ELSEVIER

Journal of Pure and Applied Algebra 169 (2002) 229–248

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Effective equidimensional decomposition of affine varieties

Gabriela Jeronimo *,[1], Juan Sabia [1]

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pab. I, (1428), Buenos Aires, Argentina

Received 11 September 2000; received in revised form 28 February 2001
Communicated by M.-F. Roy

Abstract

In this paper we present a probabilistic algorithm which computes, from a finite set of polynomials defining an algebraic variety V, the decomposition of V into equidimensional components. If V is defined by s polynomials in n variables of degrees bounded by an integer $d \geqslant n$ and $V = \bigcup_{\ell=0}^{r} V_\ell$ is the equidimensional decomposition of V, the algorithm obtains in sequential time bounded by $s^{O(1)} d^{O(n)}$, for each $0 \leqslant \ell \leqslant r$, a set of $n+1$ polynomials of degrees bounded by $\deg(V_\ell)$ which define V_ℓ.

MSC: Primary 14Q20; secondary 68W30

0. Introduction

Different problems appearing nowadays are related to systems of polynomial equations. Some of these problems can be solved simply by deciding whether the associated polynomial equation system is consistent or not. However, when the system is consistent, it is sometimes necessary to describe the set of its solutions. The set of solutions of a polynomial equation system is called an *algebraic variety*.

A well-known result states that any algebraic variety V over an algebraically closed field K can be uniquely decomposed into a union of irreducible algebraic varieties $C_1, \ldots, C_t$ definable by polynomials with coefficients in K such that $C_i \not\subseteq C_j$ for $i \neq j$.

* Corresponding author.
E-mail addresses: jeronimo@dm.uba.ar (G. Jeronimo), jsabia@dm.uba.ar (J. Sabia).

[1] Partially supported by the following Argentinian research grants: CONICET: PIP '97 4571; UBACyT: EX TW80 (1998).

0022-4049/02/$ - see front matter
PII: S0022-4049(01)00083-4

The varieties C_i are called the *irreducible components* of V. Therefore, a possible way to describe the variety V is to characterize each of the irreducible components of V. However, if V is defined by polynomials with coefficients in a subfield k of the algebraically closed field K, its irreducible components may not be definable by polynomials with coefficients in k. Then, this description of the variety is not entirely satisfactory from the algorithmic point of view.

One of the invariants related to an algebraic variety is its dimension. An algebraic variety may have irreducible components of different dimensions. When all the components of an algebraic variety have the same dimension it is called *equidimensional*. Any algebraic variety V can be decomposed into a union of equidimensional varieties. If $r = \dim V$ and, for each $0 \leqslant \ell \leqslant r$, V_ℓ is either empty or the union of all the irreducible components of V of dimension ℓ, then $V = \bigcup_{\ell=0}^{r} V_\ell$. This is called the *equidimensional decomposition* of V and the varieties V_ℓ $(0 \leqslant \ell \leqslant r)$ are called its *equidimensional components*. The problem we are concerned with is the computation of the equidimensional decomposition of V in the following way: given polynomials $f_1, \ldots, f_s$ in $k[X_1, \ldots, X_n]$ such that $V = \{x \in \bar{k}^n : f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}$ we want to obtain, for every $0 \leqslant \ell \leqslant r$, a finite set of polynomials whose set of common zeroes is V_ℓ, where k is a field of characteristic 0 and $\bar{k}$ is an algebraic closure of k.

Different algorithms describing decompositions of an algebraic variety V have been given. Chistov and Grigor'ev [1] exhibit an algorithm for the computation of the irreducible decomposition provided an algorithm that factorizes polynomials in $k[X_1, \ldots, X_n]$ is given. Giusti and Heintz [3] present an algorithm for the equidimensional decomposition which is well-parallelizable. In both cases, if V is given as the set of common zeroes of s polynomials in n variables with degrees bounded by d, the complexity bounds of the algorithms are of order $s^{O(1)}d^{O(n^2)}$. Elkadi and Mourrain [2] give a probabilistic algorithm which is based on Bézoutian matrices, but the decomposition they obtain is not minimal (some embedded components may appear).

After the works of Chistov and Grigor'ev and Giusti and Heintz, the natural next step was to obtain algorithms which solve the same task within a complexity of order $s^{O(1)}d^{O(n)}$. In this work, we present a probabilistic algorithm that, from a finite set of n-variate polynomials whose set of common zeroes is an algebraic variety V, computes, for each equidimensional component V_ℓ of V, a set of $n+1$ polynomials of degrees bounded by $\deg V_\ell$ whose set of common zeroes is V_ℓ. The algebraic complexity of our algorithm is bounded by $s^{O(1)}d^{O(n)}$, where s is the number of input polynomials, n the number of variables and $d \geqslant n$ an integer which is an upper bound for the degrees of the input polynomials. The algorithm is based on computing for each of the equidimensional components of the variety considered, the minimal polynomials of $n+1$ linear forms.

Lecerf [13] shows a probabilistic algorithm which describes the equidimensional decomposition of V by means of geometric resolutions of each equidimensional component. Lecerf's work has been done simultaneously with ours but both works are independent. One of the main differences among the above cited works is the way the equidimensional components are given: In [2] and [13] the varieties are described in

a parametric way and this description is generic; in the work of Giusti and Heintz and in this paper, the varieties are given as the set of common zeroes of a system of polynomials. This last description is more accurate. Chistov and Grigor'ev [1] use descriptions of both types.

The lower complexity of our algorithm is due to a special way of coding output polynomials, called straight line programs, which showed to be effective in the construction of algorithms to solve many algebraic and geometric problems (see, for example, [4–6]).

The paper is organized in three sections. In the next section we recall some basic definitions, we fix the notation and mention some algorithmic tools to be used. In Section 2 we show that the input data can be changed so that our algorithm works (these changes will be done randomly and, in this sense, we say our algorithm is probabilistic). In the last section, we state precisely how we will describe equidimensional varieties and finally we prove the main result of the paper:

Let $f_1,\dots,f_s \in k[X_1,\dots,X_n]$ *be polynomials and let* d *be an integer such that* $d \geqslant n$ *and* $\deg f_i \leqslant d$ *for every* $1 \leqslant i \leqslant s$. *Let* $V = \{x \in \bar{k}^n\colon f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}$ *and let* $r = \dim V$. *Then, there exists a probabilistic algorithm of sequential complexity of order* $s^{O(1)}d^{O(n)}$, *which computes the equidimensional decomposition of* V: *the input of the algorithm are the polynomials* $f_1,\dots,f_s$ *given in dense form and its output is a straight line program of length* $d^{O(n)}$ *which computes polynomials* $g_j^{(\ell)}$ $(0 \leqslant \ell \leqslant r, 1 \leqslant j \leqslant n+1)$ *such that, for every* $0 \leqslant \ell \leqslant r$, *the equidimensional component of* V *of dimension* ℓ *is*

$$V_\ell = \{x \in \bar{k}^n\colon g_1^{(\ell)}(x) = 0 \wedge \cdots \wedge g_{n+1}^{(\ell)}(x) = 0\}.$$

For every $0 \leqslant \ell \leqslant r$, *the degrees of* $g_j^{(\ell)}$ $(1 \leqslant j \leqslant n+1)$ *are bounded by* $\deg V_\ell \leqslant d^{n-\ell}$.

The probability of success of each step of our algorithm will appear in several remarks throughout the paper. In a final remark, after the proof of the main theorem, the probability of success of the whole algorithm is stated.

A summary of the results obtained in this work can be found in [10].

1. Preliminaries

1.1. Definitions and notation

Let k be a field of characteristic 0. We suppose k to be effective: this means that the arithmetic operations (addition, subtraction, multiplication) and basic equality checking (comparison) between elements of k are realizable by algorithms.

For any polynomial $f \in k[X]$, $\mathrm{rad}(f)$ will denote the monic square-free polynomial in $k[X]$ whose zeroes are exactly the zeroes of f.

Given polynomials $g_1,\dots,g_s \in k[X]$, $\gcd(g_1,\dots,g_s)$ will denote, as usual, the greatest common divisor of $g_1,\dots,g_s$.

If $X_1,\ldots,X_n$ are indeterminates over k and $f \in k[X_1,\ldots,X_n]$ is a polynomial, its total degree will be denoted by $\deg f$.

Let $\bar{k}$ be an algebraic closure of k. We denote by $\mathbb{A}^n(\bar{k})$ (or $\mathbb{A}^n$) the n-dimensional affine space over $\bar{k}$, equipped with its Zariski topology.

For any $I \subset k[X_1,\ldots,X_n]$, we denote by $V(I)$ the affine variety of $\mathbb{A}^n(\bar{k})$ formed by the common zeroes of all the polynomials which belong to I. Given polynomials $f_1,\ldots,f_s$, the variety $V(f_1,\ldots,f_s) \subseteq \mathbb{A}^n$ will be called the variety *defined by* $f_1,\ldots,f_s$.

