On the Bit Complexity of Finding Points in Connected Components of a Smooth Real Hypersurface

Jesse Elliott
Cheriton School of Computer Science
University of Waterloo
jakellio@uwaterloo.ca

Mark Giesbrecht
Cheriton School of Computer Science
University of Waterloo
mwg@uwaterloo.ca

Éric Schost
Cheriton School of Computer Science
University of Waterloo
eschost@uwaterloo.ca

Abstract

We present a full analysis of the bit complexity of an efficient algorithm for the computation of at least one point in each connected component of a smooth real hypersurface. This is a basic and important operation in semi-algebraic geometry: it gives an upper bound on the number of connected components of a real hypersurface, and is also used in many higher level algorithms.

Our starting point is an algorithm by Safey El Din and Schost (*Polar varieties and computation of one point in each connected component of a smooth real algebraic set*, ISSAC'03). This algorithm uses random changes of variables that are proved to generically ensure certain desirable geometric properties. The cost of the algorithm was given in an algebraic complexity model; the analysis of the bit complexity and the error probability were left for future work.

Our paper answers these questions. Our main contribution is a quantitative analysis of several genericity statements, such as Thom's weak transversality theorem or Noether normalization properties for polar varieties.

CCS Concepts

• **Computing methodologies** → **Algebraic algorithms**.

Keywords

Real algebraic geometry; weak transversality; Noether position; complexity

ACM Reference Format:
Jesse Elliott, Mark Giesbrecht, and Éric Schost. 2020. On the Bit Complexity of Finding Points in Connected Components of a Smooth Real Hypersurface. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Kalamata, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3373207.3404058

1 Introduction

Background and problem statement. Computing one point in each connected component of a real algebraic set S is a basic subroutine in real algebraic and semi-algebraic geometry; it is also useful in its own right, since it allows one to decide if S is empty or not.

In this paper, we consider the case where S is given as $S = V \cap \mathbb{R}^n$, where $V = V(f) \subset \mathbb{C}^n$ is a complex hypersurface defined by a squarefree polynomial $f \in \mathbb{Z}[X_1, \dots, X_n]$. Algorithms for this task have been known for decades, and their complexity is to some extent well understood. Suppose that f has degree d, and coefficients of bit-size h. Without making any assumption on f, the algorithm given in [7, Section 13.1] solves our problem using $d^{O(n)}$ operations in $\mathbb{Q}$; in addition, the output of the algorithm is represented by polynomials of degree $d^{O(n)}$, with coefficients of bit-size $hd^{O(n)}$. The key idea behind this algorithm goes back to [18]: sample points are found through the computation of critical points of well-chosen functions on $V(f)$.

The number of connected components of $V(f)$ admits the lower bound $d^{\Omega(n)}$, so up to polynomial factors this result is optimal. However, due to the generality of the algorithm, the constant hidden in the exponent $O(n)$ in its runtime turns out to be rather large: the algorithm relies on infinitesimal deformations, that affect runtime non-trivially.

In this paper, we will work under the additional assumption that $V = V(f)$ is a *smooth* complex hypersurface. We place ourselves in the continuation of the line of work initiated by [4]: that reference deals with cases where V is smooth and $V \cap \mathbb{R}^n$ is compact, pointing out how *polar varieties* (that were introduced in the 1930's in order to define characteristic classes [25, 34]) can play a role in effective real geometry. This paper was extended in several directions: to V being a smooth complete intersection, still with $V \cap \mathbb{R}^n$ compact [5], then without the compactness assumption [6, 28]; the smoothness assumption was then partly dropped in [2, 3].

Our starting point is the algorithm in [28]. In the hypersurface case, its runtime is $d^{(4+o(1))n}$ operations in $\mathbb{Q}$. As with many results in this vein, the algorithm is randomized: we need to assume that we are in generic coordinates; this is done by applying a random change of coordinates prior to all computations. In addition, the algorithm relies on procedures for solving systems of polynomial equations that are themselves randomized. Altogether, we choose $n^{O(1)}$ random vectors, each of them in an affine space of dimension $n^{O(1)}$; every time a choice is made, there exists a hypersurface of the parameter space that one has to avoid in order to guarantee success. In this paper, we revisit this algorithm and give a complete analysis of its probability of success and its bit complexity.

Data structures. The output of the algorithm is a finite set in $\overline{\mathbb{Q}}^n$. To represent it, we rely on a widely used data structure based on univariate polynomials [1, 13–16, 22, 23, 26]. For a zero-dimensional algebraic set $S \subset \mathbb{C}^n$ defined over $\mathbb{Q}$, a *zero-dimensional parameterization* $\mathscr{Q} = ((q, v_1, \dots, v_n), \lambda)$ of S consists in polynomials $(q, v_1, \dots, v_n)$, such that $q \in \mathbb{Q}[T]$ is monic and squarefree, all v_i's

ISSAC '20, July 20–23, 2020, Kalamata, Greece

ACM ISBN 978-1-4503-7100-1/20/07…$15.00
https://doi.org/10.1145/3373207.3404058

are in $\mathbb{Q}[T]$ and satisfy $\deg(v_i) < \deg(q)$, and in a $\mathbb{Q}$-linear form λ in variables $X_1, \ldots, X_n$, such that

- $\lambda(v_1, \ldots, v_n) = Tq' \bmod q$;
- we have the equality $S = \left\{ \left(\frac{v_1(\tau)}{q'(\tau)}, \ldots, \frac{v_n(\tau)}{q'(\tau)} \right) \mid q(\tau) = 0 \right\}$.

The constraint on λ says that the roots of q are the values taken by λ on S. The parameterization of the coordinates by rational functions having q' as a denominator goes back to [22, 23]: as pointed out in [1], it allows one to control precisely the size of the coefficients of $v_1, \ldots, v_n$.

Main result. To state our main result, we need to define the *height* of a rational number, and of a polynomial with rational coefficients.

The *height* of a non-zero $a = u/v \in \mathbb{Q}$ is the maximum of $\ln(|u|)$ and $\ln(v)$, where $u \in \mathbb{Z}$ and $v \in \mathbb{N}$ are coprime. For a polynomial f with rational coefficients, if $v \in \mathbb{N}$ is the minimal common denominator of all non-zero coefficients of f, then the *height* $\mathrm{ht}(f)$ of f is defined as the maximum of the logarithms of v and of the absolute values of the coefficients of vf.

Theorem 1.1. *Suppose that $f \in \mathbb{Z}[X_1 \ldots, X_n]$ is squarefree, satisfies $\deg(f) \le d$ and $\mathrm{ht}(f) \le b$, and that $V(f) \subset \mathbb{C}^n$ is smooth. Also suppose that $0 < \epsilon < 1$.*

There exists a randomized algorithm that takes f and ϵ as input and produces n zero-dimensional parameterizations, the union of whose zeros includes at least one point in each connected component of $V(f) \cap \mathbb{R}^n$, with probability at least $1 - \epsilon$. Otherwise, the algorithm either returns a proper subset of the points, or FAIL. In any case, the algorithm uses

$$O^{\sim}(d^{3n+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$

bit operations. The polynomials in the output have degree at most d^n, and height

$$O^{\sim}(d^{n+1}(b + \log 1/\epsilon)).$$

Here we assume that f is given as a dense polynomial. Following references such as [4, 14–16, 28], it would be possible to refine the runtime estimate by assuming that f is given by a *straight-line program* (that is, a sequence of operations $+, -, \times$ that takes as input $X_1, \ldots, X_n$ and evaluates f). Any polynomial of degree d in n variables can be computed by a straight-line program that does $O(d^n)$ operations: evaluate all monomials of degree up to d in n variables, multiply them by their respective coefficients and sum the results. However, some inputs may be given by shorter straight-line program, and the algorithm would actually be able to benefit from this.

