

Computing an Equidimensional Decomposition of an Algebraic Variety by means of Geometric Resolutions

Grégoire Lecerf

Laboratoire GAGE, École polytechnique
F-91128 Palaiseau, France
lecerf@gage.polytechnique.fr

Abstract

Let f_1, \dots, f_s be polynomials in n variables over a field of characteristic zero and d be the maximum of their total degree. We propose a new probabilistic algorithm for computing a *geometric resolution* of each equidimensional part of the variety defined by the system $f_1 = \dots = f_s = 0$. The returned resolutions are encoded by means of *Straight-Line Programs* and the complexity of the algorithm is polynomial in a *geometric degree* of the system. In the worst case this complexity is asymptotically polynomial in sd^n .

Introduction

Let k be a field of characteristic zero, f_1, \dots, f_s be s polynomials in $k[x_1, \dots, x_n]$ and d be the maximum of their total degree. Let $\mathcal{V} = \mathcal{V}(f_1, \dots, f_s)$ be the algebraic variety defined by the system $f_1 = \dots = f_s = 0$ in the n dimensional affine space over an algebraic closure \bar{k} of k . We are interested in computing an exact description of \mathcal{V} , from the computer algebra point of view.

Up to now, the best complexity upper bound known is asymptotically polynomial in sd^{n^2} : in [3] Chistov and Grigoriev present an algorithm with such a complexity for computing a decomposition of \mathcal{V} into irreducible components; Giusti and Heintz give in [9] another method with the same complexity, moreover their decomposition into equidimensional parts is well-parallelizable; Elkadi and Mourrain propose in [4] a method based on Bézoutian matrices, their algorithm is probabilistic.

Our aim is to present an algorithm which computes a *geometric resolution* of each equidimensional part of the variety \mathcal{V} with a complexity polynomial in some intrinsic degree of the system and, by the way, polynomial in sd^n in the worst case.

Our algorithm stores eliminating polynomials by means of *Straight-Line Programs* (SLP) without division; our method lies in the continuation of a series of papers initiated by Giusti, Heintz, Hägele, Morais, Montaña, Morgenstern and Pardo: in [7, 11] they give an algorithm for computing

the isolated points solutions of any polynomial equation system with a complexity polynomial in an *intrinsic degree* of the system. In [12] we simplify and redesign the algorithm and explain how to implement it. Our aim is now to extend the theoretical method in order to compute not only the isolated roots but a description of all the components.

In the sequel, L represents the complexity of the given SLP encoding the input system f_1, \dots, f_s . When considering degrees of algebraic varieties we use *Heintz' degree* [13], that is the sum of the degrees of all the isolated irreducible components appearing in a minimal decomposition of the variety.

Let $t_{i,j}$ for $1 \leq i \leq n+1$ and $1 \leq j \leq s$, be some new generic parameters taking their value in k . Let g_i be the generic linear combination $\sum_{j=1}^s t_{i,j} f_j$, for $1 \leq i \leq n+1$. We define the *intermediate varieties* \mathcal{V}_i as $\mathcal{V}(g_1, \dots, g_i)$ for $0 \leq i \leq n+1$ and we define the *intrinsic degree* δ of the system as being the maximum of the degrees δ_i of \mathcal{V}_i , $0 \leq i \leq n$. Note that by convention \mathcal{V}_0 represents the whole space \bar{k}^n .

Theorem 1 *There exist a dense open subset \mathcal{G} of $k^{(n+1)s}$ and a deterministic algorithm such that: if the values of the $t_{i,j}$ are taken in \mathcal{G} , it computes a minimal geometric resolution, encoded by SLP, of \mathcal{V} with a non-uniform complexity polynomial in $Lns\delta\delta$, in terms of the number of arithmetic operations in k .*

Let α be a positive integer, if Ω is a set of points of size $3\alpha(d+1)^{3n}$ in k , a random point $t_{i,j}$ in $\Omega^{(n+1)s}$ belongs to \mathcal{G} with probability of success at least $1 - (sn)^c/\alpha$ for some universal positive constant c .

The definition of geometric resolutions is stated in the next section and the complexity model in §3.1. Note that δ is bounded by d^n , using the Bézout inequality [13].

The deterministic algorithm of the theorem admits a bounded error probabilistic counterpart in a uniform complexity model (see discussion in §3.1).

Our algorithm relies on the properties of the \mathcal{V}_i and their relation with \mathcal{V} ; we adapt the results of [11] in order to perform splittings when irregular intersections occur. So the paper is organized as follows: we first recall the definition of a geometric resolution, then we describe the properties of the generic system $g_1 = \dots = g_{n+1} = 0$ and the last part is devoted to the description of the algorithm and the proof of Theorem 1. Appendix 3.3 details a technical result contained in [11] but without an independent statement.

1 Definitions

Let \mathcal{W} be a r -equidimensional algebraic variety and \mathfrak{I} its annihilating ideal in $k[x_1, \dots, x_n]$.

Let M be an invertible $n \times n$ square matrix with entries in k , we say that the new coordinates $y = M^{-1}x$ are in *Noether position* with respect to \mathcal{W} if the following two conditions hold: the variables y_1, \dots, y_r are *free*, which means that the canonical projection from \mathcal{W} to the affine space generated by y_1, \dots, y_r is surjective, and the ring morphism

$$R := k[y_1, \dots, y_r] \longrightarrow k[y_1, \dots, y_n]/(f_1, \dots, f_s) =: B$$

defines an integral ring extension.

