Polar varieties and computation of one point in each connected component of a smooth real algebraic set

Mohab Safey El Din, LIP6, Université Paris 6, France
Mohab.Safey@lip6.fr,
Éric Schost, GAGE, École polytechnique, 91128 Palaiseau, France
Eric.Schost@polytechnique.fr

ABSTRACT

Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ that generate a radical ideal and let V be their complex zero-set. Suppose that V is smooth and equidimensional; then we show that computing suitable sections of the polar varieties associated to generic projections of V gives at least one point in each connected component of $V \cap \mathbb{R}^n$. We deduce an algorithm that extends that of Bank, Giusti, Heintz and Mbakop to non-compact situations. Its arithmetic complexity is polynomial in the complexity of evaluation of the input system, an intrinsic algebraic quantity and a combinatorial quantity.

1. INTRODUCTION

Let V be a smooth and equidimensional complex algebraic variety. This paper is devoted to design an algorithm computing at least one point in each connected component of $V \cap \mathbb{R}^n$. This is a question of importance, since it is for instance one of the basic subroutines used to study semi-algebraic sets, a question which occurs frequently in real-life applications.

In [3, 4], Bank, Giusti, Heintz and Mbakop treat this problem, respectively for complex hypersurfaces and complete intersections, with compact, smooth real part. To this effect, they introduce the notion of *polar varieties*, which we now recall.

The *polar varieties* are the critical loci of a family of projections defined on V. The last of these polar varieties describes the critical points of the projection on a line, so it has dimension zero, in generic enough coordinates. Furthermore, if $V \cap \mathbb{R}^n$ is compact, then any projection on a line has a critical point on each connected component of $V \cap \mathbb{R}^n$. Thus, the last polar variety has dimension zero and gives one point on each connected component of $V \cap \mathbb{R}^n$.

In [3, 4], a local description of the polar varieties by means of regular, reduced sequences enabled to use the elimination techniques of [10, 9, 8, 11] to treat this question with good complexity: the algorithms of [3, 4] have polynomial complexity in an intrinsic geometric degree, the complexity of evaluation of the input system and a combinatorial quantity.

In this paper, we propose an algorithm extending these ideas to smooth varieties, dropping the compactness assumption. We show that in this case, studying suitable zero-dimensional sections of the polar varieties enables to obtain one point on each connected component of $V \cap \mathbb{R}^n$.

Unfortunately, we can no longer use the local description of the polar varieties mentioned above, so our algorithms require stronger elimination techniques. Namely, we use the results of [16], that gives an algorithm with good complexity for zero-dimensional polynomial system solving, without the assumptions of regularity or reducedness.

We deduce an algorithm with a polynomial complexity in the complexity of evaluation of the input system, a quantity bounding the algebraic degrees of some intermediate varieties met during the computation, and a combinatorial quantity. The study of its practical behavior is left to a future work.

Notation and basic definitions.

All along this article, we consider algebraic subsets of $\mathbb{C}^n$ and real algebraic sets in $\mathbb{R}^n$, for some given n. Let $f_1, \ldots, f_s$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$, let V be their complex zero-set and d its dimension. We assume that the polynomials $f_1, \ldots, f_s$ define a radical ideal and that V is equidimensional and smooth.

For i in $1, \ldots, d$, denote by π_i the canonical projection

$$\begin{array}{ccc} \mathbb{C}^n & \to & \mathbb{C}^i \\ (x_1, \ldots, x_n) & \mapsto & (x_1, \ldots, x_i). \end{array}$$

For simplicity, we also denote by π_i its restriction to a map $\mathbb{R}^n \to \mathbb{R}^i$.

Let J be the Jacobian matrix of $f_1, \ldots, f_s$:

$$J = \begin{bmatrix} \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_1}{\partial X_1} \\ \vdots & & \vdots \\ \frac{\partial f_s}{\partial X_n} & \cdots & \frac{\partial f_s}{\partial X_1} \end{bmatrix}.$$

We now describe the critical loci of $\pi_1, \ldots, \pi_d$ on V by means of suitable minors of this matrix.

First, for $i = d+1$, we define Δ_{n-d} as $\langle f_1, \ldots, f_s \rangle$. Then for $i = 1, \ldots, d$, Δ_{n-i+1} is the ideal generated by $f_1, \ldots, f_s$ and all minors of size $n-d$ in J built upon the columns $1, \ldots, n-i$ (that is, using the derivatives with respect to variables $X_{i+1}, \ldots, X_n$). Note that Δ_{n-i+1} is generated by

$$S_i := \begin{pmatrix} s \\ n-d \end{pmatrix} \begin{pmatrix} n-i \\ n-d \end{pmatrix}$$

minors. The i-th *polar variety* W_{n-i+1} is then defined as the zero-set of Δ_{n-i+1}; in particular, $W_{n-d} = V$.

Since the ideal $\langle f_1, \ldots, f_s \rangle$ is radical and V is equidimensional and smooth, the points in W_{n-i+1} are the critical points of the restriction of π_i to V, for $i \leq d$. After a generic change of variables, W_{n-i+1} is expected to have codimension $n-i+1$ for all i, which accounts for the indexation we used.

Changes of variables.

In what follows, we repeatedly use linear changes of variables, so we introduce dedicated notations.

For $f \in \mathbb{Q}[X_1, \ldots, X_n]$ and $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$, $f(\mathbf{AX})$ is the polynomial obtained by applying the change of variables $\mathbf{A}$ to f. For simplicity, we also write $f^{\mathbf{A}} = f(\mathbf{AX})$.

For $i \in \{1, \ldots, d+1\}$, the ideal $\Delta^{\mathbf{A}}_{n-i+1}$ is defined by the polynomials $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$ and all minors of size $n-d$ from the first $n-i$ columns of their Jacobian matrix. The polar variety associated to this ideal is denoted by $W^{\mathbf{A}}_{n-i+1}$, so as to make the dependence with respect to $\mathbf{A}$ explicit. For consistency, we denote by $V^{\mathbf{A}} = W^{\mathbf{A}}_{n-d}$ the zero-set of $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$.

Geometric results.

Following [3, 4], to compute one point in each connected component of $V \cap \mathbb{R}^n$, we may compute the last polar variety W_n, which describes the critical points of the projection on the X_1-axis, restricted to V.

Unfortunately, this might not answer the question if $V \cap \mathbb{R}^n$ is not compact, since there might be connected components without critical points. In this situation, an answer will come from the study of the images of the connected components of $V \cap \mathbb{R}^n$ by the projections $\pi_1, \ldots, \pi_d$.

To inspect these images, we want to ensure closedness properties. Recall that a map $f : A \subset \mathbb{C}^n \to \mathbb{C}^i$ is *proper* at $b \in \mathbb{C}^i$ if there exists a neighborhood $\mathcal{O}$ of b such that $f^{-1}(\overline{\mathcal{O}})$ is compact, where $\overline{\mathcal{O}}$ denotes the closure of $\mathcal{O}$ for the strong topology. If f is proper everywhere on its image, we say simply that f is proper; then f is closed for the strong topology.

