Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Symbolic Computation 38 (2004) 843–872
Journal of Symbolic Computation
www.elsevier.com/locate/jsc

Computing generators of the ideal of a smooth affine algebraic variety

Cristina Blanco, Gabriela Jeronimo*, Pablo Solernó

Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

Received 1 April 2003; accepted 16 February 2004

Abstract

Let $\mathbb{K}$ be an algebraically closed field, $V \subset \mathbb{K}^n$ be a smooth equidimensional algebraic variety and $I(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ be the ideal of all polynomials vanishing on V. We show that there exists a system of generators $f_1, \ldots, f_m$ of $I(V)$ such that $m \leq (n - \dim V)(1 + \dim V)$ and $\deg(f_i) \leq \deg V$ for $i = 1, \ldots, m$. If $\mathrm{char}(\mathbb{K}) = 0$ we present a probabilistic algorithm which computes the generators $f_1, \ldots, f_m$ from a set-theoretical description of V. If V is given as the common zero locus of s polynomials of degrees bounded by d encoded by straight-line programs of length L, the algorithm obtains the generators of $I(V)$ with error probability bounded by ε within complexity $s(nd^n)^{O(1)} \log^2(\lceil 1/\varepsilon \rceil)L$.

MSC (2000): 14Q20; 13P10

Keywords: Number and degree of generators of polynomial ideals; Efficient generation of polynomial ideals; Computation of the radical of a regular ideal; Straight-line programs; Regular rings

1. Introduction

The paper deals with quantitative considerations about the generation of the ideal of a *smooth* equidimensional affine algebraic variety.

Let $\mathbb{K}$ be an algebraically closed field, $\mathbb{A}^n$ be the affine space $\mathbb{K}^n$ equipped with the Zariski topology and $V \subset \mathbb{A}^n$ be an algebraic variety. We denote by $I(V)$ the ideal of all

* Corresponding author. Tel.: +54-4576-3335; fax: +54-4576-3335.
E-mail addresses: cblanco@dm.uba.ar (C. Blanco), jeronimo@dm.uba.ar (G. Jeronimo), psolerno@dm.uba.ar (P. Solernó).

0747-7171/$ - see front matter © 2004 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jsc.2004.02.002

polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ vanishing on V. The dimension and the geometric degree of V are denoted by $\dim V$ and $\deg V$ respectively.

Roughly speaking, we consider the following two problems related to the ideal $I(V)$ for an arbitrary *smooth* equidimensional affine variety V:

(I) Existence of a system of generators of $I(V)$ with "few" polynomials and "low" degree (see Theorem I below).
(II) If V is given (set-theoretically) as the set of solutions of a polynomial equation system, exhibit an "efficient" algorithm which constructs a system of generators of $I(V)$ as in (I) (see Theorem II below).

The estimation of upper bounds for the number of *equations* defining an algebraic variety (not necessarily smooth) has been a main object of study in algebraic geometry through the last century (see the survey Lyubeznik (1989) for a description of the development of the field). The first modern result on the subject goes back to Kronecker (1882), who states that any algebraic variety in a n-dimensional ambient space can be described set-theoretically by $n+1$ polynomial equations (see Kunz, 1985, Chapter I, Section 5, Exercise 1 for an elementary proof). Only in 1972 did Storch (1972) and Eisenbud and Evans (1973) show independently that, in fact, the upper bound $n+1$ can be replaced by n (a proof of this result may be found in Kunz, 1985, Chapter V, Section 1, Theorem 1.4). It is easy to see that in the zero-dimensional case the upper bound n is optimal (see for instance Shafarevich, 1994, Chapter I, Section 6.2, Corollary 5).

Neither Kronecker's nor Storch–Eisenbud–Evans's results seem to contain a discussion about the degrees of the defining equations involved. However, in Heintz (1983, Proposition 3) a version of Kronecker's theorem with degree bounds is exhibited: every affine algebraic variety $V \subset \mathbb{A}^n$ can be defined by $n+1$ equations with degrees bounded by $\deg V$. Nevertheless, up to now, we do not know whether a similar effective degree upper bound for the Storch–Eisenbud–Evans theorem holds.

As the estimation of the number of equations is in some sense a geometrical problem, it is not surprising that the methods and results concerning the number and degree of generators of the ideal $I(V)$, for an affine or projective algebraic variety V, are quite different from the previous ones and involve more sophisticated pure algebraic tools.

Unlike the bounds for the number of defining equations, no general bound depending only on the dimension of the ambient space can be expected for the number of generators of the ideal $I(V)$ without additional assumptions on the variety V. An example due to Macaulay (1916, Chapter II, Section 34) and studied by Abhyankar (1973) shows that for each $m \in \mathbb{N}$ there exists an *affine* algebraic curve $V_m \subset \mathbb{A}^3$ such that $I(V_m)$ cannot be generated by less than m polynomials. Another interesting example of the same kind for *projective* zero-dimensional (hence regular) varieties in $\mathbb{P}^2$ has been shown by Geramita (1983). However, a remarkable "analog" of the Storch–Eisenbud–Evans theorem holds for locally complete intersection polynomial ideals:

Theorem (Kumar, 1978 and Sathaye, 1978; see also Kunz, 1985, Chapter V, Section 5, Theorem 5.21 for a proof). *Let $V \subset \mathbb{A}^n$ be an algebraic variety such that $I(V)$ is a locally complete intersection (this holds, for instance, if V is a smooth variety). Then $I(V)$ can be generated by n polynomials.*

Unfortunately, from the proofs of this result it does not seem clear how to deduce an estimate for the degree of the n generators of $I(V)$ stated in the theorem, at least in terms of elementary geometric invariants of the variety V (as dimension or degree).

On the other hand, concerning only estimates for the degree of generators of $I(V)$, sharp upper bounds for certain classes of *projective* varieties $V \subset \mathbb{P}^n$ can be obtained from the study of the Castelnuovo–Mumford regularity $\mathrm{reg}(V)$. Roughly speaking, $\mathrm{reg}(V)$ is the minimal upper bound for the degrees of the generators of the modules of syzygies associated with $\mathbb{K}[x_0, \ldots, x_n]/I(V)$ (see Eisenbud, 1994, Section 20.5, for precise definitions). In particular, $\mathrm{reg}(V)$ becomes an upper bound for the maximal degree $d(V)$ of a minimal system of generators of $I(V)$. Despite the doubly exponential gap between Castelnuovo–Mumford regularity and degrees of generators of a homogeneous ideal in the worst case (see Giusti, 1984 and Bayer and Mumford, 1993, Example 3.9), under suitable hypotheses, $\mathrm{reg}(V)$ provides better bounds for $d(V)$: for instance, if $V \subset \mathbb{P}^n$ is assumed smooth and equidimensional, the inequality $d(V) \leq \mathrm{reg}(V) \leq (\dim V + 1)(\deg V - 2) + 2$ holds (cf. Bayer and Mumford, 1993, Theorem 3.12). See also Nagel and Schenzel (1998) for sharp bounds for generalized locally Cohen–Macaulay projective varieties.

In the case of a smooth irreducible variety $V \subset \mathbb{A}^n$ it is also possible to exhibit an upper bound for the degrees of the generators of $I(V)$ in terms of $\deg V$ by means of elementary geometric (not homological) tools:

Theorem (Mumford, 1970; see also Seidenberg, 1975; Catanese, 1992 and Proposition 8 below). *Let $V \subset \mathbb{A}^n$ be a smooth irreducible algebraic variety. Then $I(V)$ can be generated by polynomials whose degrees are bounded by* $\deg V$.

The same result is re-obtained by Seidenberg (1975) and by Catanese (1992) considering generic linear projections and their associated eliminating polynomials, which can be viewed as suitable specializations of the Chow form of the variety V (see also Proposition 8 and Corollary 16 below). Let us remark that no explicit "low" upper bound for the number of generators is given in Mumford (1970), Seidenberg (1975) or Catanese (1992).

However, based on the Seidenberg–Catanese approach, we are able to obtain a "low" upper bound for the number of generators of $I(V)$ with degrees bounded by $\deg V$ by reconstructing the defining ideal of V from sufficiently many linear projections of V onto suitably chosen linear spaces of dimension $\dim V + 1$. The construction, which is described in Section 3, may be summarized as follows: the image of each of the projections mentioned is a hypersurface that is defined by a single polynomial of degree at most $\deg V$. Then, associated with a family of $n - \dim V$ such projections we have $n - \dim V$ polynomials which generate $I(V)$ locally at the points of an open dense subset of V (that is, the set of "bad points" at which $I(V)$ is not generated by the $n - \dim V$ polynomials is contained in a closed subvariety of V of dimension at most $\dim V - 1$). By choosing different families of projections, the dimension of the set of "bad points" is reduced successively to $\dim V - 2, \ldots, 0, -1$. So, after considering $\dim V + 1$ families of projections, each of which adds $n - \dim V$ new polynomials, we obtain a family of polynomials which generate $I(V)$ locally at each point and, therefore, is a system of generators of $I(V)$.

Thus we provide an answer to the problem (I) (in some sense, a weak mixture of Kumar–Sathaye and Mumford–Seidenberg–Catanese theorems):

Theorem I (See Theorem 10 below). *Let* $V \subset \mathbb{A}^n$ *be a smooth equidimensional algebraic variety and set* $m := (n - \dim V)(1 + \dim V)$. *There exist polynomials* $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ *with degrees bounded by* $\deg V$ *such that* $I(V) = (f_1, \ldots, f_m)$.

As Professor M. Chardin (Université Pierre et Marie Curie, Paris) kindly pointed out to us, this result seems not to be completely new and it might be known by some specialists in the area. Anyway we have decided to include a complete proof of it in this paper for several reasons: we are unaware of a precise reference, and we do not even know whether it is actually published. Besides, our proof is quite elementary, requiring only a basic knowledge of commutative algebra and algebraic geometry (see for instance Kunz, 1985, Chapter VI, Section 1 and Shafarevich, 1977, Chapter I). On the other hand, the correctness of our algorithm solving problem (II) is strongly based on that proof and so we need it for the sake of comprehensiveness.

Concerning the problem (II), suppose now that an algebraic variety $V \subset \mathbb{A}^n$ is given by a finite set of polynomial defining equations $g_1 = 0, \ldots, g_s = 0$. A basic question in computer algebra is how to construct from the polynomials $g_i, 1 \leq i \leq s$, a set of generators of the ideal $I(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ (or equivalently, by Hilbert Nullstellensatz, a system of generators of the *radical* of the polynomial ideal $(g_1, \ldots, g_s)$).

Although many general effective procedures have been provided during the last 15 years (see for instance Gianni et al., 1988; Alonso et al., 1991; Vasconcelos, 1992; Krick and Logar, 1992; Eisenbud et al., 1992; Matsumoto, 2001; Fortuna et al., 2002; Kemper, 2002), all of them involve (explicitly or implicitly) Gröbner basis computations and, therefore, their algebraic complexity behaviors become at least *doubly exponential* in some of the natural input parameters (the number or degree of polynomials g_i, or number of variables n, or $\dim V$, etc.). An alternative single-exponential approach avoiding rewriting techniques is given in Armendáriz and Solernó (1995), but this method only works when the input polynomials $g_1, \ldots, g_s$ form a regular sequence and the variety V is assumed to be Cohen–Macaulay. Up to now, the problem of finding a single-exponential algorithm for the computation of the radical of an arbitrary polynomial ideal remains open.

Here we combine the arguments used to prove Theorem I and the fast computation of the Chow form of an arbitrary algebraic variety developed in Jeronimo et al. (in press) or Jeronimo (2002) (see also Section 5.2 below) in order to obtain a probabilistic algorithm which runs in *single-exponential* time and computes the ideal $I(V)$ for any *smooth* equidimensional algebraic variety $V \subset \mathbb{A}^n$.

The Chow form is a classical tool that has been extensively used in the resolution of different problems involving algebraic varieties. For instance, it is a well known fact that defining equations of an equidimensional variety can be derived easily from its Chow form (see for example van der Waerden (1939, Sections 36, 37) for a classical approach or Jeronimo et al. (2001) for an algorithmic version of this result). In this paper, we show that under our assumptions the generators of $I(V)$ stated in Theorem I can also be obtained from the Chow form of V by suitable generic specializations (see Section 4).

This procedure—computation and specialization of the Chow form of V—leads to the construction of an algorithm (see Section 5.3) which allows us to prove the following complexity result (see Section 5.1 for a brief discussion about the computational model):

Theorem II (See Theorem 18 below). *Suppose* $\mathrm{char}(\mathbb{K}) = 0$. *Let* $g_1, \ldots, g_s$ *be polynomials in* $\mathbb{K}[x_1, \ldots, x_n]$ *of degrees bounded by* d. *Set* $V := \{x \in \mathbb{A}^n : g_1(x) = 0, \ldots, g_s(x) = 0\}$. *Assume that* V *is smooth equidimensional and* $0 < \dim V < n - 1$.

Then there is a probabilistic algorithm which computes, for any $\varepsilon \in (0, 1)$, *a set of* $(n - \dim V)(1 + \dim V)$ *polynomials of degrees bounded by* $\deg V$ *which generates the ideal* $I(V)$ *with error probability bounded by* ε. *The input of the algorithm is the family of defining polynomials* $g_1, \ldots, g_s$ *encoded by straight-line programs of length* L *and the parameter* ε, *and its output is a family of straight-line programs of length* $s(nd^n)^{O(1)}L$ *encoding the generators of the ideal* $I(V)$. *The overall complexity of the algorithm is bounded by* $s(nd^n)^{O(1)} \log^2(\lceil 1/\varepsilon \rceil)L$.

Note that, in addition to improving the theoretical complexity of the computation of generators for $I(V)$ with respect to the known results (single exponential versus double exponential), Theorem II produces *few* generators with degrees bounded by an *intrinsic* invariant of V.

Let us observe that the extremal cases $\dim V = 0$ or $\dim V = n - 1$ (not considered in the statement of Theorem II) are well known: for the zero-dimensional case it is not difficult to adapt slightly several of the above mentioned procedures computing the radical in order to obtain complexity upper bounds as in Theorem II; the case of a hypersurface (not necessarily smooth) is a direct consequence of the known GCD algorithms for multivariate polynomials (see for instance Kaltofen, 1988).