Let K be the field of fractions of R and B' the finite-dimensional K -vector space $K \otimes B$. A linear form u is said to be a primitive element of \mathcal{W} if its set of powers generates B' .

A *geometric resolution* of \mathcal{W} is defined by:

- an invertible $n \times n$ square matrix M with entries in k such that the new coordinates $y = M^{-1}x$ are in Noether position with respect to \mathcal{W} ;
- a primitive element $u = \lambda_{r+1}y_{r+1} + \dots + \lambda_n y_n$ of \mathcal{W} , with the λ_j in k ;
- the minimal polynomial $q(T) \in R[T]$ of u in B' , monic in T , with degree in T equal to the dimension of B' and
- the *parametrization* of \mathcal{W} by the zeros of q , given by polynomials

$$\rho y_{r+1} - v_{r+1}(T), \dots, \rho y_n - v_n(T),$$

where ρ is in R and the v_j are in $R[T]$ with degree in T strictly less than the one of q and such that B' is isomorphic to $K[T]/(q(T), \rho y_{r+1} - v_{r+1}(T), \dots, \rho y_n - v_n(T))$.

The total degree of q is bounded by $\deg(\mathcal{W})$ and those of ρ and the v_j can be bounded by $\deg(\mathcal{W})^5$ [12, 23].

If \mathcal{W} is not equidimensional, we call a *minimal geometric resolution* a decomposition of \mathcal{W} in $\mathcal{W}_0 \cup \mathcal{W}_1 \cup \dots \cup \mathcal{W}_n$ such that \mathcal{W}_i is either empty or an algebraic variety of codimension i and no component of any \mathcal{W}_j is included in another one, each \mathcal{W}_j being described by means of a geometric resolution.

2 Preparation Lemmas

The first part of our algorithm is incremental in the number of the g_i 's: we give geometric resolutions of $\mathcal{V}_0, \mathcal{V}_1, \dots, \mathcal{V}_{n+1}$ in sequence. The following lemmas give the properties of this sequence when the $t_{i,j}$ are chosen generic enough.

The first lemma shows that the "interesting" successive intersections of the g_i 's are regular. Note that this lemma is a local version of [10, §3.4.1] of Giusti and Heintz (see also [13, 9]).

Lemma 1 *For all $i, 0 \leq i \leq n$, for any $t_{k,l}$ in $k, 1 \leq k \leq i, 1 \leq l \leq s$, there exists a nonzero polynomial P_{i+1} in $k[(T_{i+1,l})_{1 \leq l \leq s}]$ of total degree bounded by d^i such that: for all $t_{i+1,l}, 1 \leq l \leq s, P_{i+1}((t_{i+1,l})_{1 \leq l \leq s}) \neq 0$ implies that for any irreducible component \mathcal{M} of codimension i of the variety \mathcal{V}_i the following alternative holds: \mathcal{M} is in \mathcal{V} or $\mathcal{V}(g_{i+1})$ intersects \mathcal{M} regularly.*

Proof. Let \mathcal{M} be an irreducible component of \mathcal{V}_i of codimension i not included in \mathcal{V} , so that there exists some m such that \mathcal{M} is not included in the hypersurface defined by $f_m = 0$. We take a point $C_{\mathcal{M}}$ in \mathcal{M} not in $\mathcal{V}(f_m)$. Let us associate such a point $C_{\mathcal{M}}$ to each irreducible component of \mathcal{V}_i of codimension i not included in \mathcal{V} . Let P_{i+1} be the polynomial defined by

$$\prod_{\mathcal{M}} (T_{i+1,1} f_1(C_{\mathcal{M}}) + \dots + T_{i+1,s} f_s(C_{\mathcal{M}})).$$

By construction P_{i+1} is not identically zero, has total degree bounded by d^i and has the required property. \square

We apply incrementally the lemma: first we choose values for $t_{1,1}, \dots, t_{1,s}$, then for $t_{2,1}, \dots, t_{2,s}$ and so on until $t_{n+1,1}, \dots, t_{n+1,s}$. The system of g_i 's we obtain satisfies the following property, denoted by R_1 in the sequel:

R₁: for all $i, 0 \leq i \leq n$, an irreducible component of \mathcal{V}_i of codimension i is either included in \mathcal{V} or regularly intersected by g_{i+1} .

We now quantify the probability of success of this construction.

Proposition 1 *Let α be a strictly positive integer, and Ω be a set of points of k of cardinal αd^n . A random choice of all the $t_{i,j}, 1 \leq i \leq n+1, 1 \leq j \leq s$, in $\Omega^{(n+1)s}$ leads to polynomials g_i satisfying the property R_1 with a probability at least $1 - (sn)^{c_1}/\alpha$, for some universal positive constant c_1 .*

Proof. Using Zippel-Schwartz' zero test [24, 25], the probability that a point $(t_{i+1,1}, \dots, t_{i+1,s})$ chosen at random in Ω^s is not a zero of P_{i+1} is at least $1 - s/\alpha$. Thus the probability that some $t_{i,j}$ chosen at random in $\Omega^{(n+1)s}$ define some g_i satisfying the property R_1 is at least $(1 - s/\alpha)^{n+1} \geq 1 - s(n+1)/\alpha$. \square

In the sequel we denote by \mathcal{V}_i^P (Pure codimension) the variety composed of the components of \mathcal{V}_i of codimension i , by \mathcal{V}_i^R (Regularly intersected) the ones of \mathcal{V}_i^P being intersected regularly by g_{i+1} and \mathcal{V}_i^I (Improper) the ones of \mathcal{V}_i^P included in the hypersurface defined by $g_{i+1} = 0$.