We are interested in properness properties of the projections π_i restricted to our family of polar varieties. Such properties might not hold in the initial coordinates, so we will perform linear changes of coordinates to get back to this favorable situation. We will thus denote by $\mathcal{P}(\mathbf{A})$ the following assertion: *for $i \in \{1, \ldots, d+1\}$, the restriction of π_{i-1} to $W^{\mathbf{A}}_{n-i+1}$ is proper.* By convention, for $i = 1$, in what follows, this means that $W_n^{\mathbf{A}}$ *has dimension zero.* An important part of this article is then devoted to prove that $\mathcal{P}(\mathbf{A})$ holds for generic $\mathbf{A}$.

Theorem 1 *There exists a non-empty Zariski-open set Γ in $\mathrm{GL}_n(\mathbb{C})$ such that for $\mathbf{A}$ in Γ, $\mathcal{P}(\mathbf{A})$ holds.*

Under this condition, the following theorem enables to compute one point on each connected component of $V \cap \mathbb{R}^n$. Indeed, if the matrix $\mathbf{A}$ in Theorem 2 below is in $\mathrm{GL}_n(\mathbb{Q})$, then the connected components of $V^{\mathbf{A}} \cap \mathbb{R}^n$ are in trivial bijection with those of $V \cap \mathbb{R}^n$.

Theorems 1 and 2 can be considered as our main contributions. They extend the properties used in notably [3, 4], where it was enough to consider the last polar variety $W_n^{\mathbf{A}}$, due to the compactness assumption.

Theorem 2 *Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$ be such that $\mathcal{P}(\mathbf{A})$ holds. Let $p_d = (x_1, \ldots, x_d)$ be any point in $\mathbb{R}^d$. For $j \in \{1, \ldots, d-1\}$, define $p_j = (x_1, \ldots, x_j) \in \mathbb{R}^i$. For $j = 0$, formally define $\pi_0^{-1}(p_0)$ as $\mathbb{C}^n$.*

Then the algebraic sets $W^{\mathbf{A}}_{n-j} \cap \pi_j^{-1}(p_j)$, $j \in \{0, \ldots, d\}$, are either empty or zero-dimensional. Their reunion meets every connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$.

Complexity issues.

On the basis of Theorem 2, we propose an algorithm to compute one point on each connected component of $V \cap \mathbb{R}^n$. We simply proceed by solving all zero-dimensional systems described in Theorem 2. Their solutions will be represented by a family of *geometric resolution.* In this article, we define a geometric resolution of a zero-dimensional set $Z \subset \mathbb{C}^n$ defined over $\mathbb{Q}$ as the data of a linear form u separating the points in Z and polynomials $Q, Q_1, \ldots, Q_n$ in $\mathbb{Q}[T]$ such that the relations

$$Q(u) = 0, \quad \begin{cases} X_1 = Q_1(u), \\ \quad \vdots \\ X_n = Q_n(u), \end{cases}$$

form a description of the points in Z.

To state our complexity result, we need to define an important algebraic quantity associated to $f_1, \ldots, f_s$, denoted by δ. To this effect, we describe more precisely the systems defining the polar varieties.

Let $\mathbf{A}$ be a matrix in $\mathrm{GL}_n(\mathbb{C})$. Recall that S_i denotes the number of minors necessary to define the ideal $\Delta^{\mathbf{A}}_{n-i+1}$, $1 \leq i \leq d+1$. For $i = 1, \ldots, d+1$, we denote by $M^{\mathbf{A}}_{i,1}, \ldots, M^{\mathbf{A}}_{i,S_i}$ the ordered sequence of these minors. Due to the definition of the ideals $\Delta^{\mathbf{A}}_{n-i+1}$, we are free to assume that these sequences are ordered such that $M^{\mathbf{A}}_{i,1}, \ldots, M^{\mathbf{A}}_{i,S_i}$ is a prefix of $M^{\mathbf{A}}_{j,1}, \ldots, M^{\mathbf{A}}_{j,S_j}$ for $i \geq j$. Thus $M^{\mathbf{A}}_{1,1}, \ldots, M^{\mathbf{A}}_{1,S_1}$ is the longest of these sequences.

Let us now consider the long ordered sequence

$$\mathcal{G}^{\mathbf{A}} = f^{\mathbf{A}}_1, \ldots, f^{\mathbf{A}}_s, M^{\mathbf{A}}_{1,1}, \ldots, M^{\mathbf{A}}_{1,S_1}.$$

Given any prefix subsequence G of $\mathcal{G}^{\mathbf{A}}$, define the quantity $\delta^{\mathbf{A}}_G$ as the sum of the algebraic degrees of the irreducible components of the variety defined by G. We define $\delta^{\mathbf{A}}$ as the maximum of all $\delta^{\mathbf{A}}_G$, and δ as the supremum of all $\delta^{\mathbf{A}}$ for $\mathbf{A}$ in $\mathrm{GL}_n(\mathbb{Q})$ such that $\mathcal{P}(\mathbf{A})$ holds.

A definition of algebraic degree can be found in [16]. If $f_1, \ldots, f_s$ are of degree bounded by D, then δ is bounded by $n(D(n-d))^n$ [16, page 108].

We can now state our complexity result. We denote by $M(x)$ the number of operations necessary to multiplying polynomials of degree x. The notation $f \in \mathcal{O}_{\log}(x)$ means that $f \in \mathcal{O}(x \log(x)^a)$, for some constant a.

Theorem 3 *Let $f_1, \ldots, f_s$ be polynomials of degree bounded by D in $\mathbb{Q}[X_1, \ldots, X_n]$, given by a Straight-Line Program of length L. Suppose that $\langle f_1, \ldots, f_s \rangle$ is a radical, equidimensional ideal and that $V = V(f_1, \ldots, f_s) \subset \mathbb{C}^n$ is smooth of dimension d.*

There exists a probabilist algorithm computing a family of geometric resolutions, the reunion of whose real zeros contains at least one point in each connected component of $V \cap \mathbb{R}^n$. In case of success, its complexity is within

$$\mathcal{O}_{\log}\left(Ln^{10} S_1(s+S_1) M\left(D(n-d)\delta\right)^3\right)$$

arithmetic operations.

The probabilist aspects come from putting the system in general position, and also appear during the execution of the algorithm of [16, Chapter IV]. From Theorem 1, the probability of success depends on the choice of points outside proper Zariski-closed sets.

Our complexity result is similar to that of [3, 4], in that it depends on the evaluation properties of the input system, a combinatorial number (here denoted by S_1) and a suitable intrinsic quantity (here denoted by δ). We were not able to use the local description of polar varieties by regular sequences from [3, 4], whence the intricate definition of our quantity δ. Simplifying these matters is the subject of future work.

Related work.

In [12, 13, 14, 5, 6, 7], the authors consider arbitrary real algebraic sets, and reduce to the study of smooth and compact real algebraic hypersurfaces, via sums of squares and infinitesimal deformations. Then, the zero-dimensional critical locus of a projection on a well-chosen line is studied. This yields algorithms with complexities simply exponential in the number of variables; no mention of intrinsic quantities is made.

In [18, 2, 19, 20], the problem is treated with a view toward practical efficiency. To deal with non-compact situations, the authors of [18, 2, 19] compute the critical points of the square of the distance to a given point, whereas in [20] we study the set of non properness of a family of projections. No complexity estimates are given.