The algorithm itself is rather simple. To describe it, we need to define *polar varieties*, which will play a crucial role in this paper. Let $V = V(f)$, for f as in the theorem. For $i \in \{1, \ldots, n-1\}$, denote by $\pi_i : \mathbb{C}^n \to \mathbb{C}^i$ the projection $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i)$. The i-th *polar variety*

$$W(\pi_i, V) := \{\boldsymbol{x} \in V \mid \dim \pi_i(T_{\boldsymbol{x}} V) < i\}$$

is the set of critical points of π_i on V. It is thus defined by the vanishing of

$$f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}.$$

In general, we cannot say much about the geometry of $W(\pi_i, V)$, but if we apply a generic change of coordinates $\boldsymbol{A}$ to f, then $W(\pi_i, V)$ is known to be equidimensional of dimension $(i-1)$ or empty [4], and to be in so-called *Noether position* [28] (background notions in algebraic geometry are in [12, 24, 33]; we will recall key definitions). If this is the case, it suffices to choose arbitrary $\sigma_1, \ldots, \sigma_{n-1}$ in $\mathbb{Q}$, and solve the systems defined by

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}, \qquad (1)$$

for $i = 1, \ldots, n$. They all admit finitely many solutions, and Theorem 2 in [28] proves that the union of their solution sets contains one point on each connected component of $V \cap \mathbb{R}^n$.

Our main contribution is to analyze precisely what conditions on our change of coordinates $\boldsymbol{A}$ guarantee success. This is done by revisiting the key ingredients in the proofs given in [4] and [28], and giving quantitative versions of these results, bounding the degree of the hypersurfaces we have to avoid. To solve the equations (1), we use the algorithm in [31], for which a complete bit complexity analysis is available.

This work should be seen as a first step toward the analysis of further randomized algorithms in real algebraic geometry. An immediate follow-up question would be to handle the case of algebraic sets defined by *regular sequences*: the algorithm in [28] still applies, but the modifications needed are beyond the scope of this publication. Further still, randomized algorithms for deciding *connectivity queries* on smooth, compact algebraic sets have been developed in a series of papers [29, 32], and could be revisited using the techniques introduced here.

2 Genericity properties

Consider $f \in \mathbb{Z}[X_1, \ldots, X_n]$ with total degree d, and assume that f is squarefree and that $V(f) \subset \mathbb{C}^n$ is smooth. The key to the proof of Theorem 1.1 is the following quantitative version of facts we stated above, namely that in generic coordinates, polar varieties are smooth, equidimensional, and in Noether position (or empty).

We recall that an equidimensional algebraic set $X \subset \mathbb{C}^n$ of dimension d is in *Noether position* for the projection π_d when the extension $\mathbb{C}[X_1, \ldots, X_d] \to \mathbb{C}[X_1, \ldots, X_n]/I(X)$ is integral; here, $I(X) \subset \mathbb{C}[X_1, \ldots, X_n]$ is the defining ideal of X. In this case, for any $\boldsymbol{x} \in \mathbb{C}^d$, the fiber $X \cap \pi_d^{-1}(\boldsymbol{x})$ has dimension zero (so it is finite and not empty).

For i in $\{1, \ldots, n\}$ and f as above, we will let $\mathfrak{I}(i, f)$ denote the sequence of $n - (i-1)$ polynomials $(f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n)$. As pointed out in the introduction, their zero-set is the i-th polar variety $W(\pi_i, V(f))$. Then, we say that f satisfies $\mathbf{H}_i$ if

(1) For any $\boldsymbol{x}$ in $W(\pi_i, V(f))$, the Jacobian matrix $\mathbf{jac}_{\boldsymbol{x}}(\mathfrak{I}(i, f))$ has full rank $n - (i-1)$ at $\boldsymbol{x}$.
By the Jacobian Criterion [12, Corollary 16.20], this implies that $W(\pi_i, V(f))$ is either empty or $(i-1)$-equidimensional, and that $\mathfrak{I}(i, f)$ defines a radical ideal.

(2) $W(\pi_i, V(f))$ is either empty or in Noether position for π_{i-1}.

Given $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1})$ in $\mathbb{C}^{i-1}$, we further say that f and $\boldsymbol{\sigma}$ satisfy $\mathbf{H}'_i$ if

(1) For any root $\boldsymbol{x}$ of

$$(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n),$$

the Jacobian matrix of these equations at $\boldsymbol{x}$ has full rank n. *By the Jacobian Criterion [12, Corollary 16.20], this implies that there are finitly many solutions to these equations.*

Even if f does not initially satisfy $\mathbf{H}_i$, it does after applying a generic change of variables. The precise statement is as follows, for which we use the following notation. For a matrix $\boldsymbol{A}$ in $\mathbb{C}^{n\times n}$ and g in $\mathbb{C}[X_1,\dots,X_n]$ we write $g^{\boldsymbol{A}} := g(\boldsymbol{AX}) \in \mathbb{C}[X_1,\dots,X_n]$, where $\boldsymbol{X}$ is the column vector with entries $X_1,\dots,X_n$.

Note that for a variety $Y \subset \mathbb{C}^n$, we can define $Y^{\boldsymbol{A}}$ as the image of Y by the map $\phi_{\boldsymbol{A}} : \boldsymbol{x} \mapsto \boldsymbol{A}^{-1}\boldsymbol{x}$. Note that $W(\pi_i, V(f^{\boldsymbol{A}}))$ may not equal $W(\pi_i, V(f))^{\boldsymbol{A}}$, as, for instance, their dimensions may vary.

We will also have to consider matrices with generic entries. For this, we introduce n^2 new indeterminates $(\mathfrak{A}_{j,k})_{1\le j,k\le n}$. Then, $\mathfrak{A}$ will denote the matrix with entries $(\mathfrak{A}_{j,k})_{1\le j,k\le n}$, $\mathbb{C}(\mathfrak{A})$ will denote the rational function field $\mathbb{C}((\mathfrak{A}_{j,k})_{1\le j,k\le n})$ and $\mathbb{C}[\mathfrak{A}]$ the polynomial ring $\mathbb{C}[(\mathfrak{A}_{j,k})_{1\le j,k\le n}]$. For f as above, we will then define the polynomial $f^{\mathfrak{A}} := f(\mathfrak{A}\boldsymbol{X})$, which we may consider in either $\mathbb{C}(\mathfrak{A})[X_1,\dots,X_n]$ or $\mathbb{C}[\mathfrak{A}, X_1,\dots,X_n]$.

This being said, our two key results are the following.

Theorem 2.1. *For $i = 1,\dots,n$, there exists a non-zero polynomial $\Delta_i \in \mathbb{C}[\mathfrak{A}]$ of degree at most $5n^2(2d)^{2n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel Δ_i, then $\boldsymbol{A}$ is invertible and $f^{\boldsymbol{A}}$ satisfies $\boldsymbol{H}_i$.*

Theorem 2.2. *For $i = 1,\dots,n$, suppose that f satisfies $\boldsymbol{H}_i$, then there exists a non-zero polynomial $\Xi_i \in \mathbb{C}[S_1,\dots,S_{i-1}]$ of degree at most d^{2n} such that if $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel Ξ_i, then f and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}'_i$.*

The proof of these theorems occupies the next two sections. Some related results appear in the literature; for instance, Lemma 5 in [20] or Proposition 4.5 in [21] are quantitative Noether position statements. However, Theorem 2.1 does not follow from these previous results. Indeed, those references would allow us to quantify when $W(\pi_i, V(f))^{\boldsymbol{A}}$ is in Noether position, whereas we need to understand when $W(\pi_i, V(f^{\boldsymbol{A}}))$ is. As we pointed out before, these two sets are in general different.