Proposition 2 *For choices of $t_{i,j}$ such that properties R_1 holds, the varieties \mathcal{V}_i satisfy the following properties.*

1. For $i \geq 0$, the minimal equidimensional decomposition of \mathcal{V}_i is given by

$$\mathcal{V}_0^I \cup \dots \cup \mathcal{V}_{i-1}^I \cup \mathcal{V}_i^P.$$

2. The minimal decomposition of \mathcal{V} into equidimensional parts is

$$\mathcal{V}_0^I \cup \mathcal{V}_1^I \cup \dots \cup \mathcal{V}_n^I.$$

Proof. We prove the first point by induction on i . The case $i = 0$ is trivial, let us assume that the property is true for a given $i \geq 0$. The variety \mathcal{V}_{i+1} is the intersection of \mathcal{V}_i by the hypersurface defined by g_{i+1} , the property R_1 implies that all the $\mathcal{V}_j^I, 1 \leq j \leq i$, are included in \mathcal{V} , thus in the hypersurface defined by g_{i+1} . Hence \mathcal{V}_{i+1} equals $\mathcal{V}_0^I \cup \dots \cup \mathcal{V}_i^R \cup \mathcal{V}_i^I \cap \mathcal{V}(g_{i+1})$. The variety \mathcal{V}_{i+1}^P is then the union of the irreducible components of $\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1})$ not included in $\mathcal{V}_0^I \cup \dots \cup \mathcal{V}_i^I$. The property holds at $i+1$.

For the second point, the inclusion of $\mathcal{V}_0^I \cup \mathcal{V}_1^I \cup \dots \cup \mathcal{V}_n^I$ in \mathcal{V} is a direct consequence of the property R_1 . For the reverse inclusion, let \mathcal{M} be an irreducible component of \mathcal{V} of codimension $i > 0$. The variety \mathcal{M} is included in \mathcal{V}_0^R , let j be the greatest index such that \mathcal{M} is included in \mathcal{V}_j^R and not in \mathcal{V}_{j+1}^R . Necessarily \mathcal{M} is included in $\mathcal{V}_j^R \cap \mathcal{V}(g_{j+1})$. If \mathcal{M} is included in one of the \mathcal{V}_k^I for a given $k \leq j$ we are done, otherwise \mathcal{M} is included in \mathcal{V}_{j+1}^P , and thus in \mathcal{V}_{j+1}^I . \square

Let us now turn to the question of the multiplicities of the components of the \mathcal{V}_i . The next lemma is a weak local version of Bertini's first theorem, the complete proof we give of our assertion has been inspired by Bertini's original one as explained by Kleiman in [16]. This result is also a local version of [17, Proposition 37] or [23, Proposition 4.4].

Lemma 2 *For each i , $0 \leq i \leq n$, there exists a non zero polynomial Q_i in $\bar{k}[(T_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s}]$ of total degree bounded by $3(d+1)^{3i}$ such that: for all $t_{k,l}$ in k , $1 \leq k \leq i$, $1 \leq l \leq s$, $Q_i((t_{i+1,l})_{1 \leq l \leq s}) \neq 0$ implies that for any irreducible component \mathcal{M} of codimension i of the variety \mathcal{V}_i the following alternative holds: \mathcal{M} is included in \mathcal{V} or \mathcal{M} is reduced with respect to g_1, \dots, g_i .*

Proof. First we prove that when the $t_{k,l}$ are generic the alternative holds.

In this proof R represents the polynomial ring $k[(T_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s}]$, K its field of functions, G_i the polynomials $T_{i,1}f_1 + \dots + T_{i,s}f_s$, for $1 \leq i \leq n$. Let us now fix i in the range $0 \dots n$, let r be $n - i$ and \mathcal{M} be an irreducible component of the variety defined by G_1, \dots, G_i in $K[x_1, \dots, x_n]$. Let us consider a geometric resolution of \mathcal{M} : let y_1, \dots, y_n be the variables in Noether position, $y = M^{-1}x$, u the primitive element, q the minimal polynomial and the parametrization given by $\rho y_j = v_j(u)$, $r + 1 \leq j \leq n$. Let us assume that the component is multiple with respect to G_1, \dots, G_i . This means that there exist polynomials H_1, \dots, H_i in $K(y_1, \dots, y_r)[u]$, such that q is prime with one of them, say H_k , and such that

$$\sum_{j=1}^i H_j \text{grad}(G_j \circ M)(y_1, \dots, y_r, v_{r+1}(u)/\rho, \dots, v_n(u)/\rho)$$

has all its entries in the ideal (q) , the gradient being considered with respect to the variables y_{r+1}, \dots, y_n . This implies that

$$\sum_{j=1}^i (H_j(G_j \circ M))(y_1, \dots, y_r, v_{r+1}(u)/\rho, \dots, v_n(u)/\rho)$$

belongs to the ideal generated by q^2 . Let Y represent the vector $(v_{r+1}(u)/\rho, \dots, v_n(u)/\rho)$. Differentiating the last expression with respect to $T_{k,l}$ we get that