In this article, we represent the solutions of a zero-dimensional polynomial system by means of geometric resolutions. This notion appeared in the series of articles [10, 8, 9, 11], see further references therein. For the similar notion of Rational Univariate Representation and its use in real geometry, we refer to [1, 17, 18].

Organization of the paper.

The three remaining sections are devoted to prove respectively Theorems 1, 2 and 3.

2. PROPERNESS PROPERTIES

This section is devoted to prove that in generic coordinates, all polar varieties satisfy a properness property. This is the content of Theorem 1, which we now restate.

There exists a Zariski-open set Γ in $\mathrm{GL}_n(\mathbb{C})$ such that for $\mathbf{A}$ in Γ and $i \in \{1, \ldots, d+1\}$, the restriction of the projection π_{i-1} to the polar variety $W^{\mathbf{A}}_{n-i+1}$ associated to the polynomials $f^{\mathbf{A}}_1, \ldots, f^{\mathbf{A}}_s$ is proper.

The intuition is the following. Through an inductive reasoning, consider that we have found coordinates ensuring a proper projection for $W^{\mathbf{A}}_{n-i}$. In these coordinates, the restriction of π_{i-1} to $W^{\mathbf{A}}_{n-i+1}$ may not be proper; then an arbitrary small change of free variables $X_1, \ldots, X_i$ will not alter $W^{\mathbf{A}}_{n-i+1}$, but will restore the properness of π_{i-1}.

To obtain the existence of the Zariski-open set Γ, we must nevertheless adopt an algebraic point of view. The notion of properness of a projection is strongly related to that of Noether normalization, so we will actually prove that all polar varieties satisfy a Noether normalization statement. Many ideas used below, notably that of examining an incremental intersection process, originate from [10, 9, 8]. In what follows, for $r \leq n$, $\mathbf{X}_{\leq r}$ denotes $X_1, \ldots, X_r$, and $\mathbf{X}$ denotes $X_1, \ldots, X_n$.

2.1 Strategy of proof

Proving Theorem 1 requires to handle generic linear changes of variables. Let thus $\mathfrak{A}$ be a $n \times n$ matrix whose entries are new indeterminates $(\mathfrak{A}_{i,j})_{1 \leq i,j \leq n}$. We mimic the definitions of the introduction for this "generic" change of variables.

For $k \in \{1, \ldots, s\}$, define $f_k^{\mathfrak{A}} \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$ as $f_k^{\mathfrak{A}} = f_k(\mathfrak{A}\mathbf{X})$. For $i \leq d+1$, we define the ideal $\Delta_{n-i+1}^{\mathfrak{A}}$ similarly to $\Delta_{n-i+1}^{\mathbf{A}}$ above, that is, using the polynomials $f_k^{\mathfrak{A}}$ and all minors of size $n-d$ from the first $n-i$ columns of their Jacobian matrix. Then $W_{n-i+1}^{\mathfrak{A}}$ is the zero-set of $\Delta_{n-i+1}^{\mathfrak{A}}$. Thus $W_{n-i+1}^{\mathfrak{A}}$ is the polar varieties associated to the "generic" change of variables $\mathfrak{A}$.

Subsection 2.2 is devoted to introduce some technical notation. Then in Subsection 2.3 we prove that the ideals $\Delta_{n-i+1}^{\mathfrak{A}}$ satisfy a Noether normalization property:

Proposition 1 *Let $i \in \{1, \ldots, d+1\}$, let P be one of the prime components of the radical of the ideal $\Delta_{n-i+1}^{\mathfrak{A}}$, and let r be its dimension. Then r is at most $i-1$ and the extension $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}] \to \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]/P$ is integral.*

In Subsection 2.4 we show how this property specializes. We use the notation relative to changes of variables, that was defined in the introduction.

Proposition 2 *There is a Zariski-open set Γ in $\mathrm{GL}_n(\mathbb{C})$ such that for $\mathbf{A}$ in Γ, the following holds. Let $i \in \{1, \ldots, d+1\}$, let $P^{\mathbf{A}}$ be one of the prime components of the radical of $\Delta_{n-i+1}^{\mathbf{A}}$, and r its dimension. Then r is at most $i-1$ and $\mathbb{C}[\mathbf{X}_{\leq r}] \to \mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}$ is integral.*

In Subsection 2.5, we will conclude the proof of Theorem 1 by using a result of [15] to relate the properness property and the above normalization result:

Proposition 3 *Let $\mathbf{A}$ be in $\mathrm{GL}_n(\mathbb{C})$ and $i \in \{1, \ldots, d+1\}$. The following assertions are equivalent.*

- *For every prime component $P^{\mathbf{A}}$ of the radical of $\Delta_{n-i+1}^{\mathbf{A}}$, the following holds. Let r be the dimension of $P^{\mathbf{A}}$; then r is at most $i-1$ and $\mathbb{C}[\mathbf{X}_{\leq r}] \to \mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}$ is integral.*
- *The restriction of π_{i-1} to $W_{n-i+1}^{\mathbf{A}}$ is proper.*

2.2 Preliminaries

The above propositions rely on the properties of some ring extensions. For the sake of shortness, we introduce the following notation related to these extensions. Let k be a field; given an ideal $I \subset k[\mathbf{X}]$, we denote by $\mathcal{Q}(I)$ the following property: *Let P be a prime ideal appearing in the prime decomposition of $\sqrt{I}$, and r its dimension. Then $k[\mathbf{X}_{\leq r}] \to k[\mathbf{X}]/P$ is integral.*

For instance, Proposition 1 can then be rephrased as: *the ideal $\Delta_{n-i+1}^{\mathfrak{A}}$ satisfies property $\mathcal{Q}$, and has dimension at most $i-1$.* The following result will be useful to prove that proposition; the proof is immediate.

Lemma 1 *Suppose that I is equidimensional of dimension r and that $k[\mathbf{X}_{\leq r}] \to k[\mathbf{X}]/I$ is an integral ring extension. Then I satisfies property $\mathcal{Q}$.*

2.3 Proof of Proposition 1

We prove the property of Proposition 1 by decreasing induction on $i = d+1, \ldots, 1$. Let us first settle the case $i = d+1$. Then the ideal $\Delta_{n-d}^{\mathfrak{A}}$ is generated by the polynomials $f_1^{\mathfrak{A}}, \ldots, f_s^{\mathfrak{A}} = f_1(\mathfrak{A}\mathbf{X}), \ldots, f_s(\mathfrak{A}\mathbf{X})$. Thus the validity of assertion $\mathcal{P}_{d+1}$ follows from the Noether Normalization Theorem.

Let us now assume that the property holds for index $i+1$, and prove it for index i. We first establish property $\mathcal{Q}(\Delta_{n-i+1}^{\mathfrak{A}})$, then prove the dimension property.

Preliminaries.
By definition, $\Delta_{n-i+1}^{\mathfrak{A}}$ is obtained by adjoining suitable minors of the Jacobian matrix of $f_1^{\mathfrak{A}}, \ldots, f_s^{\mathfrak{A}}$ to the ideal $\Delta_{n-i}^{\mathfrak{A}}$. Denote by $M_1^{\mathfrak{A}}, \ldots, M_N^{\mathfrak{A}}$ these minors. Proving property $\mathcal{Q}(\Delta_{n-i+1}^{\mathfrak{A}})$ will follow from seeing this intersection process incrementally.

