^3 r^2 d^2)}$,
  $l(\phi) \leq (M_1 + M_2) d_2 \delta^{O(r^3)} d^{r^3 d^{O(n^3)}}$.

Proposition 3.4 proves that the components of the varieties $V^{(a)}$ are the varieties $W^{(a)}_{v_m}$ associated with leaves v_m of $T^{(a)}$. The following corollary describes them.

Corollary 3.6. *Each element $\mathcal{F}$ of the finite partition of the parameters space of Theorem 3.5 satisfies:*

(1) *The number of absolutely irreducible components is constant in $\mathcal{F}$, i.e., for any $a, b \in \mathcal{F}$, the number of absolutely irreducible components of the variety $V^{(a)}$ is equal to that of $V^{(b)}$.*

(2) *Each absolutely irreducible component $W^{(a)}$ of $V^{(a)}$ is represented by a parametric representative system and by a parametric effective generic point. The bounds on the degrees and the binary lengths of the expressions involving in their representation are as in Theorem 3.5.*

Proof. By Lemma 0.2, we can examine if a variety $W^{(a)}_{v_m}$ of the tree $T^{(a)}$ given by an effective generic point is a component of $V^{(a)}$ or not. The other items of the corollary follow from Theorem 3.5. □

We will prove this theorem by induction on the level m of the trees of components (i.e., the codimension m). At each step of this induction, the parameters space will be divided suitably to lead to the results desired in Theorem 3.5.

3.2. Basis of the induction

For $m = 1$, one takes $h_1 = f_1 \in F[u_1, \ldots, u_r, X_0, X_1, \ldots, X_n]$ and we apply the algorithm of the absolute factorization of parametric polynomials (Theorem 2.14) to h_1. This algorithm decomposes $\mathcal{P}$ into constructible sets such that for each set U_1 among them, it computes polynomials $G_1, \ldots, G_s \in F(C, u)[X_0, \ldots, X_n]$ and a polynomial $\chi \in F(u)[C]$ which represent the absolute irreducible factors of h_1 for all specialization $a \in U_1$ of the parameters (see Theorem 2.14).

For any $a \in U_1$, there exists $c \in \overline{F}$, a root of $\chi^{(a)}$ such that the varieties $W_{v_1}^{(a)}$, where v_1 ranges over all nodes of level 1 of $T^{(a)}$ are the hypersurfaces $W_j^{(a)} := V(G_j^{(c,a)})$, $1 \leq j \leq s$. The set $\{G_j\}$ is a parametric representative system of the variety $W_j^{(a)}$. To compute a parametric effective generic point for each $W_j^{(a)}$, we use Lemmas 2.2 and 2.3 from [Gri] which we recall in the following:

Lemma 3.7. *Let $V = V(g_1, \ldots, g_s) \subset P^n(\overline{F})$ be a projective variety of codimension m, defined by homogeneous polynomials $g_1, \ldots, g_s \in F[X_0, \ldots, X_n]$. Then the following conditions are equivalent:*

(1) $V \cap V(X_0, \ldots, X_{n-m}) = \varnothing$.

(2) *The system of equations*

$$g_i(X_0, t_1 X_0, \ldots, t_{n-m} X_0, X_{n-m+1}, \ldots, X_n) = 0, \quad 1 \leq i \leq s$$

with coefficients from the field $F(t_1, \ldots t_{n-m})$, where $t_1, \ldots t_{n-m}$ are algebraically independent over F, has only a finite number of solutions in $P^m(\overline{F(t_1, \ldots t_{n-m})})$ and has no solutions at infinity, i.e., solutions which are contained in the hyperplane $V(X_0)$.

Moreover, under these conditions, for any irreducible component W of the highest dimension of V, i.e., $\dim(W) = n - m$, the rational functions $\frac{X_1}{X_0}, \ldots, \frac{X_{n-m}}{X_0}$ form a transcendence basis of $\overline{F}(W)$ over $\overline{F}$.

Lemma 3.8. *One can construct a family $M_{n,n-m,d}$ consisting of $(n - m + 1)$-tuples of linear forms in $X_0, \ldots X_n$ with coefficients in H such that for any variety $V \subset P^n(\overline{F})$, $\operatorname{codim}(V) = m$, $\deg(V) \leq d$, there exists $(Y_0, \ldots, Y_{n-m}) \in M_{n,n-m,d}$ such that $V \cap V(Y_0, \ldots, Y_{n-m}) = \varnothing$. Moreover, $\operatorname{card}(M_{n,n-m,d}) = \binom{nd+1}{n-m+1}$ and $M_{n,n-m,d}$ can be constructed in polynomial-time in $\operatorname{card}(M_{n,n-m,d})$.*

Remark 3.9. One finds a better construction of Lemma 3.8 in [12], but in our case, it does not improve the bounds on the degrees of the output of the algorithm.

For each element $(Y_0^{(t)}, \ldots, Y_{n-1}^{(t)})$ of the family $M_{n,n-1,d}$, we associate subsets $U_{1,t}$ and $\widetilde{U}_{1,t}$ of U_1 defined by:

$$U_{1,t} = \{a \in U_1, \quad W_j^{(a)} \cap V(Y_0^{(t)}, \ldots, Y_{n-1}^{(t)}) = \varnothing \quad \text{for all} \quad 1 \leq j \leq s\}.$$

and

$$\widetilde{U}_{1,t} = U_{1,t} \setminus \bigcup_{1 \leq t' < t} U_{1,t'}$$

Lemma 3.8 proves that the sets $\widetilde{U}_{1,t}$, $1 \leq t \leq \mathrm{card}(M_{n,n-1,d})$ form a partition of U_1. Each set $U_{1,t}$ is the $\overline{F}$-realization in U_1 of the following quantifier formula:

$$\exists C, \quad G_j(0, \ldots, 0, 1) \neq 0, \quad \chi(C) = 0 \quad 1 \leq j \leq s.$$

By application of the main algorithm in Lemma 2 of [10] to this formula, one gets equations and inequations which define the constructible set $U_{1,t}$.