$$\begin{aligned} & \sum_{j=1}^i \left(\frac{\partial}{\partial T_{k,l}} (H_j(y_1, \dots, y_r, Y)) \right) (G_j \circ M)(y_1, \dots, y_r, Y) \\ & + \sum_{j=1}^i H_j(y_1, \dots, y_r, Y) \text{grad}(G_j \circ M)(y_1, \dots, y_r, Y) \cdot \left(\frac{\partial}{\partial T_{k,l}} Y \right) \\ & + \sum_{j=1}^i H_j(y_1, \dots, y_r, Y) \left(\frac{\partial}{\partial T_{k,l}} (G_j \circ M) \right) (y_1, \dots, y_r, Y), \end{aligned}$$

which is in (q) . Since the two first terms are in (q) , the last one is also in (q) . But the last term A equals $H_k(y_1, \dots, y_r, Y) \left(\frac{\partial}{\partial T_{k,l}} G_k \circ M \right) (y_1, \dots, y_r, Y)$ and thus equals $H_k(y_1, \dots, y_r, Y) (f_l \circ M)(y_1, \dots, y_r, Y)$. Since $H_k(y_1, \dots, y_r, Y)$ is invertible modulo q , this implies that $f_l(y_1, \dots, y_r, Y)$ belongs to (q) . This property is true for all l , we deduce that \mathcal{M} is included in \mathcal{V} , which achieves the first part of the proof.

We now prove constructively the existence of the desired polynomial Q_i . Let \mathfrak{J} be the ideal generated by (G_1, \dots, G_i) in $k[(T_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s}, x_1, \dots, x_n]$ and \mathcal{W} be the corresponding variety.

Let \mathcal{M} be an irreducible component of \mathcal{W} and \mathfrak{J} be its annihilating ideal.

First we consider the case $\mathfrak{J} \cap R \neq (0)$: if π denotes the canonical projection $\bar{k}^s \times \bar{k}^n \rightarrow \bar{k}^s$, $\overline{\pi(\mathcal{W})}$ is contained in a hypersurface of degree bounded by the degree of \mathcal{M} . Thus there exists a non zero polynomial F in $\mathfrak{J} \cap R$ of total degree bounded by the degree of \mathcal{M} . If $t_{k,l}$ are such that $F(t_{k,l}) \neq 0$ then $\mathfrak{J} + ((T_{k,l} - t_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s}) = (1)$.

Now consider the case $\mathfrak{J} \cap R = (0)$. There exists a geometric resolution of \mathfrak{J} in $K[x_1, \dots, x_n]$: let y_j , $1 \leq j \leq n$, be the variables in Noether position, u the primitive element, q its minimal polynomial and ρ, v_i be the parametrization such that $\rho y_j = v_j$ for $j \geq n - i + 1$ and

$$\mathfrak{J} \phi \psi \rho = (q(u), \rho y_{n-i+1} - v_{n-i+1}(u), \dots, \rho y_n - v_n(u)) \phi \psi \rho,$$

where ψ is the discriminant of q with respect to u and ϕ the leading coefficient of q . Let $t_{k,l}$ be such that $\phi \psi \rho(t) \neq 0$ then

$$\begin{aligned} & \mathfrak{J} + ((T_{k,l} - t_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s}) \\ & = (q_t(u), \rho_t y_{n-i+1} - v_{t,n-i+1}(u), \dots, \rho_t y_n - v_{t,n}(u)), \end{aligned}$$

where q_t, ρ_t and $v_{t,j}$ represent respectively the values of q, ρ and the v_j , when the $T_{k,l}$ are specialized at the $t_{k,l}$, for $1 \leq k \leq i, 1 \leq l \leq s$. Since q_t is square free, the ideal $\mathfrak{J} + ((T_{k,l} - t_{k,l})_{1 \leq k \leq i, 1 \leq l \leq s})$ is reduced. Hence we let Q_i be one of the coefficients of $\phi \psi \rho$ with respect to the free variables y_1, \dots, y_{n-i} .

It remains to give a bound on the degrees of ϕ, ψ and ρ . According to the bound given by Schost in [20, Proposition 1], the polynomial q can be chosen to be a polynomial in $R[y_1, \dots, y_r][u]$ of total degree bounded by the degree of \mathcal{M} , and the total degree of ρ bounded by $\deg(\mathcal{M})^3$. Since the degree of \mathcal{M} is bounded by $(d+1)^i$, the total degree of $\phi \psi \rho$ is bounded by $3(d+1)^{3i}$. \square

We denote by R_2 the following property:

R₂: for any irreducible component \mathcal{M} of codimension i of the variety \mathcal{V}_i the following alternative holds: \mathcal{M} is included in \mathcal{V} or \mathcal{M} is reduced with respect to g_1, \dots, g_i .

Proposition 3 *Let α be a strictly positive integer, and Ω be a set of points of k of cardinal $3\alpha(d+1)^{3n}$. A random choice of all the $t_{i,j}$, $1 \leq i \leq n+1, 1 \leq j \leq s$, in $\Omega^{(n+1)s}$ leads to polynomials g_i satisfying the property R_2 with a probability at least $1 - (sn)^{c_2}/\alpha$, for a universal positive constant c_2 .*

Proof. Zippel-Schwartz' zero test implies that a random choice of the $t_{i,j}$ in the set $\Omega^{(n+1)s}$ is not a root of the product of all the Q_i , for $1 \leq i \leq n$, with a probability at least $1 - (n+1)^2 s/\alpha$. \square

3 Algorithm

In this section we assume that we have chosen values of the $t_{i,j}$ such that g_i 's satisfies the properties R_1 and R_2 . In this situation we adapt the algorithm given in [11] in order to give a complete solution of the input system $f_1 = \dots = f_s = 0$.