For $j = 1, \ldots, N$, let $\Delta_{n-i+1,j}^{\mathfrak{A}}$ be $\Delta_{n-i}^{\mathfrak{A}} + \left(M_1^{\mathfrak{A}}, \ldots, M_j^{\mathfrak{A}}\right)$ and define $\Delta_{n-i+1,0}^{\mathfrak{A}} = \Delta_{n-i}^{\mathfrak{A}}$. Thus, $\mathcal{Q}(\Delta_{n-i+1,0}^{\mathfrak{A}})$ holds, and we want to establish $\mathcal{Q}(\Delta_{n-i+1,N}^{\mathfrak{A}})$. Thus to conclude, it is enough to prove that $\mathcal{Q}(\Delta_{n-i+1,j}^{\mathfrak{A}})$ implies $\mathcal{Q}(\Delta_{n-i+1,j+1}^{\mathfrak{A}})$, for $j = 0, \ldots, N-1$.

Since i and j are fixed, we simplify the notation by letting $\Delta = \Delta_{n-i+1,j}^{\mathfrak{A}}$, $\Delta' = \Delta_{n-i+1,j+1}^{\mathfrak{A}}$ and $M = M_{j+1}^{\mathfrak{A}}$, so that $\Delta' = \Delta + M$. Then Δ satisfies property $\mathcal{Q}$ and we want to show that it is also the case for Δ'. We first perform some immediate simplifications.

Let $\cap_{\ell \leq L} P_\ell$ be the prime decomposition of $\sqrt{\Delta}$, for some integer L. Then the prime components of $\sqrt{\Delta'}$ are the reunion of the prime components of $\sqrt{P_\ell + M}$, for $\ell \leq L$, so it is enough to prove that for every ℓ such that $P_\ell + M \neq (1)$, $P_\ell + M$ satisfies property $\mathcal{Q}$. By assumption, P_ℓ has dimension $\leq i$ for all ℓ; for fixed $r \leq i$, we partition the set $\{1, \ldots, L\}$ as follows:

- ℓ belongs to L^+ if $\dim P_\ell = r$ and P_ℓ contains M.
- ℓ belongs to L^- if $\dim P_\ell = r$, P_ℓ does not contain M and $P_\ell + M \neq (1)$.
- ℓ belongs to S if $\dim P_\ell = r$, P_ℓ does not contain M and $P_\ell + M = (1)$.
- ℓ belongs to R if $\dim P_\ell \neq r$.

It is enough to prove that $\mathcal{Q}(P_\ell + M)$ holds for ℓ in $L^+ \cup L^-$, since letting r vary will conclude the proof.

If M belongs to P_ℓ, the ideal $P_\ell + M$ coincides with P_ℓ and the assumption hypothesis concludes; thus we need only consider ℓ in L^-. In this situation, by Krull's Principal Ideal Theorem, and since P_ℓ is prime, $P_\ell + M$ is equidimensional of dimension $r-1$. Thus by Lemma 1, it is enough to prove that the extension

$$\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r-1}] \to \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]/(P_\ell + M)$$

is integral for $\ell \in L^-$.

The auxiliary polynomials α_ℓ.
By assumption, $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}] \to A_\ell := \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]/P_\ell$ is an integral ring extension for ℓ in $L^+ \cup L^- \cup S$. Thus we need only prove that for $\ell \in L^-$, $P_\ell + M$ contains a monic polynomial in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r-1}][X_r]$.

By Quillen-Suslin's Theorem, A_ℓ is a free $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]$-module. Let χ_ℓ be the characteristic polynomial of the multiplication by M in A_ℓ, seen as a free module, and $\alpha_\ell \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]$ its constant term. For $\ell \in L^-$, the image of M is a non-zero divisor in A_ℓ, so α_ℓ is not zero, and $P_\ell + M \neq (1)$ so α_ℓ is not constant. Cayley-Hamilton's Theorem implies that α_ℓ belongs to the ideal $P_\ell + M$. It is thus enough to prove that α_ℓ is monic in X_r to prove $\mathcal{Q}(\Delta^{\mathfrak{A}}_{n-i+1})$.

Introduction of a change of free variables.
Let $\mathbf{B}$ be a matrix in $\mathrm{GL}_n(\mathbb{Q})$ of the form

$$\mathbf{B} = \begin{bmatrix} \mathbf{B}' & 0 \\ 0 & \mathbf{I}_{n-r} \end{bmatrix},$$

such that $\mathbf{B}'$ is square of size r, $\mathbf{I}_{n-r}$ is the $n-r$ identity matrix and $\alpha_\ell(\mathbf{BX})$ is monic in X_r for all ℓ in L^-. For the construction of such a matrix, we refer to [10, 8, 9].

We use the change of variables $\mathbf{B}$ in two different ways to conclude.

- If P is an ideal in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, we denote by $P^{\mathbf{B}}$ the ideal $\{f(\mathbf{BX}), f \in P\}$; if P is prime, $P^{\mathbf{B}}$ is prime of the same dimension. We then have the decomposition $\sqrt{\Delta^{\mathbf{B}}} = \cap_{\ell \leq L} P^{\mathbf{B}}_\ell$.

  Let $\ell \in L^+ \cup L^- \cup S$. We claim that the constant term of the characteristic polynomial of the multiplication by $M(\mathbf{BX})$ modulo $P^{\mathbf{B}}_\ell$ is $\alpha_\ell(\mathbf{BX})$. Indeed, let $\{G_1, \ldots, G_D\}$ be a basis of the free $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]$-module A_ℓ. The linear change of variables $\mathbf{B}$ affects only the first r variables, so $\{G_1(\mathbf{BX}), \ldots, G_D(\mathbf{BX})\}$ is a $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r}]$-basis of $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]/P^{\mathbf{B}}_\ell$; our assertion follows.

- Let $(\mathfrak{C}_{i,j})_{1 \leq i,j \leq n}$ be the entries of the matrix $\mathfrak{A}\mathbf{B}$; thus all $\mathfrak{C}_{i,j}$ are linear forms in the entries of $\mathfrak{A}$ with rational coefficients. Given a polynomial f in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, we denote by $\mathrm{Subs}_{\mathfrak{C}}(f) \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$ the polynomial f where each variable $\mathfrak{A}_{i,j}$ is substituted by the linear form $\mathfrak{C}_{i,j}$.

  If P is an ideal in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, we denote by $P^{\mathfrak{C}}$ the ideal $\{\mathrm{Subs}_{\mathfrak{C}}(f), f \in P\}$. As above, if P is prime, $P^{\mathfrak{C}}$ is prime of the same dimension and we have the equality $\sqrt{\Delta^{\mathfrak{C}}} = \cap_{\ell \leq L} P^{\mathfrak{C}}_\ell$.

  Let $\ell \in L^+ \cup L^- \cup S$. Using the same argumentation as above, we see that the constant term of the characteristic polynomial of the multiplication by $\mathrm{Subs}_{\mathfrak{C}}(M)$ modulo $P^{\mathfrak{C}}_\ell$ is $\mathrm{Subs}_{\mathfrak{C}}(\alpha_\ell)$.