3 Weak transversality and applications

Sard's lemma states that the set of critical values of a smooth function $\mathbb{R}^n \to \mathbb{R}^m$ has measure zero. One can give "algebraic" versions of it, for semi-algebraic mappings $\mathbb{R}^n \to \mathbb{R}^m$ as in [9, Chapter 9], or polynomial mappings $\mathbb{C}^n \to \mathbb{C}^m$ as in [24, Chapter 3], for which the sets of critical values are contained in strict semi-algebraic, resp. algebraic sets in the codomain. Thom's weak transversality lemma, as given for instance in [11], generalizes Sard's lemma. In this section, we consider a particular case of this result (transversality to a point), and establish a quantitative version of it; this will allow us to establish the first item in property $\mathbf{H}_i$, as well as property $\mathbf{H}'_i$.

3.1 Weak transversality

Transversality to a point can be rephrased entirely in terms of critical and regular values. Recall that if Ψ is a mapping from a smooth algebraic set Y to $\mathbb{C}^t$, with $t \le \dim(Y)$, a *critical point* of Ψ is a point $\boldsymbol{y} \in Y$ such that the image of the tangent space $T_{\boldsymbol{y}}Y$ by the differential $d_Y\Psi$ has dimension less than t. When for instance $Y = \mathbb{C}^v$, we have $T_{\boldsymbol{y}}Y = \mathbb{C}^v$ and this condition is equivalent to the Jacobian of Ψ having rank less than t at $\boldsymbol{y}$. *Critical values* are the images by Ψ of critical points; the complement of this set are the *regular values* (so a regular value is not necessarily in the image of Ψ).

Let then n, s, and m be positive integers, with $m \le n$, and denote by $\boldsymbol{\Phi} : \mathbb{C}^n \times \mathbb{C}^s \to \mathbb{C}^m$ a mapping defined by polynomials in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{\Theta}]$, where $\boldsymbol{X}$, resp. $\boldsymbol{\Theta}$, is a set of n, resp. s, indeterminates. For $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$, let $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}} : \mathbb{C}^n \to \mathbb{C}^m$ be the induced mapping $\boldsymbol{x} \mapsto \boldsymbol{\Phi}(\boldsymbol{x}, \boldsymbol{\vartheta})$. The transversality result we will need is the following.

Proposition 3.1 (Weak transversality). *Suppose that $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}$. Then there exists a non-zero polynomial $\Gamma \in \mathbb{C}[\boldsymbol{\Theta}]$ of degree at most d^{m+n} such that for $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$, if $\Gamma(\boldsymbol{\vartheta}) \ne 0$, then $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$.*

The following simple example shows this result at work. Consider a squarefree f in $\mathbb{C}[X_1, X_2]$, such that $V(f)$ is a smooth curve in $\mathbb{C}^2$, and let the mapping $\boldsymbol{\Phi} : \mathbb{C}^2 \times \mathbb{C} \to \mathbb{C}^2$ be defined by $\boldsymbol{\Phi}(X_1, X_2, \Theta) = (f(X_1, X_2), X_1 - \Theta)$. One checks that the Jacobian of $\boldsymbol{\Phi}$ with respect to (X_1, X_2, Θ) has rank two at any point in $\boldsymbol{\Phi}^{-1}(\mathbf{0})$, so the assumptions of the proposition apply. We deduce that for a generic ϑ in $\mathbb{C}$, that is, for all ϑ in $\mathbb{C}$ except a finite number, the ideal $(f(X_1, X_2), X_1 - \vartheta)$ is radical in $\mathbb{C}[X_1, X_2]$; equivalently, $f(\vartheta, X_2)$ is squarefree. We will revisit this example in Section 3.3.

The rest of the subsection is devoted to the proof of the proposition. The proof of [30, Theorem B.3] already shows the existence of Γ; it is essentially the classical proof for smooth mappings [11, Section 3.7], written in an algebraic context. In what follows, we revisit this proof, establishing a bound on the degree of Γ.

Put $V := \boldsymbol{\Phi}^{-1}(\mathbf{0})$. If V is empty, there is nothing to do, since all values $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$ satisfy the conclusion of the proposition. Thus, we assume that V is not empty. Then, the Jacobian criterion shows that V is smooth and $(n + s - m)$-equidimensional.

We will reuse the following fact, proved in [30]. Consider the projection $\pi : (\boldsymbol{x}, \boldsymbol{\vartheta}) \in \mathbb{C}^n \times \mathbb{C}^s \mapsto \boldsymbol{\vartheta} \in \mathbb{C}^s$. Let Z be the set of critical points of $\pi_{|V}$, and consider its projection $\pi(Z)$ in $\mathbb{C}^s$. This is the set of critical values of $\pi_{|V}$; hence, by the algebraic form of Sard's lemma (see [24, Theorem 3.7] for irreducible V and [30, Proposition B.2] for general V), its Zariski closure $\overline{\pi(Z)}$ is a strict closed subset of $\mathbb{C}^s$. As we will see below, if $\boldsymbol{\vartheta} \in \mathbb{C}^s$ is not in $\overline{\pi(Z)}$, then $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$.

To describe the set Z of critical points of $\pi_{|V}$, let $\boldsymbol{M}$ denote the $(s + m) \times (s + n)$ Jacobian matrix with entries in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{\Theta}]$ given by $\boldsymbol{M} := \mathbf{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\pi, \boldsymbol{\Phi})$, that is,

$$\boldsymbol{M} = \begin{bmatrix} \mathbf{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\pi) \\ \mathbf{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\boldsymbol{\Phi}) \end{bmatrix} = \begin{bmatrix} \mathbf{0}_{s\times n} & \mathbf{I}_s \\ \multicolumn{2}{c}{\mathbf{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\boldsymbol{\Phi})} \end{bmatrix}.$$

Lemma 3.2. *For $(\boldsymbol{x}, \boldsymbol{\vartheta})$ in V, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ is in Z if and only if the matrix $\boldsymbol{M}$ has rank less than $s + m$ at $(\boldsymbol{x}, \boldsymbol{\vartheta})$.*

Proof. Take $(\boldsymbol{x}, \boldsymbol{\vartheta})$ on V, and let $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})$ be the Jacobian matrix $\mathbf{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\boldsymbol{\Phi})$ taken at $(\boldsymbol{x}, \boldsymbol{\vartheta})$. Then, the rank of $\boldsymbol{M}(\boldsymbol{x}, \boldsymbol{\vartheta})$ can be written as $\operatorname{rank}(\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})) + \operatorname{rank}([\mathbf{0}_{s\times n}\ \mathbf{I}_s] \mid \ker \boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta}))$, where the latter is the rank of the restriction of $[\mathbf{0}_{s\times n}\ \mathbf{I}_s]$ to the nullspace of $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})$.