The algorithm is almost incremental. Indeed we would expect to compute resolutions of \mathcal{V}_{i+1}^J and \mathcal{V}_{i+1}^R from the one of \mathcal{V}_i^R . But doing this way yields a recursive dependency between the \mathcal{V}_i^J and thus an exponential factor in the complexity. Our strategy consists in computing first a resolution of the system, not necessarily minimal, and at the end we deduce a minimal one. The first task is called the *incremental resolution* and the second one the *minimization*.

For each i , $0 \leq i \leq n-1$, we define the variety \mathcal{V}_{i+1}^J composed of the components of $\mathcal{V}_{i+1}^R \cap \mathcal{V}(g_{i+1})$ which are included in the hypersurface defined by $g_{i+2} = 0$; in other words $\mathcal{V}_{i+1}^R \cap \mathcal{V}(g_{i+1})$ is the (minimal) union of the components of \mathcal{V}_{i+1}^J and the ones of \mathcal{V}_{i+1}^R ; moreover the variety \mathcal{V}_{i+1}^J is included in \mathcal{V}_{i+1}^J . By convention we define \mathcal{V}_0^J to be \mathcal{V}_0^J , so that the following set equalities hold:

$$\mathcal{V}_i = \mathcal{V}_0^J \cup \dots \cup \mathcal{V}_i^J \cup \mathcal{V}_i^R, \quad 0 \leq i \leq n,$$

$$\mathcal{V} = \mathcal{V}_0^J \cup \mathcal{V}_1^J \cup \dots \cup \mathcal{V}_n^J.$$

Here is the outlook of the algorithm:

I. Incremental Resolution We compute geometric resolutions of each \mathcal{V}_i^J , it is incremental in i : at the i th step we compute resolutions of \mathcal{V}_{i+1}^J and \mathcal{V}_{i+1}^R from the one of \mathcal{V}_i^R . Each step divides into three parts:

1. *Compression* of the SLP of the geometric resolution of \mathcal{V}_i^R .
2. Computation of the *intersection* of \mathcal{V}_i^R by g_{i+1} .
3. *Splitting* $\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1})$ into \mathcal{V}_{i+1}^J and \mathcal{V}_{i+1}^R .

II. Minimization We compute the \mathcal{V}_i^J using the equality

$$(*) \quad \mathcal{V}_i^J = \overline{\mathcal{V}_i^J \setminus \cup_{0 \leq j < i} \mathcal{V}_j^J}, \quad 0 \leq i \leq n.$$

Note that this formula for the \mathcal{V}_i^J is not recursive.

The next subsections are devoted to the presentation of the complexity model we use, the description of each elementary block of the algorithm and a proof of Theorem 1.

3.1 Complexity Model

We assume that k is an effective field for which each elementary operation (addition, subtraction, multiplication, division and equality test) has cost 1. The multivariate polynomials we use in our algorithm are stored by means of Straight-Line Programs (SLP) without test nor division, we refer to Strassen [21], von zur Gathen [6] or Heintz [14] for precise definitions.

The only non-trivial point when dealing with this data structure is equality checking (or zero testing). One can perform this task by evaluating the SLP at sufficiently many points. This is formalized in terms of *correct test sequences* of points with coordinates from k according to a theorem due to Heintz and Schnorr [15], which we recall for completeness.

Let D and L be two positive integers, and let us define the subset $W(D, n, L)$ of polynomials of $k[x_1, \dots, x_n]$, of degree at most D , which can be coded by a SLP with at most L arithmetic operations. Furthermore given a subset Γ of k , a family $\gamma := \{\gamma_1, \dots, \gamma_m\}$ (with $\gamma_i \in \Gamma$) of m points in k^n is called a *correct test sequence* for $W(D, n, L)$ if every polynomial in the latter vanishing on the points of γ is actually identically zero.

Theorem 2 [15] *Given a subset Γ of k of cardinality $\#\Gamma = 2L(D+1)^2$, and a cardinality $m := 6(L+n)(L+n+1)$, the subset $\tau(D, n, L, \Gamma) \in \Gamma^{m^m}$ of correct test sequences for $W(D, n, L)$ satisfies:*

$$\#\tau(D, n, L, \Gamma) \geq (\#\Gamma)^{nm} (1 - (\#\Gamma)^{-\frac{m}{6}}).$$

In other words, if we have precomputed all the correct test sequences needed for a fixed range of applications we have a polynomial time algorithm for testing the nullity of our SLP. In this sense we say that our complexity model is *non-uniform*. Finally, we say that *all the operations (addition, multiplication, zero test) on SLP have a non-uniform complexity polynomial in their size and their number of variables*.

All our results remain valid in a uniform complexity model if we replace correct test sequences by the probabilistic test given in [5] asserting that a SLP of size L can be tested to represent zero or not in time polynomial in L and n with a probability of failure uniformly bounded by $1/262144$.

3.2 Incremental Resolution

Let us now turn to the description of the elementary blocks constituting the core of the loop of the first part of the algorithm.

Compression The compression technique is fundamental: it avoids the growth of the SLP representing the geometric resolution of the successive \mathcal{V}_i^R . It is based on a Newton-Hensel iterator. We adapt the result [11, Lemma 5] to our situation:

Lemma 3 *Let β be the size of a SLP encoding a geometric resolution of \mathcal{V}_i^R , for $i \leq n$, there exists a deterministic algorithm with a non-uniform complexity polynomial in $\beta Lsn \deg(\mathcal{V}_i^R)$ returning a SLP encoding a geometric resolution of \mathcal{V}_i^R of size polynomial in $Lsn \deg(\mathcal{V}_i^R)$.*

Note that the size of the output is independent of β .