Finally, we remark that Theorem II admits a similar version where the complexity bound depends on the geometric degree δ of the input polynomial system instead of the Bézout number d^n (see Theorem 19 below).

The paper is organized as follows. Sections 2 and 3 are devoted to proving Theorem I above, as well as to developing the tools we use in the subsequent sections. In Section 4 we show that the eliminating polynomials defined in Section 2 are in fact suitable specializations of the Chow form of the variety V (Corollary 16). Section 5 is devoted to the algorithm underlying Theorem II: in Section 5.1 we sketch the computational model, in Section 5.2 we introduce the algorithm that will be applied for the computation of Chow forms, in Section 5.3 we describe our algorithm and in Sections 5.4 and 5.5 we compute its error probability and its total complexity.

2. Preliminaries

2.1. Notation and definitions

Throughout this paper $\mathbb{K}$ denotes an algebraically closed field and $\mathbb{N}$ the set of positive integers.

Let $n \in \mathbb{N}$. We denote by $\mathbb{A}^n$ the affine space $\mathbb{K}^n$ equipped with the Zariski topology and by $\mathbb{K}[x_1, \ldots, x_n]$ the polynomial ring in n indeterminates.

Let $V \subset \mathbb{A}^n$ be an algebraic variety. We adopt the usual notions of dimension and degree of an affine algebraic variety, which we denote by $\dim V$ and $\deg V$ respectively. For definitions see for instance the classic books Shafarevich (1977, 1994) or Mumford (1995). For a reducible variety we follow Heintz (1983, Definition 1 and Remark 2) defining its degree as the sum of the degrees of all its irreducible components. We denote by $I(V) \subset \mathbb{K}[x_1, \ldots, x_n]$ the ideal of all polynomials vanishing on V and by $\mathbb{K}[V] := \mathbb{K}[x_1, \ldots, x_n]/I(V)$ the ring of coordinates of V.

If $I(V)$ is generated by polynomials $f_1, \ldots, f_s$ we say that V is smooth at a point $p \in V$ (or that $p \in V$ is a regular point of V) if the Jacobian matrix $J := \left(\partial f_j/\partial x_i\,(p)\right)_{\substack{1\le j\le s\\ 1\le i\le n}}$ has rank $n - \dim V$. We also say that V is smooth if it is smooth at each of its points.

2.2. Generic projections

Let $V \subset \mathbb{A}^n$ be an equidimensional algebraic variety of dimension k, with $0 \le k < n$.

For every $h = (h_{ij})_{\substack{0\le i\le n\\ 1\le j\le k+1}} \in (\mathbb{A}^{n+1})^{k+1}$ we define linear polynomials $\ell_{h_j} \in \mathbb{K}[x_1, \ldots, x_n]$ as $\ell_{h_j} := h_{0j} + h_{1j}x_1 + \cdots + h_{nj}x_n$, for $j = 1, \ldots, k+1$, and we denote by π_h the linear map

$$\pi_h : \mathbb{A}^n \to \mathbb{A}^{k+1}, \qquad (x_1, \ldots, x_n) \mapsto (\ell_{h_1}, \ldots, \ell_{h_{k+1}}). \tag{1}$$

Set $L_h \subset \mathbb{A}^n$ for the linear variety defined as $L_h := \{x \in \mathbb{A}^n : \ell_{h_1}(x) = 0, \ldots, \ell_{h_{k+1}}(x) = 0\}$, and let L_h^0 be the vector subspace associated with L_h:

$$L_h^0 := \{x \in \mathbb{A}^n : \ell_{h_1}(x) - h_{01} = 0, \ldots, \ell_{h_{k+1}}(x) - h_{0k+1} = 0\}. \tag{2}$$

Let $G \subset (\mathbb{A}^{n+1})^k$ be a Zariski dense open set whose elements induce Noether positions with respect to the variety V (see Eisenbud, 1994, Theorem 13.3) and let

$$U_0 := (G \times \mathbb{A}^{n+1}) \cap \{h \in (\mathbb{A}^{n+1})^{k+1} / \dim L_h = n - k - 1\}, \tag{3}$$

which is a Zariski dense open subset of $(\mathbb{A}^{n+1})^{k+1}$.

Fix $h \in U_0$ and consider the restriction of the map π_h to the variety V, which we call $\pi_{h,V}$. If $\pi : \mathbb{A}^{k+1} \to \mathbb{A}^k$ denotes the canonical projection $(x_1, \ldots, x_{k+1}) \mapsto (x_1, \ldots, x_k)$, then $\pi \circ \pi_{h,V}$ is a finite and surjective morphism between V and $\mathbb{A}^k$ (in fact, it is a projection in Noether position as we suppose $h \in U_0$). In particular, by the theorem of fibers (e.g. Shafarevich, 1994, Chapter I, Section 6.3), $\pi_{h,V}$ has finite fibers and, therefore, $\pi_h(V) \subset \mathbb{A}^{k+1}$ is a k-equidimensional Zariski closed set. Then there exists a square-free polynomial f_h in $k+1$ new indeterminates $y_1, \ldots, y_{k+1}$ such that

$$\pi_h(V) = \{y \in \mathbb{A}^{k+1} / f_h(y) = 0\}. \tag{4}$$

Since $\pi_{h,V}$ is a linear morphism, the inequality $\deg f_h = \deg \pi_h(V) \le \deg V$ holds (see for instance Heintz, 1983, Lemma 2).

Specializing f_h in $\ell_{h_1}, \ldots, \ell_{h_{k+1}}$, we obtain a new polynomial

$$f_h^* := f_h(\ell_{h_1}, \ldots, \ell_{h_{k+1}}) \in \mathbb{K}[x_1, \ldots, x_n], \tag{5}$$

which belongs to the ideal $I(V)$ and verifies the following degree bound:

$$\deg f_h^* \leq \deg V. \tag{6}$$

In the next section, we will prove that for a smooth equidimensional variety V, the ideal $I(V)$ can be generated by polynomials of the form f_h^*.

3. Generators for the ideal of a smooth variety

In this section we prove the existence of "few" generators of "low" degree for the ideal of a smooth equidimensional affine variety. We maintain the notation introduced in the previous section.

3.1. Cones and generic projections

We start with an elementary review of affine cones and well known basic properties related to them (see also Harris, 1992), which will enable us to state the conditions needed in order that the polynomials f_h^* defined in the previous subsection generate the ideal of V locally at the regular points of V.

Let $C \subset \mathbb{A}^n$ be a k-dimensional *irreducible* affine variety and let $p \in \mathbb{A}^n$ be an arbitrary point in the ambient n-dimensional affine space. We define the cone $\widehat{C}_p$ associated with the variety C with center p as the Zariski closure in $\mathbb{A}^n$ of the set $\{\lambda(q-p)+p;\ \lambda \in \mathbb{K}, q \in C\}$.

If $p := (p_1, \ldots, p_n)$, it is easy to see that the ideal $I(\widehat{C}_p) \subset \mathbb{K}[x_1, \ldots, x_n]$ is a $(x_i - p_i)$-homogeneous ideal; in particular, for every $q \in \widehat{C}_p \setminus \{p\}$, the straight line defined by p and q is completely contained in the cone $\widehat{C}_p$.

Since the map $(\lambda, q) \mapsto \lambda(q-p)+p$ is a dominant morphism between $\mathbb{A}^1 \times C$ and $\widehat{C}_p$, we infer that $\widehat{C}_p$ is irreducible and $\dim \widehat{C}_p \leq \dim(\mathbb{A}^1 \times C) = k+1$. Since $C \subset \widehat{C}_p$, we have the inequality $k \leq \dim \widehat{C}_p \leq k+1$. Under certain conditions the equality $\dim \widehat{C}_p = k+1$ holds:

Remark 1. Suppose that the variety C and the point p satisfy one of the following conditions:

(1) $p \notin C$.
(2) $p \in C$ is a regular point of C and C is not a linear variety.

Then $\dim \widehat{C}_p = k+1$.

Proof. Let us suppose first that condition 1 holds. As $p \in \widehat{C}_p \setminus C$, we have $C \subsetneq \widehat{C}_p$ and so $\dim \widehat{C}_p = k+1$.

Now assume that condition 2 holds and that $\dim \widehat{C}_p = k$ (or equivalently, $C = \widehat{C}_p$). Since the ideal $I(\widehat{C}_p)$ is $(x_i - p_i)$-homogeneous, this is also true for $I(C)$ and so there exist $(x_i - p_i)$-homogeneous polynomials $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ generating $I(C)$.

Let $(\partial g_l/\partial x_i(p))_{\substack{1 \leq l \leq s \\ 1 \leq i \leq n}}$ be the Jacobian matrix of the system $g_1, \ldots, g_s$ in p, which has rank exactly $n-k$, as p is assumed to be a regular point of C. From the homogeneity, if a polynomial g_l has degree at least 2, the associated l-row in the Jacobian matrix $(\partial g_l/\partial x_1(p), \ldots, \partial g_l/\partial x_n(p))$ is identically zero. Therefore there must be $n-k$ polynomials among $g_1, \ldots, g_s$ whose total degrees are exactly 1 and are $\mathbb{K}$-linearly

independent. Since $\dim C = k$, we conclude that these polynomials of degree 1 generate $I(C)$ and then C is a linear variety, which contradicts the assumption. □

From this remark we deduce the following result in terms of linear projections:

Remark 2. For any $p \in \mathbb{A}^n$ satisfying one of the following conditions:

(1) $p \notin C$; or
(2) $p \in C$ is a regular point,

there exists a Zariski dense open subset $U_{p,C} \subset (\mathbb{A}^{n+1})^{k+1}$ such that for every $h \in U_{p,C}$, $\pi_h^{-1}(\pi_h(p)) \cap \widehat{C}_p = \{p\}$ holds, where $\pi_h : \mathbb{A}^n \to \mathbb{A}^{k+1}$ is the linear map associated with h defined in (1).

Proof. If C is a linear variety and $p \in C$ is an arbitrary point we take $U_{p,C}$ as a product $G \times \mathbb{A}^{n+1}$, where $G \subset (\mathbb{A}^{n+1})^k$ is any open set containing only Noether positions for C. Therefore, without loss of generality we may assume that p and C satisfy conditions (1) or (2) of Remark 1. In particular, $\dim \widehat{C}_p = k + 1$.

Let $U_{p,C} \subset (\mathbb{A}^{n+1})^{k+1}$ be a Zariski dense open set (depending on p) such that for every $h \in U_{p,C}$ the ring extension $\mathbb{K}[\ell_{h_1}, \ldots, \ell_{h_{k+1}}] \hookrightarrow \mathbb{K}[\widehat{C}_p]$ is injective and integral (a Noether position for the cone $\widehat{C}_p$).

We claim that $U_{p,C}$ meets the requirements of the statement of the remark: if $h \in U_{p,C}$, the associated linear map π_h restricted to the cone $\widehat{C}_p$ is onto and finite, which implies that $\pi_h^{-1}(\pi_h(p)) \cap \widehat{C}_p$ is a finite set containing the point p. On the other hand, a point $q \in \widehat{C}_p, q \neq p$, obeys $\pi_h(p) = \pi_h(q)$ if and only if q is a solution of the $(x_i - p_i)$-homogeneous linear system

$$\ell_{h_1}(x) = \ell_{h_1}(p), \ldots, \ell_{h_{k+1}}(x) = \ell_{h_{k+1}}(p).$$

This in turn implies that any point of the straight line defined by q and p (which is contained in $\widehat{C}_p$) is also a solution of this linear system and, therefore, lies in $\pi_h^{-1}(\pi_h(p)) \cap \widehat{C}_p$, contradicting the fact that this set is finite. It follows that $\pi_h^{-1}(\pi_h(p)) \cap \widehat{C}_p = \{p\}$. □

Consider now a k-equidimensional variety $V \subset \mathbb{A}^n$. From the previous results we deduce:

Proposition 3. *Let $p \in \mathbb{A}^n$ be such that $p \notin V$ or $p \in V$ is a regular point. Then, there is a Zariski dense open set $U_p \subset (\mathbb{A}^{n+1})^{k+1}$ verifying:*

(1) *If $p \notin V$, $\pi_h(p) \notin \pi_h(V)$ for every $h \in U_p$.*
(2) *If $p \in V$ is a regular point, $\pi_h^{-1}(\pi_h(p)) \cap V = \{p\}$ for every $h \in U_p$.*

Proof. Let $V = C_1 \cup \cdots \cup C_R$ be the decomposition of V into irreducible components. Observe that p obeys one of the hypotheses of Remark 2 for each of the irreducible components $C_1, \ldots, C_R$. Then, there exist Zariski dense open sets $U_{p,C_1}, \ldots, U_{p,C_R} \subset (\mathbb{A}^{n+1})^{k+1}$ as in Remark 2. Define $U_p := U_{p,C_1} \cap \cdots \cap U_{p,C_R}$. □

Suppose now that $p \in V$ is a regular point. Let $g_1, \ldots, g_s$ be a system of generators of the ideal $I(V)$. Note that $\dim V = k$ implies $s \geq n - k$. For each $h \in (\mathbb{A}^{n+1})^{k+1}$,

denote by $J_{p,h} \in \mathbb{K}^{(s+k)\times n}$ the Jacobian matrix associated with the polynomials $g_1, \ldots, g_s, \ell_{h_1}, \ldots, \ell_{h_k}$ at the point p. Since p is a regular point of V, the set

$$U_p^J := \{h \in (\mathbb{A}^{n+1})^{k+1} / \operatorname{rank}(J_{p,h}) = n\} \tag{7}$$

is a Zariski dense open subset of $(\mathbb{A}^{n+1})^{k+1}$.

Definition 4. Let U_0 be the Zariski open set defined in (3). For every $p \in \mathbb{A}^n$ such that $p \notin V$ or $p \in V$ is a regular point, consider a Zariski dense open set U_p obeying the condition stated in Proposition 3. We define a Zariski dense open set $\mathcal{U}_p \subset \left(\mathbb{A}^{n+1}\right)^{k+1}$ associated with p as follows:

- If $p \notin V, \mathcal{U}_p := U_p \cap U_0$.
- If $p \in V$ is a regular point, $\mathcal{U}_p := U_p \cap U_p^J \cap U_0$.