If V is an affine variety in $\mathbb{A}^n(\bar{k})$, we denote by $I(V)$ the ideal in $\bar{k}[X_1,\ldots,X_n]$ of the polynomials vanishing over V.

The dimension of an algebraic variety V defined over k will be denoted by $\dim V$.

Let $V \subseteq \mathbb{A}^n$ be an affine variety. We will call the *minimal irreducible decomposition of* V to the representation $V = \bigcup_{i=1}^{t} C_i$, where, for each $1 \leqslant i \leqslant t$, C_i is an irreducible closed set in $\mathbb{A}^n$, and $C_i \not\subseteq C_j$ for $i \neq j$. The varieties C_i will be called the *irreducible components* of V. If $r = \dim V$, we will call the *equidimensional decomposition of* V to the representation $V = \bigcup_{i=0}^{r} V_i$ where, for each $\leqslant i \leqslant r$, V_i is either empty or the union of all the irreducible components of V of dimension i.

We say that the variables $X_1,\ldots,X_n$ are in *Noether position with respect to the variety* V defined over k if the canonical morphism $k[X_1,\ldots,X_r] \to k[X_1,\ldots,X_n]/I(V)$ is an integral monomorphism, where $r = \dim V$. This condition is equivalent to the fact that the canonical projection in the first r coordinates $\pi : V \to \mathbb{A}^r$ is a finite morphism of affine varieties. Note that, if the variety V is equidimensional (i.e., all the irreducible components of V have the same dimension) and the variables are in Noether position with respect to V, then they are in Noether position with respect to each irreducible component of V.

If $V \subseteq \mathbb{A}^n$ is an irreducible closed set of dimension r, the *degree* of V is, as usual,

$$\deg V := \sup\{\#H_1 \cap \cdots \cap H_r \cap V;\ H_1,\ldots,H_r \text{ affine hyperplanes in } \mathbb{A}^n \text{ such that } H_1 \cap \cdots \cap H_r \cap V \text{ is a finite set}\}.$$

For an arbitrary algebraic variety $V \subseteq \mathbb{A}^n$, $\deg V$ is the sum of the degrees of all the irreducible components of V.

1.2. Probabilistic and algorithmic tools

The algorithms we are going to consider will be described by families of arithmetic networks over k, which are represented by acyclic oriented graphs. The *sequential complexity* of the algorithm is the number of nodes of its associated graph (without taking into account the nodes representing input data). Therefore, the sequential complexity of an algorithm is the number of arithmetic operations and comparisons between elements of k (each operation or comparison is considered to have unitary cost).

The multivariate polynomials we will deal with in our algorithm will be encoded in one of the following ways:

- *Dense form*, that is, as arrays (vectors) of elements of k.

- *Straight line programs*, which are arithmetic circuits (networks without branches). They contain neither selectors nor (propositional) Boolean operations. (For an exact definition and elementary properties of the notion of straight line program we refer to [8] and [9].)
- Combining both dense form and straight line programs, i.e. in dense form with respect to some distinguished variables and their coefficients, which are polinomials in the remaining ones, encoded by a straight line program.

The algorithm for the computation of the equidimensional decomposition of an affine variety we describe in this paper is based on the well-known methods of effective linear algebra which rely on well-parallelizable algorithms without divisions and on the techniques used in [4,11] to describe the isolated points of an algebraic variety. The main result of these works we use is the following (see [4, Section 3.4.7; 11, Proposition 27]):

Lemma 1. *Let R be a polynomial ring over k and let K be an algebraic closure of the quotient field of R. Let $f_1,\dots,f_n \in R[X_1,\dots,X_n]$ be polynomials of degree (in $X_1,\dots,X_n$) bounded by $d \geqslant n$ given in dense form with respect to $X_1,\dots,X_n$. Let $V \subset K^n$ denote the variety defined by these polynomials. Then, there exists an algorithm of complexity bounded by $d^{O(n)}$ that computes a linear form $u = \lambda_1 X_1 + \cdots + \lambda_n X_n \in k[X_1,\dots,X_n]$, an element $\rho \in R$ and univariate polynomials $v_i \in R[U]$ $(1 \leqslant i \leqslant n)$ of degrees bounded by $d^{O(n)}$ such that:*

- *The linear form u separates the isolated zeroes of V.*
- *The coordinates $x = (x_1,\dots,x_n)$ of the isolated zeroes of V verify the equations $\rho x_i = v_i(u(x))$ $(1 \leqslant i \leqslant n)$.*

Both ρ and the coefficients of the polynomials v_i $(1 \leqslant i \leqslant n)$ are polynomials in the coefficients of $f_1,\dots,f_n$ of degree bounded by $d^{O(n)}$ and they can be evaluated from them by a straight line program of length $d^{O(n)}$.

Whenever we need to compute quotients of polynomials given by straight line programs we will use Strassen's procedure of Vermeidung von Divisionen ([16], see also [11]).

The algorithm we construct in this paper works under certain generic conditions depending on parameters. The values of these parameters will be chosen randomly (and, in this sense, we say the algorithm is *probabilistic*). In order to estimate the probabilities of success of our computations we will use the following result taken from [15, Lemma 1]:

Lemma 2. *Let E be an integral domain and let $M \subset E$ be a finite set. Let f be a non-zero polynomial in $E[X_1,\dots,X_n]$. Then, for randomly selected $a_1,\dots,a_n \in M$ the probability*

$$\text{Prob}\,(f(a_1,\dots,a_n)=0) \leqslant \frac{\deg(f)}{\text{card}\,(M)}.$$

2. Modifying the input data

2.1. Changing the input polynomials

The first step of our algorithm is to define the affine variety we are considering by means of $n+1$ polynomials. Moreover, we ask these $n+1$ polynomials to satisfy certain additional conditions about dimension. This will be done by choosing random linear combinations of the input polynomials. The existence of these combinations is shown in the following lemma adapted from [4].

Lemma 3. *Let $f_1,\dots,f_s \in k[X_1,\dots,X_n]$ be polynomials and let $V=\{x\in\bar{k}^n\colon f_1(x)=0 \wedge\cdots\wedge f_s(x)=0\}$. Then there exist $t_{ij}\in k$ $(1\leqslant i\leqslant n+1,\ 1\leqslant j\leqslant s)$ such that the polynomials $\hat{f}_1,\dots,\hat{f}_{n+1}$ defined by*

$$\hat{f}_i = t_{i1}f_1+\cdots+t_{is}f_s \quad (1\leqslant i\leqslant n+1)$$

satisfy the following condition:

For every h, $1\leqslant h\leqslant n+1$, the dimension of each irreducible component of

$$V(\hat{f}_1,\dots,\hat{f}_h)=\{x\in\bar{k}^n\colon \hat{f}_1(x)=0\wedge\cdots\wedge\hat{f}_h(x)=0\}$$

not being an irreducible component of V is $n-h$.

Proof. We are going to show the existence of the elements t_{hj} $(1\leqslant h\leqslant n+1, 1\leqslant j\leqslant s)$ by induction on h.

Let T_j $(1\leqslant j\leqslant s)$ be indeterminates over k.

If $h=1$, let $p\in\mathbb{A}^n-V$ and let $P_1\in k[T_1,\dots,T_s]$ be the polynomial

$$P_1 = T_1f_1(p)+\cdots+T_sf_s(p).$$

Then, for every choice of $t_{11},\dots,t_{1s}$ such that $P_1(t_{11},\dots,t_{1s})\neq 0$, $\hat{f}_1$ satisfies the required condition.

Suppose now that there exist elements t_{ij} $(1\leqslant i\leqslant h, 1\leqslant j\leqslant s)$ satisfying the desired conditions. Consider the variety

$$V(\hat{f}_1,\dots,\hat{f}_h)=\{x\in\bar{k}^n\colon \hat{f}_1(x)=0\wedge\cdots\wedge\hat{f}_h(x)=0\}.$$

Let $\mathscr{C}_h$ be the set of the irreducible components of $V(\hat{f}_1,\dots,\hat{f}_h)$ which are not irreducible components of V. If $\mathscr{C}_h=\emptyset$, any choice of $t_{h+1\,1},\dots,t_{h+1\,s}$ produces a polynomial $\hat{f}_{h+1}$ which satisfies the required condition.

If $\mathscr{C}_h\neq\emptyset$, for every $C\in\mathscr{C}_h$, let p_C be a point in $C-V$. Let $P_{h+1}\in k[T_1,\dots,T_s]$ be the polynomial

$$P_{h+1}=\prod_{C\in\mathscr{C}_h}(T_1f_1(p_C)+\cdots+T_sf_s(p_C)).$$

It is easy to check that this polynomial is not the zero polynomial, and every point $(t_{h+1\,1},\dots,t_{h+1\,s})$ in k^n such that $P_{h+1}(t_{h+1\,1},\dots,t_{h+1\,s})\neq 0$ defines a polynomial $\hat{f}_{h+1}$ that satisfies the desired condition. □

Remark 4. Note that the condition defining suitable t_{1j} $(1 \leqslant j \leqslant s)$ is open and that, for every h $(1 \leqslant h \leqslant n)$, if we have chosen t_{ij} $(1 \leqslant i \leqslant h, 1 \leqslant j \leqslant s)$ such that the polynomials $\hat{f}_1, \ldots, \hat{f}_h$ satisfy the conditions of Lemma 3, the condition on the suitable t_{h+1j} $(1 \leqslant j \leqslant s)$ is also open.