Intersection The second step is also taken from [11, Proposition 15]. It consists in computing a resolution of the intersection of \mathcal{V}_i^R by the hypersurface defined by the equation $g_{i+1} = 0$.

Lemma 4 *Let β be the size of a SLP of a geometric resolution of \mathcal{V}_i^R , there exists a deterministic algorithm with a non-uniform complexity polynomial in $\beta Lsnd \deg(\mathcal{V}_i^R)$ which computes a geometric resolution of $\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1})$ encoded by a SLP of size polynomial in $\beta Lsnd \deg(\mathcal{V}_i^R)$.*

Splitting From a resolution of $\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1})$ we want to compute its decomposition into \mathcal{V}_{i+1}^R and \mathcal{V}_{i+1}^J .

Lemma 5 *Let β be the size of the SLP encoding a geometric resolution of $\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1})$, there exists a deterministic algorithm of non-uniform complexity polynomial in $\beta \text{Lnsd deg}(\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1}))$ which computes geometric resolutions of \mathcal{V}_{i+1}^R and \mathcal{V}_{i+1}^J encoded by a SLP of size polynomial in $\beta \text{Lnsd deg}(\mathcal{V}_i^R \cap \mathcal{V}(g_{i+1}))$.*

Proof. We apply directly Proposition 4 of the appendix with the equation of g_{i+2} . \square

Let us introduce C to represent the expression $\text{Lnsd}\delta$. First we note that the degrees of all the varieties \mathcal{V}_i^J appearing during the resolution process are bounded by $d\delta$. At each step of the loop, the compression produces a SLP of size bounded by $C^{\mathcal{O}(1)}$, after the intersection we also get a SLP bounded by $C^{\mathcal{O}(1)}$, and the same holds for the splitting. This induces that each step of the loop has a complexity at most polynomial in C and that the computed SLP of the \mathcal{V}_i^J have size polynomial in C .

3.3 Minimization

Let us turn to the second part of the algorithm: from the resolutions of the \mathcal{V}_i^J computed above, we want to compute resolutions of the \mathcal{V}_i^J . Using equality (*), it is enough to remove the components of \mathcal{V}_i^J which are included in $\mathcal{V}_0^J \cup \dots \cup \mathcal{V}_{i-1}^J$. First we show that testing if a point belongs to an algebraic variety is equivalent to testing the nullity of the Chow form of the variety at the given point, then we give an algorithm for computing the Chow form of an equidimensional variety from a geometric resolution.

Let \mathcal{W} be an r -equidimensional variety given by a geometric resolution; y denotes the variables in Noether position, $y = M^{-1}x$, u the primitive element, q the minimal polynomial, ρ and v_j the parametrizations, such that $\rho y_j = v_j(u)$, $j > r$. Let B represent $k[\mathcal{W}]$ and B' be $k(y_1, \dots, y_r) \otimes B$.

Let $\Lambda_{r+1}, \dots, \Lambda_n$ be new generic parameters, and $\chi(y_1, \dots, y_r, T)$ the characteristic polynomial of the endomorphism of multiplication by the generic linear form $U = \Lambda_{r+1}y_{r+1} + \dots + \Lambda_n y_n$, in B' . The polynomial χ is called the Chow form of \mathcal{W} , it is polynomial in the y_i and the Λ_i , monic in T , square free, its total degree in the y_i does not exceed the degree of \mathcal{W} and its total degree in the y_i and Λ_i does not exceed $2 \text{deg}(\mathcal{W})$; moreover $\chi(u) = 0$ holds in B [12, Corollary 2].

Lemma 6 *A point $P = (P_1, \dots, P_n)$ of \overline{k}^n belongs to \mathcal{W} (in the coordinates y) if and only if $\chi(P_1, \dots, P_r, U(P))$ is zero.*

Proof. First, if P belongs to \mathcal{W} the Chow form vanished at P . Reciprocally, let P be a point such that $\chi(P_1, \dots, P_r, U(P))$ is zero. Let π denotes the canonical projection onto the free variables, using the theorem concerning the multiplicity of a specialization [19, p.89] the specialization of χ leads to the formula

$$\chi(P_1, \dots, P_r, T) = \prod_{i=1}^N (T - Z_i)^{m_i},$$

where the Z_i are the point of $\pi^{-1}(P_1, \dots, P_r)$ of multiplicity m_i . This implies that there exists i such that $U(P) = Z_i$;

since the Z_i are independent of the Λ_j , necessarily P equals Z_i . \square

Let β be the size of the SLP encoding the given geometric resolution of \mathcal{W} , we are able to compute χ quite easily as a SLP depending on the Λ_i and the free variables.