3.2. *Existence of generators of low degrees*

Let $p \in V$ be a regular point and let $T_p(V)$ be the tangent space of V at the point p translated to the origin. In other words, if $g_1, \ldots, g_s$ is a system of generators of the ideal $I(V)$, then $T_p(V)$ is the kernel of the Jacobian matrix $J_p(g_1, \ldots, g_s) \in \mathbb{K}^{s\times n}$ of the polynomials $g_l (1 \le l \le s)$ in the point p. Let $\mathcal{U}_p \subset \left(\mathbb{A}^{n+1}\right)^{k+1}$ be the Zariski dense open set introduced in Definition 4.

Lemma 5. *Let $p \in V$ be a regular point and let $h \in \mathcal{U}_p$. Then $\pi_h(p)$ is a regular point of $\pi_h(V)$. Moreover, the identity of local rings $\mathcal{O}_{p,V} = \mathcal{O}_{\pi_h(p),\pi_h(V)}$ holds.*

Proof. Set $q := \pi_h(p)$, $Z := \pi_h(V)$ and, for $j = 1, \ldots, k+1$, $z_j := \ell_{h_j} - \ell_{h_j}(p)$. Since $h \in \mathcal{U}_p \subset U_0$, the linear map $\pi_{h,V} : V \to Z$ induces the integral ring inclusion

$$\mathbb{K}[Z] = \mathbb{K}[\overline{z}_1, \ldots, \overline{z}_{k+1}] \subset \mathbb{K}[V], \tag{8}$$

where, for $j = 1, \ldots, k+1$, $\overline{z}_j$ denotes the class of z_j in the ring of coordinates $\mathbb{K}[V]$. In particular, $\mathbb{K}[V]$ is a finite $\mathbb{K}[Z]$-module. Set

- $\mathfrak{M}_q := (z_1, \ldots, z_k, z_{k+1})\mathbb{K}[Z]$ (the maximal ideal associated with q) and $\mathcal{O}_{q,Z} := \mathbb{K}[Z]_{\mathfrak{M}_q}$;
- $\mathfrak{M}_p$ for the maximal ideal of p in the ring $\mathbb{K}[V]$ and $\mathcal{O}_{p,V} := \mathbb{K}[V]_{\mathfrak{M}_p}$.

As $\mathcal{O}_{p,V}$ is a regular ring and $h \in \mathcal{U}_p \subset U_p^J$, Definition 4 and condition (7) imply that $z_1, \ldots, z_k$ generate the maximal ideal of the local ring $\mathcal{O}_{p,V}$, that is, $\mathfrak{M}_p\mathcal{O}_{p,V} = (z_1, \ldots, z_k)\mathcal{O}_{p,V}$. On the other hand, as $q = \pi_{h,V}(p)$, we have that $\mathfrak{M}_p \cap \mathbb{K}[Z] = \mathfrak{M}_q$ and that the local ring inclusion $\mathcal{O}_{q,Z} \subset \mathcal{O}_{p,V}$ holds. Moreover, since $h \in U_p$, Proposition 3 states that $\pi_{h,V}^{-1}(q) = \{p\}$ or equivalently, in the language of rings, that $\mathfrak{M}_q\mathbb{K}[V]$ is a $\mathfrak{M}_p$-primary ideal. Then, we deduce that

$$\mathfrak{M}_q\mathbb{K}[V] = \mathfrak{M}_p. \tag{9}$$

Let S be the multiplicative closed set $S := \mathbb{K}[Z] \setminus \mathfrak{M}_q$ and let us consider $\mathbb{K}[V]$ as a $\mathbb{K}[Z]$-module. We claim that the following equality holds:

$$S^{-1}\mathbb{K}[V] = \mathcal{O}_{p,V}. \tag{10}$$

The inclusion $S^{-1}\mathbb{K}[V] \subset \mathcal{O}_{p,V}$ follows immediately from the definitions. On the other hand, from identity (9) we infer that $S^{-1}\mathbb{K}[V]$ is a local ring with maximal ideal $\mathfrak{M}_p S^{-1}\mathbb{K}[V]$. For every $\alpha \in \mathbb{K}[V] \setminus \mathfrak{M}_p$, we have $\alpha \notin \mathfrak{M}_p S^{-1}\mathbb{K}[V]$, since $S \cap \mathfrak{M}_p = S \cap \mathfrak{M}_q = \varnothing$. Hence, any fraction $\beta/\alpha \in \mathcal{O}_{p,V}$ with $\beta \in \mathbb{K}[V]$ and $\alpha \in \mathbb{K}[V] \setminus \mathfrak{M}_p$ belongs to $S^{-1}\mathbb{K}[V]$ because α is a unit in the local ring $S^{-1}\mathbb{K}[V]$. Therefore $\mathcal{O}_{p,V} \subset S^{-1}\mathbb{K}[V]$ and so claim (10) is proved.

Now, localizing the integral inclusion (8) at the multiplicative set S, we deduce that $\mathcal{O}_{p,V}$ is a finite $\mathcal{O}_{q,Z}$-module. As $\mathcal{O}_{p,V}/\mathfrak{M}_q\mathcal{O}_{p,V} = \mathbb{K}$, Nakayama's lemma implies that $\mathcal{O}_{p,V}$ is an $\mathcal{O}_{q,Z}$-module with rank 1 and so $\mathcal{O}_{p,V} = \mathcal{O}_{q,Z}$. □

Corollary 6. *Let $p \in V$ be a regular point. For every $h \in \mathcal{U}_p$, the polynomial $f_h^* := f_h(\ell_{h_1}, \ldots, \ell_{h_{k+1}}) \in \mathbb{K}[x_1, \ldots, x_n]$ is the equation of a hypersurface W_h containing V and smooth at p. The tangent space $T_p(W_h)$ is the sum $T_p(V) + L_h^0$, where L_h^0 is the subspace defined in (2).*

Proof. From the definition of the polynomial f_h^*, it follows that $V \subset W_h$. The tangent space $T_p(W_h)$ is the kernel of the row matrix $\nabla f_h^*(p)$ which, using the chain rule, can be written as

$$\nabla f_h^*(p) = \nabla f_h(\pi_h(p)).\left(\frac{\partial \ell_{h_j}}{\partial x_i}(p)\right)_{\substack{1 \le j \le k+1 \\ 1 \le i \le n}}.$$

Observe that $\nabla f_h^*(p) \neq 0$, because $\operatorname{rank}(\partial \ell_{h_j}/\partial x_i(p)) = k+1$ (recall that $h \in \mathcal{U}_p \subset U_0$) and $\nabla f_h(\pi_h(p)) \neq 0$ as $\pi_h(p)$ is a regular point of $\pi_h(V)$ (Lemma 5). Therefore W_h is smooth at p.

Moreover, since $\ker(\partial \ell_{h_j}/\partial x_i(p)) = L_h^0$, the inclusion $L_h^0 \subset T_p(W_h)$ holds and, from the fact that $f_h^* \in I(V)$, we deduce that $T_p(V) \subset T_p(W_h)$. Finally, observe that for every $h \in \mathcal{U}_p \subset U_p^J$ we have $T_p(V) \cap L_h^0 = \{0\}$ and, therefore, $\dim(T_p(V) + L_h^0) = \dim T_p(V) + \dim L_h^0 = k + (n-k-1) = n-1$. We conclude that the equality $T_p(W_h) = T_p(V) + L_h^0$ holds. □

Now we show that the ideal $I(V)$ is locally generated at each regular point of V by polynomials of low degrees.

Lemma 7. *Let $p \in V$ be a regular point, let $I(V)$ be the ideal of the variety V and let $\mathcal{O}_{p,\mathbb{A}^n}$ be the local ring of the point p in the ambient space $\mathbb{A}^n$. Set I_p for the ideal generated by the polynomials f_h^* where h runs over the open set $\mathcal{U}_p$ (see Definition 4). Then $I(V)\mathcal{O}_{p,\mathbb{A}^n} = I_p\mathcal{O}_{p,\mathbb{A}^n}$. Moreover, the identity*

$$I(V)\mathcal{O}_{p,\mathbb{A}^n} = (f_{h^{(1)}}^*, \ldots, f_{h^{(n-k)}}^*)\mathcal{O}_{p,\mathbb{A}^n}$$

holds for every $h^{(1)}, \ldots, h^{(n-k)} \in \mathcal{U}_p$ obeying $\bigcap_{l=1}^{n-k}(T_p(V) + L_{h^{(l)}}^0) = T_p(V)$.

Proof. As $\mathcal{U}_p \subset (\mathbb{A}^{n+1})^{k+1}$ is a Zariski dense open set, there exist vectors $h^{(1)}, \ldots, h^{(n-k)} \in \mathcal{U}_p$ such that $\bigcap_{l=1}^{n-k}(T_p(V) + L_{h^{(l)}}^0) = T_p(V)$. This equality and Corollary 6 imply that, if $f_{h^{(l)}}^* (1 \le l \le n-k)$ are the polynomials defined in (5), then $\bigcap_{l=1}^{n-k} \ker(\nabla f_{h^{(l)}}^*(p)) = T_p(V)$.

From elementary arguments for regular local rings (cf. for instance Kunz, 1985, Chapter VI, Proposition 1.5 or Mumford, 1970, Lemma, p. 34), we infer that the identity $I(V)\mathcal{O}_{p,\mathbb{A}^n} = (f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}})\mathcal{O}_{p,\mathbb{A}^n}$ holds. □

If the variety V is globally smooth (i.e. smooth at each of its points) Lemma 7 admits a well known global version (see Mumford, 1970, Theorem 1; Seidenberg, 1975, Section 2 or Catanese, 1992, Theorem 1.14):

Proposition 8. *Let $V \subset \mathbb{A}^n$ be a smooth equidimensional variety. Then, the ideal $I(V)$ can be generated by the polynomials f^*_h, where h runs over the open set U_0 defined in (3). In particular, $I(V)$ can be generated by polynomials of total degree bounded by* $\deg V$.

Proof. Let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be the ideal generated by the polynomials f^*_h, where h runs over the open set U_0. Since for every $p \in V$ the open set $\mathcal{U}_p$ is contained in U_0, by Lemma 7, the identity $I(V)\mathcal{O}_{p,\mathbb{A}^n} = I\mathcal{O}_{p,\mathbb{A}^n}$ holds for any point $p \in V$. If $q \notin V$, let h be an element of the Zariski dense open set $\mathcal{U}_q \subset U_0$ (see Definition 4). By Proposition 3 we have $\pi_h(q) \notin \pi_h(V)$ and so $f^*_h(q) \neq 0$. Hence, $I\mathcal{O}_{q,\mathbb{A}^n} = \mathcal{O}_{q,\mathbb{A}^n} = I(V)\mathcal{O}_{q,\mathbb{A}^n}$. From the local–global principle we deduce $I(V) = I$.

The upper bound for the degrees of the generators is a consequence of (6). □

3.3. Existence of a few generators of low degree

The goal of this subsection is to refine Proposition 8 in order to obtain, for any k-equidimensional smooth variety V, a "small" number of generators of $I(V)$ of degrees bounded by $\deg V$ (cf. Theorem 10 below).

First, we prove a technical result which enables us to give a recursive proof of the main theorem.

Lemma 9. *Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety and let $Z \subset \mathbb{A}^n$ be an equidimensional variety such that no irreducible component of Z is included in V. Then, for any finite subset $\{p_1, \ldots, p_R\} \subset V$, there exist $h^{(1)}, \ldots, h^{(n-k)} \in U_0$ (see definition (3)) such that:*

(1) *The polynomials $f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}}$ generate the ideal $I(V)$ locally at p_u for $u = 1, \ldots, R$, that is, $I(V)\mathcal{O}_{p_u,\mathbb{A}^n} = (f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}})\mathcal{O}_{p_u,\mathbb{A}^n}$ holds for any point p_u.*

(2) *$\{x \in \mathbb{A}^n / f^*_{h^{(1)}}(x) = 0, \ldots, f^*_{h^{(n-k)}}(x) = 0\} \cap (V \cup Z) = V \cup Z'$, where $Z' = \varnothing$ or Z' is an equidimensional variety with $\dim Z' = \dim Z - (n-k)$ and no irreducible component contained in V. (In particular $Z' = \varnothing$ if $\dim Z < (n-k)$.)*

Proof. Without loss of generality we will suppose $Z \neq \varnothing$ (if $Z = \varnothing$ the argument runs in a similar way).

Following Definition 4, let us consider for $u = 1, \ldots, R$ the Zariski dense open set $\mathcal{U}_{p_u} \subset (\mathbb{A}^{n+1})^{k+1}$. For each irreducible component C of Z, let q_C be a point in $C \setminus V$ and consider the corresponding open set $\mathcal{U}_{q_C} \subset (\mathbb{A}^{n+1})^{k+1}$ also introduced

in Definition 4. Let

$$h^{(1)} \in \bigcap_{u=1}^{R} \mathcal{U}_{p_u} \cap \bigcap_{C} \mathcal{U}_{q_C},$$

which is a Zariski dense open subset of U_0.

By Corollary 6, the polynomial $f^*_{h^{(1)}}$ defines a hypersurface containing V that is smooth at p_u for $u = 1, \ldots, R$. Furthermore, Proposition 3 implies that $f^*_{h^{(1)}}(q_C) \neq 0$ for every irreducible component C of Z. Therefore

$$\{x \in \mathbb{A}^n / f^*_{h^{(1)}}(x) = 0\} \cap (V \cup Z) = V \cup Z_1,$$

where $Z_1 = \varnothing$ or Z_1 is an equidimensional variety with $\dim Z_1 = \dim Z - 1$. Without loss of generality we may assume that $Z_1 \neq \varnothing$ and no irreducible component of Z_1 is contained in V.

Now, for each irreducible component C of Z_1, let $q'_C \in C \setminus V$. Let $h^{(2)} \in (\mathbb{A}^{n+1})^{k+1}$ be a point obeying the conditions

- $h^{(2)} \in \bigcap_{u=1}^{R} \mathcal{U}_{p_u} \cap \bigcap_C \mathcal{U}_{q'_C}$ and
- $\dim_{\mathbb{K}}((L^0_{h^{(1)}} + T_{p_u}(V)) \cap (L^0_{h^{(2)}} + T_{p_u}(V))) = n - 2$ for $u = 1, \ldots, R$.

Observe that such an element $h^{(2)}$ exists because both conditions are given by belonging to Zariski dense open sets.