We fix a certain t and we take $Y_0^{(t)} = Y_0, \ldots, Y_{n-1}^{(t)} = Y_{n-1}$ which are linearly independent over H by their construction (see the proof of Lemma 3.8, i.e., the proof of Lemmas 2.2 and 2.3 in [27]), we complete them to a basis $Y_0, \ldots, Y_n$ of the space of linear forms in $X_0, \ldots, X_n$ with coefficients in H. By Lemma 3.7, the rational functions $t_1 = \frac{Y_1}{Y_0}, \ldots, t_{n-1} = \frac{Y_{n-1}}{Y_0}$ form a transcendence basis of $\overline{F}(W_j^{(a)})$ over $\overline{F}$ for all j and for all $a \in \widetilde{U}_{1,t}$. We represent each G_j as an element of $F(C, u_1, \ldots, u_r)[Y_0, \ldots, Y_n]$ and we write it in the form $G_j = \widetilde{G}_j\big(Y_0^{p^{\nu_j}}, \ldots, Y_n^{p^{\nu_j}}\big)$, where $\widetilde{G}_j \in F(C, u_1, \ldots, u_r)[Z_0, \ldots, Z_n]$, $Z_0, \ldots, Z_n$ are new variables. One poses $\theta_j = \left(\frac{Y_n}{Y_0}\right)^{p^{\nu_j}}$ and

$$\phi_j(Z) = \widetilde{G}_j(1, t_1, \ldots, t_{n-1}, Z) \in F(C, u_1, \ldots, u_r)(t_1, \ldots, t_{n-1})[Z].$$

For any $a \in \widetilde{U}_{1,t}$, the polynomial $\phi_j^{(c,a)}(Z) \in \overline{F}(t_1, \ldots, t_{n-1})[Z]$ admits θ_j as a root. This defines an effective generic point of $W_j^{(a)}$. The number of arithmetic operations in H of the basis of the induction is $(\delta d_2)^{O(r^2 l)}(dd_1)^{O(nr^2 ld^3)}$ and its binary complexity is

$$(pM_1M_2)^{O(1)}(\delta d_2)^{O(r^2 l)}(dd_1)^{O(nr^2 ld^3)}.$$

These bounds follow from Theorem 2.14 and from those of Lemma 2 in [28, p. 28].

3.3. Induction hypothesis

We suppose at the step $m+1$ of the induction that the polynomials $h_1, \ldots, h_m$ are computed and all the nodes v of level $\leq m$ of the trees of components are constructed in the following way: The parameters space $\mathcal{P}$ is decomposed into $\mathcal{N}_m \leq (\delta d d_1)^{O(mnr^2d^2)}$ constructible sets such that for each set U_m among them, the following properties hold.

There exists a linear transformation $Y_0, \ldots, Y_n$ of variables such that each absolutely irreducible variety W_{v_j} of codimension $j \leq m$, associated with a node v_j is represented by a parametric representative system $(\chi, \psi_1, \ldots, \psi_N)$ and by a parametric effective generic point $(\phi, B_1, \ldots, B_n)$ as in Theorem 3.5 but with the following bounds on the degrees and the binary lengths:

- $\deg_C(\psi_j),\ \deg_C(\chi),\ \deg_C(B_j),\ \deg_C(\phi) \leq \delta d^{O(md)}$.
- $\deg_u(\psi_j),\ \deg_u(\chi),\ \deg_u(B_j),\ \deg_u(\phi) \leq \delta^{O(r)} d^{O(mrd^2)}$.
- $\deg_{T_1,\ldots,T_l}(\psi_j),\ \deg_{T_1,\ldots,T_l}(\chi)$, $\deg_{T_1,\ldots,T_l}(B_j),\ \deg_{T_1,\ldots,T_l}(\phi) \leq \delta^{O(r)} d_2 d^{O(mrd^2)}$.
- $\deg_{t_1,\ldots,t_{n-m}}(B_j),\ \deg_{t_1,\ldots,t_{n-m}}(\phi) \leq d^{O(m)}$.
- $\deg_Z(B_j) < \deg_Z(\phi) \leq d^{O(m)}$ and $p^\nu \leq d^{O(m)}$.
- $l(\psi_j), l(\chi), l(B_j), l(\phi) \leq (M_1 + M_2)\delta^{O(r)} d_2 d^{O(mrd^2)}$.
- $N \leq d^{O(mn)}$.

3.4. Core of the induction

The step $m+1$ of the induction consists in further dividing each U_m into constructible sets and calculating the polynomial h_{m+1}. Also we compute parametric representative systems and parametric effective generic points of the absolutely irreducible components $W^{(a)}_{w_m}$ of the variety $\mathcal{W}^{(a)}_{v_m} := W^{(a)}_{v_m} \cap V(h^{(a)}_{m+1})$ which is defined by (11) (the w_m's are the sons of the nodes v_m which are not leaves of the tree of components).

3.4.1. Construction of h_{m+1}

The construction of h_{m+1} is based on Lemma 0.2 and the following Lemma [27].