Moreover, if the total degrees of the polynomials $f_1, \ldots, f_s$ are bounded by an integer d, for every h $(1 \leqslant h \leqslant n+1)$, the degree of the polynomial P_h appearing in the proof of Lemma 3 is bounded by d^{h-1}. Then, if we choose the elements t_{ij} $(1 \leqslant i \leqslant n+1, 1 \leqslant j \leqslant s)$ from a subset of k with N elements randomly, the probability that the polynomials $\hat{f}_1, \ldots, \hat{f}_{n+1}$ satisfy the conditions stated in Lemma 3 is at least $\prod_{h=1}^{n+1}(1 - d^{h-1}/N) \geqslant 1 - \sum_{h=1}^{n+1} d^{h-1}/N$.

2.2. Noether position of the variables

Suppose we are given s polynomials $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ with total degrees bounded by an integer $d \geqslant n$. We denote by V the set of their common zeroes in $\mathbb{A}^n$. Applying Lemma 3, by means of a random choice of linear combinations of the input polynomials, we may suppose that we have $n+1$ polynomials $\hat{f}_1, \ldots, \hat{f}_{n+1} \in k[X_1, \ldots, X_n]$ of degrees bounded by d such that:

- $V(\hat{f}_1, \ldots, \hat{f}_{n+1}) = V$.
- For every $0 \leqslant \ell \leqslant n$, the dimension of each irreducible component of $V(\hat{f}_1, \ldots, \hat{f}_{n-\ell})$ not being an irreducible component of V is ℓ.

Let $r := \dim V$ and let $V = \bigcup_{i=0}^{r} V_i$ be the equidimensional decomposition of V, where, for every $0 \leqslant i \leqslant r$, either $V_i = \emptyset$ or $\dim V_i = i$. Note that, if $\ell \leqslant r$, the equidimensional decomposition of $V(\hat{f}_1, \ldots, \hat{f}_{n-\ell})$ is

$$V(\hat{f}_1, \ldots, \hat{f}_{n-\ell}) = V_r \cup \ldots \cup V_{\ell+1} \cup V'_\ell,$$

where $V'_\ell = V_\ell \cup Z_\ell$ and Z_ℓ is either empty or an equidimensional variety of dimension ℓ with no common irreducible components with V_ℓ.

We are now going to choose a random change of variables such that the new variables $\tilde{X}_1, \ldots, \tilde{X}_n$ satisfy:

- The projection $\pi_r : V_r \cup Z_r \to \mathbb{A}^r$ defined by $\pi_r(x) = (\tilde{x}_1, \ldots, \tilde{x}_r)$ is finite.
- For every ℓ $(1 \leqslant \ell \leqslant r-1)$, provided $Z_{\ell+1} \cap \{\hat{f}_{n-\ell} = 0\} \neq \emptyset$, the projection $\pi_\ell : Z_{\ell+1} \cap \{\hat{f}_{n-\ell} = 0\} \to \mathbb{A}^\ell$ defined by $\pi_\ell(x) = (\tilde{x}_1, \ldots, \tilde{x}_\ell)$ is finite.

This means that the new variables $\tilde{X}_1, \ldots, \tilde{X}_n$ will be in Noether position with respect to the varieties $V_r \cup Z_r$ and $Z_{\ell+1} \cap \{\hat{f}_{n-\ell} = 0\}$ for every $1 \leqslant \ell \leqslant r-1$, simultaneously.

The existence of this change of variables is given by the following lemma:

Lemma 5. *Let $W \subseteq \mathbb{A}^n$ be an equidimensional variety defined over k and let ℓ be the dimension of W. Let U_{ij} $(1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant n)$ be indeterminates over $k[X_1, \ldots, X_n]$. Then there exists a polynomial $G \in k[U_{ij}]_{\substack{1 \leqslant i \leqslant \ell \\ 0 \leqslant j \leqslant n}} - \{0\}$ with $\deg G \leqslant 2\ell \deg^2 W$*

such that, if $G(u_{ij}) \neq 0$, *the morphism* $\pi : W \to \mathbb{A}^{\ell}$ *defined by*

$$\pi(x) = (u_{10} + u_{11}x_1 + \cdots + u_{1n}x_n, \ldots, u_{\ell 0} + u_{\ell 1}x_1 + \cdots + u_{\ell n}x_n)$$

is finite.

Proof. It is an immediate consequence of Proposition 4.5 and Lemma 2.13 in [12]. □

The previous lemma gives a condition to obtain free variables, which can be extended to a whole set of variables in Noether position, with respect to an equidimensional variety. In order to get a whole set of new variables, we are going to consider the polynomial $H := \det(U_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$.

Applying Lemma 5 to our situation, there exist

- a polynomial G_r with $\deg G_r \leqslant 2r(\deg(Z_r \cup V_r))^2 \leqslant 2rd^{2(n-r)}$ and,
- for each $\ell = r-1, \ldots, 1$, a polynomial G_{ℓ} with

$$\deg G_{\ell} \leqslant 2\ell(\deg(Z_{\ell+1} \cap \{\hat{f}_{n-\ell} = 0\}))^2 \leqslant 2\ell d^{2(n-\ell)}$$

such that, if $H(u_{ij}).\prod_{\ell=1}^{r} G_{\ell}(u_{ij}) \neq 0$, then the new variables $\tilde{X}_i = u_{i0} + u_{i1}X_1 + \cdots + u_{in}X_n$ $(1 \leqslant i \leqslant n)$ satisfy the desired conditions.

Remark 6. Note that the condition defining suitable changes of variables is open. As $d \geqslant n$, the degree of the polynomial $H.\prod_{\ell=1}^{r} G_{\ell} \in k[U_{ij}]_{\substack{1 \leqslant i \leqslant n \\ 0 \leqslant j \leqslant n}}$ is bounded by d^{2n}. Then, if we choose the elements u_{ij} $(1 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant n)$ from a subset of k with N elements randomly, the probability that the change of variables they define satisfy the desired conditions is at least $1 - d^{2n}/N$.

3. Equidimensional decomposition

3.1. Describing equidimensional varieties

Our algorithm is essentially based on the description of any equidimensional variety in $\mathbb{A}^n$ as the set of common zeroes of $n+1$ polynomials with bounded degrees. In this section we are going to explain how this can be done.

Let $W \subset \mathbb{A}^n(\bar{k})$ be an equidimensional variety of dimension $\ell < n$ definable by polynomials in $k[X_1, \ldots, X_n]$. Suppose that the variables $X_1, \ldots, X_n$ are in Noether position with respect to W (that is to say, the projection $\pi : W \to \mathbb{A}^{\ell}$ defined by $\pi(x) = (x_1, \ldots, x_{\ell})$ is finite).

Given a linear form $u = \lambda_{\ell+1}X_{\ell+1} + \cdots + \lambda_n X_n$ with $\lambda_{\ell+1}, \ldots, \lambda_n \in k$, consider the morphism $\pi_u : \mathbb{A}^n \to \mathbb{A}^{\ell+1}$ defined by $\pi_u(x) = (x_1, \ldots, x_{\ell}, u(x))$. The image of W under π_u is a hypersurface in $\mathbb{A}^{\ell+1}$ and, therefore, is defined by a uniquely determined square-free polynomial $m_u \in k[X_1, \ldots, X_{\ell}, U]$. Moreover, m_u is monic in the variable U

and its total degree is bounded by $\deg W$ (see [7, Lemmas 2 and 3] or [14, Proposition 1]). We will call m_u the *minimal polynomial of u with respect to W*.

Now we are going to show that W can be defined by means of the minimal polynomials of $n+1$ suitable linear forms.

Lemma 7. *Let $W \subseteq \mathbb{A}^n$ be an equidimensional variety of dimension $\ell < n$. Suppose the variables $X_1,\ldots,X_n$ are in Noether position with respect to W. Then there exist $n+1$ linear forms*

$$u_i = \lambda_{\ell+1}^{(i)} X_{\ell+1} + \cdots + \lambda_n^{(i)} X_n \quad (1 \leqslant i \leqslant n+1)$$

with $\lambda_j^{(i)} \in k$ $(1 \leqslant i \leqslant n+1, \ell+1 \leqslant j \leqslant n)$ such that W is the set of common zeroes of the minimal polynomials of the linear forms u_i $(1 \leqslant i \leqslant n+1)$ with respect to W evaluated in each u_i, that is

$$W = \{x \in \bar{k}^n \colon m_{u_1}(x_1,\ldots,x_\ell,u_1(x)) = 0,\ldots,m_{u_{n+1}}(x_1,\ldots,x_\ell,u_{n+1}(x)) = 0\}.$$

Proof. We are going to show the existence of such linear forms inductively: Let $u_1 = \lambda_{\ell+1}^{(1)} X_{\ell+1} + \cdots + \lambda_n^{(1)} X_n$ be any linear form different from zero and let m_{u_1} be its minimal polynomial with respect to W. Then $V(m_{u_1}) := V(m_{u_1}(X_1,\ldots,X_\ell,u_1)) \subseteq \mathbb{A}^n$ is an equidimensional variety of dimension $n-1$ such that $W \subseteq V(m_{u_1})$.