With a similar argument to the above we deduce that

$$\begin{aligned}\{x \in \mathbb{A}^n / f^*_{h^{(1)}}(x) = 0,\ f^*_{h^{(2)}}(x) = 0\} \cap (V \cup Z) \\ = \{x \in \mathbb{A}^n / f^*_{h^{(2)}}(x) = 0\} \cap (V \cup Z_1) = V \cup Z_2,\end{aligned}$$

where $Z_2 = \varnothing$ or Z_2 is an equidimensional variety with $\dim Z_2 = \dim Z_1 - 1 = \dim Z - 2$. We may also assume that no irreducible component of Z_2 is contained in V.

After applying this procedure $n-k$ times recursively in a similar way, we have elements $h^{(1)}, \ldots, h^{(n-k)} \in \bigcap_{u=1}^{R} \mathcal{U}_{p_u}$ such that:

- For $u = 1, \ldots, R$, $\dim_{\mathbb{K}} \bigcap_{l=1}^{n-k} (L^0_{h^{(l)}} + T_{p_u}(V)) = n - (n-k) = k$ holds and hence $\bigcap_{l=1}^{n-k} (L^0_{h^{(l)}} + T_{p_u}(V)) = T_{p_u}(V)$. In particular, by Lemma 7, the polynomials $f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}}$ meet the first condition of the statement.
- There exists a decomposition

  $$\{x \in \mathbb{A}^n / f^*_{h^{(1)}}(x) = 0, \ldots, f^*_{h^{(n-k)}}(x) = 0\} \cap (V \cup Z) = V \cup Z_{n-k},$$

  where $Z_{n-k} = \varnothing$ or Z_{n-k} is an equidimensional variety with $\dim Z_{n-k} = \dim Z - (n-k)$. Taking $Z' := Z_{n-k}$ we have the second condition of the statement.

This finishes the proof of the lemma. □

Now we are able to prove the main result of this section concerning the number and degree of generators of $I(V)$.

Theorem 10. *Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety and set $m := (n-k)(k+1)$. Then, there exist polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ with degrees bounded*

by $\deg V$ *such that* $I(V) = (f_1, \ldots, f_m)$. *Moreover, for every* $1 \leq t \leq m$, *there exists* $h^{(t)} \in (\mathbb{A}^{n+1})^{k+1}$ *such that* $f_t = f^*_{h^{(t)}}$.

Proof. Without loss of generality, we may suppose $0 < k < n-1$, as the result is well known for $k = 0$ (the so-called "Shape lemma"; see e.g. Cox et al., 1998, Chapter 2, Section 4, Exercise 16) and for $k = n-1$ (where $I(V)$ is a principal ideal). We proceed recursively, applying the previous lemma in each step.

Step 1. For each irreducible component of V choose an arbitrary point, and call these points $p_1, \ldots, p_R$. Applying Lemma 9 to $\{p_1, \ldots, p_R\}$ and the closed set $Z := \mathbb{A}^n$, there exist $h^{(11)}, \ldots, h^{(1(n-k))}$ in U_0 such that

- $I(V)\mathcal{O}_{p_u,\mathbb{A}^n} = (f^*_{h^{(11)}}, \ldots, f^*_{h^{(1(n-k))}})\mathcal{O}_{p_u,\mathbb{A}^n}$ for $u = 1, \ldots, R$; and
- $\{x \in \mathbb{A}^n / f^*_{h^{(11)}}(x) = 0, \ldots, f^*_{h^{(1(n-k))}}(x) = 0\} = V \cup Z_1$, where $Z_1 = \varnothing$ or Z_1 is an equidimensional variety with $\dim Z_1 = n - (n-k)$ and no irreducible component contained in V.

Let $Y_1 \subset V$ be the Zariski closed set consisting of those points of V where the Jacobian matrix $(\partial f^*_{h^{(1l)}}/\partial x_i)_{\substack{1 \leq l \leq n-k \\ 1 \leq i \leq n}}$ has rank at most $n-k-1$. From the Jacobian criterion (see e.g. Kunz, 1985, Chapter VI, Section 1, Proposition 1.5), the points $p_1, \ldots, p_R$ do not belong to Y_1. Then, $\dim Y_1 \leq k-1$. Furthermore, the polynomials $f^*_{h^{(11)}}, f^*_{h^{(12)}}, \ldots, f^*_{h^{(1(n-k))}}$ generate the ideal $I(V)$ locally at any point lying in $V \setminus Y_1$.

Step 2. Choosing one point in each irreducible component of Y_1 we obtain a new finite set $\{p'_1, \ldots, p'_{R'}\} \subset V$. Now we apply Lemma 9 to this set and the variety Z_1 given in Step 1 to obtain new elements $h^{(21)}, \ldots, h^{(2(n-k))}$ in U_0 such that their associated polynomials $f^*_{h^{(21)}}, \ldots, f^*_{h^{(2(n-k))}} \in I(V)$ verify:

- $f^*_{h^{(21)}}, \ldots, f^*_{h^{(2(n-k))}}$ generate the ideal $I(V)$ locally at the points p'_u for $u = 1, \ldots, R'$; and
- $\{x \in \mathbb{A}^n / f^*_{h^{(21)}}(x) = 0, \ldots, f^*_{h^{(2(n-k))}}(x) = 0\} \cap (V \cup Z_1) = V \cup Z_2$, where $Z_2 = \varnothing$ or Z_2 is an equidimensional variety with $\dim Z_2 = \dim Z_1 - (n-k) = n - 2(n-k)$ and no irreducible component contained in V.

Moreover, from the definition of Z_1, we also have that

$$\{x \in \mathbb{A}^n / f^*_{h^{(11)}}(x) = 0, \ldots, f^*_{h^{(1(n-k))}}(x) = 0,\ f^*_{h^{(21)}}(x) = 0, \ldots, f^*_{h^{(2(n-k))}}(x) = 0\}$$

equals $V \cup Z_2$.

Let $Y_2 \subset V$ be the closed set consisting of those points of V for which the rank of the Jacobian matrix of the polynomials $f^*_{h^{(jl)}}\,(j = 1, 2;\ 1 \leq l \leq n-k)$ is at most $n-k-1$. From the definitions, it follows that $Y_2 \subset Y_1$. Moreover, since $p'_1, \ldots, p'_{R'} \in Y_1 \setminus Y_2$ (for the polynomials $f^*_{h^{(2j)}}$ generate the ideal $I(V)$ locally at these points), we deduce that $\dim Y_2 < \dim Y_1 \leq k-1$ and so $\dim Y_2 \leq k-2$.

The procedure continues recursively in a similar way, and after $k+1$ steps we have polynomials $f^*_{h^{(jl)}} \in I(V)$ for $1 \leq j \leq k+1, 1 \leq l \leq n-k$ such that:

- The set $Y_{k+1} \subset V$ where the Jacobian matrix $(\partial f^*_{h^{(jl)}}/\partial x_i)$ associated with the polynomials $f^*_{h^{(jl)}}(1 \leq j \leq k+1, 1 \leq l \leq n-k)$ has rank at most $n-k-1$

obeys $\dim Y_{k+1} \leq \dim V - (k+1)$ and so $Y_{k+1} = \varnothing$. Therefore, the polynomials $f^*_{h^{(jl)}}$ $(1 \leq j \leq k+1, 1 \leq l \leq n-k)$ generate $I(V)$ locally at any point of V.

- The following set-theoretical equality holds:

$$\{x \in \mathbb{A}^n / f^*_{h^{(jl)}}(x) = 0; 1 \leq j \leq k+1, 1 \leq l \leq n-k\} = V \cup Z_{k+1},$$

where $Z_{k+1} = \varnothing$ or Z_{k+1} is an equidimensional variety with $\dim Z_{k+1} \leq n - (k+1)(n-k) = k^2 + k - kn = k(k+1-n)$. Since $0 < k < n-1$, we conclude that $Z_{k+1} = \varnothing$ and then the set of common zeros of the polynomials $f^*_{h^{(jl)}}$ is exactly the variety V.

Hence, the polynomials $f^*_{h^{(jl)}}$ with $1 \leq j \leq k+1, 1 \leq l \leq n-k$ generate the ideal $I(V)$. Inequality (6) gives the upper bound for the degrees of the generators. □

4. Generators and the Chow form

In this section we show how the polynomials f^*_h defined in (5) can be obtained by means of suitable specialization of the Chow form of the variety V (see also Seidenberg, 1975 and Catanese, 1992). This fact is crucial in order to construct an algorithm with "low" complexity bounds for the computation of generators for the ideal of a smooth variety (see Section 5 below).

Let $V \subset \mathbb{A}^n$ be a k-equidimensional affine variety (not necessarily smooth) and let $\overline{V} \subset \mathbb{P}^n$ be its projective closure. We have $\dim V = \dim \overline{V}$ and $\deg V = \deg \overline{V}$. Let H_{ij}, with $0 \leq i \leq n$ and $1 \leq j \leq k+1$, be new indeterminates over the field $\mathbb{K}$. For each index j, set $H_j := (H_{0j}, \ldots, H_{nj})$ and Λ_{H_j} for the generic linear form

$$\Lambda_{H_j} := H_{0j}x_0 + H_{1j}x_1 + \cdots + H_{nj}x_n \in \mathbb{K}[H_1, \ldots, H_{k+1}][x_0, \ldots, x_n].$$

We denote by $\mathcal{F} \in \mathbb{K}[H_1, \ldots, H_{k+1}]$ the Chow form of the projective variety $\overline{V}$ (see for instance Shafarevich (1977, Chapter 1, Sections 5 and 6) for the definition and basic properties of this polynomial). We also say that $\mathcal{F}$ is the Chow form of the affine variety V.

We recall that the Chow form $\mathcal{F}$ is a multihomogeneous polynomial of degree $\deg V$ in each group of variables H_j and, up to scalar factors, it is the unique square-free polynomial in $\mathbb{K}[H_1, \ldots, H_{k+1}]$ with the following property:

$$\mathcal{F}(h_1, \ldots, h_{k+1}) = 0 \Longleftrightarrow \overline{V} \cap \{\Lambda_{h_1} = 0, \ldots, \Lambda_{h_{k+1}} = 0\} \neq \varnothing \text{ in } \mathbb{P}^n. \tag{11}$$

Set $D := \deg V$ and $e := (1, 0, \ldots, 0) \in \mathbb{K}^{n+1}$. The expansion of $\mathcal{F}$ into powers of the variable $H_{0\,k+1}$ is

$$\mathcal{F} = \mathcal{F}(H_1, \ldots, H_k, e)H^D_{0k+1} + C_{D-1}H^{D-1}_{0k+1} + \cdots + C_0, \tag{12}$$

where $C_l \in \mathbb{K}[H_1, \ldots, H_k, H_{1k+1}, \ldots, H_{nk+1}]$ for $0 \leq l \leq D-1$.

Remark 11. Since $\dim(\overline{V} \cap \{x_0 = 0\}) = k-1$, a generic projective linear subvariety of codimension k does not intersect $\overline{V} \cap \{x_0 = 0\}$ and so, by property (11), the polynomial $\mathcal{F}(H_1, \ldots, H_k, e) \in \mathbb{K}[H_1, \ldots, H_k]$ is not the zero polynomial. Moreover,

for $(h_1, \ldots, h_k) \in (\mathbb{A}^{n+1})^k$ we have $\mathcal{F}(h_1, \ldots, h_k, e) \neq 0$ if and only if the system

$$h_{11}x_1 + \cdots + h_{n1}x_n = 0, \ldots, h_{1k}x_1 + \cdots + h_{nk}x_n = 0, x_0 = 0 \tag{13}$$

has no solutions in $\overline{V}$.

Now, we define a condition on the vectors $h \in (\mathbb{A}^{n+1})^{k+1}$ which ensures that the associated polynomials f_h^* can be obtained from the Chow form of V.

Lemma 12. *Let T be a new variable and set*

$$\mathfrak{D} := \operatorname{discr}_T \mathcal{F}(H_1, \ldots, H_k, H_{k+1} - Te) \in \mathbb{K}[H_1, \ldots, H_{k+1}]$$

for the discriminant with respect to the variable T. Then, $\mathfrak{D}$ is not the zero polynomial.

Proof. First, observe that from identity (12) and Remark 11 we have

$$\deg_T \mathcal{F}(H_1, \ldots, H_k, H_{k+1} - Te) = D.$$

Then, in order to prove the lemma it suffices to show that for a suitable specialization of the variables $(H_1, \ldots, H_{k+1}) \mapsto (h_1, \ldots, h_{k+1})$ the univariate polynomial $\mathcal{F}(h_1, \ldots, h_k, h_{k+1} - Te)$ has exactly D many different roots.

Let $(h_1, \ldots, h_k) \in (\mathbb{A}^{n+1})^k$ be such that

$$\#(V \cap \{\ell_{h_1} = 0, \ldots, \ell_{h_k} = 0\}) = D. \tag{14}$$

In other words, $\ell_{h_1}, \ldots, \ell_{h_k}$ is a family of linear polynomials defining a linear variety which intersects V in exactly $\deg V$ many points. Set $Z := V \cap \{\ell_{h_1} = 0, \ldots, \ell_{h_k} = 0\} = \{P_1, \ldots, P_D\}$.

Let $h_{k+1} \in \mathbb{A}^{n+1}$ be a vector such that the associated linear polynomial $\ell_{h_{k+1}}$ separates the points of Z (i.e. $\ell_{h_{k+1}}(P_i) \neq \ell_{h_{k+1}}(P_j)$ for $i \neq j$). Then, there exist $t \in \mathbb{K}$ and $p \in V$ solving the system

$$\ell_{h_1}(p) = 0, \ldots, \ell_{h_k}(p) = 0, \ell_{h_{k+1}}(p) = t$$

if and only if $t \in \{\ell_{h_{k+1}}(P_1), \ldots, \ell_{h_{k+1}}(P_D)\}$ and so $\ell_{h_{k+1}}(P_1), \ldots, \ell_{h_{k+1}}(P_D)$ are D different roots of the polynomial $\mathcal{F}(h_1, \ldots, h_k, h_{k+1} - Te)$.