Lemma 3.10. *For any $a \in U_m$, the number of nodes v_m of level m of $T^{(a)}$ does not exceed d^m.*

Proposition 3.11. *Let* $\mathcal{N} := (k-1)d^m + 1$ *and* $\alpha_1, \ldots \alpha_{\mathcal{N}} \in H$, $\mathcal{N}$ *nonzero pairwise distinct elements of* H. *For any* $a \in U_m$, *there exists a polynomial among* $h^{(a)}_{\alpha_1}, \ldots, h^{(a)}_{\alpha_{\mathcal{N}}}$, *where* $1 \leq s \leq \mathcal{N}$,

$$h_{\alpha_s} := \sum_{1 \leq j \leq k} \alpha_s^{j-1} f_j,$$

which does not vanish identically on $W^{(a)}_{v_m}$ *for any node* v_m *of level* m *of* $T^{(a)}$, *which is of the second type (Definition* 3.2*).*

Proof. If not, by Lemma 3.10 and by pigeon-hole principle, there exists a node v_m of the second type, of level m of $T^{(a)}$ and k elements $\alpha_{s_1}, \ldots, \alpha_{s_k}$ among $\alpha_1, \ldots, \alpha_{\mathcal{N}}$ such that $h^{(a)}_{\alpha_{s_1}}, \ldots, h^{(a)}_{\alpha_{s_k}}$ vanish identically on $W^{(a)}_{v_m}$. Then $f^{(a)}_1, \ldots, f^{(a)}_k$ vanish identically on $W^{(a)}_{v_m}$ because $\alpha_{s_1}, \ldots, \alpha_{s_k}$ are pairwise distinct, this is a contradiction with the fact that v_m is of the second type. □

For any $1 \leq s \leq \mathcal{N}$, we associate subsets $U_{m,s}$ and $\widetilde{U}_{m,s}$ of U_m which are defined by:

$$U_{m,s} = \{a \in U_m,\ h^{(a)}_{\alpha_s} \text{ does not vanish identically on } W^{(a)}_{v_m} \text{ for any } v_m \text{ of the second type}\}$$

and

$$\widetilde{U}_{m,s} = U_{m,s} \setminus \bigcup_{1 \leq s' < s} U_{m,s'}.$$

Proposition 3.11 proves that the sets $\widetilde{U}_{m,s}$, $1 \leq s \leq \mathcal{N}$ form a partition of U_m. Lemma 0.2 proves that each $U_{m,s}$ is the realization of the following quantifier formula which is defined over the field $F(t_1, \ldots, t_{n-m})$ by:

$$\exists C,\ \theta, \quad h_{\alpha_s}\Big(1, B_1(C,\theta), \ldots, B_n(C,\theta)\Big) \neq 0, \quad \chi(C) = 0, \quad \phi(C,\theta) = 0$$

for all nodes v_m of the second type. By application of the algorithm in Lemma 2 of [10] to this formula, one gets equations and inequations which define the constructible set $U_{m,s}$.

3.4.2. Reduction to the zero-dimensional parametric case

We fix a certain constructible set $\widetilde{U}_{m,s}$ and we are interested in the varieties:

$$\mathcal{W}^{(a)}_{v_m} = W^{(a)}_{v_m} \cap V(h^{(a)}_{\alpha_s}) = V(\psi^{(c,a)}_1, \ldots, \psi^{(c,a)}_N, h^{(a)}_{\alpha_s}) \subset P^n(\overline{F})$$

for any nodes v_m of $T^{(a)}$ of the second type and any value $a \in \widetilde{U}_{m,s}$, where $(\chi, \psi_1, \ldots, \psi_N)$ is a parametric representative system of $W_{v_m}^{(a)}$.

The following lemma constructs a common transcendence basis of the field of rational functions of all the components $W_{w_m}^{(a)}$.

Lemma 3.12. *Under the above hypotheses, one can produce a finite decomposition of $\widetilde{U}_{m,s}$ into $d^{O(n)}$ sets such that for each set $\mathcal{V}$ among them, there exists a nonsingular linear transformation $Z_0, \ldots, Z_n$ with coefficients in H such that any value $a \in \mathcal{V}$ and any node v_m of the second type of $T^{(a)}$ satisfy the following properties*

(i) *The components $W_{w_m}^{(a)}$ do not lie in the hyperplane $V(Z_0)$.*

(ii) *The rational functions $t_1 := \frac{Z_1}{Z_0}, \ldots, t_{n-m-1} := \frac{Z_{n-m-1}}{Z_0}$ form a common transcendence basis of all components $W_{w_m}^{(a)}$ of $\mathcal{W}_{v_m}^{(a)}$.*

Proof. Let $M := M_{n,n-m-1,d^{m+1}}$ be a family defined by Lemma 3.8. For any element $(Z_0, \ldots, Z_{n-m-1})$ of M, we associate a subset $\mathcal{V}$ of $\widetilde{U}_{m,s}$ defined by:

$$\mathcal{V} := \Big\{ a \in \widetilde{U}_{m,s},\ \mathcal{W}_{v_m}^{(a)} \cap V(Z_0, \ldots, Z_{n-m-1}) = \varnothing \quad \text{for all } v_m \text{ of the second type} \Big\}.$$

Lemma 3.8 proves that the union of the sets $\mathcal{V}$ associated with all elements of M is equal to $\widetilde{U}_{m,s}$. Lemma 3.7 proves conditions (i) and (ii). □

We fix a certain set $\mathcal{V}$ from Lemma 3.12 with the basis $(Z_0, \ldots, Z_n)$. We write each polynomial ψ_j as an element of $F(C, u_1, \ldots, u_r)[Z_0, \ldots, Z_n]$, h_{α_s} as an element of $F[u_1, \ldots, u_r, Z_0, \ldots, Z_n]$ and we write $\mathcal{V}$ as an intersection of the following sets (for all nodes v_m of the second type):

$$\mathcal{V}_{v_m} := \{ a \in \widetilde{U}_{m,s}, \quad \mathcal{W}_{v_m}^{(a)} \cap V(Z_0, \ldots, Z_{n-m-1}) = \varnothing \}.$$