Suppose that, after j steps we have j linear forms $u_1,\ldots,u_j$ such that W is a subset of

$$V(m_{u_1},\ldots,m_{u_j}) := V(m_{u_1}(X_1,\ldots,X_\ell,u_1),\ldots,m_{u_j}(X_1,\ldots,X_\ell,u_j))$$

and that each irreducible component of $V(m_{u_1},\ldots,m_{u_j})$ which is not an irreducible component of W has dimension $n-j$.

Let $\mathscr{C}_j$ be the set of irreducible components of $V(m_{u_1},\ldots,m_{u_j})$ not being irreducible components of W. If $\mathscr{C}_j = \emptyset$, let $u_{j+1} = \lambda_{\ell+1}^{(j+1)} X_{\ell+1} + \cdots + \lambda_n^{(j+1)} X_n$ be any linear form. If $\mathscr{C}_j \neq \emptyset$, for each component $C \in \mathscr{C}_j$, take a point $x_C \in C - W$.

Let $\pi\colon \mathbb{A}^n \to \mathbb{A}^\ell$ be the canonical projection in the first ℓ-coordinates. For each $C \in \mathscr{C}_j$, consider the finite set $M_C = \pi^{-1}(\pi(x_C)) \cap W$.

Take any linear form $u_{j+1} = \lambda_{\ell+1}^{(j+1)} X_{\ell+1} + \cdots + \lambda_n^{(j+1)} X_n$ such that

$$u_{j+1}(x) \neq u_{j+1}(x_C) \quad \forall x \in M_C \quad \forall C \in \mathscr{C}_j.$$

Note that this condition implies that, for any x_C $(C \in \mathscr{C}_j)$, the minimal polynomial $m_{u_{j+1}}$ of u_{j+1} with respect to W, evaluated in u_{j+1}, does not vanish in x_C.

Therefore, any irreducible component of

$$V(m_{u_1},\ldots,m_{u_{j+1}}) := V(m_{u_1}(X_1,\ldots,X_\ell,u_1),\ldots,m_{u_{j+1}}(X_1,\ldots,X_\ell,u_{j+1}))$$

which is not an irreducible component of W has dimension $n-j-1$. □

Remark 8. Let us analyze the conditions to choose the linear forms stated in the previous lemma:

- u_1 can be any non-zero linear form.
- Suppose we have j linear forms $u_1,\ldots,u_j$ such that each irreducible component of $V(m_{u_1},\ldots,m_{u_j})$ not being an irreducible component of W has dimension $n-j$. Following the notations of the lemma, the condition we ask the linear form u_{j+1} is $\prod_{C\in\mathscr{C}_j}\prod_{x\in M_C} u_{j+1}(x-x_C)\neq 0$. This is a polynomial expression in $\lambda_{\ell+1}^{(j+1)},\ldots,\lambda_n^{(j+1)}$ with degree bounded by $(\deg W)^{j+1}$.

3.2. Changing the base field

In this section, we are going to show how irreducible decomposition behaves when extending the base field, providing the variables satisfy the conditions stated before. As this situation will be considered in many different instances, we are going to explain it in a general case.

Notation. Let $S=\bar{k}[X_1,\ldots,X_\ell]-\{0\}$. Given a variety $W\subset\mathbb{A}^n(\bar{k})$, we denote by $\tilde{W}\subset\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$ the variety defined by the ideal $S^{-1}(I(W))$. Note that, if the variety $W\subset\mathbb{A}^n(\bar{k})$ is defined by an ideal $J\subset\bar{k}[X_1,\ldots,X_n]$, then $\tilde{W}\subset\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$ is defined by $S^{-1}(J)$.

Let I be an ideal in $\bar{k}[X_1,\ldots,X_n]$ and let $V(I)$ be the variety defined by I in $\mathbb{A}^n(\bar{k})$. Let ℓ be an integer such that, for every irreducible component C of $V(I)$, $\dim C\geqslant\ell$. Suppose the variables $X_1,\ldots,X_\ell$ are free with respect to each irreducible component of $V(I)$.

Let $V(I)=\bigcup_{i=1}^t C_i$ be the minimal irreducible decomposition of $V(I)$ in $\mathbb{A}^n(\bar{k})$. Then, considering the associated ideals, we have that $rad(I)=\bigcap_{i=1}^t I(C_i)$ in $\bar{k}[X_1,\ldots,X_n]$.

As the variables $X_1,\ldots,X_\ell$ are free for each irreducible component of $V(I)$, for every i, $1\leqslant i\leqslant t$, $S\cap I(C_i)=\emptyset$ holds. Then, localizing at S, we obtain

$$S^{-1}(rad(I))=\bigcap_{i=1}^{t} S^{-1}(I(C_i))$$

which is a minimal prime decomposition of $S^{-1}(rad(I))$ in $\bar{k}(X_1,\ldots,X_\ell)[X_{\ell+1},\ldots,X_n]$.

Then the minimal irreducible decomposition of $\tilde{V}(I)$ in the $\bar{k}(X_1,\ldots,X_\ell)$-Zariski topology of $\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$ is

$$\tilde{V}(I)=\bigcup_{i=1}^{t}\tilde{C}_i.$$

Note that, for every $1\leqslant i\leqslant t$, $\dim(\tilde{C}_i)=\dim(C_i)-\ell$.

Consider now the $\overline{k(X_1,\ldots,X_\ell)}$-Zariski topology of $\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$. For each i ($1\leqslant i\leqslant t$), all the irreducible components of $\tilde{C}_i$ are of the same dimension (which is $\dim(\tilde{C}_i)$). Moreover, it is easy to see that, if $i\neq j$, no irreducible component of $\tilde{C}_i$ is included in $\tilde{C}_j$. In other words, given the irreducible decomposition of $V(I)=\bigcup_{i=1}^t C_i$,

we can obtain the *irredundant* irreducible decomposition of $\tilde{V}(I)$ over $\overline{k(X_1,\ldots,X_\ell)}$ as the union of all the irreducible components of $\tilde{C}_i$ $(1 \leqslant i \leqslant t)$.

3.3. Main result

The main result of this paper is the following theorem:

Theorem 9. *Let $f_1,\ldots,f_s \in k[X_1,\ldots,X_n]$ be polynomials and let d be an integer such that $d \geqslant n$ and $\deg f_i \leqslant d$ for every $1 \leqslant i \leqslant s$. Let $V = \{x \in \bar{k}^n\colon f_1(x) = 0 \wedge \cdots \wedge f_s(x) = 0\}$ and let $r = \dim V$. Then, there exists a probabilistic algorithm of sequential complexity of order $s^{O(1)}d^{O(n)}$, which computes the equidimensional decomposition of V: the input of the algorithm are the polynomials $f_1,\ldots,f_s$ given in dense form and its output is a straight line program of length $d^{O(n)}$ which computes polynomials $g_j^{(\ell)}$ $(0 \leqslant \ell \leqslant r, 1 \leqslant j \leqslant n+1)$ such that, for every $0 \leqslant \ell \leqslant r$, the equidimensional component of V of dimension ℓ is*

$$V_\ell = \{x \in \bar{k}^n\colon g_1^{(\ell)}(x) = 0 \wedge \cdots \wedge g_{n+1}^{(\ell)}(x) = 0\}.$$

For every $0 \leqslant \ell \leqslant r$, the degrees of $g_j^{(\ell)}$ $(1 \leqslant j \leqslant n+1)$ are bounded by $\deg V_\ell \leqslant d^{n-\ell}$.

Proof. First, we compute r, the dimension of V. This can be done in sequential time $s^{O(1)}d^{O(n)}$ applying the algorithm described in [4]. (This step can be avoided, as we explain in Remark 11, but we include it here to make the algorithm easier to understand.)

Now, we change the input data in the sense of Section 2. By means of a random choice of $n+1$ linear combinations of the input polynomials, we may assume the variety V is defined by $n+1$ polynomials of degrees bounded by d which satisfy the conditions stated in Lemma 3. Again, by a random change of variables, we may assume the new variables satisfy the conditions stated in Section 2.2. In order to simplify notation, we denote the new variables by $X_1,\ldots,X_n$ and the linear combinations of the input polynomials in these new variables by $f_1,\ldots,f_{n+1}$.