Finally, let us observe that the polynomial $\mathcal{F}(h_1, \ldots, h_k, h_{k+1} - Te)$ is not identically zero due to (14) and Remark 11. The lemma follows. □

Definition 13. For any k-equidimensional variety $V \subset \mathbb{A}^n$ we define a Zariski dense open set $\mathcal{U}_0 \subset (\mathbb{A}^{n+1})^{k+1}$ as follows:

- If V is not a linear variety, $\mathcal{U}_0 := \{h \in (\mathbb{A}^{n+1})^{k+1} / \mathfrak{D}(h_1, \ldots, h_{k+1}) \neq 0\}$.
- If V is a linear variety (i.e. $\deg V = 1$),

$$\mathcal{U}_0 := \{h \in (\mathbb{A}^{n+1})^{k+1} / \mathcal{F}(h_1, \ldots, h_k, e) \neq 0\} \cap \{h \in (\mathbb{A}^{n+1})^{k+1} / G_0(h) \neq 0\},$$

where $G_0 \in \mathbb{K}[H_1, \ldots, H_{k+1}]$ is the determinant of the matrix $(H_{ij})_{\substack{0 \leq i \leq k \\ 1 \leq j \leq k+1}}$.

Let us observe that $\mathcal{F}(h_1, \ldots, h_k, e) \neq 0$ for every $h := (h_1, \ldots, h_{k+1}) \in \mathcal{U}_0$ (if V is not a linear variety the condition $\mathfrak{D}(h_1, \ldots, h_{k+1}) \neq 0$ means that the univariate polynomial $\mathcal{F}(h_1, \ldots, h_k, h_{k+1} - Te)$ has exactly D simple roots in $\mathbb{K}$ and in particular, by (12), its

leading coefficient $(-1)^D\mathcal{F}(h_1,\ldots,h_k,e)$ is not zero). Hence, for $h \in \mathcal{U}_0$ we have that $\overline{V} \cap \{\Lambda_{h_1} = 0,\ldots,\Lambda_{h_k} = 0, x_0 = 0\} = \varnothing$ and therefore, $\overline{V} \cap \{\Lambda_{h_1} = 0,\ldots,\Lambda_{h_k} = 0\}$ is a finite set in $\mathbb{P}^n$. Moreover, it consists of exactly D points, all of them lying in V, that is

$$\#(V \cap \{\ell_{h_1} = 0,\ldots,\ell_{h_k} = 0\}) = \deg V.$$

It is not difficult to show (see for instance Krick et al., 2001, Lemma 2.14 and Assumption 1.5) that under this last condition the canonical morphism $\mathbb{K}[\ell_{h_1},\ldots,\ell_{h_k}] \hookrightarrow \mathbb{K}[V]$ becomes an integral and injective extension (geometrically, a Noether position for V). This implies that $\ell_{h_1},\ldots,\ell_{h_k}$ are linearly independent polynomials.

Moreover, if V is not a linear variety, we also have that $\ell_{h_1},\ldots,\ell_{h_k},\ell_{h_{k+1}}$ are linearly independent (otherwise, $T = 0$ would be a multiple root of $\mathcal{F}(h_1,\ldots,h_k,h_{k+1} - Te)$). If V is a linear variety the linear independence of $\ell_{h_1},\ldots,\ell_{h_{k+1}}$ follows from the condition $G_0(h) \neq 0$.

From the previous arguments we conclude that the open set $\mathcal{U}_0 \subset (\mathbb{A}^{n+1})^{k+1}$ meets the requirements for the open set U_0 defined in (3) of Section 2 (namely, Noether positions for V and linear independence of the polynomials $\ell_{h_1},\ldots,\ell_{h_{k+1}}$). Hence:

Remark 14. For any $h \in \mathcal{U}_0$, the map $\pi_{h,V} : V \to \mathbb{A}^{k+1}$ is a finite morphism and then there exists a square-free polynomial $f_h \in \mathbb{K}[y_1,\ldots,y_{k+1}]$ such that $\pi_h(V) = \{f_h = 0\}$ (see Section 2.2).

We devote the remaining part of this section to showing that for any $h \in \mathcal{U}_0$ the polynomial f_h can be obtained by suitable specialization of the variables $H_1,\ldots,H_{k+1}$ of the Chow form $\mathcal{F}$ (and so the same holds for f_h^*).

Proposition 15. *Let $h := (h_1,\ldots,h_{k+1}) \in \mathcal{U}_0$ and let $y_1,\ldots,y_{k+1}$ be new indeterminates over $\mathbb{K}$. Then $f_h = \mathcal{F}(h_1 - y_1e,\ldots,h_{k+1} - y_{k+1}e)$.*

Proof. Denote by $\mathfrak{F}_h := \mathcal{F}(h_1 - y_1e,\ldots,h_{k+1} - y_{k+1}e) \in \mathbb{K}[y_1,\ldots,y_{k+1}]$. First we prove that the polynomials $\mathfrak{F}_h$ and f_h have the same zeros in $\mathbb{A}^{k+1}$.

Let $q = (q_1,\ldots,q_{k+1}) \in \{\mathfrak{F}_h = 0\}$. The condition $\mathfrak{F}_h(q) = 0$ means that the system

$$\begin{cases} (h_{01} - q_1)x_0 + h_{11}x_1 + \cdots + h_{n1}x_n & = & 0 \\ \qquad\qquad\vdots & \vdots & \vdots \\ (h_{0k+1} - q_{k+1})x_0 + h_{1k+1}x_1 + \cdots + h_{nk+1}x_n & = & 0 \end{cases} \tag{15}$$

has a solution in $\overline{V}$. Any solution to (15) lying in $\overline{V}$ belongs in fact to the affine part V, since if $(0 : p_1 : \cdots : p_n) \in \overline{V}$ is a solution to (15), then it is also a solution of the linear system (13), which leads to a contradiction with the choice of h in $\mathcal{U}_0$. Therefore, there exists $p := (p_1,\ldots,p_n) \in V$ such that $(1 : p_1 : \cdots : p_n)$ is a solution to (15) and thus, $q = \pi_h(p)$. Conversely, if $q = \pi_h(p)$ for some $p \in V$, then the point $(1 : p_1 : \cdots : p_n) \in \overline{V}$ is a solution to (15) and hence $\mathfrak{F}_h(q_1,\ldots,q_{k+1}) = 0$.

Now, since f_h and $\mathfrak{F}_h$ define set-theoretically the same variety in $\mathbb{A}^{k+1}$, it follows that the two polynomials have the same irreducible factors. On the other hand, the fact that $\operatorname{discr}_T\mathcal{F}(h_1,\ldots,h_k,h_{k+1} - Te) \neq 0$ implies that the polynomial $\mathfrak{F}_h(0,\ldots,0,T) = \mathcal{F}(h_1,\ldots,h_k,h_{k+1} - Te)$ has exactly $\deg V$ different *simple* roots. As f_h is a square-free polynomial, we conclude that $\mathfrak{F}_h = f_h$ up to a scalar factor. □

From the definition of the polynomials f_h^* (see (5)) and Proposition 15, we deduce (see also Seidenberg, 1975, Section 2 and Catanese, 1992, Proof of Theorem (1.14)(a)):

Corollary 16. *Let $\mathcal{F}$ be the Chow form of the variety V and set $e := (1, 0, \ldots 0)$. Then, for any $h \in \mathcal{U}_0$ we have $f_h^* = \mathcal{F}(h_1 - \ell_{h_1} e, \ldots, h_{k+1} - \ell_{h_{k+1}} e)$.* □

Now we are able to restate Theorem 10 in terms of the Chow form of V:

Corollary 17. *Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety and set $m := (n - k)(k + 1)$. There exist $h^{(1)}, \ldots, h^{(m)} \in (\mathbb{A}^{n+1})^{k+1}$ such that the ideal $I(V)$ is generated by the polynomials*

$$\mathcal{F}(h_1^{(1)} - \ell_{h_1^{(1)}} e, \ldots, h_{k+1}^{(1)} - \ell_{h_{k+1}^{(1)}} e), \ldots, \mathcal{F}(h_1^{(m)} - \ell_{h_1^{(m)}} e, \ldots, h_{k+1}^{(m)} - \ell_{h_{k+1}^{(m)}} e). \quad \square$$

5. Algorithmic computation of the generator set

In the following, we assume $\mathrm{char}(\mathbb{K}) = 0$.

We present a probabilistic algorithm for the computation of a set of generators for the ideal of a smooth equidimensional variety $V \subset \mathbb{A}^n$. From a given set of polynomials defining V set-theoretically, the algorithm computes a family of $(n - \dim V)(\dim V + 1)$ polynomials of degrees bounded by $\deg V$ which generate $I(V)$. The algorithm is based on the construction underlying Theorem 10 and on Corollary 16. Our main result is the following:

Theorem 18. *Let $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials of degrees bounded by d. Set $V := \{x \in \mathbb{A}^n : g_1(x) = 0, \ldots, g_s(x) = 0\}$. Assume that V is smooth equidimensional and $0 < \dim V < n - 1$.*

Then there is a probabilistic algorithm which computes, for any $\varepsilon \in (0, 1)$, a set of $(n - \dim V)(1 + \dim V)$ polynomials of degrees bounded by $\deg V$ which generates the ideal $I(V)$ with error probability bounded by ε. The input of the algorithm is the family of defining polynomials $g_1, \ldots, g_s$ encoded by straight-line programs of length L and the parameter ε, and its output is a family of straight-line programs of length $s(nd^n)^{O(1)}L$ encoding the generators of the ideal $I(V)$. The overall complexity of the algorithm is bounded by $s(nd^n)^{O(1)} \log^2(\lceil 1/\varepsilon \rceil)L$.

Although the complexity bounds stated in Theorem 18 are exponential in the input parameters, we can provide *polynomial* complexity bounds by introducing an additional geometric parameter associated with the problem: the *geometric degree* of the input polynomial system. This parameter appears naturally in the complexity estimates when considering certain problems in computational algebraic geometry.

The geometric degree of a polynomial equation system, which is a suitable generalization of the geometric degree of a zero-dimensional system introduced in Giusti et al. (1998), measures the degree of the varieties successively cut out by linear combinations of the input polynomials. For a precise definition we refer the reader to Jeronimo et al. (in press, Section 3.4). For a system of polynomials in n variables

with degrees bounded by d, the geometric degree is bounded by the Bézout number d^n. However, there are many situations in which it is much smaller than this upper bound.

The introduction of this geometric degree in the complexity estimates enables us to derive the following complexity result:

Theorem 19. *Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety with $0 < k < n-1$. Assume that V is the common zero locus of a system of polynomials $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$ of degrees bounded by d which can be encoded by straight-line programs of length L. Let δ be the geometric degree of the system $g_1, \ldots, g_s$.*

Then there exist $(n - \dim V)(1 + \dim V)$ polynomials of degrees bounded by $\deg V$ that generate the ideal $I(V)$ which can be encoded by straight-line programs of length $s(nd\delta)^{O(1)}L$.

In the following subsection we make precise the computational model and the data structure we use. In Section 5.2 we sketch the algorithm given by Jeronimo et al. (in press) for the computation of Chow forms. Our algorithm is described in Section 5.3. The last two subsections of the paper are devoted to proving Theorems 18 and 19.

5.1. Algorithmic model

The algorithms we consider in this paper are described by arithmetic networks (see von zur Gathen, 1986) over a base field $\mathbb{K}$ with $\mathrm{char}(\mathbb{K}) = 0$ which is assumed to be effective (i.e. the arithmetic operations and comparisons between elements in $\mathbb{K}$ are realizable by algorithms). An arithmetic network is represented by means of a directed acyclic graph. The external nodes of the graph correspond to the input and output of the algorithm. Each of the internal nodes of the graph is associated with one of the following operations: an arithmetic operation in $\mathbb{K}$, a comparison between elements in $\mathbb{K}$ (followed by a selection of another node), or a random choice (of a digit 0 or 1).

We assume that the cost of each operation in the algorithm is 1 and so we define the *complexity* of the algorithm as the number of internal nodes in its associated graph.

The algorithm we construct in the next subsection works (that is, it computes the desired output) under certain genericity conditions depending on parameters whose values are chosen randomly. In this sense, we say that the algorithm is *probabilistic*. More precisely, probability is introduced by choosing a random element with equidistributed probability in a set $\{0, \ldots, N-1\}$ for a given positive integer N, which is achieved by means of a procedure that chooses the binary digits of the integer at random. Hence, the complexity of this procedure is $O(\log N)$, where here and in the following, log denotes logarithm in base 2.

As a randomly chosen parameter may not satisfy the required genericity conditions, the algorithm may produce a wrong answer or its execution may finish with an error message. Anyway the probability that this happens can be made arbitrarily small: for each random choice, there exists a non-zero multivariate polynomial F such that every a with $F(a) \neq 0$ leads to a correct computation. Then, the error probability of choosing the parameter a

at random is estimated by the Zippel–Schwartz zero-test (see Zippel, 1979 and Schwartz, 1980) which states that

$$\text{Prob}(F(a) = 0) \leq \frac{\deg F}{N}$$

if the coordinates of a are chosen at random from the set $\{0, \ldots, N-1\}$. This enables us to estimate the error probability of the algorithm and to reduce it as much as desired by choosing N big enough.

The objects our algorithm deals with are polynomials with coefficients in $\mathbb{K}$. The data structure we adopt to represent them is the *straight-line program* encoding. The input, output and intermediate objects computed by our algorithm are polynomials codified by (division-free) straight-line programs defined over $\mathbb{K}$. Roughly speaking, a straight-line program over $\mathbb{K}$ encoding a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ is a program which enables one to evaluate the polynomial f at any given point in $\mathbb{K}^n$. Each of the instructions in this program is an addition, subtraction or multiplication in $\mathbb{K}[x_1, \ldots, x_n]$, or an addition or multiplication by a scalar. The number of instructions in the program is called the *length* of the straight-line program. For a precise definition of straight-line program we refer the reader to Bürgisser et al. (1997, Definition 4.2) (see also Heintz and Schnorr, 1982).

Let us observe that from the vector of coefficients of a polynomial f it is easy to obtain a straight-line program encoding f. The length of this straight-line program is essentially the number of coefficients of the polynomial. Conversely, from a straight-line program of length L encoding an n-variate polynomial f and a positive integer d which is an upper bound for its degree, the usual representation of the polynomial as a vector of coefficients can be computed by means of a straightforward procedure (see, for instance, Bürgisser et al., 1997, Lemma 21.25) within complexity $d^{O(n)}L$.