Two useful equalities.
We now prove that $\Delta^{\mathbf{B}} = \Delta^{\mathfrak{C}}$ and $M(\mathbf{BX}) = \mathrm{Subs}_{\mathfrak{C}}(M)$. Recall that the polynomials $f^{\mathfrak{A}}_1, \ldots, f^{\mathfrak{A}}_s$ together with some minors of their Jacobian matrix generate the ideal Δ. We need not be more precise on these minors, and simply denote them by $M^{\mathfrak{A}}_1, \ldots, M^{\mathfrak{A}}_Q$. To prove the above equalities, it is enough to prove that if f is any of the polynomials $f^{\mathfrak{A}}_1, \ldots, f^{\mathfrak{A}}_s, M^{\mathfrak{A}}_1, \ldots, M^{\mathfrak{A}}_Q, M$, the equality $f(\mathbf{BX}) = \mathrm{Subs}_{\mathfrak{C}}(f)$ holds.

Consider first the polynomials $f^{\mathfrak{A}}_k$. They are defined by $f^{\mathfrak{A}}_k = f_k(\mathfrak{A}\mathbf{X})$, from which we deduce $\mathrm{Subs}_{\mathfrak{C}}(f^{\mathfrak{A}}_k) = f_k(\mathfrak{C}\mathbf{X}) = f_k(\mathfrak{A}\mathbf{B}\mathbf{X}) = f^{\mathfrak{A}}_k(\mathbf{BX})$ for $k \leq s$, as requested.

We now turn to the minors $M^{\mathfrak{A}}_1, \ldots, M^{\mathfrak{A}}_Q$ and M. They are defined using the first $n-i$ columns of the Jacobian matrix of the polynomials $f^{\mathfrak{A}}_k$, *i.e.*, with partial derivatives of these polynomials with respect to $X_{i+1}, \ldots, X_n$. It is then enough to prove that $(\partial f^{\mathfrak{A}}_k/\partial X_j)(\mathbf{BX}) = \mathrm{Subs}_{\mathfrak{C}}(\partial f^{\mathfrak{A}}_k/\partial X_j)$ for $k \leq s$ and $j > i$. But this is an immediate consequence of the definition of the polynomials $f^{\mathfrak{A}}_k$, and of the fact that the change of variables $\mathbf{B}$ acts trivially on the variables $X_{i+1}, \ldots, X_n$ since $r \leq i$.

Proof of property $\mathcal{Q}(\Delta^{\mathfrak{A}}_{n-i+1})$.
The equality $\Delta^{\mathbf{B}} = \Delta^{\mathfrak{C}}$ implies $\cap_{\ell \leq L} P^{\mathbf{B}}_\ell = \cap_{\ell \leq L} P^{\mathfrak{C}}_\ell$, and uniqueness of the prime decomposition yields

$$\{P^{\mathbf{B}}_\ell, \ell \in L\} = \{P^{\mathfrak{C}}_\ell, \ell \in L\}.$$

Since $\dim P^{\mathbf{B}}_\ell = \dim P^{\mathfrak{C}}_\ell = \dim P_\ell$ for all ℓ, we deduce

$$\{P^{\mathbf{B}}_\ell, \ell \in L^+ \cup L^- \cup S\} = \{P^{\mathfrak{C}}_\ell, \ell \in L^+ \cup L^- \cup S\}.$$

Let ℓ in L^-. By the last equality, there exists ℓ' in $L^+ \cup L^- \cup S$, such that $P^{\mathfrak{C}}_\ell = P^{\mathbf{B}}_{\ell'}$. Since $M^{\mathbf{B}} = \mathrm{Subs}_{\mathfrak{C}}(M)$, the characteristic polynomial of $\mathrm{Subs}_{\mathfrak{C}}(M)$ modulo $P^{\mathfrak{C}}_\ell$ is the characteristic polynomial of $M^{\mathbf{B}}$ modulo $P^{\mathbf{B}}_{\ell'}$, so $\mathrm{Subs}_{\mathfrak{C}}(\alpha_\ell) = \alpha_{\ell'}(\mathbf{BX})$ by the above discussion.

Since α_ℓ is neither zero nor constant, $\alpha_{\ell'}$ is neither zero nor constant, so $\ell' \in L^-$. Thus $\alpha_{\ell'}(\mathbf{BX}) = \mathrm{Subs}_{\mathfrak{C}}(\alpha_\ell)$ is monic in X_r, and so is α_ℓ.

Conclusion.
It only remains to prove that $W^{\mathfrak{A}}_{n-i+1}$ has dimension at most $i-1$. Let $\mathfrak{K}$ be an algebraic closure of $\mathbb{Q}(\mathfrak{A}_{i,j})$ and Π_i the canonical projection $\mathfrak{K}^n \to \mathfrak{K}^i$. Due to our definitions, $W^{\mathfrak{A}}_{n-d} \subset \mathfrak{K}^n$ is smooth and equidimensional, and $W^{\mathfrak{A}}_{n-i+1}$ is the critical locus of Π_i on $W^{\mathfrak{A}}_{n-d}$ for $i \leq d$.

We deduce that for $i \leq d$, $W^{\mathfrak{A}}_{n-i+1}$ is contained in the reunion of *(i)* the singular locus of $W^{\mathfrak{A}}_{n-i}$ and *(ii)* the critical locus of the restriction of π_i to the regular locus of $W^{\mathfrak{A}}_{n-i}$. It is thus enough to prove that this last object has dimension at most $i-1$.

Let us write the irreducible decomposition of $W^{\mathfrak{A}}_{n-i}$ as $\cup_{\ell \leq L} Z_\ell$. By the induction assumption, all Z_ℓ have dimension at most i; it is thus enough to consider the components of dimension i to conclude. The induction statement asserts that the restriction of π_i to any of these components is a finite map. Then the conclusion follows from the algebraic Bertini-Sard Theorem [21].

2.4 Proof of Proposition 2

Fix $i \in \{1, \ldots, d+1\}$, and consider the ideal $\Delta^{\mathfrak{A}}_{n-i+1}$. Since i is fixed, we write $\Delta = \Delta^{\mathfrak{A}}_{n-i+1}$. Let $(P_\ell)_{\ell \leq L}$ be the prime components of $\sqrt{\Delta}$ in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$, so that $\sqrt{\Delta} = \cap_{\ell \leq L} \sqrt{P_\ell}$, and let $G_{\ell,1}, \ldots, G_{\ell,N_\ell} \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$ be some generators of P_ℓ.

There is a Zariski-open subset Γ of $\mathrm{GL}_n(\mathbb{C})$ such that for $\mathbf{A}$ in Γ, the entries of Γ cancel none of the denominators of the coefficients of $G_{\ell,i}$, for $\ell \leq L$ and $i \leq N_\ell$. Then we denote by $G^{\mathbf{A}}_{\ell,i}$ the polynomial in $\mathbb{C}[\mathbf{X}]$ obtained by evaluating all coefficients of $G_{\ell,i}$ at the entries of $\mathbf{A}$, and by $Q^{\mathbf{A}}_\ell$ the ideal generated by $G^{\mathbf{A}}_{\ell,1}, \ldots, G^{\mathbf{A}}_{\ell,N_\ell}$.