Summarizing, if we are given a set of N elements of k and we can choose elements of it randomly, we have, with probability at least $1-(d^{2n}/N)-\sum_{h=1}^{n+1}(d^{h-1}/N) \geqslant 1-(d^{2n}+2d^n)/N$ (see Remarks 4 and 6), $n+1$ polynomials $f_1,\ldots,f_{n+1}$ in the variables $X_1,\ldots,X_n$ satisfying these conditions (in the following, we will call them *normal conditions*):

- $V = V(f_1,\ldots,f_{n+1})$.
- For every $0 \leqslant \ell \leqslant n$, the dimension of each irreducible component of $V(f_1,\ldots,f_{n-\ell})$ which is not an irreducible component of V is ℓ.
- The projection $\pi_r : V(f_1,\ldots,f_{n-r}) \to \mathbb{A}^r$ (where $r = \dim V$) defined by $\pi_r(x) = (x_1,\ldots,x_r)$ is finite.
- For every j, $0 \leqslant j \leqslant r$, let Z_j be the union of the irreducible components of $V(f_1,\ldots,f_{n-j})$ not being irreducible components of V. Then, for every $1 \leqslant \ell \leqslant r-1$,

provided $Z_{\ell+1} \cap \{f_{n-\ell} = 0\} \neq \emptyset$, the projection $\pi_\ell : Z_{\ell+1} \cap \{f_{n-\ell} = 0\} \to \mathbb{A}^\ell$ defined by $\pi_\ell(x) = (x_1, \ldots, x_\ell)$ is finite.

Let $V = \bigcup_{\ell=0}^{r} V_\ell$ be the equidimensional decomposition of V and suppose the polynomials $f_1, \ldots, f_{n+1}$ in the variables $X_1, \ldots, X_n$ randomly obtained satisfy the "normal conditions" stated above.

The general idea of our algorithm is the following:

In a first step, it computes polynomials defining V_r and polynomials defining Z_r. Then, in intermediate steps, it computes, for $\ell = r-1, \ldots, 0$, polynomials defining Z_ℓ and polynomials defining a variety $V_\ell \cup Y_\ell$, with $Y_\ell \subset \bigcup_{h=\ell+1}^{r} V_h$ and $\dim Y_\ell \leqslant \ell$. Finally, from all these polynomials, the algorithm obtains polynomials defining each equidimensional component of V.

First step. In this step we are going to compute polynomials defining V_r and Z_r. In fact, we are going to define V_r and Z_r by means of the minimal polynomials of $n+1$ suitable chosen linear forms with respect to V_r and Z_r (see Lemma 7). In order to do this, we are going to consider zero-dimensional varieties in the sense of Section 3.2:

Consider $f_1, \ldots, f_{n-r}$ as polynomials in $k(X_1, \ldots, X_r)[X_{r+1}, \ldots, X_n]$. Let $\overline{k(X_1, \ldots, X_r)}$ be an algebraic closure of $k(X_1, \ldots, X_r)$ and let $\tilde{V}(f_1, \ldots, f_{n-r})$ be the set of common zeroes of $f_1, \ldots, f_{n-r}$ in $\overline{k(X_1, \ldots, X_r)}^{n-r}$. Note that $\dim \tilde{V}(f_1, \ldots, f_{n-r}) = 0$ and, as $V(f_1, \ldots, f_{n-r}) = V_r \cup Z_r$, then $\tilde{V}(f_1, \ldots, f_{n-r}) = \tilde{V}_r \cup \tilde{Z}_r$, where $\tilde{V}_r$ and $\tilde{Z}_r$ do not have common irreducible components.

We are going to compute the minimal polynomials of a proper linear form with respect to $\tilde{V}_r$ and $\tilde{Z}_r$, respectively, by adapting the algorithm shown in [11, Proposition 27 and Theorem 22] (see also [4, Sections 3.4.7 and 3.4.8]). The minimal polynomials we will obtain coincide with the minimal polynomials of the linear form with respect to V_r and Z_r.

The algorithm in [11] computes a polynomial $F_r \in k[X_1, \ldots, X_r][T_{r+1}, \ldots, T_n]$ with degree in the variables $T_{r+1}, \ldots, T_n$ bounded by $d^{c(n-r)}$ (where c is a positive constant) such that, if $F_r(\lambda_{r+1}, \ldots, \lambda_n) \neq 0$, the linear form $u = \lambda_{r+1}X_{r+1} + \cdots + \lambda_n X_n$ is a primitive element for $\tilde{V}(f_1, \ldots, f_{n-r})$ (that is to say, it separates the points of $\tilde{V}(f_1, \ldots, f_{n-r})$).

Let $u = \lambda_{r+1}X_{r+1} + \cdots + \lambda_n X_n$ be a linear form such that $F_r(\lambda_{r+1}, \ldots, \lambda_n) \neq 0$. We are going to compute its minimal polynomials with respect to V_r and Z_r.

First, we apply the algorithm described in [11, Proposition 27] (see Lemma 1) to compute an element $\rho \in k[X_1, \ldots, X_r]$ and polynomials $v_{r+1}(U), \ldots, v_n(U) \in k[X_1, \ldots, X_r][U]$, with $\deg_U v_i \leqslant d^{O(n-r)}$, such that the coordinates $(x_{r+1}, \ldots, x_n)$ of the points in $\tilde{V}(f_1, \ldots, f_{n-r})$ verify the equations

$$\rho x_i = v_i(u(x)) \quad i = r+1, \ldots, n. \tag{1}$$

The sequential complexity of this step is $d^{O(n)}$ and ρ and the coefficients of $v_{r+1}(U), \ldots, v_n(U)$ are polynomials of degrees bounded by $d^{O(n-r)}$ given by a straight line program of length $d^{O(n)}$.

Note that, as $V_r \subseteq \{f_{n-r+1} = 0\}$ but no irreducible component of Z_r is contained in $\{f_{n-r+1} = 0\}$, the points in $\tilde{V}_r$ are exactly the points in $\tilde{V}(f_1, \ldots, f_{n-r})$ where f_{n-r+1}

vanishes. Then, $\tilde{V}_r$ is the set of common zeroes in $\overline{k(X_1,\ldots,X_r)}^{n-r}$ of the polynomials $f_1,\ldots,f_{n-r},f_{n-r+1}$ and these common zeroes satisfy (1).

Consider the polynomials

$$F_i^{(r)}(U):=\rho^d f_i\left(x_1,\ldots,x_r,\frac{v_{r+1}(U)}{\rho},\ldots,\frac{v_n(U)}{\rho}\right)\quad i=1,\ldots,n-r+1.$$

We compute the dense representation of these polynomials with respect to the variable U and obtain a straight line program of length $d^{O(n)}$ which computes their coefficients, which are polynomials in $k[X_1,\ldots,X_r]$.

Applying the algorithms in [11, Lemmas 11, 12] following [17], we obtain a straight line program of length $d^{O(n)}$ which computes the coefficients of a polynomial $\tilde{p}(U)$ which is a multiple by a polynomial in $k[X_1,\ldots,X_r]$ of

$$p(U)=\mathrm{rad}(\gcd(F_1^{(r)}(U),\ldots,F_{n-r+1}^{(r)}(U)))\in k[X_1,\ldots,X_r][U],$$

the minimal polynomial of u with respect to $\tilde{V}_r$.

Using *Vermeidung von Divisionen* (see [16]) to divide the polynomial $\tilde{p}(U)$ by its leading coefficient, we obtain a straight line program of length $d^{O(n)}$ which computes the coefficients of $p(U)$ with respect to the variable U. Note that $\deg p(U)\leqslant \deg V_r$.

In order to compute the minimal polynomial of u with respect to Z_r, we observe that the points in $\tilde{Z}_r$ are exactly those in $\tilde{V}(f_1,\ldots,f_{n-r})$ in which f_{n-r+1} does not vanish.

Therefore, the minimal polynomial of u with respect to $\tilde{Z}_r$ is

$$q(U)=\frac{\mathrm{rad}(\gcd(F_1^{(r)}(U),\ldots,F_{n-r}^{(r)}(U))}{\mathrm{rad}(\gcd(F_1^{(r)}(U),\ldots,F_{n-r}^{(r)}(U),F_{n-r+1}^{(r)}(U)))}.$$

As before, we compute a multiple $\tilde{q}(U)$ of this polynomial by a factor in $k[X_1,\ldots,X_r]$ and then, we divide this polynomial by its leading coefficient. In this way, we obtain a straight line program of length $d^{O(n)}$ which computes the coefficients of $q(U)\in k[X_1,\ldots,X_r][U]$.

We apply the algorithm described above to $n+1$ randomly chosen linear forms. If the coefficients of these linear forms are randomly chosen from a set of N elements of k, we have, with probability at least $1-(1/N)((n+1)d^{c(n-r)}+2d^{(n-r)(n+1)})$ (see Remark 8), $n+1$ linear forms $u_1^{(r)},\ldots,u_{n+1}^{(r)}$ satisfying the conditions (in the sequel, we will refer to them as *proper linear forms conditions in step r*):

- The polynomial F_r, which states a condition to be a primitive element, does not vanish in the coefficients of $u_1^{(r)},\ldots,u_{n+1}^{(r)}$.
- Z_r is the set of common zeroes of the minimal polynomials of $u_1^{(r)},\ldots,u_{n+1}^{(r)}$ with respect to Z_r (evaluated in $u_1^{(r)},\ldots,u_{n+1}^{(r)}$, respectively).
- V_r is the set of common zeroes of the minimal polynomials of $u_1^{(r)},\ldots,u_{n+1}^{(r)}$ with respect to V_r (evaluated in $u_1^{(r)},\ldots,u_{n+1}^{(r)}$, respectively).