This observation implies that our algorithm can be adapted so that it could be applied even when the input family is represented by vectors of coefficients, and also that the standard representation of the output by coefficients can be obtained with a controlled increase in the complexity. However, the use of straight-line programs in the intermediate computations of the algorithm is crucial in order to avoid an explosion of the complexity.

Finally, we remark that if $\mathbb{K} = \mathbb{C}$ and the input of our algorithm is a family of polynomials with coefficients in the field of rational numbers $\mathbb{Q}$ encoded by straight-line programs over $\mathbb{Q}$, all of our computations can be performed in the base field $\mathbb{Q}$. In this case, the complexity model may be modified by replacing the unit cost of each arithmetic operation in $\mathbb{Q}$ by its cost as a binary operation (bit complexity model). This does not change the single-exponential behavior of the complexity of our algorithm.

5.2. *Computation of Chow forms*

The main algorithmic tool we will use is the probabilistic algorithm for the computation of the Chow form of an algebraic variety presented in Jeronimo et al. (in press), which we will describe here briefly for the sake of comprehensiveness of our main result and convenience for the reader.

The algorithm is based on a recursive application of a procedure which computes the Chow form of an equidimensional variety $W \subset \mathbb{A}^n$ from a particular description (a *geometric resolution*) of a zero-dimensional subvariety Z of W (the intersection of W with a linear variety of complementary dimension) with $\deg W$ points and a family of $n - \dim W$ polynomials which generate the ideal of W at the points of Z. The crucial ingredient in this procedure is a product formula which enables one to represent the Chow form of W in terms of the Chow forms of zero-dimensional varieties obtained by intersecting of W with generic linear varieties. The Chow forms of these varieties are computed directly from suitable approximations of their points, which in turn are obtained by means of a symbolic version of Newton's algorithm applied to the input zero-dimensional subvariety of W. This leads to an overall complexity polynomial in n, $\deg W$ and an upper bound for the degrees of the input polynomials, and linear in the input length.

We describe the main algorithm in our particular setting, that is, for an affine k-equidimensional variety $V \subset \mathbb{A}^n$ given by s polynomial equations of degrees bounded by d.

The first step consists in a preprocessing of the input data: the algorithm takes $n-k+1$ random linear combinations of the input polynomials and a random linear change of variables so that the varieties $W_i := V(q_1, \ldots, q_i)(1 \leq i \leq n-k)$ successively defined by the new polynomials $q_1, \ldots, q_{n-k+1}$ are equidimensional of dimension $n-i$ and their defining equations generate their ideals locally at the points of conveniently chosen zero-dimensional subvarieties. In addition, $W_{n-k} = V \cup V'$, where V' is a k-equidimensional variety with no irreducible components contained in $V(q_{n-k+1})$.

Then, the Chow forms of the varieties W_i for $i = 1, \ldots, n-k$ are computed recursively by applying the above mentioned procedure and a direct computation of geometric resolutions of zero-dimensional varieties from Chow forms. Finally, the algorithm recovers the Chow form of V as factor of the Chow form of $W_{n-k} = V \cup V'$ using the polynomial q_{n-k+1}.

If the input polynomials are encoded by straight-line programs of length L and $D := \max\{\deg W_i;\ 1 \leq i \leq n-k\}$, the algorithm computes a straight-line program of length $s(ndD)^{O(1)}L$ for the Chow form of V, with error probability bounded by ε, within complexity of order $s(ndD)^{O(1)} \log^2(\lceil 1/\varepsilon \rceil)L$.

We remark that the Bézout inequality implies that $D \leq d^n$. Moreover, if the random choices made during the execution of the algorithm meet the required conditions, D is bounded by the geometric degree of the input system.

5.3. Description of the algorithm

We summarize the algorithm underlying the proof of Theorem 18 in Algorithm 1. Therein, ChowForm$(n, d, g, k, \varepsilon)$ is a procedure which computes, with error probability bounded by ε, the Chow form of the k-equidimensional variety defined in $\mathbb{A}^n$ by the system g of polynomials with degrees bounded by d. Random(a, b, N) denotes a subroutine which selects a vectors of b coordinates each by choosing randomly ab integers from the set $\{0, \ldots, N-1\}$.

Algorithm 1. Computing generators of an ideal

---

procedure Generators$(n, g, d, k, \varepsilon)$

\# n is the number of variables,
\# $g = (g_1, \ldots, g_s)$ is a system of defining equations for a smooth
\# equidimensional affine variety $V \subset \mathbb{A}^n$,
\# d is an upper bound for the degrees of the polynomials g_i $(1 \leq i \leq s)$,
\# $k = \dim V$,
\# $\varepsilon \in \mathbb{Q}$, $0 < \varepsilon < 1$.

\# The procedure returns $(n-k)(k+1)$ polynomials generating $I(V)$ with
\# error probability bounded by ε.

1. $\mathcal{F} :=$ ChowForm$(n, d, g, k, \frac{\varepsilon}{2})$;
2. $N := \lceil 1/\varepsilon \rceil 16(k+1)(n-k)d^{2n}\big((n-k)^{k+1}d^{n(k+1)} + (k+1)d^{n^2}\big)$;
3. **for** j **from** 1 **to** $k+1$ **do**
4. **for** l **from** 1 **to** $n-k$ **do**
5. $h^{(jl)} :=$ Random$(k+1, n+1, N)$;
6. $f^*_{h^{(jl)}} := \mathcal{F}(h_1^{(jl)} - \ell_{h_1^{(jl)}} e, \ldots, h_{k+1}^{(jl)} - \ell_{h_{k+1}^{(jl)}} e)$;
7. **od**;
8. **od**;
9. **return**$(f^*_{h^{(jl)}}; 1 \leq j \leq k+1, 1 \leq l \leq n-k)$

end

5.4. Probability estimates

We have shown in Section 3.3 (Lemma 9 and Theorem 10) that if $k := \dim V$, a generic choice of $(n-k)(k+1)$ linear projections induces a system of generators of the ideal $I(V)$. Now we analyze more deeply this genericity in order to estimate the probability of success of our algorithm, which is computed from the degrees of the polynomials giving the genericity conditions by means of the Zippel–Schwartz zero-test.

Thus, we first obtain upper bounds for the degrees of inequalities defining the open sets appearing in our theoretical discussion of Sections 3 and 4. We gather these estimates in the following remarks. As before, we denote by H_j $(1 \leq j \leq k+1)$ a vector of $n+1$ variables $(H_{0j}, \ldots, H_{nj})$.

We begin with a characterization of the condition on $h \in (\mathbb{A}^{n+1})^{k+1}$ which ensures that the eliminating polynomial f^*_h can be obtained as a specialization of the Chow form of V (see Corollary 16 above).

Remark 20. Let $\mathcal{U}_0 \subset (\mathbb{A}^{n+1})^{k+1}$ be the open set introduced in Definition 13. Then, $\mathcal{U}_0$ can be defined as $\{G \neq 0\}$, where $G \in \mathbb{K}[H_1, \ldots, H_{k+1}] \setminus \{0\}$ and $\deg G \leq 2(k+1)(\deg V)^2$.

Proof. First we consider the case when V is not a linear variety. By Definition 13, the polynomial G can be taken as the discriminant $\mathfrak{D} := \operatorname{disc}_T \mathcal{F}(H_1, \ldots, H_k, H_{k+1} - Te)$, where $\mathcal{F}$ is the Chow form of V and $e := (1, 0, \ldots, 0)$ is the first vector of the canonical basis of $\mathbb{K}^{n+1}$. The degree bound for G is a direct consequence of the definition of discriminant and the degree estimates for the Chow form.

If V is a linear variety, let $G_0 \in \mathbb{K}[H_1, \ldots, H_{k+1}]$ be the determinant of the matrix $(H_{ij})_{\substack{0\le i\le k \\ 1\le j\le k+1}}$ and let $\mathcal{F}$ be the Chow form of V. Then, the polynomial $G := G_0\, \mathcal{F}(H_1, \ldots, H_k, e)$ obeys $\mathcal{U}_0 = \{G \neq 0\}$ and $\deg G \le 2k + 1$. □

The following remark deals with the open sets giving the condition of regularity of a hypersurface $\{f_h^* = 0\}$ at a fixed point of V (see Corollary 6 above).

Remark 21. Let $p \in V$ and let U_p^J be the dense open subset of $(\mathbb{A}^{n+1})^{k+1}$ defined in (7). Then, there exists a Zariski dense open set $U_p \subset U_p^J$ obeying the condition stated in Proposition 3 which can be defined as $\{G \neq 0\}$, where $G \in \mathbb{K}[H_1, \ldots, H_{k+1}] \setminus \{0\}$ and $\deg G \le 2(k+1)(\deg V)^2 + k$.

Proof. Following the proof of Proposition 3, the open set U_p is defined as $U_p = \bigcap_C U_{p,C}$, where the intersection runs over the irreducible components C of V and each $U_{p,C}$ is a Zariski dense open set giving the condition stated in Remark 2.

Let C be an irreducible component of V. Without loss of generality we suppose that C is not a linear variety (the case of a linear variety C is similar). The proof of Remark 2 implies that any open set containing only Noether positions for the cone $\widehat{C}_p$ meets the required condition. Taking into account that $\deg \widehat{C}_p \le \deg C$ (see for instance Harris, 1992, Example 18.16), we conclude by Krick et al. (2001, Lemma 2.14) that there exists a polynomial $G_C \in \mathbb{K}[H_1, \ldots, H_{k+1}]$ with $\deg G_C \le 2(k+1)(\deg C)^2$ such that $G_C(h) \neq 0$ implies h induces a Noether position for the cone $\widehat{C}_p$. Write $G_1 := \prod_C G_C$. Observe that $\deg G_1 \le 2(k+1)\sum_C (\deg C)^2 \le 2(k+1)(\deg V)^2$.

On the other hand, any $n \times n$ non-zero minor of the Jacobian matrix $J_{p,H}$ associated with a system of generators of $I(V)$ and the linear forms induced by the vector $H := (H_1, \ldots, H_k)$ defines a polynomial G_2 of degree k in the vector variables H, such that $G_2(h) \neq 0$ implies $h \in U_p^J$.

We take $U_p = \{G_1 G_2 \neq 0\}$. □

With the same arguments it is easy to show:

Remark 22. Let $q \in \mathbb{A}^n \setminus V$. Then, there exists a non-zero polynomial $G \in \mathbb{K}[H_1, \ldots, H_{k+1}]$, with $\deg G \le 2(k+1)(\deg V)^2$, such that $U_q := \{G \neq 0\}$ is a Zariski dense open set obeying the condition of Proposition 3.

Finally, we consider an additional technical condition in order to ensure that the constructed polynomials generate the ideal $I(V)$ locally at a given point of the variety (see Lemma 7).

Remark 23. Let $p \in V$ and let $\mathcal{U}_p$ be a dense open subset of $(\mathbb{A}^{n+1})^{k+1}$ as in Definition 4. There exists a Zariski dense open set $\mathcal{G}_p \subset (\mathbb{A}^{n+1})^{(k+1)(n-k)}$

such that for every $(h^{(1)},\dots,h^{(n-k)}) \in \mathcal{G}_p \cap (\mathcal{U}_p)^{n-k}$ the following identity holds:

$$\bigcap_{l=1}^{n-k}(T_p(V)+L^0_{h^{(l)}}) = T_p(V).$$

Moreover, the open set $\mathcal{G}_p$ can be defined as $\mathcal{G}_p = \{G_p \neq 0\}$, where $G_p \in \mathbb{K}[H^{(1)},\dots,H^{(n-k)}]$ and $\deg G_p \leq (n-k)(k+1)$. (Here, each $H^{(l)}$ denotes a vector $(H^{(l)}_1,\dots,H^{(l)}_{k+1})$ where $H^{(l)}_j$ is a vector of $n+1$ variables for every $1 \leq j \leq k+1$.)

Proof. Since $\dim T_p(V) = k$ and $T_p(V) \subset \bigcap_{l=1}^{n-k}(T_p(V)+L^0_{h^{(l)}})$ for any choice of vectors $h^{(1)},\dots,h^{(n-k)}$, it suffices to consider an open set $\mathcal{G}_p$ such that for every $(h^{(1)},\dots,h^{(n-k)}) \in \mathcal{G}_p \cap (\mathcal{U}_p)^{n-k}$, $\dim\bigcap_{l=1}^{n-k}(T_p(V)+L^0_{h^{(l)}}) = k$ holds.

Let $\{v_1,\dots,v_k\}$ be a $\mathbb{K}$-basis of $T_p(V)$. For $1 \leq l \leq n-k$, if $h^{(l)} \in \mathcal{U}_p$, $T_p(V)+L^0_{h^{(l)}}$ is the $(n-1)$-dimensional subspace in $\mathbb{K}^n$ defined by the equation

$$\varphi_l : M^{(l)}_1 \ell^0_{h^{(l)}_1} + \cdots + M^{(l)}_{k+1}\ell^0_{h^{(l)}_{k+1}} = 0,$$

where, for every $1 \leq j \leq k+1$, $\ell^0_{h^{(l)}_j} := h^{(l)}_{1j}x_1 + \cdots + h^{(l)}_{nj}x_n$ and $M^{(l)}_j$ denotes the $(k\times k)$-minor obtained by deleting the j-th column of the matrix $(\ell^0_{h^{(l)}_\rho}(v_t))_{t\rho} \in \mathbb{K}^{k\times(k+1)}$. We consider the linear equations $\Phi_1,\dots,\Phi_{n-k}$ constructed as $\varphi_1,\dots,\varphi_{n-k}$ but replacing $h^{(1)},\dots,h^{(n-k)}$ with vectors of variables $H^{(1)},\dots,H^{(n-k)}$.

By elementary linear algebra arguments, it is not difficult to prove the existence of a vector $(h^{(1)},\dots,h^{(n-k)})$ such that $\dim\bigcap_{l=1}^{n-k}(T_p(V)+L^0_{h^{(l)}}) = k$ holds. Hence, the matrix of coefficients of the linear system given by $\Phi_1,\dots,\Phi_{n-k}$ has a $(n-k)\times(n-k)$ non-zero minor G_p. We take $\mathcal{G}_p := \{G_p \neq 0\}$ and the lemma follows. □

Now we are ready to prove an analog of the technical Lemma 9 including probability estimates.