Remark: The letter P is used for prime ideals; we do not claim that $(G^{\mathbf{A}}_{\ell,1}, \ldots, G^{\mathbf{A}}_{\ell,N_\ell})$ remains prime, this is why we use the letter Q.

To prove Proposition 2, we proceed as follows. We first prove that the equality $\sqrt{\Delta^{\mathbf{A}}} = \cap_{\ell \leq L} \sqrt{Q^{\mathbf{A}}_\ell}$ holds for all $\mathbf{A}$ in Γ. In a second time we prove that every ideal $Q^{\mathbf{A}}_\ell$ satisfies property $\mathcal{Q}$ and is equidimensional of dimension at most $i-1$. Even if $Q^{\mathbf{A}}_\ell$ is not prime, this is enough to prove Proposition 2. Proving these results may require to remove strict Zariski-closed sets from Γ.

First Step: $\sqrt{\Delta^{\mathbf{A}}} = \cap_{\ell \leq L} \sqrt{Q^{\mathbf{A}}_\ell}$.

Let $f^{\mathfrak{A}}_1, \ldots, f^{\mathfrak{A}}_s, M^{\mathfrak{A}}_1, \ldots, M^{\mathfrak{A}}_N$ be the polynomials generating the ideal Δ. By definition, for $\ell \leq L$, all these polynomials belong to P_ℓ, which can be expressed by a series of equalities in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$ giving them as a combination of $G_{\ell,1}, \ldots, G_{\ell,N_\ell}$. In all these equalities, the indeterminates $\mathfrak{A}_{i,j}$ can be replaced by the entries of any matrix $\mathbf{A} \in \Gamma$, yielding equalities in $\mathbb{C}[\mathbf{X}]$. Thus, for $\mathbf{A}$ in Γ, $\Delta^{\mathbf{A}} \subset \cap_\ell Q^{\mathbf{A}}_\ell$, whence $\sqrt{\Delta^{\mathbf{A}}} \subset \cap_\ell \sqrt{Q^{\mathbf{A}}_\ell}$.

Conversely, let us form the products $G_{1,i_1} \cdots G_{L,i_L}$, for all possible multi-indices $i = (i_1, \ldots, i_L)$. All these products belong to the radical of Δ, so there exists $N \in \mathbb{N}$ such that every $(G_{1,i_1} \cdots G_{L,i_L})^N \in \Delta$. Then every product $(G^{\mathbf{A}}_{1,i_1} \cdots G^{\mathbf{A}}_{L,i_L})^N$ belongs to $\Delta^{\mathbf{A}}$ for all $\mathbf{A} \in \Gamma$, whence $(Q^{\mathbf{A}}_1 \cdots Q^{\mathbf{A}}_L)^N \subset \Delta^{\mathbf{A}}$. Taking radicals yields $\cap_\ell \sqrt{Q^{\mathbf{A}}_\ell} \subset \sqrt{\Delta^{\mathbf{A}}}$.

Second Step: Properties of $Q^{\mathbf{A}}_\ell$.

Let $\ell \leq L$ and r_ℓ the dimension of P_ℓ. Up to removing a Zariski-closed subset from Γ, we claim that $Q^{\mathbf{A}}_\ell$ is equidimensional of dimension r_ℓ too. As quick way to see this, remark that an equidimensional decomposition can be performed by an algorithm without factorization. Then for $\mathbf{A}$ in a suitable Zariski-open set, the execution over $\mathbb{C}[\mathbf{X}]$ for the polynomials defining $Q^{\mathbf{A}}_\ell$ is the trace of the execution in $\mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}]$ for the polynomials defining P_ℓ, which is assumed to give an equidimensional result of dimension r_ℓ.

To conclude, it is thus enough to prove property $\mathcal{Q}$ for $Q^{\mathbf{A}}_\ell$. By Proposition 1, for $\ell \leq L$ and $i \in \{r_\ell + 1, \ldots, n\}$ there exists a polynomial $m_i \in \mathbb{Q}(\mathfrak{A}_{i,j})[\mathbf{X}_{\leq r_\ell}][T]$ such that $m_i(X_i)$ belongs to P_ℓ. Again, after removing the Zariski-closed subset from Γ that is defined by the denominators appearing in the underlying equalities, we deduce that $\mathbb{C}[\mathbf{X}_{\leq r_\ell}] \to \mathbb{C}[\mathbf{X}]/Q^{\mathbf{A}}_\ell$ is integral for $\mathbf{A} \in \Gamma$. We deduce that $Q^{\mathbf{A}}_\ell$ satisfies property $\mathcal{Q}$ by Lemma 1.

2.5 Proving properness

We finish the proof of Theorem 1 by proving Prop. 3. Let $\mathbf{A}$ be in $\mathrm{GL}_n(\mathbb{C})$ and $i \in \{2, \ldots, d+1\}$ (case $i = 1$ is trivial).

Let $(P^{\mathbf{A}}_\ell)_{\ell \leq L}$ be the prime components of $\Delta^{\mathbf{A}}_{n-i+1}$ and $(r_\ell)_{\ell \leq L}$ their dimensions. The restriction of π_{i-1} to $W^{\mathbf{A}}_{n-i+1}$ is proper if and only if all its restrictions to the zero-sets $V(P^{\mathbf{A}}_\ell)$ are proper. Thus to conclude, we prove that the restriction of π_{i-1} to $V(P^{\mathbf{A}}_\ell)$ is proper if and only if the extension $\mathbb{C}[\mathbf{X}_{\leq r_\ell}] \to \mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}_\ell$ is integral and $r_\ell \leq i-1$, for $\ell \leq L$.

For j in $r_\ell + 1, \ldots, n$, let $m_j \in \mathbb{C}(\mathbf{X}_{\leq r_\ell})[T]$ be the monic minimal polynomial of X_j in the algebraic field extension $\mathbb{C}(\mathbf{X}_{\leq r_\ell}) \to \mathfrak{frac}(\mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}_\ell)$. Lemma 3.10 in [15] states that the set of non-properness for the restriction of π_{r_ℓ} to $V(P^{\mathbf{A}}_\ell)$ is the reunion of the zero-sets of the denominators of the coefficients of the polynomials m_j. Thus the restriction of π_{r_ℓ} to $V(P^{\mathbf{A}}_\ell)$ is proper if and only if the extension $\mathbb{C}[\mathbf{X}_{\leq r_\ell}] \to \mathbb{C}[\mathbf{X}]/P^{\mathbf{A}}_\ell$ is integral.

Then, the restriction of π_{i-1} to $V(P^{\mathbf{A}}_\ell)$ is proper if and only if the restriction of π_{r_ℓ} to $V(P^{\mathbf{A}}_\ell)$ is proper and $r_\ell \leq i-1$. This concludes the proof.

Remark: Dimension of fibers.

By [21, Chapter 1.5.3], all fibers of the restriction of π_{r_ℓ} to $V(P_\ell)$ are finite, for $\ell \leq L$. Since $r_\ell \leq i-1$, we deduce that all fibers of the restriction of π_{i-1} to $W^{\mathbf{A}}_{n-i+1}$ have finite cardinality. This proves the first statement of Theorem 2.