Since V is smooth, $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})$ has full rank $\operatorname{codim}(V) = m$. On the other hand, the nullspace of $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})$ is the tangent space $T_{\boldsymbol{x},\boldsymbol{\vartheta}}V$, and $\operatorname{rank}([\mathbf{0}_{s\times n}\ \mathbf{I}_s] \mid \ker \boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta}))$ is the dimension of $\pi(T_{\boldsymbol{x},\boldsymbol{\vartheta}}V)$. In other words, the rank of $\boldsymbol{M}(\boldsymbol{x}, \boldsymbol{\vartheta})$ is equal to $m + \dim(\pi(T_{\boldsymbol{x},\boldsymbol{\vartheta}}V))$; this implies the claim in the lemma. □

Therefore, we can characterize the set Z of critical points of $\pi_{|V}$ as those points satisfying $\boldsymbol{\Phi}(\boldsymbol{x}, \boldsymbol{\vartheta}) = \boldsymbol{0}$ and where all minors of $\boldsymbol{M}$ of order $s + m$ vanish. We can actually describe this set using a smaller matrix, by discarding certain minors that are identically zero. Let indeed $\boldsymbol{J}$ denote the $m \times n$ submatrix of the Jacobian of $\boldsymbol{\Phi}$ consisting of the first n columns. This is the Jacobian matrix of $\boldsymbol{\Phi}$ with respect to $\boldsymbol{X}$.

Lemma 3.3. *For $(\boldsymbol{x}, \boldsymbol{\vartheta})$ in V, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ is in Z if and only if $\boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta})$ has rank less than m.*

Proof. Notice

$$M(\boldsymbol{x}, \boldsymbol{\vartheta}) = \begin{bmatrix} \mathbf{0}_{s\times n} & \mathbf{I}_s \\ \boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta}) & \boldsymbol{J}'(\boldsymbol{x}, \boldsymbol{\vartheta}) \end{bmatrix},$$

where $\boldsymbol{J}'$ consists of the remaining columns of the Jacobian matrix of $\boldsymbol{\Phi}$. Then, the rank of the former matrix is equal to the rank of

$$M(\boldsymbol{x}, \boldsymbol{\vartheta}) = \begin{bmatrix} \mathbf{0}_{s\times n} & \mathbf{I}_s \\ \boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta}) & \mathbf{0}_{m\times s} \end{bmatrix},$$

and the conclusion follows. □

In particular, take $\boldsymbol{\vartheta}$ in $\mathbb{C}^s - \overline{\pi(Z)}$. Then for all $\boldsymbol{x}$ in $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}^{-1}(\mathbf{0})$, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ is in V, so it is not in Z. The previous lemma then implies that the Jacobian matrix $\boldsymbol{J}$ of $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$ has full rank m at $(\boldsymbol{x}, \boldsymbol{\vartheta})$. In other words, $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$, as claimed.

Our next step is to bound the degree of Z. In that, we use the definition of degree given in [19]: the degree of an irreducible algebraic set is the number of intersection points it has with a generic hyperplane of complementary dimension, and the degree of an arbitrary algebraic set is the sum of the degrees of its irreducible components. To obtain an estimate on the degree of Z, rather than considering minors of $\boldsymbol{J}$, we will rewrite the condition that $\boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta})$ has rank less than m as the existence of a non-trivial left kernel element.

For this, we let $\boldsymbol{L} = [L_1, \ldots, L_m]$ be new variables, thought of as Lagrange multipliers, and consider the "Lagrange polynomials" $\mathscr{L}_1, \ldots, \mathscr{L}_n$, with

$$[\mathscr{L}_1 \cdots \mathscr{L}_n] := \boldsymbol{L} \cdot \boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta}).$$

Denote by $\mathfrak{Z} \subset \mathbb{C}^{n+s+m}$ the algebraic set defined by the vanishing of $\mathscr{L}_1, \ldots, \mathscr{L}_n$, and $\boldsymbol{\Phi}$, and by $\mathfrak{Z}'$ the algebraic set

$$\mathfrak{Z}' := \overline{\mathfrak{Z} - \{(\boldsymbol{x}, \boldsymbol{\vartheta}, 0, \ldots, 0) \in \mathbb{C}^{n+s+m} \mid (\boldsymbol{x}, \boldsymbol{\vartheta}, 0 \ldots, 0) \in \mathfrak{Z}\}},$$

where the bar denotes Zariski closure (we have to remove such points, since $L_1 = \cdots = L_m = 0$ is always a trivial solution to the Lagrange equations). Finally, consider the projection

$$\begin{aligned} \mu :\ \mathbb{C}^{n+s+m} &\to \mathbb{C}^{n+s} \\ (\boldsymbol{x}, \boldsymbol{\vartheta}, \boldsymbol{\ell}) &\mapsto (\boldsymbol{x}, \boldsymbol{\vartheta}). \end{aligned}$$

Lemma 3.4. *The algebraic set Z is equal to the projection $\mu(\mathfrak{Z}')$.*

Proof. Take $(\boldsymbol{x}, \boldsymbol{\vartheta})$ in Z. Then, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ cancels all polynomials $\boldsymbol{\Phi}$, and there exists $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_m)$, not identically zero, such that $(\boldsymbol{x}, \boldsymbol{\vartheta}, \boldsymbol{\ell})$ cancels the Lagrange polynomials. This implies that $(\boldsymbol{x}, \boldsymbol{\vartheta}, \boldsymbol{\ell})$ is in $\mathfrak{Z} - \{(\boldsymbol{x}', \boldsymbol{\vartheta}', 0, \ldots, 0) \in \mathbb{C}^{n+s+m} \mid (\boldsymbol{x}', \boldsymbol{\vartheta}', 0 \ldots, 0) \in \mathfrak{Z}\}$, and thus in $\mathfrak{Z}'$. This proves the inclusion $Z \subset \mu(\mathfrak{Z}')$.

Conversely, take an irreducible component Y of $\mathfrak{Z}'$. We prove that $\mu(Y)$ is contained in Z. By construction, there exists an open dense subset $Y^o \subset Y$ such that for any $(\boldsymbol{x}, \boldsymbol{\vartheta}, \boldsymbol{\ell})$ in Y^o, $\boldsymbol{\ell}$ is not identically zero. As a result, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ is in Z, that is, $\mu(Y^o)$ is in Z. This implies that its Zariski closure $\overline{\mu(Y^o)}$ is in Z. Since $\mu(Y)$ is contained in $\overline{\mu(Y^o)}$, we deduce $\mu(Y) \subset Z$. Taking the union over all Y, we get $\mu(\mathfrak{Z}') \subset Z$, as claimed. □

Corollary 3.5. *The degree of Z is at most d^{m+n}.*

Proof. The algebraic set $\mathfrak{Z}$ is defined by $m + n$ equations, all of them having degree at most d. It follows from Bézout's Theorem [19] that $\deg(\mathfrak{Z}) \le d^{m+n}$, and the same upper bound holds for $\deg(\mathfrak{Z}')$, since it consists of certain irreducible components of $\mathfrak{Z}$. Applying the projection μ yields the result, since degree cannot increase through projection. □

In particular, we obtain the same degree bound for $\overline{\pi(Z)}$. It then suffices to take for Γ any non-zero polynomial of degree at most d^{m+n} that vanishes on $\overline{\pi(Z)}$; this proves Proposition 3.1.

3.2 Application: property $\mathbf{H}_i(1)$

Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ have total degree d, with $V(f) \subset \mathbb{C}^n$ smooth. In what follows, we fix i in $1, \ldots, n$, and we prove the following: *there exists a non-zero polynomial $\Delta_{i,1} \in \mathbb{C}[\mathfrak{A}]$ of degree at most $2nd^{2n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel $\Delta_{i,1}$, then $\boldsymbol{A}$ is invertible and $f^{\boldsymbol{A}}$ satisfies $\boldsymbol{H}_i(1)$.*

The following construction is already in [4]; our contribution is the degree estimate. We let $\Phi : \mathbb{C}^n \times \mathbb{C}^{n\times n} \to \mathbb{C}^{n-i+1}$ be the mapping defined by the polynomials

$$\big(f,\ \mathbf{grad}(f) \cdot \mathfrak{A}_{i+1},\ \ldots,\ \mathbf{grad}(f) \cdot \mathfrak{A}_n\big),$$

where $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ denote the columns of $\mathfrak{A}$ and $\cdot$ is the dot-product.