Let $F' := F(t_1, \ldots, t_{n-m-1})$ and for any node v_m of the second type, we define a parametric polynomial system S_{v_m} by:

$$S_{v_m} : \begin{cases} \psi_j(Z_0, t_1 Z_0, \ldots, t_{n-m-1} Z_0, Z_{n-m}, \ldots, Z_n) = 0, & 1 \le j \le N \\ h_{\alpha_s}(Z_0, t_1 Z_0, \ldots, t_{n-m-1} Z_0, Z_{n-m}, \ldots, Z_n) = 0 \end{cases}$$

For any $a \in \mathcal{V}$, we denote by $S_{v_m}^{(a)}$ the polynomial system with coefficients in $\overline{F'}$ obtained from S_{v_m} by specialization of its equations on (c, a), where c is a root of $\chi^{(a)} \in \overline{F}[C]$. This system is zero-dimensional in $P^{m+1}(\overline{F'})$ and has no solutions at infinity by Lemma 3.7.

Theorem 3.13. *Under the above hypotheses and notations, there is an algorithm which decomposes each set $\mathcal{V}_{v_m}$ into $(\delta d d_1)^{r^3 d^{O(m^2 n)}}$ constructible sets such that for each set $\mathcal{E}$ among them, it computes polynomials $\mathcal{B}_{n-m}, \ldots, \mathcal{B}_n \in F'(C,u)[Z]$ of degrees w.r.t. Z bounded by $d^{O(m^2)}$ and a polynomial $\chi_2 \in F(u)[C]$. For any $a \in \mathcal{E}$, there exists $c \in \overline{F}$, a root of $\chi_2^{(a)}$ such that the denominators of the coefficients of $\mathcal{B}_{n-m}, \ldots, \mathcal{B}_n$ do not vanish on (c,a) and the following property holds.*

The solution set of the system $S_{v_m}^{(a)}$ is decomposed into $d^{O(m^2 n)}$ classes $\mathcal{S}$ of solutions. For each class $\mathcal{S}$, the algorithm computes a polynomial $\Gamma \in F(C,u)[t_1, \ldots, t_{n-m-1}, Z]$ such that a parametric representation of elements of $\mathcal{S}$ is given by

$$\Gamma^{(c,a)}(\eta) = 0, \quad \begin{cases} \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu} & = & \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ & \vdots & \\ \left(\frac{Z_n}{Z_0}\right)^{p^\mu} & = & \mathcal{B}_n^{(c,a)}(\eta) \end{cases}$$

Moreover, the following bounds on the degrees and the binary lengths hold:

- $\deg_C(\mathcal{B}_j) \leq \delta d^{O(m^3 d)}$ *and* $\deg_C(\Gamma), \deg_C(\chi_2) \leq \delta^{O(r^2)} d^{r^2 d^{O(m^2 n)}}$.
- $\deg_u(\mathcal{B}_j), \deg_{T_1,\ldots,T_l}(\mathcal{B}_j) \leq d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$.
- $\deg_u(\Gamma), \deg_u(\chi_2), \deg_{T_1,\ldots,T_l}(\Gamma)$, $\deg_{T_1,\ldots,T_l}(\chi_2) \leq d_2 \delta^{O(r^3)} d^{r^3 d^{O(m^2 n)}}$.
- $\deg_{t_1,\ldots,t_{n-m-1}}(\mathcal{B}_j), \deg_{t_1,\ldots,t_{n-m-1}}(\Gamma) \leq d^{O(m^2 n)}$.
- $l(\mathcal{B}_j) \leq (M_1 + M_2) d_2 \delta^{O(r^2)} d^{O(m^3 r^2 d^2)}$, $l(\Gamma), l(\chi_2) \leq (M_1 + M_2) d_2 \delta^{O(r^3)} d^{r^3 d^{O(m^2 n)}}$.

Proof. We apply the algorithm of Theorem 1.9 to the zero-dimensional parametric polynomial system S_{v_m}. This algorithm gives a finite partition of $\mathcal{V}_{v_m}$ into constructible sets such that for each set $\mathcal{A}$ among them, it computes polynomials $\Lambda, \mathcal{B}_{n-m}, \ldots, \mathcal{B}_n \in F'(C,u)[Z]$. For any $a \in \mathcal{A}$, there exists $c \in \overline{F}$, a root of $\chi^{(a)}$ such that the solutions of $S_{v_m}^{(a)}$ are given by:

$$\Lambda^{(c,a)}(\eta) = 0, \quad \begin{cases} \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu} & = & \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ & \vdots & \\ \left(\frac{Z_n}{Z_0}\right)^{p^\mu} & = & \mathcal{B}_n^{(c,a)}(\eta) \end{cases}$$

The bounds on the degrees and on the binary lengths of $\mathcal{B}_j$ and Λ follow from Theorem 1.9 taking into account those of the equations of S_{v_m} by the induction hypothesis.