Lemma 7 *There exists a deterministic algorithm which computes a SLP of the Chow form χ of \mathcal{W} of size polynomial in $n\beta \text{deg}(\mathcal{W})$, the non-uniform complexity is polynomial in the same quantity.*

Proof. Let D be the dimension of B' and M_i be the multiplication matrices of the ρx_i for $r+1 \leq i \leq n$, in the basis $1, u, \dots, u^{D-1}$. The matrix $\Lambda_{r+1}M_{r+1} + \dots + \Lambda_n M_n$ is the multiplication matrix by ρU , let $\Psi(T)$ be its characteristic polynomial, then $\chi(T)$ equals $\Psi(\rho T)/\rho^D$, this division is exact. Since the matrices have size $D \times D$ and D is at most the degree of \mathcal{W} , their construction can be done with a complexity polynomial in $n\beta \text{deg}(\mathcal{W})$. We use Berkowitz' algorithm [2, 1] to compute the characteristic polynomial and "Vermeidung von Divisionen" [22] to compute the exact division, this yields the claimed complexity. \square

We are now ready to explain the minimization method. Let \mathcal{M} be a component of one the \mathcal{V}_i^J for $i > 0$, testing whether \mathcal{M} is included in one of the \mathcal{V}_j^J with $j < i$ is equivalent to testing if a Zariski dense subset of \mathcal{M} is included or not. Let y, u, q, ρ, v be the components of a geometric resolution of \mathcal{M} and χ be the Chow form of \mathcal{V}_j^J expressed in the variables y . The condition of the above lemma can be restated as: \mathcal{M} is included in \mathcal{V}_j^J if and only if $\chi(y_1, \dots, y_{n-i}, v_{n-i+1}(u)/\rho, \dots, v_n(u)/\rho)$ reduces to zero modulo q or not (in $k(y_1, \dots, y_{n-i}[T])$).

Lemma 8 *Let β_j be the size of the SLP encoding a geometric resolution of \mathcal{V}_j^J , for $0 \leq j \leq n$, and D_j be the degree of \mathcal{V}_j^J , there exists a deterministic algorithm with non-uniform complexity polynomial in $n(\beta_1 D_1 + \dots + \beta_i D_i)$ which computes a geometric resolution of \mathcal{V}_i^J of size polynomial in the same quantity.*

Proof. With the above notations, χ_j , the Chow form of \mathcal{V}_j^J can be computed in time polynomial in $n\beta_j D_j$. Proposition 4 of the appendix applied on the product of the χ_j , $j < i$, yields the claimed complexity. \square

Proof of Theorem 1 Let C still be $\text{Lnsd}\delta$. Since the output of the first part of the algorithm is polynomial in C and the degrees of all the \mathcal{V}_i^J are bounded by $d\delta$, the minimization part is also polynomial in C . This proves the first part of Theorem 1. For the second part, it suffices to put together the probabilities that the election of the $t_{i,j}$ leads to a sequence of g_i satisfying the properties R_1 and R_2 of Propositions 1 and 3.

Appendix: Splitting a Resolution

Let \mathcal{W} be an equidimensional variety of codimension i , given by a geometric resolution encoded by a SLP of size β . Let h be a polynomial in $k[x_1, \dots, x_n]$, we explain in this section how one can split the given geometric resolution into two parts, one for the components of \mathcal{W} included in the hypersurface defined by $h = 0$ and the other for the rest.

Let $r = n - i$ and the notations of the geometric resolution be:

- M represents an invertible matrix with entries in k , the coordinates in Noether position are $y = M^{-1}x$: the variables y_1, \dots, y_r are free.
- $u = \lambda_{r+1}y_{r+1} + \dots + \lambda_n y_n$ is the primitive element, the λ_i are in k .
- q is the minimal polynomial of u , monic in u .
- $\rho y_j = v_j(u)$, for $r+1 \leq j \leq n$ are the parametrizations, ρ is polynomial in the free variables and the v_j are polynomial in the free variables and u .

Let $A(y_1, \dots, y_r, u)$ denote

$$h \circ M(y_1, \dots, y_r, v_{r+1}(u)/\rho, \dots, v_n(u)/\rho),$$

$q_1(u)$ be the greatest common divisor of A and q in $k(y_1, \dots, y_r)[u]$, and let $q_2 = q/q_1$. Since q is monic and polynomial in the free variables, q_1 and q_2 are also monic and polynomial in the free variables. We set GR_i the geometric resolution defined by M , u , q_i , ρ and the remainders of the v_j modulo q_i , for $i = 1, 2$. The resolution GR_1 (respectively GR_2) is a geometric resolution of the components \mathcal{W}_1 (respectively \mathcal{W}_2) of \mathcal{W} included (respectively not included) in the hypersurface defined by $h = 0$. Our aim is now to give a bound on the size of the SLP of the GR_i in function of β .

Proposition 4 *Let L_h be the size of the SLP encoding h , d_h a bound on the total degree of h , both GR_1 and GR_2 can be computed by a deterministic algorithm in non-uniform time polynomial in $nL_h d_h \beta \deg(\mathcal{W})$. The sizes of the resulting SLP are polynomial in $nL_h d_h \beta \deg(\mathcal{W})$.*

Proof. Let H be the homogenized polynomial with respect to the new variable y_0 of $h \circ M$ can be computed in time polynomial in $nL_h d_h$, the resulting SLP having size also polynomial in $nL_h d_h$. Now let $B = H(\rho, \rho y_1, \dots, \rho y_r, v_{r+1}(u), \dots, v_n(u))$, B is proportional to A up to a ρ^{d_h} and its SLP is polynomial in $nL_h d_h \beta$. Using [11, Lemma 10] the greatest common divisor of B and q can be computed in time polynomial in $nL_h \beta d_h \beta \deg(\mathcal{W})$, this gives q_1 and q_2 . \square

Conclusion

Our algorithm for computing a minimal geometric resolution of an algebraic variety gives as a byproduct the degree of the variety, and if we are looking for an irreducible decomposition it is sufficient to factorize the minimal polynomials of the computed geometric resolutions.