Lemma 3.6. *$\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}$.*

Proof. Let $(\boldsymbol{x}, \boldsymbol{A}) \in \mathbb{C}^n \times \mathbb{C}^{n\times n}$ be a zero of $\boldsymbol{\Phi}$. We have to show that the Jacobian matrix of the equations defining $\boldsymbol{\Phi}$, taken with respect to $\boldsymbol{X}$ and $\mathfrak{A}$, has full rank $n - i + 1$ at $(\boldsymbol{x}, \boldsymbol{A})$. If we set

$$F_j = \frac{\partial f}{\partial X_1} A_{i+j,1} + \ldots + \frac{\partial f}{\partial X_n} A_{i+j,n},\ 1 \le j \le n - i,$$

this Jacobian matrix is equal to

$$\begin{bmatrix} \frac{\partial f}{\partial X_1} \cdots \frac{\partial f}{\partial X_n} & \cdots & 0 \ldots 0 & \cdots & 0 \ldots 0 \\ \frac{\partial F_1}{\partial X_1} \cdots \frac{\partial F_1}{\partial X_n} & \cdots & \frac{\partial f}{\partial X_1} \cdots \frac{\partial f}{\partial X_n} & \cdots & 0 \ldots 0 \\ \ddots & \ddots & \ddots & \ddots & \ddots \\ \frac{\partial F_{n-i}}{\partial X_1} \cdots \frac{\partial F_{n-i}}{\partial X_n} & \cdots & 0 \ldots 0 & \cdots & \frac{\partial f}{\partial X_1} \cdots \frac{\partial f}{\partial X_n} \end{bmatrix},$$

where the first columns are indexed by $X_1, \ldots, X_n$ and the further ones by $\mathfrak{A}_{1,i+1}, \ldots, \mathfrak{A}_{n,i+1}, \ldots, \mathfrak{A}_{1,n}, \ldots, \mathfrak{A}_{n,n}$. Since $f(\boldsymbol{x}) = 0$, our assumption on f implies that at least one of its partial derivatives is non-zero at $\boldsymbol{x}$, and the conclusion follows. □

Since all equations defining $\boldsymbol{\Phi}$ have degree at most d, it follows by Proposition 3.1 that there exists a non-zero polynomial $\Gamma_i \in \mathbb{C}[\mathfrak{A}]$ of degree at most $d^{2n-i+1} \le d^{2n}$, with the property that, if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel Γ_i, then the Jacobian matrix of

$$\boldsymbol{\Phi}_{\boldsymbol{A}} = \big(f,\ \mathbf{grad}(f) \cdot \boldsymbol{A}_{i+1},\ \ldots,\ \mathbf{grad}(f) \cdot \boldsymbol{A}_n\big),$$

taken with respect to $\boldsymbol{X}$, has full rank $n-i+1$ at all $\boldsymbol{x}$ that cancels equations. We then define $\Delta_{i,1} := \Gamma_i \det(\mathfrak{A})$; this is a non-zero polynomial of degree at most $d^{2n}+n \le 2nd^{2n}$.

Let us verify that $\Delta_{i,1}$ satisfies the claim in the preamble. Take $\boldsymbol{A}$ in $\mathbb{C}^{n\times n}$, such that $\Delta_{i,1}(\boldsymbol{A})$ is non-zero. Clearly, $\boldsymbol{A}$ is invertible; it remains to check that $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i(1)$. Thus, we take $\boldsymbol{x}$ that cancels $(f^{\boldsymbol{A}}, \partial f^{\boldsymbol{A}}/\partial X_{i+1}, \ldots, \partial f^{\boldsymbol{A}}/\partial X_n)$, and we prove that the Jacobian matrix of these equations, taken with respect to $\boldsymbol{X}$, has full rank $n-i+1$ at $\boldsymbol{x}$. Using the chain rule, the equations above can be rewritten as $\boldsymbol{\Phi}_{\boldsymbol{A}}(\boldsymbol{A}\boldsymbol{x})$, so their Jacobian matrix at $\boldsymbol{x}$ has the same rank as that of $\boldsymbol{\Phi}_{\boldsymbol{A}}$ at $\boldsymbol{A}\boldsymbol{x}$, that is, $n-i+1$. Our claim is proved.

In Section 4, we will need the following by-product of this result: if we consider $f^{\mathfrak{A}} \in \mathbb{C}(\mathfrak{A}_{j,k})[X_1, \ldots, X_n]$ as defined in Section 2, this polynomial satisfies the rank property $\mathbf{H}_i(1)$.

3.3 Application: property $\mathbf{H}'_i$

Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ and i be as before. We now assume that f satisfies $\mathbf{H}_i(1)$, and we prove the following: *there exists a non-zero polynomial $\Xi_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most d^{2n} such that if $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ does not cancel Ξ_i, then for any root $\boldsymbol{x}$ of*

$$(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n),$$

the Jacobian matrix of these equations at $\boldsymbol{x}$ has full rank n.

Let $\boldsymbol{\Psi} : \mathbb{C}^n \times \mathbb{C}^{i-1} \to \mathbb{C}^n$ be the mapping defined by the polynomials

$$(X_1 - S_1, \ldots, X_{i-1} - S_{i-1}, f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n)\,.$$

Lemma 3.7. *$\boldsymbol{0}$ is a regular value of $\boldsymbol{\Psi}$.*

Proof. At all zeros $(\boldsymbol{x}, \boldsymbol{\sigma})$ of $\boldsymbol{\Psi}$, the Jacobian matrix of $\boldsymbol{\Psi}$ has full rank n. Indeed, indexing columns by $X_1, \ldots, X_n, S_1, \ldots, S_{i-1}$, this matrix is equal to

$$\begin{bmatrix} \mathbf{I}_{i-1} & \boldsymbol{0}_{(i-1)\times(n-i+1)} & -\mathbf{I}_{i-1} \\ \mathbf{jac}_{\boldsymbol{x}}\left(f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}\right) & & \boldsymbol{0}_{(n-i+1)\times(i-1)} \end{bmatrix}.$$

Since the Jacobian of $f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n$ at $\boldsymbol{x}$ is non-zero (by $\mathbf{H}_i$), the entire matrix must have full rank n. Thus, $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Psi}$. □

Since all polynomials defining $\boldsymbol{\Psi}$ have degree at most d, it follows by Proposition 3.1 that there exists a non-zero polynomial Ξ_i in $\mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most d^{2n}, with the following property: if $\Xi_i(\boldsymbol{\sigma}) \neq 0$ then at any root $\boldsymbol{x}$ of

$$(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f, \partial f/\partial X_{i+1}, \ldots, \partial f/\partial X_n),$$

the Jacobian matrix of these equations has full rank n. Theorem 2.2 is proved.

4 Property $\mathrm{H}_i(2)$: Noether position

Throughout this section, f and $i \in \{1, \ldots, n\}$ are fixed. We prove that there exists a non-zero polynomial Δ_i in n^2 variables and of degree at most $5n^2(2d)^{2n}$ such that if $\boldsymbol{A}$ does not cancel Δ_i, then $\boldsymbol{A}$ is invertible and satisfies both conditions in $\mathbf{H}_i$.