We can write Λ in the form $\Lambda = \frac{\Lambda_1}{\Lambda_2}$ where

$$\Lambda_1 \in F(C,u)[t_1,\ldots,t_{n-m-1},Z], \quad \Lambda_2 \in F[t_1,\ldots,t_{n-m-1}].$$

We apply the algorithm of Theorem 2.14 to the parametric multivariate polynomial Λ_1 in the variables $t_1,\ldots,t_{n-m-1},Z$. This algorithm decomposes $\mathcal{A}$ into constructible sets such that for each set $\mathcal{G}$ among them, it computes $d^{O(m^2n)}$ polynomials $G \in F(C,u)[t_1,\ldots,t_{n-m-1},Z]$ and a polynomial $\chi_1 \in F(u)[C]$ such that for any $a \in \mathcal{G}$, there exists $c \in \overline{F}$, a root of $\chi_1^{(a)}$ which satisfies:

$$\Lambda_1^{(c,a)} = \prod_G G^{(c,a)}, \quad G^{(c,a)} \text{ is absolutely irreducible.}$$

We apply now the algorithm of [28] for computing parametric greatest common divisor (gcd) of χ and χ_1 in $F(u)[C]$. It decomposes again $\mathcal{G}$ into constructible sets $\mathcal{E}$, each of them with a parametric gcd $\chi_2 \in F(u)[C]$, i.e., for any $a \in \mathcal{E}$, the polynomial $\chi_2^{(a)}$ is a gcd of $\chi^{(a)}$ and $\chi_1^{(a)}$ in $\overline{F}[C]$.

For any polynomial G, one takes $\Gamma := \frac{G}{\Lambda_2} \in F'(C,u)[Z]$, these polynomials divide the solution set of the system $S_{v_m}^{(a)}$ in the sense of Theorem 3.13. The number of elements of the partition of $\mathcal{V}_{v_m}$ and the bounds on the degrees and the binary lengths follow from Theorems 1.9, 2.14, and from [28]. □

3.4.3. Construction of parametric effective generic point for any component $W_{wm}^{(a)}$

We fix a certain constructible set $\mathcal{E}$ of Theorem 3.13. For any couple $(c,a) \in \overline{F} \times \mathcal{E}$, where c is a root of $\chi_2^{(a)}$, one considers the coordinate ring of the affine variety $\mathcal{W}_{v_m}^{(a)} \cap \{Z_0 \neq 0\}$ over $\overline{F}$:

$$A = \overline{F}[\mathcal{W}_{v_m}^{(a)} \cap \{Z_0 \neq 0\}] = \overline{F}\Big[Z_1,\ldots,Z_n\Big] \Big/ \Big(\psi_1^{(c,a)}(1,Z_1,\ldots,Z_n) \\ ,\ldots,\psi_N^{(c,a)}(1,Z_1,\ldots,Z_n), h_{\alpha_s}^{(a)}(1,Z_1,\ldots,Z_n)\Big)$$

Let $P = \overline{F}[Z_1,\ldots,Z_{n-m-1}] \setminus \{0\} \subset A$ be a multiplicatively closed subset and $P^{-1}A$ be the localization of A at P. The following lemma is an adaptation of Lemma 2.5 of [27] to the parametric case.

Lemma 3.14. *Under the above notations, there exist bijective correspondences between the following three sets:*

(1) *The set of absolutely irreducible components $W_{w_m}^{(a)}$ of the variety $\mathcal{W}_{v_m}^{(a)}$, i.e., the set of all sons w_m of the node v_m of $T^{(a)}$.*

(2) *The set of classes of homomorphisms of algebras $P^{-1}A \longrightarrow \overline{F'}$ having the same kernel over the field $F' = F(t_1, \ldots, t_{n-m-1})$.*

(3) *The set of classes $(\mathcal{S}, \Gamma^{(c,a)})$ of the system $S_{v_m}^{(a)}$ (see Theorem 3.13).*

Corllary 3.15. *Under the above notations, we can construct an effective generic point for any component $W_{w_m}^{(a)}$ of the variety $\mathcal{W}_{v_m}^{(a)}$. The bounds on the degrees and the binary lengths of the expressions involved in its representation are as in Theorem 3.15.*

Proof. Let w_m be a son of v_m. By Lemma 3.14, we associate to it a class $(\mathcal{S}, \Gamma^{(c,a)})$ of solutions of the system $S_{v_m}^{(a)}$ and a homomorphism of F'-algebra $\sigma : P^{-1}A \longrightarrow \overline{F'}$ of kernel $P^{-1}I_{w_m}$. Then there is a homomorphism $P^{-1}A/P^{-1}I_{w_m} \longrightarrow \overline{F'}$ and one has the following coincidence of fields

$$\overline{F'}[\eta] = \overline{F'}\Big[\sigma(Z_{n-m})^{p^\mu}, \ldots, \sigma(Z_n)^{p^\mu}\Big],$$

where η is a root of $\Gamma^{(c,a)}$. Thus, one has the following field isomorphism:

$$\overline{F'}[\eta] \simeq \overline{F}\left(\frac{Z_1}{Z_0}, \ldots, \frac{Z_{n-m-1}}{Z_0}, \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu}, \ldots, \left(\frac{Z_n}{Z_0}\right)^{p^\mu}\right) \subset \overline{F}(W_{w_m}^{(a)}).$$

This isomorphism is defined by the following expressions:

$$\Gamma^{(c,a)}(\eta), \quad \begin{cases} \frac{Z_1}{Z_0} & = & t_1 \\ & \vdots & \\ \frac{Z_{n-m-1}}{Z_0} & = & t_{n-m-1} \\ \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu} & = & \mathcal{B}_{n-m}^{(c,a)}(\eta) \\ & \vdots & \\ \left(\frac{Z_n}{Z_0}\right)^{p^\mu} & = \mathcal{B}_n^{(c,a)}(\eta). & \end{cases} \qquad (*)$$

The complexity bounds are given in the statement of Theorem 3.13. □

3.4.4. Construction of parametric representative system for any component $W_{w_m}^{(a)}$

We fix a son w_m of the node v_m, of the second type and a couple $(c,a) \in \overline{F} \times \mathcal{E}$, where c is a root of $\chi_2^{(a)}$. We associate to them a vector subspace Ω_{w_m} of the space of homogeneous polynomials from $\overline{F}[Z_0,\ldots,Z_n]$ of degrees d^{m+1} which is defined by:

$$\Omega_{w_m} := \Big\{ g \in \overline{F}[Z_0,\ldots,Z_n] \ \text{ homogeneous} \\ \deg(g) = d^{m+1},\ g \equiv 0 \ \text{ on } \ W_{w_m}^{(a)} \}.$$

We have $W_{w_m}^{(a)} \subset V(\Omega_{w_m})$, where $V(\Omega_{w_m}) \subset P^n(\overline{F})$ is the set of common zeros of all polynomials of Ω_{w_m}. To prove the equality between these two varieties, we will use the following lemma [32, 27].