Then, supposing that the change of variables and the linear combinations of the input polynomials satisfy the "normal conditions" and that the linear forms satisfy the "proper

linear forms condition in step r" stated above, we obtain polynomials $p_1^{(r)},\dots,p_{n+1}^{(r)}$ and $q_1^{(r)},\dots,q_{n+1}^{(r)}$ such that

$$V_r=\{x\in\bar{k}^n\colon\ p_1^{(r)}(x_1,\dots,x_r,u_1^{(r)}(x))=0\wedge\cdots\wedge p_{n+1}^{(r)}(x_1,\dots,x_r,u_{n+1}^{(r)}(x))=0\}$$

$$Z_r=\{x\in\bar{k}^n\colon\ q_1^{(r)}(x_1,\dots,x_r,u_1^{(r)}(x))=0\wedge\cdots\wedge q_{n+1}^{(r)}(x_1,\dots,x_r,u_{n+1}^{(r)}(x))=0\}$$

(see Lemma 7).

Intermediate steps. In these steps, we are going to compute for each $\ell=r-1,\dots,0$ polynomials which define certain components of $V(f_1,\dots,f_{n-\ell})$ which will be used later to obtain the equidimensional decomposition of V.

Recall that, for each $0\leqslant\ell\leqslant r-1$, the equidimensional decomposition of $V(f_1,\dots,f_{n-\ell})$ is

$$V(f_1,\dots,f_{n-\ell})=V_r\cup\cdots\cup V_{\ell+1}\cup V'_\ell$$

where $V'_\ell=V_\ell\cup Z_\ell$ with $\dim V_j=j$ or $V_j=\emptyset$ $(\ell\leqslant j\leqslant r)$ and Z_ℓ is either empty or an equidimensional variety of dimension ℓ with no common irreducible components with V_ℓ. For $\ell=r-1,\dots,0$, we are going to compute, from the polynomials $f_1,\dots,f_{n-\ell+1}$, a set of $n+1$ polynomials defining Z_ℓ. Simultaneously, we are going to compute, from the polynomials defining $Z_{\ell+1}$ and the polynomials $f_1,\dots,f_{n-\ell+1}$, a set of $n+1$ polynomials defining a variety $V_\ell\cup Y_\ell$ with $Y_\ell\subseteq\bigcup_{h=\ell+1}^{r}V_h$ and $\dim Y_\ell\leqslant\ell$. Moreover, the polynomials we are going to compute are minimal polynomials of suitable chosen linear forms with respect to certain equidimensional varieties evaluated in the corresponding linear forms.

Let ℓ be fixed, $0\leqslant\ell\leqslant r-1$.

Consider the variety defined in $\bar{k}^n$ by the polynomials $f_1,\dots,f_{n-\ell}$. We have

$$V(f_1,\dots,f_{n-\ell})=V_r\cup\cdots\cup V_{\ell+1}\cup V_\ell\cup Z_\ell,$$

where Z_ℓ is either empty or an equidimensional variety of dimension ℓ.

Let $\tilde{V}(f_1,\dots,f_{n-\ell})\subseteq\mathbb{A}^{n-\ell}(\overline{k(X_1,\dots,X_\ell)})$ be the affine variety defined by $f_1,\dots,f_{n-\ell}$ considered as polynomials in $k(X_1,\dots,X_\ell)[X_{\ell+1},\dots,X_n]$.

Then,

$$\tilde{V}(f_1,\dots,f_{n-\ell})=\tilde{V}_r\cup\cdots\cup\tilde{V}_{\ell+1}\cup\tilde{V}_\ell\cup\tilde{Z}_\ell,$$

where, for every $\ell\leqslant j\leqslant r$, $\tilde{V}_j=\emptyset$ (if $V_j=\emptyset$) or $\dim\tilde{V}_j=\dim V_j-\ell$, and $\tilde{Z}_\ell=\emptyset$ or $\dim\tilde{Z}_\ell=0$ (see Section 3.2).

We are going to consider the isolated points of $\tilde{V}(f_1,\dots,f_{n-\ell})$ to get information about V_ℓ and Z_ℓ. We will adapt the algorithm given for the computation of the minimal polynomials in the first step (that is, the zero-dimensional case) to this more general situation. Again, our algorithm will be based on the techniques described in [11].

The algorithm in [11, Proposition 27] deals with a linear form which is a primitive element for the isolated zeroes of $f_1,\dots,f_{n-\ell}$. In order to obtain such a linear form, it computes a polynomial $F_\ell\in k[X_1,\dots,X_\ell][T_{\ell+1},\dots,T_n]$ such that, if $F_\ell(\lambda_{\ell+1},\dots,\lambda_n)\neq0$

then the linear form $u=\lambda_{\ell+1}X_{\ell+1}+\cdots+\lambda_nX_n$ separates the isolated points of $\tilde{V}(f_1,\ldots,f_{n-\ell})$. The degree of F_ℓ is bounded by $d^{c(n-\ell)}$ where c is a positive constant.

Let $u=\lambda_{\ell+1}X_{\ell+1}+\cdots+\lambda_nX_n$ be a linear form such that $F_\ell(\lambda_{\ell+1},\ldots,\lambda_n)\neq 0$. Then, using the algorithm in [11, Proposition 27] (see Lemma 1 above), we are able to compute an element $\rho\in k[X_1,\ldots,X_\ell]$ and polynomials $v_{\ell+1}(U),\ldots,v_n(U)\in k[X_1,\ldots,X_\ell][U]$, with $\deg_U(v_i)\leqslant d^{O(n-\ell)}$, such that the coordinates of all the isolated zeroes of $\tilde{V}(f_1,\ldots,f_{n-\ell})$ verify the equations

$$\rho x_i=v_i(u(x))\quad i=\ell+1,\ldots,n. \tag{2}$$

The sequential complexity of this step is $d^{O(n)}$ and ρ and the coefficients of $v_{\ell+1}(U),\ldots,v_n(U)$ are polynomials of degrees bounded by $d^{O(n-\ell)}$ given by a straight line program of length $d^{O(n)}$.

The computation of the minimal polynomial of u with respect to $\tilde{Z}_\ell$ follows as in the first step:

Let us consider the polynomials

$$F_i^{(\ell)}(U):=\rho^d f_i\left(x_1,\ldots,x_\ell,\frac{v_{\ell+1}(U)}{\rho},\ldots,\frac{v_n(U)}{\rho}\right)\quad i=1,\ldots,n-\ell+1. \tag{3}$$

Taking into account that $\tilde{Z}_\ell$ is the set of points in $\tilde{V}(f_1,\ldots,f_{n-\ell})$ where $f_{n-\ell+1}$ does not vanish, and all the points in $\tilde{Z}_\ell$ are isolated zeroes of $f_1,\ldots,f_{n-\ell}$, we conclude that

$$q(U)=\frac{\operatorname{rad}(\gcd(F_1^{(\ell)}(U),\ldots,F_{n-\ell}^{(\ell)}(U))}{\operatorname{rad}(\gcd(F_1^{(\ell)}(U),\ldots,F_{n-\ell}^{(\ell)}(U),F_{n-\ell+1}^{(\ell)}(U)))}\in k(X_1,\ldots,X_\ell)[U]$$

is the minimal polynomial of u with respect to $\tilde{Z}_\ell$.

The "normal conditions" imply the variables are in Noether position with respect to Z_ℓ and, therefore, the minimal polynomial $q(U)$ of u with respect to Z_ℓ must be in $k[X_1,\ldots,X_\ell][U]$.

In order to obtain $q(U)$, we compute first a multiple of it by a factor in $k[X_1,\ldots,X_\ell]$, and then we obtain $q(U)$ as the quotient of the (exact) division of this polynomial by its leading coefficient. The polynomial $q(U)$ is given in dense form with respect to U and its coefficients, which are polynomials in $k[X_1,\ldots,X_\ell]$, are given by means of a straight line program of length $d^{O(n)}$.

We would like to get polynomials defining V_ℓ as we did in the first step, but the same procedure may lead to the appearance of extraneous components. In order to control somehow the sets where the polynomials we compute vanish, we will take into account that the irreducible components of V in V_ℓ are included in $Z_{\ell+1}$.