Consider again the matrix of indeterminates $\mathfrak{A} = (\mathfrak{A}_{j,k})_{1\le j,k\le n}$ and the field $\mathbb{C}(\mathfrak{A})$, and define $f^{\mathfrak{A}} \in \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]$. Since i is fixed, to simplify notation, let $\mathfrak{I}^{\mathfrak{A}}$ denote the following polynomials in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]$:

$$\mathfrak{I}(i, f^{\mathfrak{A}}) = (f^{\mathfrak{A}}, \partial f^{\mathfrak{A}}/\partial X_{i+1}, \ldots, \partial f^{\mathfrak{A}}/\partial X_n),$$

and let $W^{\mathfrak{A}}$ denote their zero-set, that is, $W(\pi_i, V(f^{\mathfrak{A}}))$. In Section 3.2, we saw that $f^{\mathfrak{A}}$ satisfies $\mathbf{H}_i(1)$, so that $\mathfrak{I}^{\mathfrak{A}}$ defines a radical ideal, and $W^{\mathfrak{A}}$ is equidimensional of dimension $i-1$. We now point out that $f^{\mathfrak{A}}$ also satisfies $\mathbf{H}_i(2)$.

Lemma 4.1. *The extension*

$$\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}] \to \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]/\mathfrak{I}^{\mathfrak{A}}$$

is integral.

Proof. Let $(\mathfrak{P}_\ell)_{1\le\ell\le L}$ be the prime components of the radical ideal $\mathfrak{I}^{\mathfrak{A}}$. By [28, Proposition 1], for all ℓ,

$$\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}] \to \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]/\mathfrak{P}_\ell$$

is integral. Therefore polynomials $q_{\ell,j} \in \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}, X_j]$ exist, all monic in X_j, with $q_{\ell,j}(X_j) \in \mathfrak{P}_\ell$ for each j in $\{i, \ldots, n\}$. Thence, $Q_j := \prod_{1\le\ell\le L} q_{\ell,j}$ is monic in X_j and satisfies $Q_j \in \mathfrak{I}^{\mathfrak{A}}$, for each $j \in \{i, \ldots, n\}$. This proves our claim. □

If P is any polynomial in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]$, we will let $D \in \mathbb{C}[\mathfrak{A}]$ be the minimal common denominator of all its coefficients, and we will write $\overline{P} := DP$, so that $\overline{P}$ is in $\mathbb{C}[\mathfrak{A}, X_1, \ldots, X_n]$.

Lemma 4.2. *For $j = i, \ldots, n$, there exists a polynomial P_j in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}, X_j]$, monic in X_j, with $\overline{P_j}$ in $\mathfrak{I}^{\mathfrak{A}}$, and such that $\deg(\overline{P_j}) \le (2d)^n$.*

Proof. We let $\mathfrak{L}^{\mathfrak{A}}$ denote the extension of $\mathfrak{I}^{\mathfrak{A}}$ given by $\mathfrak{L}^{\mathfrak{A}} := \mathfrak{I}^{\mathfrak{A}} \cdot \mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1})[X_i, \ldots, X_n]$. Then,

$$\mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1}) \to \mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1})[X_i, \ldots, X_n]/\mathfrak{L}^{\mathfrak{A}} \qquad (2)$$

is an algebraic extension. On the other hand, the previous lemma states that

$$\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}] \to \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]/\mathfrak{I}^{\mathfrak{A}} \qquad (3)$$

is integral; from this, Proposition 3.3.1 in [17] implies that it is actually a free module. Any basis of the latter is also a basis of (2); as a consequence, for j in $i, \ldots, n$, the characteristic polynomials of X_j in (2) or (3) are the same. Let P_j be the minimal polynomial of X_j in (2). The previous discussion implies that the characteristic polynomial χ_j of X_j in (2), and thus also P_j, are in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}, X_j]$ and monic in X_j.

By definition, χ_j is in $\mathfrak{I}^{\mathfrak{A}}$ and since there exists an integer k such that χ_j divides ${P_j}^k$ in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}][X_j]$, ${P_j}^k$ is in $\mathfrak{I}^{\mathfrak{A}}$. Since the latter ideal is radical, we conclude that P_j is in $\mathfrak{I}^{\mathfrak{A}}$. This implies that $\overline{P_j}$ is in $\mathfrak{I}^{\mathfrak{A}}$ as well.

Now, consider the polynomials $f^{\mathfrak{A}}, \partial f^{\mathfrak{A}}/\partial X_{i+1}, \ldots, \partial f^{\mathfrak{A}}/\partial X_n$ in $\mathbb{C}[\mathfrak{A}, X_1, \ldots, X_n]$, let $\mathfrak{W}$ be their zero-set, and let $\deg(\mathfrak{W})$ be its degree, in the sense of [19]. Proposition 1 in [27] implies that $\overline{P_j}$ has degree at most $\deg(\mathfrak{W})$. Since all polynomials defining $\mathfrak{W}$, seen in $\mathbb{C}[\mathfrak{A}, X_1, \ldots, X_n]$, have degree at most $2d$, the Bézout inequality of [19] gives $\deg(\overline{P_j}) \le (2d)^{n-i+1} \le (2d)^n$. □

Our next step is to give degree bounds on the coefficients appearing in the membership equality $\overline{P_j} \in \mathfrak{I}^{\mathfrak{A}}$. This is done using Rabinovicz's trick. Let T be a new variable; applying the Nullstellensatz in $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n, T]$, and clearing denominators, we obtain the existence of α_j in $\mathbb{C}[\mathfrak{A}] - \{0\}$ and $C_{j,\ell}, B_j$ in $\mathbb{C}[\mathfrak{A}][X_1, \ldots, X_n][T]$, such that

$$\alpha_j = \sum_{\ell=1}^{n-i+1} C_{j,\ell} G_\ell + B_j(1 - \overline{P_j}T), \quad G_\ell \in \left\{ f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n} \right\}. \tag{4}$$

Let us then define

$$\Delta_i := \Delta_{i,1} \alpha_i \cdots \alpha_n D_i \cdots D_n,$$

where $\Delta_{i,1}$ was defined in Section 3.2 and for all j, α_j is as above and D_j is the leading coefficient of $\overline{P_j}$ with respect to X_j. Thus, Δ_i is a non-zero polynomial in $\mathbb{C}[\mathfrak{A}]$; we will estimate its degree below.

Lemma 4.3. *Suppose that $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel Δ_i. Then $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i$.*

Proof. By assumption, $\Delta_{i,1}(\boldsymbol{A})$ is non-zero, so that $\boldsymbol{A}$ is invertible and $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i(1)$. In particular, the ideal $\mathfrak{I}(i, f^{\boldsymbol{A}})$ is radical, and its zero-set $W(\pi_i, V(f^{\boldsymbol{A}}))$ is either empty or $(i-1)$-equidimensional. If it is empty, we are done.

Otherwise, for $j = i, \ldots, n$, evaluate all indeterminates in $\mathfrak{A}$ at the corresponding entries of $\boldsymbol{A}$ in (4). This gives us an equality in $\mathbb{C}[X_1, \ldots, X_n, T]$ of the form

$$a_j = \sum_{\ell=1}^{n-i+1} c_{j,\ell} g_\ell + b_j(1 - p_j T), \quad g_\ell \in \left\{ f^{\boldsymbol{A}}, \frac{\partial f^{\boldsymbol{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial X_n} \right\},$$

for a_j in $\mathbb{C}$, polynomials $c_{j,\ell}$ and b_j in $\mathbb{C}[X_1, \ldots, X_n, T]$ and p_j in $\mathbb{C}[X_1, \ldots, X_{i-1}, X_j]$. Since neither α_j nor D_j vanish at $\boldsymbol{A}$, a_j is non-zero and the leading coefficient of p_j in X_j is a non-zero constant.