With our experience in implementing algorithms using SLP [8, 12, 18] we expect to have soon an implementation of the method presented here.

References

- [1] ABDELJAOUED, J. *Algorithmes rapides pour le Calcul du Polynôme Caractéristique*. PhD thesis, Université de Franche Comté, Besançon, France, 1997.
- [2] BERKOWITZ, S. J. On computing the determinant in small parallel time using a small number of processors. *Information Processing Letters* 18 (1984), 147–150.
- [3] CHISTOV, A. L., AND GRIGORIEV, D. Y. Subexponential time solving systems of algebraic equations. LOMI preprint E-9-83, E-10-83, Steklov Institute, Leningrad, 1983.
- [4] ELKADI, M., AND MOURRAIN, B. A new algorithm for the geometric decomposition of a variety. In *Proceedings of the 1999 International Symposium on Symbolic and Algebraic Computation* (1999), S. Dooley, Ed.
- [5] FITCHAS, N., GIUSTI, M., AND SMIETANSKI, F. Sur la complexité du théorème des zéros. In *Approximation and Optimization in the Caribbean II, Proceedings 2nd Int. Conf. on Non-Linear Optimization and Approximation*, J. Guddat, Ed., vol. 8 of *Approximation and Optimization*. Peter Lange Verlag, Frankfurt am Main, 1995, pp. 247–329.
- [6] GATHEN VON ZUR, J. Parallel arithmetic computations: a survey. In *Proceedings of the 12th Symposium on Mathematical Foundations of Computer Science* (Bratislava, Czechoslovakia, Aug. 1986), B. R. J. Gruska and J. Wiedermann, Eds., vol. 233 of *LNCS*, Springer, pp. 93–112.
- [7] GIUSTI, M., HÄGELE, K., HEINTZ, J., MORAIS, J. E., MONTAÑA, J. L., AND PARDO, L. M. Lower bounds for diophantine approximation. *Journal of Pure and Applied Algebra* 117,118 (1997), 277–317. Proceedings of MEGA'96.
- [8] GIUSTI, M., HÄGELE, K., LECERF, G., MARCHAND, J., AND SALVY, B. The projective noether Maple package: Computing the dimension of a projective variety. GAGE laboratory, manuscript, 1998. <http://www.gage.polytechnique.fr/gage/notes/1998.html>.
- [9] GIUSTI, M., AND HEINTZ, J. Algorithmes - disons rapides - pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionnelles. In *Proceedings of MEGA'90* (1991), T. Mora and C. Traverso, Eds., vol. 94 of *Progress in Mathematics*, Birkhäuser, pp. 169–194.
- [10] GIUSTI, M., AND HEINTZ, J. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. In *Computational Algebraic Geometry and Commutative Algebra* (1993), D. Eisenbud and L. Robbiano, Eds., vol. XXXIV of *Symposia Mathematica*, Cambridge University Press, pp. 216–256.
- [11] GIUSTI, M., HEINTZ, J., MORAIS, J. E., MORGENSTERN, J., AND PARDO, L. M. Straight-line programs in geometric elimination theory. *J. of Pure and App. Algebra* 124 (1998), 101–146.
- [12] GIUSTI, M., LECERF, G., AND SALVY, B. A Gröbner free alternative for polynomial system solving. *Journal of Complexity* (2000). To appear.
- [13] HEINTZ, J. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.* 24, 3 (1983), 239–277.
- [14] HEINTZ, J. On the computational complexity of polynomials and bilinear mappings. A survey. In *Applied Algebra, Algebraic Algorithms and Error Correcting*

- Codes, Proceedings of AAEECC-5* (1989), vol. 356 of LNCS, Springer, pp. 269–300.
- [15] HEINTZ, J., AND SCHNORR, C. P. Testing polynomials which are easy to compute. In *Logic and Algorithmic* (1982), vol. 30 of *Monographie de l'Enseignement Mathématique*, pp. 237–254.
- [16] KLEIMAN, S. L. Bertini and his two fundamental theorems. In *Rendiconti del circolo matematico di Palermo* (1997).
- [17] KRICK, T., AND PARDO, L. M. Une approche informatique pour l'approximation diophantienne. *C. R. Acad. Sci. Paris* 318, 1 (1994), 407–412.
- [18] LECERF, G. Kronecker version 0.1, July 1999. <http://kronecker.medicis.polytechnique.fr/>.
- [19] SAMUEL, P. *Méthodes d'algèbre abstraite en géométrie algébrique*, 2nd ed. Springer-Verlag, 1967.
- [20] SCHOST, E. Computing parametric geometric resolutions. GAGE laboratory, manuscript submitted to IS-SAC'2000, January 2000. <http://www.gage.polytechnique.fr/gage/notes/2000.html>.
- [21] STRASSEN, V. Berechnung und Programm. I, II. *Acta Informatica* 1, 4 (1972), 320–355; *ibid.* 2(1), 64–79 (1973).
- [22] STRASSEN, V. Vermeidung von divisionen. *Crelle J. Reine Angew. Math*, 264 (1973), 182–202.
- [23] T. KRICK, L. P., AND SOMBRA, M. Sharp estimates for the arithmetic Nullstellensatz. December 1999.
- [24] ZIPPEL, R. Probabilistic algorithms for sparse polynomials. In *Proceedings EUROSAM' 79* (1979), no. 72 in LNCS, Springer, pp. 216–226.
- [25] ZIPPEL, R. *Effective Polynomial Computation*. Kluwer Academic Publishers, 1993.