3. PROOF OF THEOREM 2

We now investigate the relation between the polar varieties of $f_1, \ldots, f_s$ and the connected components of $V \cap \mathbb{R}^n$. Namely, we conclude the proof of Theorem 2:

Let $\mathbf{A} \in \mathrm{GL}_n(\mathbb{C})$ be such that $\mathcal{P}(\mathbf{A})$ holds. Let $p_d = (x_1, \ldots, x_d)$ be any point in $\mathbb{R}^d$. For $j \in \{1, \ldots, d-1\}$, define $p_j = (x_1, \ldots, x_j) \in \mathbb{R}^i$, and $\pi_0^{-1}(p_0) = \mathbb{C}^n$. Then the algebraic sets $W^{\mathbf{A}}_{n-j} \cap \pi_j^{-1}(p_j)$, $j \in \{0, \ldots, d\}$, are either empty or zero-dimensional. Their reunion meets every connected component of $V^{\mathbf{A}} \cap \mathbb{R}^n$.

Since the matrix $\mathbf{A}$ is fixed once and for all in this section, there is no need to systematically make explicit mention of it. Thus, in all the rest of this section, we simply write W_{n-i+1} and V instead of $W^{\mathbf{A}}_{n-i+1}$ and $V^{\mathbf{A}}$. Our hypothesis will simply be denoted by $\mathcal{P}$: *for all i in $1, \ldots, d+1$, the restriction of π_{i-1} to W_{n-i+1} is proper.*

In what follows, we first prove a geometric result on the frontier of the projections of the connected components of $V \cap \mathbb{R}^n$, then conclude the proof of Theorem 2.

The frontier of $A \subset \mathbb{R}^i$ is the closure of A minus the interior of A (for the metric topology). We use the fact that for $A, B \subset \mathbb{R}^i$, if A is connected and meets both B and its complementary, then A meets the frontier of B.

Proposition 4 *Let D be a connected component of $V \cap \mathbb{R}^n$. For i in $1, \ldots, d$, the frontier of $\pi_i(D) \subset \mathbb{R}^i$ is included in $\pi_i(W_{n-i+1} \cap D)$.*

PROOF. Let us denote this property by $\mathfrak{Q}_i$. We prove it by decreasing induction on $i = d, \ldots, 1$. First, we prove $\mathfrak{Q}_d$. Let $x \in \mathbb{R}^d$ be in the frontier of $\pi_d(D)$. By assumption $\mathcal{P}$, the restriction of π_d to $V \cap \mathbb{R}^n$ is proper, so x is in the image $\pi_d(D)$. Thus, since $V \cap \mathbb{R}^n$ is smooth, from the implicit function theorem, there exists a critical point $y \in D$ of π_d restricted to V such that $\pi_d(y) = x$. This proves $\mathfrak{Q}_d$.

We now assume $\mathfrak{Q}_{i+1}$, and prove $\mathfrak{Q}_i$. Let thus $x \in \mathbb{R}^i$ be in the frontier of $\pi_i(D) \subset \mathbb{R}^i$. It is enough to prove that x is in $\pi_i(D)$: as in the previous paragraph, the implicit function theorem then proves that x is a critical point of the restriction of π_i to D, which gives property $\mathfrak{Q}_i$.

Thus, we prove that x is in $\pi_i(D)$. Let φ be the projection $\mathbb{R}^{i+1} \to \mathbb{R}^i$ that maps $(x_1, \ldots, x_{i+1})$ to $(x_1, \ldots, x_i)$; for $r > 0$, we denote by $B_r \subset \mathbb{R}^i$ the closed ball centered at x of radius r, and by $C_r \subset \mathbb{R}^{i+1}$ the preimage $\varphi^{-1}(B_r)$, which is a cylinder.

By definition, for $r > 0$, $\pi_i^{-1}(B_r)$ meets D, so C_r meets $\pi_{i+1}(D)$. On the other hand, since x is in the frontier of $\pi_i(D)$, there exists a point in B_r that is not $\pi_i(D)$, so there exists a point in C_r that is not in $\pi_{i+1}(D)$. We deduce that for $r > 0$, C_r meets the frontier of $\pi_{i+1}(D)$.

By induction hypothesis, there exists $y_r \in W_{n-i} \cap D$ such that $\pi_{i+1}(y_r) \in C_r$. Applying φ, we deduce that $\pi_i(y_r) \in B_r$. Since this holds for all $r > 0$, x is in the closure of $\pi_i(W_{n-i} \cap D)$. By assumption $\mathcal{P}$, the restriction of π_i to $W_{n-i} \cap D$ is proper, so $\pi_i(W_{n-i} \cap D)$ is closed. Thus x is in $\pi_i(W_{n-i} \cap D) \subset \pi_i(D)$, *q.e.d.* □

We are ready to prove Theorem 2. Let $p_d = (x_1, \ldots, x_d)$ be an arbitrary point in $\mathbb{R}^d$, and let $p_j = (x_1, \ldots, x_j)$ for $j = 1, \ldots, d-1$. Let D be a connected component of $V \cap \mathbb{R}^n$. We will prove that there exists $j_0 \in \{0, \ldots, d\}$ such that $\pi_j^{-1}(p_{j_0}) \cap W_{n-j_0}$ meets D, with the convention that $\pi_0^{-1}(p_0) = \mathbb{C}^n$.

For $j = 0, \ldots, d-1$, we denote by $C_j \subset \mathbb{R}^{j+1}$ the cylinder $\{p_j\} \times \mathbb{R}$ built above p_j (we take $C_0 = \mathbb{R}$); note that p_{j+1} belongs to C_j by definition.

Consider the subset $\mathcal{J} \subset \{0, \ldots, d-1\}$ such that $j \in \mathcal{J}$ if and only if C_j intersects the frontier of $\pi_{j+1}(D)$, at a point denoted by x_{j+1}. First, suppose that $\mathcal{J}$ is not empty. Then, by Proposition 4, for $j_0 \in \mathcal{J}$, x_{j_0+1} belongs to $\pi_{j_0+1}(W_{n-j_0} \cap D)$, so p_{j_0} belongs to $\pi_{j_0}(W_{n-j_0} \cap D)$, which concludes the proof.

Now, suppose that $\mathcal{J}$ is empty. We shall show below that this implies that for all $j \in \{0, \ldots, d-1\}$, C_j is included in $\pi_{j+1}(D)$. For the moment, suppose that it is true. Then for index $d-1$, this yields that C_{d-1} is contained in $\pi_d(D)$. Since p_d is in C_{d-1}, p_d is in $\pi_d(D)$, and we take $j_0 = d$ (recall that $W_{n-d} = V$).

It remains to show that, under the assumption that $\mathcal{J}$ is empty, for all $j \in \{0, \ldots, d-1\}$, C_j is included in $\pi_{j+1}(D)$. We proceed by induction on j. First take $j = 0$. By assumption, the frontier of $\pi_1(D)$ is empty, so $\pi_1(D) = \mathbb{R} = C_0$, as requested. Now, suppose that C_{j-1} is contained in $\pi_j(D)$; in particular, p_j belongs to $\pi_j(D)$, so C_j meets $\pi_{j+1}(D)$. Since $\mathcal{J}$ is empty, C_j does not intersect the frontier of $\pi_{j+1}(D)$, so C_j is contained in $\pi_{j+1}(D)$. This ends the proof.