The conclusion is now routine. Replace T by $1/p_j$ in the previous equality; after clearing denominators, this gives a membership equality of the form ${p_j}^k \in \mathfrak{I}(i, f^{\boldsymbol{A}})$, for some integer $k \geq 1$ (we cannot have $k = 0$, since we assumed that $W(\pi_i, V(f^{\boldsymbol{A}}))$ is not empty). Since $\mathfrak{I}(i, f^{\boldsymbol{A}})$ is radical, p_j is in $\mathfrak{I}(i, f^{\boldsymbol{A}})$. Repeating this for all j proves that $\mathbb{C}[X_1, \ldots, X_{i-1}] \to \mathbb{C}[X_1, \ldots, X_n]/\mathfrak{I}(i, f^{\boldsymbol{A}})$ is integral. □

To estimate the degree of Δ_i, what remains is to give an upper bound on the degree of $\alpha_i, \ldots, \alpha_n$. This will come as an application of the effective Nullstellensatz given in [10], for which we first need to determine degree bounds, separately in $\boldsymbol{X}, T$ and $\mathfrak{A}$, of the polynomials in the membership relationship:

$$\deg_{\boldsymbol{X},T} \left\{ f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n} \right\} \leq d;$$

$$\deg_{\mathfrak{A}} \left\{ f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n} \right\} \leq d;$$

$$\deg_{\boldsymbol{X},T}(1 - T\overline{P_j}) \leq (2d)^n + 1;$$

$$\deg_{\mathfrak{A}}(1 - T\overline{P_j}) \leq (2d)^n.$$

For each $j \in \{i, \ldots, n\}$, a direct application of [10, Theorem 0.5], gives $\deg(\alpha_j) \leq (n+1)d^n((2d)^n + 1)$; we will use the slightly less precise bound $\deg(\alpha_j) \leq 2n(2d)^{2n}$.

We saw in Section 3.2 that $\Delta_{i,1}$ has degree at most $2nd^{2n}$, and all D_j's have degree at most $(2d)^n$. This gives the upper bound

$$\deg(\Delta_i) \leq 2nd^{2n} + 2n^2(2d)^{2n} + n(2d)^n \leq 5n^2(2d)^{2n}.$$

This completes the proof of Theorem 2.1.

5 Proof of the main result

The following is our main algorithm; it expands on the sketch given in the introduction, by quantifying the various random choices.

In step 4, we use [31, Algorithm 2] to solve a square system. This subroutine is randomized; in order to guarantee a higher probability of success, we repeat the calculation k times, for a well-chosen parameter k.

This subroutine also requires that the input system be given by a straight-line program. We build it (at Step 3) in the straightforward manner already suggested in the introduction: given f, we can build a straight-line program that evaluates f in $O(d^n)$ operations, by computing all monomials of degree up to d, multiplying them by the corresponding coefficients in f, and adding results. To obtain a straight-line program for $f^{\boldsymbol{A}}$, we add $O(n^2)$ steps corresponding to the application of the change of variables $\boldsymbol{A}$. From this, we can compute the required partial derivatives of $f^{\boldsymbol{A}}$ for the same asymptotic cost [8]. Finally, we add the linear equations $X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}$; this gives Γ_i.

```
Algorithm 1: Main Algorithm
  Input: $f \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most $d$ and height at
         most $b$, and $0 < \epsilon < 1$
  Output: $n$ zero-dimensional parameterizations, the union of
          whose zeros includes at least one point in each
          connected component of $V(f) \cap \mathbb{R}^n$, with
          probability of success at least $1 - \epsilon$.
1 Construct $S := \{1, 2, \ldots, \lceil 3\epsilon^{-1} 5n^3 (2d)^{2n} \rceil\}$ and
  $T := \{1, 2, \ldots, \lceil 3\epsilon^{-1} n d^{2n} \rceil\}$, and randomly choose $\boldsymbol{A} \in S^{n^2}$,
  and $\boldsymbol{\sigma} \in T^{n-1}$;
2 for $i \leftarrow 1$ to $n$ do
3     Build a straight-line program $\Gamma_i$ that computes the
        equations
        $\left\{X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f^{\boldsymbol{A}}, \frac{\partial f^{\boldsymbol{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial X_n}\right\}$;
4     Run [31, Algorithm 2] $k \geq \lg(3n/\epsilon)$ times with input $\Gamma_i$;
5     Let $\mathscr{Q}_i$ be the highest cardinality zero-dimensional
        parameterization returned in step 4 ;
6 return $[\mathscr{Q}_1, \ldots, \mathscr{Q}_n]$.
```

If $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i$, and $f^{\boldsymbol{A}}$ and $(\sigma_1, \ldots, \sigma_{i-1})$ satisfy $\mathbf{H}'_i$ for all i, then Theorem 2 in [28] establishes correctness.

Bit operation cost. The following lists the costs for each step of Algorithm 1:

(1) We defined $S := \{1, 2, \ldots, \lceil 3\epsilon^{-1} 5n^3 (2d)^{2n} \rceil\}$ and therefore the height of any $a_{i,j} \in S$ is at most

$$\log 3/\epsilon + \log(5n^3(2d)^{2n}) \in O^\sim(\log 1/\epsilon + n \log d).$$

Since $|T| < |S|$, the height of any $\sigma_j \in T$ is at most the same.

(3) After computing the partial derivatives, the height grows by at most another factor of $\log d$. Thus, all polynomials in the system considered at Step 3 have height $O\tilde{~}(b + d \log 1/\epsilon + dn)$. All integer coefficients appearing in Γ_i satisfy the same bound.

(4) As a result, after applying [31, Algorithm 2] k times for each index i, with $k = O(\log n + \log 1/\epsilon)$, the total boolean cost of the algorithm is

$$O\tilde{~}(d^{3n+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$

where the polynomials in the output have degree at most d^n, and height at most

$$O\tilde{~}(d^{n+1}(b + \log 1/\epsilon)).$$

This proves the runtime estimate, as well as our bounds on the height of the output.

Probability of success. Let $\Delta_i \in \mathbb{C}[\mathfrak{A}]$ be the polynomials from Theorem 2.1. Denote by $\Delta := \prod_{i=1}^{n} \Delta_i$, and note that

$$\deg \Delta \le \sum_{i=1}^{n} \deg \Delta_i \le 5n^3(2d)^{2n}. \tag{5}$$

If $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel Δ, then $\boldsymbol{A}$ is invertible and $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i$ for all $i \in \{1, \ldots, n\}$. Now, assuming that $\boldsymbol{A}$ is such a matrix, let $\Xi_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ be the polynomials from Theorem 2.2 applied to $f^{\boldsymbol{A}}$. Denote by $\Xi := \prod_{i=1}^{n} \Xi_i$, and note that

$$\deg \Xi \le \sum_{i=1}^{n} \deg \Xi_i \le nd^{2n}. \tag{6}$$

If $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel Ξ, then $f^{\boldsymbol{A}}$ and $\boldsymbol{\sigma}$ satisfy $\mathbf{H}_i^{'}$ for all $i \in \{1, \ldots, n\}$. As we argued above, the algorithm is guaranteed to succeed, as long as our call to Algorithm 2 in [31] succeeds. That latter reference establishes that by repeating the calculation k times, and keeping the output of highest degree among those k results, we succeed with probability at least $1 - (1/2)^k$. When Algorithm 2 does not succeed, it either returns a proper subset of the solutions, or FAIL. Note that Algorithm 2 is shown to succeed in a single run with probability at least $1 - 11/32$, and we bound the probability of success with $1 - 1/2$ for simplicity. Now, by construction of

$$S := \{1, 2, \ldots, \lceil 3\epsilon^{-1} 5n^3(2d)^{2n} \rceil\}$$

and

$$T := \{1, 2, \ldots, \lceil 3\epsilon^{-1} nd^{2n} \rceil\},$$

where $\boldsymbol{A} \in S^{n^2}$ and $\boldsymbol{\sigma} \in T^{n-1}$ are randomly chosen, we have

$$\mathbb{P}[\Delta(\boldsymbol{A}) = 0] \le \frac{\deg \Delta}{|S|} = \epsilon/3$$

and

$$\mathbb{P}[\Xi(\boldsymbol{\sigma}) = 0] \le \frac{\deg \Xi}{|T|} = \epsilon/3.$$