Lemma 24. *Let $V \subset \mathbb{A}^n$ be a k-equidimensional smooth variety and let $f_1,\dots,f_s \in I(V)$ be polynomials with degrees bounded by* $\deg V$ *such that:*

- *$\{f_1 = 0,\dots,f_s = 0\} = V \cup Z$, where $Z \subset \mathbb{A}^n$ is either the empty set or an equidimensional variety with no irreducible components included in V;*
- *$(f_1,\dots,f_s)\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ for every $p \in V \setminus Y$, where Y is an equidimensional subvariety of V.*

Let $N \in \mathbb{N}$. Then choosing the coordinates of vectors $h^{(1)},\dots,h^{(n-k)} \in (\mathbb{A}^{n+1})^{k+1}$ from the set $\{0,\dots,N-1\}$ at random, the following conditions hold with error probability bounded by

$$\frac{2(k+1)(n-k)}{N}((\deg V)^2(1+\deg Y+(\deg V)^n)+(n-k)\deg Y):$$

(1) *For each $1 \leq l \leq n-k$ the polynomial $f^*_{h^{(l)}}$ is well defined (in the sense of Section 2) and it can be computed from the Chow form of V as in Corollary 16.*

(2) $\{f^*_{h^{(1)}} = 0, \ldots, f^*_{h^{(n-k)}} = 0\} \cap (V \cup Z) = V \cup Z'$, *where* $Z' \subset \mathbb{A}^n$ *is either the empty set or an equidimensional variety with* $\dim Z' = \dim Z - (n-k)$ *and no irreducible components included in* V.

(3) $(f_1, \ldots, f_s, f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ *for every* $p \in V \setminus Y'$, *where* Y' *is either the empty set or an equidimensional subvariety of* V *with* $\dim Y' = \dim Y - 1$ *and* $\deg Y' \leq (n-k)\deg(Y)\deg V$.

Proof. The proof follows closely the proof of Lemma 9. Without loss of generality we may assume that N is sufficiently big that the stated error probability is less than 1.

Let $\mathcal{U}_0$ be the open set introduced in Definition 13, which, due to Remark 20, is the complement of a hypersurface of degree bounded by

$$\delta_0 := 2(k+1)(\deg V)^2. \tag{16}$$

Without loss of generality we may assume that $Y \neq \varnothing$. Take a point in each irreducible component of Y and denote these points as $p_1, \ldots, p_R$. For $1 \leq u \leq R$, let U_{p_u} be a Zariski dense open set as in Remark 21, and let $\mathcal{U}_1 := \bigcap_{u=1}^R U_{p_u}$. Since $R \leq \deg Y$, Remark 21 implies that $\mathcal{U}_1$ is the complement of a hypersurface of degree bounded by

$$\delta_1 := (2(k+1)(\deg V)^2 + k)\deg Y. \tag{17}$$

Let $G_{p_u} \in \mathbb{K}[H^{(1)}, \ldots, H^{(n-k)}]$ $(1 \leq u \leq R)$ be the polynomials with

$$\deg G_{p_u} \leq (n-k)(k+1) \tag{18}$$

introduced in Remark 23.

Let $1 \leq r \leq n-k$ and assume that we have vectors $h^{(1)}, \ldots, h^{(r-1)} \in (\mathbb{A}^{n+1})^{k+1}$ obeying:

(i) $h^{(1)}, \ldots, h^{(r-1)} \in \mathcal{U}_0 \cap \mathcal{U}_1$,

(ii) $G_{p_u}(h^{(1)}, \ldots, h^{(r-1)}, H^{(r)}, \ldots, H^{(n-k)}) \not\equiv 0$ for every $1 \leq u \leq R$,

(iii) $\{f_1 = 0, \ldots, f_s = 0, f^*_{h^{(1)}} = 0, \ldots, f^*_{h^{(r-1)}} = 0\} = V \cup Z_{r-1}$, where Z_{r-1} is either the empty set or an equidimensional variety with $\dim Z_{r-1} = \dim Z - (r-1)$ and no irreducible components included in V.

(For $r = 1$, taking $Z_0 := Z$, it is immediate that the above conditions hold.)

Suppose that $Z_{r-1} \neq \varnothing$. For each irreducible component of Z_{r-1}, choose a point not lying in V and call these points $q_1, \ldots, q_{m_r}$. For $1 \leq j \leq m_r$, let U_{q_j} be the Zariski dense open set given in Remark 22 and let $\mathcal{V}_r := \bigcap_{j=1}^{m_r} U_{q_j}$. Taking into account that $\deg Z_{r-1} \leq (\deg V)^n$ (see the Bézout inequality stated in Heintz and Schnorr (1982, Proposition 2.3)), it follows that $\mathcal{V}_r$ is the complement of a hypersurface of degree bounded by

$$D_r := 2(k+1)(\deg V)^2 \deg Z_{r-1} \leq 2(k+1)(\deg V)^{2+n}. \tag{19}$$

If $Z_{r-1} = \varnothing$, we define $\mathcal{V}_r := (\mathbb{A}^{n+1})^{k+1}$.

For $1 \leq u \leq R$, let $G^{(r)}_{p_u} \in \mathbb{K}[H^{(r)}] \setminus \{0\}$ be a non-zero coefficient of the expansion of the polynomial $G_{p_u}(h^{(1)}, \ldots, h^{(r-1)}, H^{(r)}, \ldots, H^{(n-k)})$ with respect to the variables

of the groups $H^{(r+1)}, \ldots, H^{(n-k)}$. Let $\mathcal{W}_r := \bigcap_{u=1}^{R} \{G_{p_u}^{(r)} \neq 0\}$ that, from (18), is the complement of a hypersurface of degree bounded by

$$E_r := (n-k)(k+1)\deg Y. \tag{20}$$

Observe that under conditions (i), (ii) and (iii) the fact that $h^{(r)} \in \mathcal{U}_0 \cap \mathcal{U}_1 \cap \mathcal{V}_r \cap \mathcal{W}_r$ ensures that $G_{p_u}(h^{(1)}, \ldots, h^{(r)}, H^{(r+1)}, \ldots, H^{(n-k)}) \not\equiv 0$ for every $1 \leq u \leq R$, and

$$\{f_1 = 0, \ldots, f_s = 0, f_{h^{(1)}}^* = 0, \ldots, f_{h^{(r)}}^* = 0\} = V \cup Z_r,$$

where Z_r is either empty or an equidimensional variety of dimension $\dim Z_{r-1} - 1 = \dim Z - r$ with no irreducible components included in V.

From (16), (17), (19) and (20), it follows by the Zippel–Schwartz zero-test that choosing the coordinates of $h^{(r)} \in (\mathbb{A}^{n+1})^{k+1}$ at random from the set $\{0, \ldots, N-1\}$, the probability that $h^{(r)} \in \mathcal{U}_0 \cap \mathcal{U}_1 \cap \mathcal{V}_r \cap \mathcal{W}_r$ provided that conditions (i), (ii) and (iii) hold is at least

$$\begin{aligned} P_r &\geq 1 - \frac{1}{N}(\delta_0 + \delta_1 + D_r + E_r) \\ &\geq 1 - \frac{1}{N}(2(k+1)(\deg V)^2(1 + \deg Y + (\deg V)^n) \\ &\quad + ((n-k)(k+1) + k)\deg Y). \end{aligned}$$

Then, if we choose the coordinates of $h^{(1)}, \ldots, h^{(n-k)}$ at random from the set $\{0, \ldots, N-1\}$, the conditions

(a) $h^{(1)}, \ldots, h^{(n-k)} \in \mathcal{U}_0 \cap \mathcal{U}_1$,
(b) $(h^{(1)}, \ldots, h^{(n-k)}) \in \bigcap_{u=1}^{R} \{G_{p_u} \neq 0\}$,
(c) $\{f_1 = 0, \ldots, f_s = 0, f_{h^{(1)}}^* = 0, \ldots, f_{h^{(n-k)}}^* = 0\} = V \cup Z'$, where Z' is either the empty set or an equidimensional variety of dimension $\dim Z - (n-k)$ with no irreducible components included in V,

hold with probability at least

$$\begin{aligned} \prod_{r=1}^{n-k} P_r &\geq 1 - \frac{1}{N}(2(k+1)(n-k)(\deg V)^2(1 + \deg Y + (\deg V)^n \\ &\quad + (n-k)((n-k)(k+1) + k)\deg Y) \\ &\geq 1 - \frac{2(k+1)(n-k)}{N}((\deg V)^2(1 + \deg Y + (\deg V)^n) + (n-k)\deg Y). \end{aligned}$$

Observe that condition (a) implies condition 1 of the lemma by Corollary 16, and that (c) is condition 2. It remains to prove that condition 3 holds.

First, we observe that (a) and (b) imply that $(f_{h^{(1)}}^*, \ldots, f_{h^{(n-k)}}^*)\mathcal{O}_{p_u, \mathbb{A}^n} = I(V)\mathcal{O}_{p_u, \mathbb{A}^n}$ for every $1 \leq u \leq R$ (see Lemma 7 and Remarks 21 and 23). Let $\mathcal{J}$ be the Jacobian matrix of the system $f_{h^{(1)}}^*, \ldots, f_{h^{(n-k)}}^*$. From the previous equality of ideals, for each point p_u $(1 \leq u \leq R)$, there exists a $(n-k) \times (n-k)$-minor $\mathcal{M}_u$ of $\mathcal{J}$ such that $\mathcal{M}_u(p_u) \neq 0$. Therefore, for any generic matrix $Q \in \mathbb{Q}^{n \times n}$, the first principal $(n-k) \times (n-k)$-minor $\mathcal{M}$ of the matrix $\mathcal{J} \cdot Q$ satisfies $\mathcal{M}(p_u) \neq 0$ for every $1 \leq u \leq R$.

Set $Y' := Y \cap \{\mathcal{M} = 0\}$. Note that $\deg(\mathcal{M}) \leq (n-k)\deg V$ and then, by the Bézout inequality (see Heintz, 1983, Theorem 1), $\deg Y' \leq \deg Y \deg(\mathcal{M}) \leq (n-k)\deg Y \deg V$.

Furthermore, by the construction of $\mathcal{M}$, Y' is either the empty set or an equidimensional variety of dimension $\dim Y' = \dim Y - 1$.

Take $p \in V \setminus Y'$. If $p \in V \setminus Y$, the identity of ideals in condition 3 of the lemma holds by the hypotheses. Otherwise, $\mathcal{M}(p) \neq 0$, which implies that $(f^*_{h^{(1)}}, \ldots, f^*_{h^{(n-k)}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ and, in particular, that condition 3 holds. □

Using the previous lemma, we can deduce the following result (a version of Theorem 10 with probability estimates) which allows us to control the error probability of our algorithm:

Proposition 25. *Let $V \subset \mathbb{A}^n$ be a smooth equidimensional variety with $0 < \dim V < n - 1$. Set $k := \dim V$ and $m := (n-k)(k+1)$. Then, for any $N \in \mathbb{N}$, choosing the coordinates of vectors $h^{(1)}, \ldots, h^{(m)} \in (\mathbb{A}^{n+1})^{k+1}$ from the set $\{0, \ldots, N-1\}$ at random we have:*

(1) *for every $1 \leq t \leq m$, the polynomial $f^*_{h^{(t)}}$ is well defined (in the sense of Section 2) and it can be computed from the Chow form of V as in Corollary 16,*
(2) $(f^*_{h^{(1)}}, \ldots, f^*_{h^{(m)}}) = I(V)$

with error probability bounded by

$$\frac{8(k+1)(n-k)(\deg V)^2}{N}((n-k)^{k+1}(\deg V)^{k+1} + (k+1)(\deg V)^n).$$

Proof. We will use Lemma 24 following the recursive arguments underlying the proof of Theorem 10. We may assume that N is sufficiently big in order that the error probability stated in the proposition is less than 1.

Step 1. First, we apply Lemma 24 to the empty family of polynomials (i.e. $s = 0$) and the varieties $Z = \mathbb{A}^n$ and $Y = V$. So, choosing the coordinates of $n-k$ vectors $h^{(11)}, \ldots, h^{(1(n-k))} \in (\mathbb{A}^{n+1})^{k+1}$ at random from the set $\{0, \ldots, N-1\}$, we obtain, with error probability bounded by

$$\varepsilon_1 := \frac{2(k+1)(n-k)}{N}((\deg V)^2(1 + \deg V + (\deg V)^n) + (n-k)\deg V),$$

polynomials $f^*_{h^{(11)}}, \ldots, f^*_{h^{(1(n-k))}}$ as in Corollary 16 such that

- $\{f^*_{h^{(1)}} = 0, \ldots, f^*_{h^{(1(n-k))}} = 0\} = V \cup Z_1$, where $Z_1 \subset \mathbb{A}^n$ is either the empty set or an equidimensional variety with $\dim Z_1 = k$ and no irreducible components included in V;
- $(f^*_{h^{(11)}}, \ldots, f^*_{h^{(1(n-k))}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ for every $p \in V \setminus Y_1$, where Y_1 is either the empty set or an equidimensional subvariety of V with $\dim Y_1 = k-1$ and $\deg Y_1 \leq (n-k)(\deg V)^2$.

Assume now that $r \leq k$ and we have chosen $h^{(jl)} \in (\mathbb{A}^{n+1})^{k+1}$ $(1 \leq j \leq r, 1 \leq l \leq n-k)$ such that the associated polynomials $f^*_{h^{(jl)}} \in I(V)$ obey:

- $\{f^*_{h^{(11)}} = 0, \ldots, f^*_{h^{(1(n-k))}} = 0, \ldots, f^*_{h^{(r1)}} = 0, \ldots, f^*_{h^{(r(n-k))}} = 0\} = V \cup Z_r$, where $Z_r \subset \mathbb{A}^n$ is either the empty set or an equidimensional variety with $\dim Z_r = n - r(n-k)$ and no irreducible components included in V;

- $(f^*_{h^{(11)}}, \ldots, f^*_{h^{(1(n-k))}}, \ldots, f^*_{h^{(r1)}}, \ldots, f^*_{h^{(r(n-k))}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ for every $p \in V \setminus Y_r$, where Y_r is either the empty set or an equidimensional subvariety of V with $\dim Y_r = k - r$ and $\deg Y_r \leq (n-k)^r (\deg V)^{r+1}$.