4. PROOF OF THEOREM 3

We finally present our algorithm. It takes as input $f_1, \ldots, f_s$ in $\mathbb{Q}[X_1, \ldots, X_n]$ that generate an equidimensional and radical ideal of dimension d, whose zero-set V is smooth. It returns a set of geometric resolutions describing zero-dimensional sets, whose reunion intersects every connected component of $V \cap \mathbb{R}^n$. We suppose that $f_1, \ldots, f_s$ have degree bounded by D and are given by a Straight-Line Program of size L.

The first step of the algorithm applies a randomly chosen change of variables $\mathbf{A}$ with rational coefficients to the input system. As usually, denote by $f_1^{\mathbf{A}}, \ldots, f_s^{\mathbf{A}}$ the polynomials we obtain. Then we choose an arbitrary point $p_d = (x_1, \ldots, x_d)$ in $\mathbb{Q}^d$ and compute geometric resolutions of the zero-dimensional sets $W_{n-i+1}^{\mathbf{A}} \cap \pi_{i-1}^{-1}(p_{i-1})$, for $i \in \{1, \ldots, d+1\}$. Correctness follows from Theorem 2, as soon as $\mathbf{A}$ satisfies property $\mathcal{P}$ defined in the introduction.

To estimate the complexity of the process, we use the following result adapted from [16, Chapter IV]. The notations used here are defined in the introduction.

Theorem 4 *[16] Let $g_1, \ldots, g_S$ be polynomials of degree bounded by $\mathcal{D}$ in $\mathbb{Q}[X_1, \ldots, X_n]$, represented by a Straight-Line Program of length $\mathcal{L}$ and defining a zero-dimensional variety. There exists an algorithm computing a geometric resolution of $V(g_1, \ldots, g_S)$ whose arithmetic complexity is:*

$$\mathcal{O}_{\log}\left(Sn^4(n\mathcal{L} + n^4)M(\mathcal{D}\mathfrak{d})\right)^3$$

where $\mathfrak{d}$ is the maximum of the sums of the algebraic degrees of the irreducible components of the intermediate varieties defined by $g_1, \ldots, g_i$ for i in $1, \ldots, S$.

As a shorthand, in what follows, we refer to the quantity $\mathfrak{d}$ above as *the algebraic degree of $g_1, \ldots, g_S$*.

To prove Theorem 3, we must describe the systems we use to define the zero-dimensional sets $W_{n-i+1}^{\mathbf{A}} \cap \pi_{i-1}^{-1}(p_{i-1})$. We freely make use of the notation $M_{i,j}^{\mathbf{A}}$ defined in the introduction, and adopt the same ordering

convention. Then $W^{\mathbf{A}}_{n-i+1} \cap \pi^{-1}_{i-1}(p_{i-1})$ is defined by

$$f^{\mathbf{A}}_1, \ldots, f^{\mathbf{A}}_s, M^{\mathbf{A}}_{i,1}, \ldots, M^{\mathbf{A}}_{i,S_i},$$

where $X_1, \ldots, X_i$ are specialized at $p_1, \ldots, p_i$.

All polynomials in these systems have degree at most $D(n-d)$. Due to the application of the change of variables $\mathbf{A}$, the polynomials $f^{\mathbf{A}}_k$ can be evaluated within $L+n^2$ operations. Using Baur-Strassen's and Berkowitz' algorithms, any Jacobian minor involved in the above systems can be evaluated in $(n-d)^4(L+n^2)$ operations. Since $S_i \leq S_i$ for all i, any of the above systems can be evaluated within $\mathcal{O}(S_1 n^4(L+n^2))$ operations.

To apply Theorem 4, we relate the algebraic degrees of the above systems to the quantity δ defined in the introduction. This is actually straightforward. Specializing variables only lowers the algebraic degree. Using our ordering convention, we deduce that the algebraic degrees of all the systems we solve are bounded by that of

$$f^{\mathbf{A}}_1, \ldots, f^{\mathbf{A}}_s, M^{\mathbf{A}}_{1,1}, \ldots, M^{\mathbf{A}}_{1,S_1}.$$

By definition, this quantity is bounded by δ.

The proof of Theorem 3 follows immediately. First we plug the above data into the complexity estimate of Theorem 4, and perform slight simplifications. We finally restore the initial coordinates; the cost is negligible [16].

5. REFERENCES

[1] M. E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Proceedings MEGA'94*, volume 142 of *Progress in Mathematics*, pages 1–15. Birkhäuser, 1996.

[2] P. Aubry, F. Rouillier, and M. Safey El Din. Real solving for positive dimensional systems. *Journal of Symbolic Computation*, 34(6):543–560, 2002.

[3] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real equation solving: the hypersurface case. *Journal of Complexity*, 13(1):5–27, 1997.

[4] B. Bank, M. Giusti, J. Heintz, and G.-M. Mbakop. Polar varieties and efficient real elimination. *Mathematische Zeitschrift*, 238(1):115–144, 2001.

[5] S. Basu. *Algorithms in semi-algebraic geometry.* PhD thesis, New-York University, 1996.

[6] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *Journal of ACM*, 43(6):1002–1045, 1996.

[7] S. Basu, R. Pollack, and M.-F. Roy. A new algorithm to find a point in every cell defined by a family of polynomials. In *Quantifier elimination and cylindrical algebraic decomposition.* Springer-Verlag, 1998.

[8] M. Giusti, K. Hägele, J. Heintz, J.-E Morais, J.-L. Montaña, and L.-M. Pardo. Lower bounds for Diophantine approximation. In *Proceedings of MEGA'96*, number 117, 118 in Journal of Pure and Applied Algebra, pages 277–317, 1997.

[9] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *Journal of Pure and Applied Algebra*, 124:101–146, 1998.

[10] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *Proceedings of AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[11] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[12] D. Grigoriev and N. Vorobjov. Solving systems of polynomials inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[13] J. Heintz, M.-F. Roy, and P. Solerno. On the complexity of semi-algebraic sets. In *Proceedings IFIP*, 1989.

[14] J. Heintz, M.-F. Roy, and P. Solerno. On the theoretical and practical complexity of the existential theory of the reals. *The Computer Journal*, 36(5):427–431, 1993.

[15] Z. Jelonek. Testing sets for properness of polynomial mappings. *Mathematische Annalen*, 315(1):1–35, 1999.

[16] G. Lecerf. *Une alternative aux méthodes de réécriture pour la résolution des systèmes algébriques.* PhD thesis, École polytechnique, 2001.

[17] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *AAECC Journal*, 9(5):433–461, 1999.

[18] F. Rouillier, M.-F. Roy, and M. Safey El Din. Finding at least one point in each connected component of a real algebraic set defined by a single equation. *Journal of Complexity*, 16:716–750, 2000.

[19] M. Safey El Din. *Résolution réelle des systèmes polynomiaux de dimension positive.* PhD thesis, Université Paris 6, January 2001.

[20] M. Safey El Din and É. Schost. Properness defects of projections and computation of one point in each connected component of a real algebraic set. Technical report, RR INRIA, 2002.

[21] I Shafarevich. *Basic Algebraic Geometry 1.* Springer Verlag, 1977.