Let $\mathscr{E}$ be the event that the parameterizations $[\mathscr{Q}_1, \ldots, \mathscr{Q}_n]$ returned in step 6 of Algorithm 1 are correct. Then, the probability of success is equal to

$$\mathbb{P}[\Delta(\boldsymbol{A}) \neq 0] \times \mathbb{P}[\Xi(\boldsymbol{\sigma}) \neq 0 \mid \Delta(\boldsymbol{A}) \neq 0] \times \mathbb{P}[\mathscr{E} \mid \Delta(\boldsymbol{A})\Xi(\boldsymbol{\sigma}) \neq 0].$$

Set $k = \lg(3n/\epsilon)$ so that

$$(1 - 2^{-k})^n = (1 - \epsilon/(3n))^n \ge 1 - \epsilon/3,$$

by Bernoulli's inequality. Therefore,

$$\begin{aligned}
\mathbb{P}[\text{success}] &\ge (1 - \epsilon/3)(1 - \epsilon/3)\mathbb{P}[\mathscr{E} \mid \Delta(\boldsymbol{A})\Xi(\boldsymbol{\sigma}) \neq 0] \\
&\ge (1 - \epsilon/3)(1 - \epsilon/3)(1 - 2^{-k})^n \\
&\ge (1 - \epsilon/3)(1 - \epsilon/3)(1 - \epsilon/3) \\
&\ge 1 - \epsilon.
\end{aligned}$$

This finishes the proof of our main theorem.

References

[1] M. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. 1996. Zeroes, multiplicities and idempotents for zerodimensional systems. In *Algorithms in algebraic geometry and applications. Proceedings of MEGA'94 (Progress in Mathematics)*, Vol. 142. Birkhaüser, 1–15.

[2] B. Bank, M. Giusti, and J. Heintz. 2014. Point searching in real singular complete intersection varieties: Algorithms of intrinsic complexity. *Math. Comp.* 83 (2014), 873–897.

[3] B. Bank, M. Giusti, J. Heintz, L. Lehmann, and L.-M. Pardo. 2012. Algorithms of Intrinsic Complexity for Point Searching in Compact Real Singular Hypersurfaces. *Foundations of Computational Mathematics* 12 (2012), 75–122.

[4] B. Bank, M. Giusti, J. Heintz, and G. Mbakop. 1997. Polar Varieties and Efficient Real Equation Solving: The Hypersurface Case. *Journal of Complexity* 13, 1 (1997), 5–27.

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

[6] B. Bank, M. Giusti, J. Heintz, and L.-M. Pardo. 2005. Generalized polar varieties: geometry and algorithms. *Journal of Complexity* 21, 4 (2005), 377–412.

[7] S. Basu, R. Pollack, and M.-F. Roy. 2003. *Algorithms in Real Algebraic Geometry.* Algorithms and computation in mathematics, Vol. 10. Springer-Verlag.

[8] W. Baur and V. Strassen. 1983. The complexity of partial derivatives. *Theoret. Comput. Sci.* 22, 3 (1983), 317–330.

[9] J. Bochnak, M. Coste, and M.-F. Roy. 1998. *Real algebraic geometry.* Springer-Verlag.

[10] C. D'Andrea, T. Krick, and M. Sombra. 2013. Heights of varieties in muliprojective spaces and arithmetic Nullstellensatz. *Annales scientifiques de l'École Normale Supérieure* 46, 4 (Aug 2013), 549–627.

[11] M. Demazure. 2000. *Bifurcations and catastrophes: geometry of solutions to nonlinear problems.* Springer.

[12] D. Eisenbud. 1995. *Commutative Algebra with a View Toward Algebraic Geometry* (1st. ed.). Graduate Texts in Mathematics, Vol. 150. Springer-Verlag, New York.

[13] P. Gianni and T. Mora. 1989. Algebraic solution of systems of polynomial equations using Groebner bases. In *AAECC (LNCS)*, Vol. 356. Springer, 247–257.

[14] M. Giusti, K. Hägele, J. Heintz, J.-E. Morais, J.-L. Montaña, and L.-M. Pardo. 1997. Lower bounds for diophantine approximation. *J. of Pure and Applied Algebra* 117/118 (1997), 277–317.

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

[16] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. 1995. When polynomial equation systems can be solved fast?. In *AAECC-11 (LNCS)*, Vol. 948. Springer, 205–231.

[17] M. Giusti, J. Heintz, and J. Sabia. 1993. On the efficiency of effective Nullstellensätze. *Computational Complexity* 3 (1993), 56–95.

[18] D. Grigoriev and N. Vorobjov. 1988. Solving Systems of Polynomial Inequalities in Subexponential Time. *J. Symbolic Comput.* 5 (1988), 37–64.

[19] J. Heintz. 1983. Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science* 24, 3 (May 1983), 239–277.

[20] G. Jeronimo and J. Sabia. 2002. Effective equidimensional decomposition of affine varieties. *Journal of Pure and Applied Algebra* 169 (2002), 229–248.

[21] T. Krick, L.-M. Pardo, and M. Sombra. 2001. Sharp estimates for the arithmetic Nullstellensatz. *Duke Mathematical Journal* 109, 3 (2001), 521–598.

[22] L. Kronecker. 1882. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik* 92 (1882), 1–122.

[23] F. Macaulay. 1916. *The Algebraic Theory of Modular Systems.* Cambridge University Press.

[24] D. Mumford. 1976. *Algebraic Geometry 1 : complex algebraic varieties.* Springer.

[25] R. Piene. 1978. Polar classes of singular varieties. *Annales Scientifiques de l'École Normale Supérieure* 11, 2 (1978), 247–276.

[26] F. Rouillier. 1999. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing* 9, 5 (1999), 433–461.

[27] É. Schost. 2003. Computing Parametric Geometric Resolutions. *Applicable Algebra in Engineering, Communication and Computing* 5 (2003), 349–393.

[28] É. Schost and M. Safey El Din. 2003. Polar Varieties and Computation of one Point in each Connected Component of a Smooth Real Algebraic Set. In *ISSAC'03*. ACM, 224–231.

[29] É. Schost and M. Safey El Din. 2011. A baby steps/giant steps probabilistic algorithm for computing roadmaps in smooth bounded real hypersurface. *Discrete and Computational Geometry* 5 (2011), 181–220.

[30] É. Schost and M. Safey El Din. 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM* 63, 6 (Feb. 2017), 1–48.

[31] É. Schost and M. Safey El Din. 2018. Bit complexity for multi-homogeneous system solving. Application to polynomial minimization. *Journal of Symbolic Computation* 87 (May 2018), 176–206.

[32] É. Schost, B. Saugata, M-F Roy, and M. Safey El Din. 2014. A baby step-giant step roadmap algorithm for general algebraic sets,. *Foundations of Computational Mathematics* 14 (2014), 1117–1172.

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

[34] B. Teissier. 1988. Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours. In *Sém. Annales Univ. Blaise Pascal*, Vol. 4.