Lemma 3.16. *Let $W_1 \subset W_2 \subset P^n(\overline{F})$ be two projective varieties with $\deg(W_1) \leq d$. Then there exists a homogeneous polynomial $g \in \overline{F}[Z_0,\ldots,Z_n]$ of degree $\leq d$ which vanishes identically on W_1. Moreover, for any absolutely irreducible component W_3 of W_2 which is not an absolutely irreducible component of W_1, one has $\dim(W_3 \cap V(g)) = \dim(W_3) - 1$.*

Proposition 3.17.

$$W_{w_m}^{(a)} = V(\Omega_{w_m}).$$

Proof. Suppose that there exists an element $\xi \in V(\Omega_{w_m})$ and $\xi \notin W_{w_m}^{(a)}$. We apply Lemma 3.16 to the varieties $W_1 := W_{w_m}^{(a)}$ and $W_2 := W_{w_m}^{(a)} \cup \{\xi\}$ with $\deg(W_{w_m}^{(a)}) \leq \deg(\mathcal{W}_{v_m}^{(a)}) \leq d^{m+1}$ then there exists a polynomial $g \in \Omega_{w_m}$ and so $g(\xi) = 0$, thus g vanishes identically on W_2 and for any absolutely irreducible component W_3 of W_2, one has $W_3 \cap V(g) = W_3$, this is a contradiction with Lemma 3.16. □

Lemma 3.18. *Under the above hypotheses, there is an algorithm which decomposes $\mathcal{E}$ into $d^{O(m^2n^2)}$ constructible sets $\mathcal{F}$. For each $\mathcal{F}$, it computes a parametric representative system $\Psi_1,\ldots,\Psi_M \in F(C,u)[Z_0,\ldots,Z_n]$ of W_{w_m}. The bounds on the degrees and the binary lengths of these polynomials are as in Theorem 3.5.*

Proof. Proposition 3.17 proves that if $\{g_1,\ldots,g_M\}$ is a basis of Ω_{w_m}

then

$$W_{w_m}^{(a)} = V(g_1, \ldots, g_M), \quad \text{where} \quad M := \dim_{\overline{F}}(\Omega_{w_m})$$
$$\leq \binom{n + d^{m+1}}{n} \leq (3d^{m+1})^n \leq d^{O(mn)}.$$

Lemma 0.2 proves that a polynomial $g \in \overline{F}[Z_0, \ldots, Z_n]$ of degree d^{m+1} is an element of Ω_{w_m} if and only if

$$g\left(1, t_1, \ldots, t_{n-m-1}, \left(\frac{Z_{n-m}}{Z_0}\right)^{p^\mu}, \ldots, \left(\frac{Z_n}{Z_0}\right)^{p^\mu}\right) = 0$$
$$\text{in} \quad \overline{F}(t_1, \ldots, t_{n-m-1})[\eta],$$

where the expressions of the rational functions $\left(\frac{Z_i}{Z_0}\right)^{p^\mu}$ are given by the isomorphism (*) from the end of the proof of Corollary 3.15 which defines an effective generic point of $W_{w_m}^{(a)}$. This equation defines a parametric homogeneous linear system by taking all coefficients of the monomials in $t_1, \ldots, t_{n-m-1}, \eta$ equals to zero. We apply the parametric Gaussian algorithm [32] to this system, it decomposes $\mathcal{E}$ into $d^{O(m^2n^2)}$ constructible sets such that for each set $\mathcal{F}$ among them, it computes polynomials $\Psi_1, \ldots, \Psi_M \in F(C, u)[Z_0, \ldots, Z_n]$ such that for any $a \in \mathcal{U}$, there exists $c \in \overline{F}$, a root of $\chi_2^{(a)} \in \overline{F}[C]$ satisfying the following property. The vectors of coefficients of $\Psi_1^{(c,a)}, \ldots, \Psi_M^{(c,a)} \in \overline{F}[Z_0, \ldots, Z_n]$ form a basis of the solution set Ω_{w_m} of the above parametric homogeneous linear system. □

3.5. Complexity analysis of the algorithm of Theorem 3.5

We analyze here the complexity bound of the step $m+1$ of the induction. Indeed, the complexity of the construction of the $\mathcal{N} = (k-1)d^m + 1$ sets $\widetilde{U}_{m,s}$ is just that of the quantifier elimination algorithm [10], it is $(\delta d_1 d_2)^{O(r^2 l)} d^{O(mr^2 l d^2)}$.

The complexity of the construction of all sets $\mathcal{E}$ of Theorem 3.13 is determined by those of the algorithm of solving zero-dimensional parametric polynomial systems applied to the system S_{v_m} (Theorem 1.9) and the algorithm of absolute factorization of parametric polynomials (Theorem 2.14). By taking into account the bounds established in Theorem 3.13, this complexity is bounded by:

$$(\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(m^2 n)}}.$$

This bound is double exponential in m^2n because that of Theorem 2.14 is single exponential in the degree of the factorized polynomials (here this degree is $d^{O(m^2n)}$).