Let $\tilde{q}_j^{(\ell+1)}(X_1,\ldots,X_n)=q_j^{(\ell+1)}(X_1,\ldots,X_{\ell+1},u_j^{l+1})$ $(1\leqslant j\leqslant n+1)$ be the computed polynomials defining $Z_{\ell+1}$. Consider them as polynomials in $k(X_1,\ldots,X_\ell)[X_{\ell+1},\ldots,X_n]$ and let $\tilde{Z}_{\ell+1}$ be the variety they define in $\overline{k(X_1,\ldots,X_\ell)}^{n-\ell}$. As $V_\ell\subset Z_{\ell+1}$, the points in $\tilde{V}_\ell$ are also points of $\tilde{Z}_{\ell+1}$. On the other hand, the points in $\tilde{V}_\ell$ are the isolated points of $\tilde{V}(f_1,\ldots,f_{n-\ell})$ where $f_{n-\ell+1}$ vanishes.

Therefore, the isolated points we are looking for are *some* of the common zeroes of $f_1,\ldots,f_{n-\ell},f_{n-\ell+1}$ in $\tilde{Z}_{\ell+1}$.

The points in $\tilde{V}_\ell$, being isolated zeroes of $f_1,\ldots,f_{n-\ell}$, satisfy Eq. (2). Consider the polynomials

$$Q_j^{(\ell+1)}(U)=\rho^{\deg \tilde{q}_j^{(\ell+1)}}\tilde{q}_j^{(\ell+1)}\left(x_1,\ldots,x_\ell,\frac{v_{\ell+1}(U)}{\rho},\ldots,\frac{v_n(U)}{\rho}\right)\quad j=1,\ldots,n+1 \tag{4}$$

and let

$$p(U)=\mathrm{rad}(\gcd(F_1^{(\ell)}(U),\ldots,F_{n-\ell+1}^{(\ell)}(U),\quad Q_1^{(\ell+1)}(U),\ldots,Q_{n+1}^{(\ell+1)}(U))).$$

The monic polynomial $p(U)\in k(X_1,\ldots,X_\ell)[U]$ satisfies that $p(u(x))=0$ for every $x\in\tilde{V}_\ell$. Moreover, if $\Gamma\in\overline{k(X_1,\ldots,X_\ell)}$ is a root of p, then $\Gamma=u(x)$ for some x in $\tilde{Z}_{\ell+1}\cap(\tilde{V}_r\cup\cdots\cup\tilde{V}_\ell)$.

Let W_ℓ be the union of the irreducible components of dimension ℓ of $Z_{\ell+1}\cap(V_r\cup\cdots\cup V_\ell)$. As

$$V(f_1,\ldots,f_{n-\ell-1})=V_r\cup\cdots\cup V_{\ell+1}\cup Z_{\ell+1}$$

$$V(f_1,\ldots,f_{n-\ell-1},f_{n-\ell})=V_r\cup\cdots\cup V_{\ell+1}\cup V_\ell\cup Z_\ell$$

holds, all the irreducible components in W_ℓ are also irreducible components of $Z_{\ell+1}\cap\{f_{n-\ell}=0\}$. Therefore, the variables are in Noether position with respect to W_ℓ.

Let $\tilde{W}_\ell$ be the corresponding variety in $\mathbb{A}^{n-\ell}(\overline{k(X_1,\ldots,X_\ell)})$. The monic separable polynomial $p(U)\in k(X_1,\ldots,X_\ell)[U]$ satisfies that, if $\Gamma\in\overline{k(X_1,\ldots,X_\ell)}$ is a root of p, then $\Gamma=u(x)$ for some x in $\tilde{W}_\ell$. It follows that $p(U)$ is the minimal polynomial of u with respect to a variety included in W_ℓ (see Section 3.2). Let $m_u\in k[X_1,\ldots,X_\ell][U]$ be the minimal polynomial of u with respect to W_ℓ. Then $p(U)$ is a polynomial in $k[X_1,\ldots,X_\ell][U]$ which is a factor of m_u.

As $p(U)$ evaluated in u vanishes in the isolated points of $\tilde{V}_\ell$, the minimal polynomial of u with respect to $\tilde{V}_\ell$ divides $p(U)$ and therefore

$$p(X_1,\ldots,X_\ell,u(X_{\ell+1},\ldots,X_n))$$

vanishes over V_ℓ.

As before, we compute first a multiple of $p(U)$ by an element in $k[X_1,\ldots,X_\ell]$ and then, the division of this polynomial by its leading coefficient. We obtain the dense representation of p in the variable U and its coefficients given by a straight line program of length $d^{O(n)}$.

Summarizing, given a linear form $u=\lambda_{\ell+1}X_{\ell+1}+\cdots+\lambda_nX_n$ such that $F_\ell(\lambda_{\ell+1},\ldots,\lambda_n)\neq 0$, we are able to compute the minimal polynomial of u with respect to Z_ℓ and a polynomial $p(U)$ which evaluated in u vanishes on V_ℓ and is a factor of the minimal polynomial of u with respect to W_ℓ. This can be done in sequential time $d^{O(n)}$.

We apply the procedure described above to $n+1$ randomly chosen linear forms. If we choose their coefficients from a set of N elements of k randomly, we have that

they satisfy the *proper linear form conditions in step* ℓ, that is to say:

- F_ℓ does not vanish on their coefficients,
- Z_ℓ is the set of common zeroes in $\mathbb{A}^n$ of the minimal polynomials of the $n+1$ linear forms with respect to Z_ℓ (evaluated in the corresponding linear forms),
- V_ℓ is the set of common zeroes in $\mathbb{A}^n$ of the minimal polynomials of the $n+1$ linear forms with respect to V_ℓ (evaluated in the corresponding linear forms), and
- W_ℓ is the set of common zeroes in $\mathbb{A}^n$ of the minimal polynomials of the $n+1$ linear forms with respect to W_ℓ (evaluated in the corresponding linear forms)

with probability at least $1-(1/N)((n+1)d^{c(n-\ell)}+4d^{(n-\ell)(n+1)})$ (see Remark 8).

The first condition implies we can apply the algorithm in [11] to the chosen linear forms. The second one states that the $n+1$ minimal polynomials computed for Z_ℓ evaluated in the respective linear forms define it. Finally, the third and fourth conditions will allow us to construct, from the polynomials computed in the different steps, a set of $n+1$ polynomials defining V_ℓ.

Let $u_1^{(\ell)},\ldots,u_{n+1}^{(\ell)}$ be the linear forms chosen and let $p_1^{(\ell)},\ldots,p_{n+1}^{(\ell)}$ and $q_1^{(\ell)},\ldots,q_{n+1}^{(\ell)}$ be the polynomials computed by the algorithm.

Then, if the "normal conditions" are satisfied, and the linear forms satisfy the conditions stated above, we have

$$Z_\ell=\{x\in\bar{k}^n\colon q_1^{(\ell)}(x_1,\ldots,x_\ell,u_1^{(\ell)}(x))=0,\ldots,q_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,u_{n+1}^{(\ell)}(x))=0\}.$$

We are now going to characterize the set of common zeroes of the polynomials

$$p_1^{(\ell)}(X_1,\ldots,X_\ell,u_1^{(\ell)}(X_{\ell+1},\ldots,X_n)),\ldots,p_{n+1}^{(\ell)}(X_1,\ldots,X_\ell,u_{n+1}^{(\ell)}(X_{\ell+1},\ldots,X_n)).$$

Let $m_1^{(\ell)},\ldots,m_{n+1}^{(\ell)}$ be the minimal polynomials of $u_1^{(\ell)},\ldots,u_{n+1}^{(\ell)}$ with respect to W_ℓ. As we explained before, for each $1\leqslant j\leqslant n+1$,

$$V_\ell\subseteq\{x\in\bar{k}^n\colon p_j^{(\ell)}(x_1,\ldots,x_\ell,u_j^{(\ell)}(x))=0\}\subseteq\{x\in\bar{k}^n\colon m_j^{(\ell)}(x_1,\ldots,x_\ell,u_j^{(\ell)}(x))=0\}.$$

Therefore

$$\begin{aligned}V_\ell&\subseteq\{x\in\bar{k}^n\colon p_1^{(\ell)}(x_1,\ldots,x_\ell,u_1^{(\ell)}(x))=0\wedge\cdots\wedge p_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,u_{n+1}^{(\ell)}(x))=0\}\\&\subseteq\{x\in\bar{k}^n\colon m_1^{(\ell)}(x_1,\ldots,x_\ell,u_1^{(\ell)}(x))=0\wedge\cdots\wedge m_{n+1}^{(\ell)}(x_1,\ldots,x_\ell,u_{n+1}^{(\ell)}(x))=0\}=W_\ell.\end{aligned}$$

As V_ℓ and W_ℓ are both equidimensional varieties of dimension ℓ, and $W_\ell\subseteq\bigcup_{h=\ell}^r V_h$, we conclude that the set of common zeroes of the polynomials

$$p_1^{(\ell)}(X_1,\ldots,X_\ell,u_1^{(\ell)}(X_{\ell+1},\ldots,X_n)),\ldots,p_{n+1}^{(\ell)}(X_1,\ldots,X_\ell,u_{n+1}^{(\ell)}(X_{\ell+1},\ldots,X_n))$$

is a variety $V_\ell\cup Y_\ell$, where $Y_\ell\subseteq\bigcup_{h=\ell+1}^r V_h$ and $\dim Y_\ell\leqslant\ell$.