Step $r+1$. We apply Lemma 24 to the family $f^*_{h^{(jl)}}$ $(1 \leq j \leq r, 1 \leq l \leq n-k)$ and the varieties Z_r and Y_r defined above. Then, choosing at random the coordinates of $n-k$ vectors $h^{((r+1)1)}, \ldots, h^{((r+1)(n-k))} \in (\mathbb{A}^{n+1})^{k+1}$ from the set $\{0, \ldots, N-1\}$, the following conditions hold with error probability bounded by

$$\varepsilon_{r+1} := \frac{2(k+1)(n-k)}{N}((\deg V)^2(1 + (n-k)^r(\deg V)^{r+1} + (\deg V)^n) + (n-k)^{r+1}(\deg V)^{r+1}) :$$

(1) for every $1 \leq l \leq n-k$, the polynomial $f^*_{h^{((r+1)l)}}$ is well defined (in the sense of Section 2) and it can be computed from the Chow form of V as in Corollary 16;

(2) $\{f^*_{h^{(11)}} = 0, \ldots, f^*_{h^{(1(n-k))}} = 0, \ldots, f^*_{h^{((r+1)1)}} = 0, \ldots, f^*_{h^{((r+1)(n-k))}} = 0\} = V \cup Z_{r+1}$, where $Z_{r+1} \subset \mathbb{A}^n$ is either the empty set or an equidimensional variety with $\dim Z_{r+1} = n - (r+1)(n-k)$ and no irreducible components included in V;

(3) $(f^*_{h^{(11)}}, \ldots, f^*_{h^{(1(n-k))}}, \ldots, f^*_{h^{((r+1)1)}}, \ldots, f^*_{h^{((r+1)(n-k))}})\mathcal{O}_{p,\mathbb{A}^n} = I(V)\mathcal{O}_{p,\mathbb{A}^n}$ for every $p \in V \setminus Y_{r+1}$, where Y_{r+1} is either the empty set or an equidimensional subvariety of V with $\dim Y_{r+1} = k - r - 1$ and $\deg Y_{r+1} \leq (n-k)^{r+1}(\deg V)^{r+2}$.

Observe that after $k+1$ steps, both varieties Z_{k+1} and Y_{k+1} appearing in conditions (2) and (3) respectively must be the empty set. Hence, a random choice of $(n-k)(k+1)$ vectors in $(\mathbb{A}^{n+1})^{k+1}$ with coordinates in $\{0, \ldots, N-1\}$ yields, with probability at least $P := \prod_{r=1}^{k+1}(1 - \varepsilon_r)$, a family of $(n-k)(k+1)$ polynomials associated with the Chow form of V as in Corollary 16, whose set of common zeros is V and that generate $I(V)$.

The probability P can be estimated as $P \geq 1 - \sum_{r=1}^{k+1} \varepsilon_r$, that is,

$$P \geq 1 - \frac{2(k+1)(n-k)}{N}((\deg V)^2((k+1)(1 + (\deg V)^n) + \sum_{r=1}^{k+1}(n-k)^{r-1}(\deg V)^r) \sum_{r=1}^{k+1}(n-k)^r(\deg V)^r).$$

Taking into account that $\sum_{r=0}^{k} a^r \leq 2a^k$ for every $a \geq 2$, the assumption $0 < k < n-1$ implies that

$$\begin{aligned} P &\geq 1 - \frac{4(k+1)(n-k)(\deg V)^2}{N}((n-k)^k(\deg V)^{k+1} \\ &\quad + (n-k)^{k+1}(\deg V)^{k-1} + (k+1)(\deg V)^n) \\ &\geq 1 - \frac{8(k+1)(n-k)(\deg V)^2}{N}((n-k)^{k+1}(\deg V)^{k+1} + (k+1)(\deg V)^n), \end{aligned}$$

and the proposition follows. □

5.5. *The complexity of the algorithm*

We devote this subsection to the complexity analysis of the algorithm described in Section 5.3.

First, we prove our main complexity result:

Proof of Theorem 18. The first step of the algorithm consists in the computation of the Chow form of V from the given polynomials $g_1, \ldots, g_s$ defining V. This is done with error probability bounded by $\varepsilon/2$ by means of the algorithm described in Jeronimo et al. (in press), which computes a straight-line program of length bounded by $s(nd^n)^{O(1)}L$ encoding the Chow form of V within complexity $s(nd^n)^{O(1)}\log^2(\lceil 1/\varepsilon\rceil)L$.

Let $N := \lceil 1/\varepsilon\rceil 16(k+1)(n-k)d^{2n}((n-k)^{k+1}d^{n(k+1)} + (k+1)d^{n^2})$. Then, the procedure chooses randomly the coordinates of $(n-k)(k+1)$ vectors $h^{(jl)} \in (\mathbb{A}^{n+1})^{k+1}$ for $1 \le j \le k+1, 1 \le l \le n-k$, from the set $\{0, \ldots, N-1\}$. The complexity of this step is bounded by $O((n-k)(k+1)^2(n+1)\log N) = O(n^4(\log\lceil 1/\varepsilon\rceil + n^2\log d))$ (see Section 5.1).

Finally, provided that the polynomial computed in the first step is the Chow form of V, the algorithm obtains with error probability bounded by $\varepsilon/2$ straight-line programs of length $s(nd^n)^{O(1)}L$ encoding the polynomials $f^*_{h^{(jl)}}$ $(1 \le j \le k+1, 1 \le l \le n-k)$ by specializing as in Corollary 16 the Chow form of V using the coordinates of $h^{(jl)}$ (see Proposition 25 and observe that $\deg V \le d^n$). This step does not modify the order of complexity.

The complexity of the whole algorithm is bounded by $s(nd^n)^{O(1)}\log^2(\lceil 1/\varepsilon\rceil)L$ and its error probability is at most ε. □

Remark 26. Observe that the first step of Algorithm 1 can be performed by any algorithm computing Chow forms of equidimensional varieties. For instance, applying the algorithm described in Jeronimo et al. (2001), which unlike that of Jeronimo et al. (in press) is a deterministic algorithm, we would obtain a slightly better upper bound for the total complexity in Theorem 18: $s(nd^n)^{O(1)}\log(\lceil 1/\varepsilon\rceil)L$. However, the subroutine we use enables us to obtain complexity bounds in terms of a more intrinsic parameter (see Theorem 19).

Proof of Theorem 19. The complexity of the algorithm presented in Jeronimo et al. (in press) for the computation of the Chow form of a variety V, as well as the length of the output straight-line program can be estimated using the geometric degree of the given system of defining equations for V.

This implies straightforwardly that the complexity of our algorithm and the length of their output straight-line programs can also be estimated in terms of the geometric degree δ of the input polynomial equation system $g_1, \ldots, g_s \in \mathbb{K}[x_1, \ldots, x_n]$: if all the parameters chosen at random during the execution of the algorithm satisfy the required genericity conditions, the algorithm finishes, producing a system of generators of $I(V)$, within time $s(nd\delta)^{O(1)}\log^2(\lceil 1/\varepsilon\rceil)L$, where, as before, d is an upper bound for the degree of the polynomials g_i and L is a bound for the length of the input straight-line programs. The polynomials computed by the algorithms are encoded by straight-line programs of length $s(nd\delta)^{O(1)}L$. □

Acknowledgements

C. Blanco, G. Jeronimo and P. Solernó were partially supported by UBACyT grant X198. G. Jeronimo and P. Solernó were also partially supported by Consejo Nacional de Investigaciones Científicas y Técnicas (CONICET), Argentina.

The authors wish to thank Marc Chardin for helpful comments. The third author also thanks Marc Giusti and the Laboratoire GAGE (École Polytechnique, Palaiseau), where part of this paper was prepared in spring 2002.

References

Abhyankar, S.S., 1973. On Macaulay's example. In: Conf. Comm. Algebra, Lawrence 1972, Springer LNM, vol. 311. pp. 1–16.

Alonso, M.E., Mora, T., Raimondo, M., 1991. Local decomposition algorithms. In: Proc. of AAECC-8, Tokyo 1990, Springer LNCS, vol. 508. pp. 208–221.

Armendáriz, I., Solernó, P., 1995. On the computation of the radical of polynomial complete intersection ideals. In: Cohen, G., Giusti, M., Mora, T. (Eds.), Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes. Springer LNCS, vol. 948. pp. 106–119.

Bayer, D., Mumford, D., 1993. What can be computed in Algebraic Geometry? In: Eisenbud, D., Robbiano, L. (Eds.), Computational Algebraic Geometry and Commutative Algebra, Cortona 1991. Symposia Math., vol. XXXIV. Cambridge Univ. Press, pp. 1–48.

Bürgisser, P., Clausen, M., Shokrollahi, M.A., 1997. Algebraic Complexity Theory. Springer.

Catanese, F., 1992. Chow varieties, Hilbert schemes, and moduli spaces of surfaces of general type. J. Algebraic Geom. 1, 561–595.

Cox, D., Little, J., O'Shea, D., 1998. Using Algebraic Geometry. Grad. Texts in Math., vol. 185. Springer-Verlag.

Eisenbud, D., 1994. Commutative Algebra with a View Toward Algebraic Geometry. Grad. Texts in Math. vol. 150. Springer-Verlag.

Eisenbud, D., Evans, Jr. E.G., 1973. Every algebraic set in n-space is the intersection of n hypersurfaces. Invent. Math. 19, 107–112.

Eisenbud, D., Huneke, C., Vasconcelos, W., 1992. Direct methods for primary decomposition. Invent. Math. 110, 207–235.

Fortuna, E., Gianni, P., Trager, B., 2002. Derivations and radicals of polynomial ideals over fields of arbitrary characteristic. J. Symbolic Comput. 33, 609–625.

Geramita, A., 1983. Remarks on the number of generators of some homogeneous ideals. Bull. Soc. Math. France 107, 197–207.

Gianni, P., Trager, B., Zacharias, G., 1988. Gröbner bases and primary decomposition of polynomial ideals. J. Symbolic Comput. 6, 149–167.

Giusti, M., 1984. Some effectivity problems in polynomial ideal theory. In: EUROSAM 84. Springer LNCS, vol. 204. pp. 159–171.

Giusti, M., Heintz, J., Morais, J.E., Morgenstern, J., Pardo, L.M., 1998. Straight-line programs in geometric elimination theory. J. Pure Appl. Algebra 124, 101–146.

Harris, J., 1992. Algebraic Geometry. Grad. Texts in Math., vol. 133. Springer-Verlag.

Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. 24 (3), 239–277.

Heintz, J., Schnorr, C.-P., 1982. Testing polynomials which are easy to compute. Monographie de l'Enseignement Mathématique, vol. 30. pp. 237–254.

Jeronimo. G., 2002. Descomposición equidimensional efectiva de variedades algebraicas. Ph.D. Thesis, Universidad de Buenos Aires.

Jeronimo, G., Krick, T., Sabia, J., Sombra, M., 2002. The computational complexity of the Chow form. Found. Comput. Math. 4 (1), 41–117. Available from arXiv: math.AG/021009v1.

Jeronimo, G., Puddu, S., Sabia, J., 2001. Computing Chow forms and some applications. J. Algorithms 41, 52–68.

Kaltofen, E., 1988. Greatest common divisors of polynomials given by straight-line programs. J. ACM 35 (1), 234–264.

Kemper, G., 2002. The calculation of radical ideals in positive characteristic. J. Symbolic Comput. 34, 229–238.

Krick, T., Logar, A., 1992. An algorithm for the computation of the radical of an ideal in the ring of polynomials. In: Proc. AAECC-9, New Orleans 1991, Springer LNCS, vol. 539. pp. 195–205.

Krick, T., Pardo, L.M., Sombra, M., 2001. Sharp estimates for the arithmetic Nullstellensatz. Duke Math. J. 109 (3), 521–598.

Kronecker, L., 1882. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. J. reine angew. Math. 92, 1–123.

Kumar, M., 1978. On two conjectures about polynomial rings. Invent. Math. 46, 225–236.

Kunz, E., 1985. Introduction to Commutative Algebra and Algebraic Geometry. Birkhäuser, Boston.

Lyubeznik, G., 1989. A survey of problems and results on the number of defining equations. In: Hochster, M., Huneke, C., Sally, J.D. (Eds.), Comm. Algebra. Math. Sci. Research Inst. Pub., vol. 15. Springer-Verlag, pp. 375–390.

Macaulay, F.S., 1916. The algebraic theory of modular systems. Cambridge University Press.

Matsumoto, R., 2001. Computing the radical of an ideal in positive characteristic. J. Symbolic Comput. 32, 263–271.

Mumford, D., 1970. Varieties defined by quadratic equations. In: Marchionna, C. (Ed.), Proc. of Questions on Algebraic Varieties. Centro Internazionale de Matematica Estivo, Varenna, 1969, Ed. Cremonese, Roma, pp. 29–100.

Mumford, D., 1995. Algebraic Geometry. I: Complex Projective Varieties. Classics in Math., Springer-Verlag.

Nagel, U., Schenzel, P., 1998. Degree bounds for generators of cohomology modules and regularity. Nagoya Math. J. 152, 153–174.

Sathaye, A., 1978. On the Forster–Eisenbud–Evans conjecture. Invent. Math. 46, 211–224.

Schwartz, J.T., 1980. Fast probabilistic algorithms for verification of polynomial identities. J. ACM 27, 701–717.

Seidenberg, A., 1975. On the Chow form. Math. Ann. 212, 183–190.

Shafarevich, I., 1977. Basic Algebraic Geometry. Study edition, Springer-Verlag.

Shafarevich, I., 1994. Basic Algebraic Geometry 1. Varieties in Projective Spaces. Springer-Verlag.

Storch, U., 1972. Bemerkung zu einem Satz von M. Kneser. Arch. Math. 23, 403–404.

van der Waerden, B.L., 1939. Einführung in die algebraische Geometrie. Julius Springer.

Vasconcelos, W., 1992. Jacobian matrices and constructions in algebra. In: Proc. AAECC-9, New Orleans 1991, Springer LNCS, vol. 539. pp. 45–64.

von zur Gathen, J., 1986. Parallel arithmetic computations: a survey. In: Proc. 12th FOCS, Bratislava, 1986, Springer LNCS, vol. 33. pp. 93–112.

Zippel, R., 1979. Probabilistic algorithms for sparse polynomials. In: Proc. EUROSAM'79. Springer LNCS, vol. 72. pp. 216–226.