When we pass from the step m to the step $m+1$ of the induction, the bounds pass from single exponential to double exponential. This follows from Theorem 2.14 as above, but the degree of the factorized parametric polynomial Λ_1 is still equal to $d^{O(m^2n)}$ for any step of the induction. Then at the final step of the induction, these bounds still are double exponential in n. Thus the number of arithmetic operations in H of the algorithm is

$$(\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(n^3)}}$$

and its binary complexity is

$$(pM_1M_2)^{O(1)} (\delta d_1 d_2)^{O(r^4 l)} d^{r^4 l d^{O(n^3)}}.$$

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

References

1. A. Ayad, *Complexity bound for the absolute factorization of parametric polynomials.* — Zap. Nauchn. Semin. POMI **316**, *Teor. Slozhn. Vychisl.* **9, 224** (2004), 5–29.
2. A. Ayad, *Complexité de la résolution des systèmes algébriques paramétriques.* PhD thesis, University of Rennes 1, France, October 2006.
3. S. Basu, R. Pollack, M-F. Roy, *Algorithms in real algebraic geometry.* Springer, New York, 2003.
4. E. R. Berlekamp, *Factoring polynomials over finite fields.* — Bell Systems Tech. J. **46** (1967), 1853–1859.
5. E. R. Berlekamp, *Factoring polynomials over large finite fields.* — Math. Comp. **24** (1970), 713–735.
6. B. Buchberger, *Gröbner Bases: An algorithmic method in polynomial ideal theory.* — In: Multidimensional System Theory (N. K.Bose et al., eds), Reidel, Dordrecht (1985), pp. 374–383.
7. G. Chèze, G. Lecerf, *Lifting and recombination techniques for absolute factorization.* Manuscript, Universit de Versailles Saint-Quentin-en-Yvelines, 2005.
8. A. L. Chistov, *Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time.* — J. Sov. Math. **34** (1986), No. 4, 1838–1882.

9. 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.
10. A. Chistov, D. Grigoriev, *Complexity of quantifier elimination in the theory of algebraically closed fields.* — LNCS **176** (1984), 17–31.
11. A. Chistov, D. Grigoriev, *Polynomial-time factoring of the multivariable polynomials over a global field.* Preprint LOMI E-5-82, Leningrad, 1982.
12. A. Chistov, H. Fournier, L. Gurvits, P. Koiran, *Vandermonde Matrices, NP-Completeness, and Transversal Subspaces.* — Found. Computat. Math. **3(4)** (2003), 421–427.
13. D. Cox, J. Little, D. O'shea,] *Ideals, Varieties, and Algorithms.* Second Edition, Springer, 1997.
14. D. Cox, J. Little, D. O'shea, *Using Algebraic Geometry.* Springer, 1998.
15. X. Dahan, E. Schost, *Sharp estimates for triangular sets.* Proceedings ISSAC, 2004.
16. A. Dickenstein, L. Z. Emiris, *Solving Polynomial Equations, Foundations, Algorithms, and Applications.* Springer, 2005.
17. D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry.* Springer, New York, 1995.
18. K. Gatermann, X. Bincan, *Existence of* 3 *Positive Solutions of Systems from Chemistry.* July, 2003.
19. S. Gao, *Factoring multivariate polynomials via partial differential equations.* — Amer. Math. Soc. **72**, No. 242 (2003), 801–822.
20. S. Gao, E. Kaltofen, J. May, Z. Yang, L. Zhi, *Approximate factorization of multivariate polynomials via differential equations.* ISSAC, Spain (2004), 167–174.
21. X-S. Gao, S-C. Chou, *Solving parametric algebraic systems.* ISSAC, California USA (1992), 335–341.
22. M. Giusti, E. Schost, *Solving some overdetermined polynomial systems.* — In: Proc. of the 1999 International Symposium on Symbolic and Algebraic Computation (Vancouver, BC), (electronic), ACM, New York (1999), pp. 1–8.
23. M. Giusti, J. Heintz, K. Hagele, J. E. Morais, L. M. Pardo, J. l. Montana, *Lower bounds for diophantine approximations.* — J. Pure Applied Algebra **117, 118** (1997), 277–317.
24. M. Giusti, G. Lecerf, B. Salvy, *A Gröbner free alternative for polynomial system solving.* — J. Complexity **17**, No. 1 (2001), 154–211.
25. M.-J. Gonzalez-Lopez, L. Gonzalez-Vega, C. Traverso, A. Zanoni, *Parametric.* Report Research, The FRISCO Consortium, 2000.
26. 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 Arjeh M. (ed.), Cohen, Wiley (1991), pp. 117–141.
27. D. Grigoriev, *Factorization of polynomials over a finite field and the solution of systems of algebraic equations.* — J. Sov. Math. **34** (1986), No. 4, 1762–1803.
28. D. Grigoriev, *Complexity of quantifier elimination in the theory of ordinary differential equations.* — Lect. Notes Comp. Sci. **378** (1989), 11–25.
29. D. Grigoriev, N. Vorobjov, *Bounds on numbers of vectors of multiplicities for polynomials which are easy to compute.* — In: Proc. ACM Intern. Conf. Symb and Algebraic Computations, Scotland (2000), pp. 137–145.