Final steps. In these steps, we are going to obtain, for $\ell=r-1,\ldots,0$, polynomials defining each equidimensional component V_ℓ of V. These polynomials will be computed using the polynomials obtained in the previous steps.

Fix $\ell<r$. Let $u=u_j^{(\ell)}$ $(1\leqslant j\leqslant n+1)$ and let $p(U)=p_j^{(\ell)}(U)\in k[X_1,\ldots,X_\ell][U]$ be the polynomial previously computed for u, which is the minimal polynomial of the linear form u with respect to a variety formed by the points in $\tilde{V}_\ell$ and some

other points belonging to $\tilde{V}_{\ell+1}\cup\cdots\cup\tilde{V}_r$. Let $\rho\in k[X_1,\ldots,X_\ell]$ and let $v_{\ell+1}(U),\ldots,v_n(U)\in k[X_1,\ldots,X_\ell][U]$ such that (2) holds.

To obtain the minimal polynomial of u with respect to $\tilde{V}_\ell$, we are going to compute the factor of $p(U)$ corresponding to the points in $\tilde{V}_{\ell+1}\cup\cdots\cup\tilde{V}_r$.

For every $\ell+1\leqslant i\leqslant r$, let $\bar{p}_j^{(i)}(X_1,\ldots,X_n)=p_j^{(i)}(X_1,\ldots,X_i,u_j^{(i)})$ $(1\leqslant j\leqslant n+1)$ be the previously computed polynomials such that

$$\{x\in\bar{k}^n\colon\ \bar{p}_1^{(i)}(x)=0\wedge\cdots\wedge\bar{p}_{n+1}^{(i)}(x)=0\}=V_i\cup Y_i$$

with $Y_i\subseteq\bigcup_{j=i+1}^r V_j$.

We consider the polynomials

$$P_j^{(i)}(U):=\rho^{\deg\bar{p}_j^{(i)}}\,\bar{p}_j^{(i)}\left(X_1,\ldots,X_\ell,\frac{v_{\ell+1}(U)}{\rho},\ldots,\frac{v_n(U)}{\rho}\right)\quad j=1,\ldots,n+1$$

and the polynomials defined in (3) and (4), and, applying the same techniques used before, we compute a polynomial $h_i(U)$ which is a multiple, by a factor in $k[X_1,\ldots,X_\ell]$, of

$$\operatorname{rad}(\gcd(F_1^{(\ell)}(U),\ldots,F_{n-\ell+1}^{(\ell)}(U),Q_1^{(\ell+1)}(U),\ldots,Q_{n+1}^{(\ell+1)}(U),P_1^{(i)}(U),\ldots,P_{n+1}^{(i)}(U)).$$

From the polynomials h_i $(\ell+1\leqslant i\leqslant r)$ we obtain a multiple of

$$h(U)=\operatorname{rad}\left(\prod_{i=\ell+1}^{r}h_i(U)\right).$$

This polynomial $h(U)$ is the factor of $p(U)$ corresponding to the points in $\tilde{V}_{\ell+1}\cup\cdots\cup\tilde{V}_r$.

Finally, we compute a multiple of the polynomial $p(U)/h(U)$ and the polynomial $G(U)$ which is the quotient in the division of this polynomial by its leading coefficient. The polynomial $G(U)$ is exactly the minimal polynomial of u with respect to V_ℓ, and therefore, its total degree is bounded by $\deg V_\ell$.

All this procedure can be done in sequential time $d^{O(n)}$.

Applying this procedure to the $n+1$ linear forms $u_1^{(\ell)},\ldots,u_{n+1}^{(\ell)}$ we obtain the $n+1$ polynomials $G_1^{(\ell)}(U),\ldots,G_{n+1}^{(\ell)}(U)$ associated to them. Then, if the "normal conditions" hold, and $u_1^{(\ell)},\ldots,u_{n+1}^{(\ell)}$ verify the "proper linear forms conditions in step ℓ", the polynomials

$$g_j^{(\ell)}=G_j^{(\ell)}(X_1,\ldots,X_\ell,u_j^{(\ell)}(X_{\ell+1},\ldots,X_n))\quad j=1,\ldots,n+1$$

satisfy

$$V_\ell=\{x\in\bar{k}^n\colon\ g_1^{(\ell)}(x)=0\wedge\cdots\wedge g_{n+1}^{(\ell)}(x)=0\}.$$

Note that the whole sequential complexity of this algorithm is bounded by $s^{O(1)}d^{O(n)}$. □

Remark 10. Suppose we are given a random process to select elements from a fixed subset of N elements of k. Then, using this process to obtain the linear combinations of

the input polynomials, the change of variables and the linear forms used in each step, the probability of success of our algorithm will be at least $1-(c_1 d^{n^2+n}+d^{c_2(n+1)})/N$ where c_1 and c_2 are constants.

Remark 11. The computation of the dimension of the variety V is not necessary: supposing the variety $V \neq \mathbb{A}^n$, we can start our algorithm at the instance $n-1$ instead of the instance $r = \dim V$. The sequential complexity in this case will be of order $(n+1)(2s-1)d^n + d^{O(n)}$.

If the input polynomials are given by a straight line program of length L, then the sequential complexity of our algorithm is of order $(L+(n+1)(2s-1))^{O(1)} d^{O(n)}$. Moreover, if we only want to compute polynomials defining V_ℓ, the equidimensional component of V of dimension ℓ, the sequential complexity is of order $(L+(n-\ell+1)(2s-1))^{O(1)} d^{O(n-\ell)}$.

Irreducible decomposition. Let k be a field and let $\bar{k}$ be an algebraic closure of k. We can consider $\mathbb{A}^n(\bar{k})$ with the Zariski topology induced by polynomials with coefficients in k (i.e. the closed sets are the sets of zeroes of polynomials in $k[X_1,\ldots,X_n]$). There is a well-known notion of irreducible variety associated to this topology and, therefore, a notion of unique irreducible decomposition of varieties over k.

Provided we are given an efficient algorithm to factorize polynomials in $k[X_1,\ldots,X_n]$ given by straight line programs, our algorithm can be adapted to obtain from polynomials $f_1,\ldots,f_s \in k[X_1,\ldots,X_n]$ defining a variety V, the k-irreducible decomposition of V.

Acknowledgements

The authors wish to thank Joos Heintz for his help.

References

[1] A.L. Chistov, D.Y. Grigor'ev, Subexponential time solving systems of algebraic equations, LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.
[2] M. Elkadi, B. Mourrain, A new algorithm for the geometric decomposition of a variety, Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation, 1999.
[3] M. Giusti, J. Heintz, Algorithmes -disons rapides- pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles, in: T. Mora, C. Traverso (Eds.), Effective Methods in Algebraic Geometry, Progress in Mathematics, Vol. 94, Birkhäuser, Basel, 1991, pp. 169–193.
[4] M. Giusti, J. Heintz, La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, Symposia Matematica, Vol. XXXIV, 1993, pp. 216–256.
[5] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1998) 101–146.
[6] M. Giusti, J. Heintz, J. Sabia, On the efficiency of effective Nullstellensätze, Comput. Complexity 3 (1993) 56–95.
[7] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–277.

[8] J. Heintz, On the computational complexity of polynomials and bilinear mappings, a survey, in: L. Huguet, A. Poli (Eds.), Proceedings of the Fifth International Conference AAECC 5, Lecture Notes in Computer Science, Vol. 356, Springer, Berlin, 1989, pp. 269–300.
[9] J. Heintz, C.P. Schnorr, Testing polynomials which are easy to compute, Monographie 30 de l'Enseignement Mathématique, 1982, pp. 237–254.
[10] G. Jeronimo, J. Sabia, Probabilistic equidimensional decomposition, C.R. Acad. Sci. Paris 331 (I) (2000) 485–490.
[11] T. Krick, L.M. Pardo, A computational method for diophantine aproximation, Prog. Math. 143 (1996) 193–253.
[12] T. Krick, L.M. Pardo, M. Sombra, Sharp estimates for the arithmetic Nullstellensatz, Duke Math. J., to appear.
[13] G. Lecerf, Computing an equidimensional decomposition of an algebraic variety by means of geometric resolutions, Proceedings of the ISSAC 2000 Conference, ACM, 2000.
[14] J. Sabia, P. Solernó, Bounds for traces in complete intersections and degrees in the Nullstellensatz, AAECC J. 6 (1995) 353–376.
[15] J.T. Schwartz, Fast probabilistic algorithms for verification of polynomial identities, J. ACM 27 (1980) 701–717.
[16] V. Strassen, Vermeidung von Divisionen, Crelle J. Reine Angew. Math. 264 (1973) 184–202.
[17] J. von zur Gathen, Parallel algorithms for algebraic problems, Proceedings of the 13th Conference on MFCS, Lecture Notes in Computer Science, Springer, Berlin, Vol. 233, 1986, pp. 93–112.