30. D. Grigoriev, *Constructing double–exponential number of vectors of multiplicities of solutions of polynomial systems.* — In: Contemporary Math., AMS **286** (2001), pp. 115–120.
31. J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, *Deformation Techniques for efficient polynomial equation solving.* J. Complexity, **16** (2000), 70–109.
32. J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields.* — Theor. Comput. Sci. **24**, No. 3 (1983), 239–277.
33. G. Jeronimo, J. Sabia, *Effective equidimensional decomposition of affine varieties.* — J. Pure Appl. Algebra **169**, No. 2–3 (2002), 229–248.
34. E. Kaltofen, *On the complexity of factoring polynomials with integer coefficients.* PhD thesis, Rensselaer Polytechnic Instit., Troy, N.Y., December, 1982.
35. E. Kaltofen, *Factorization of polynomials. Computer algebra.* 95–113, Springer, Vienna, 1983.
36. E. Kaltofen, V. Shoup, *Subquadratic–time factoring of polynomials over finite fields.* — In: Proc. 27th Annual ACM Symp. Theory Comput., New York, N.Y., 1995. ACM Press, pp. 398–406.
37. E. Kaltofen, *Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization.* — SIAM J. Comput. **14**, No. 2 1985, 469–489.
38. T. Krick, L. M. Pardo, *A computational method for diophantine approximation.* Algorithms Algebraic Geometry Applications, Santander (1994), 193–253.
39. S. Lang, *Algebra.* Addison–Wesley, 1993.
40. D. Lazard, *Algèbre linéaire sur $k[X_1, \ldots, X_n]$ et élimination. Bull. Soc. Math. France* **105** (1977), 165–190.
41. D. Lazard, *Résolution des systèmes d'équations algébriques.* — Theo. Comput, Sci. **15** (1981), 77–110.
42. D. Lazard, *On the specification for solvers of polynomial systems.* — In: 5th Asian Symposium on Computers Mathematics – ASCM (2001), Matsuyama, Japan Lect. Notes Series Computing **9**, World Scientific (2001), pp. 66–75.
43. D. Lazard, F. Rouillier, *Solving parametric polynomial systems.* — J. Symb. Comput. **42**, No. 6 (2007), 636–667.
44. 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), pp. 1–8.
45. D. Lazard, *Solving zero-dimensional algebraic systems.* J. Symb. Comput. **13** (1992), 117–131.
46. G. Lecerf, *Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions.* — In: Proceedings of International Symposium on Symbolic and Algebraic Computation Symbolic and Algebraic Computation, St.Andrews, Scotland (July 2000), pp. 209–216.
47. G. Lecerf, *Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers.* — J. Complexity **19**, No. 4 (2003), 564–596.
48. A. K. Lenstra, H. W. Jr. Lenstra, L. Lovasz, *Factoring polynomials with rational coefficients.* — Math. Ann. **261** (1982), No. 4, 515–534.
49. A. K. Lenstra, *Factoring multivariate polynomial over finite fields.* — J. Comput. System Sci. **30** (1985), No. 2, 235–248.
50. A. K. Lenstra, *Factoring multivariate polynomials over algebraic number fields.* — SIAM J. Comput. **16** (1987), 591–598.

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

52. A. Montes, *A new algorithm for discussing Gröbner basis with parameters.* — J. Symb. Comp. **33** (2002), 183–208.

53. T. Mora, *Solving Polynomial Equation Systems I. The Kronecker–Duval Philosophy.* Encyclopedia of Mathematics and its Applications **88**, Cambridge University Press, 2003.

54. G. Moroz, *Complexity of the Resolution of Parametric Systems of Equations and Inequations.* ISSAC, Genova, Italy, 2006.

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

56. H. Niederreiter, *Factorization of polynomials and some linear–algebra problems over finite fields.* — Linear Algebra Applications **192** (1993), 301–328.

57. K. Rimey, *A system of polynomial equations and a solution by an unusual method.* — SIGSAM Bulletin **18**, No. 1 (1984), 30–32.

58. F. Rouillier, *Solving zero–dimensional polynomial systems through the rational univariate representation.* — Appl. Alg. Eng. Comm. Comput. **9**, No. 5 (1999), 433–461.

59. E. Schost, *Computing parametric geometric resolutions.* — Appl. Alg. Eng. Commun. Comput. **13**, No. 5 (2003), 349–393.

60. E. Schost, *Sur la résolution des systèmes polynomiaux à paramètres.* — Thèse de doctorat, École polytechnique, décembre, 2000.

61. E. Schost, *Complexity results for triangular sets.* — J. Symb. Comput. **36**, No. 3–4 (2003), 555–594.

62. I. R. Shafarevich, *Basic Algebraic Geometry.* Springer, 1974.

63. W. Y. Sit, *An algorithm for solving parametric linear systems.* — J. Symb. Comput. **13** (1992), 353–394.

64. W. Y. Sit, *A theory for parametric linear systems.* — In: Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, Bonn, West Germany (1991), pp. 112–121.

65. B. L. Van Der Waerden, *Modern algebra.* Vol. 2, 1950.

66. J. von zur Gathen, J. Gerhard, *Modern Computer algebra.* Cambridge University Press, 1999.

67. J. von zur Gathen, E. Kaltofen, *Factorization of multivariate polynomials over finite fields.* — Math. Comp. **45**, No. 171 (1985), 251–261.

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

69. V. Weispfenning, *Comprehensive Gröbner bases.* — J. Symb. Comput. **14** (1991), 1–29.

70. 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), pp. 163–179.

71. O. Zariski, P. Samuel, *Commutative Algebra*. Vol. 1, Springer–Verlag, 1958; Vol. 2 Springer–Verlag, 1976.
72. H. Zassenhaus, *On Hensel factorization*. — J. Number Theory **1** (1969), 291–311.

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

E-mail: ayadali99100@hotmail.com

Поступило 20 января 2011 г.