Analysis of Randomized Algorithms in Real Algebraic Geometry

by

Jesse Elliott

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2020

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

I am the sole author of Chapters 1,2 and 9. Chapters 3,4,5, and 6 are based on the following articles: one co-authored with Éric Schost [15], another co-authored with Mark Giesbrecht and Éric Schost [24], and another co-authored with Mark Giesbrecht and Éric Schost that we are submitting for publication in December, 2020.

Abstract

Consider the problem of computing at least one point in each connected component of a smooth real algebraic set. This is a basic and important operation in real and semi-algebraic geometry: it gives an upper bound on the number of connected components of the algebraic set, it can be used to decide if the algebraic set has real solutions, and it is also used as a subroutine in many higher level algorithms.

We consider an algorithm for this problem 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 proven to generically ensure certain desirable geometric properties. The cost of the algorithm was given in an algebraic complexity model, and the analysis of the bit complexity and the error probability were left for future work.

We also consider another algorithm that solves a special case of the problem. Namely, when the algebraic set is a compact hypersurface.

We determine the bit complexity and error probability of these algorithms. Our main contribution is a quantitative analysis of several genericity statements, such as Thom's weak transversality theorem and Noether normalization properties for polar varieties. Furthermore, in doing this work, we have developed techniques that can be used in the analysis of further randomized algorithms in real algebraic geometry, which rely on related genericity properties.

Acknowledgements

I would like to thank my supervisors, Éric Schost and Mark Giesbrecht, for their patience, guidance, and influence. I thank my third and fourth readers, Rafael Oliveira and George Labahn, for their comments and feedback. I thank everyone from the Symbolic Computation Group for their support and encouragement. I also thank Michael Monagan for his guidance during my undergraduate years, which prepared me for graduate studies in computer algebra. And finally, I thank David R. Cheriton and Microsoft for their scholarship support.

Dedication

I dedicate this thesis to my parents.

Table of Contents

Chapter 1

Introduction

1.1 Randomization and generic coordinate systems

In this thesis, we focus on randomized algorithms in real algebraic geometry, where the input is a sequence of polynomials $F = (f_1, \ldots, f_p)$ in $\mathbb{C}[X_1, \ldots, X_n]$ defining a complex algebraic set $V = V(F) \subset \mathbb{C}^n$. We focus on algorithms which require the input to satisfy certain geometric properties, and which ensure these properties by applying a randomly chosen change of coordinates $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ to the input: given f in $\mathbb{C}[X_1, \ldots, X_n]$, $f^{\boldsymbol{A}}$ denotes the polynomial $f(\boldsymbol{A}X)$, and $V^{\boldsymbol{A}} = V(F^{\boldsymbol{A}})$ denotes the variety

$$V\left(f_1^{\boldsymbol{A}}, \ldots, f_p^{\boldsymbol{A}}\right).$$

The success of these algorithms depend on the change of coordinates being *lucky*, in the sense of there existing a non-empty Zariski open subset $\mathscr{O} \subset \mathbb{C}^{n \times n}$ with the property that, when the change of coordinates $\boldsymbol{A}$ is in $\mathscr{O}$, the desirable geometric properties are guaranteed for $V^{\boldsymbol{A}}$. We have developed techniques for analyzing the error probability of such algorithms, which allow us to quantify our random choices for the change of coordinates $\boldsymbol{A}$. These techniques work as follows. We bound the degree of the hypersurface defining the complement of the open set $\mathscr{O}$:

$$V(\Gamma) = \mathbb{C}^{n \times n} - \mathscr{O},\ \Gamma \in \mathbb{C}[\mathfrak{A}],$$

where $\mathfrak{A} = (\mathfrak{A}_{j,k})_{1 \le j,k \le n}$ are n^2 indeterminants. We quantify our choice of $\boldsymbol{A}$ by choosing a subset of rational numbers $S \subset \mathbb{Q}$ and constructing a matrix $\boldsymbol{A} = (a_{j,k})_{1 \le j,k \le n}$ by taking $a_{j,k} \in S$; hence, by the DeMillo-Lipton-Schwartz–Zippel lemma,

$$\mathbb{P}[\Gamma(\boldsymbol{A}) = \boldsymbol{0}] \le \frac{\deg \Gamma}{|S|}.$$

1.2 Main problem: computing one point in each connected component of a real algebraic set

1.2.1 Three cases we consider

We consider the problem of computing at least one point in each connected component of a real algebraic set S. This is a basic but important operation in real and semi-algebraic geometry. It is used in many higher level algorithms. It is also useful on its own, since it allows one to decide if S is empty or not, and it allows one to determine an upper bound on the number of connected components of S.

We consider three separate cases:

1. S is given as $S = V \cap \mathbb{R}^n$, where $V = V(f) \subset \mathbb{C}^n$ is a smooth and compact, complex hypersurface defined by a squarefree polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$.
2. S is given as $S = V \cap \mathbb{R}^n$, where $V = V(f) \subset \mathbb{C}^n$ is a smooth, complex hypersurface defined by a squarefree polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$.
3. S is given as $S = V \cap \mathbb{R}^n$, where $V = V(F) \subset \mathbb{C}^n$ is a smooth, complex algebraic set defined by a sequence of polynomials $F = (f_1, \ldots, f_p)$ in $\mathbb{Z}[X_1, \ldots, X_n]$ defining a radical ideal.

1.2.2 Overview of the algorithms for the three cases

Here we give a breif overview of the algorithms for each of the three cases. In Section 3.3, we discuss the algorithms in greater detail.

Case 1. It is sufficient to compute the critical points of the projection on a line, which has dimension zero in generic enough coordinates. Indeed, assuming that $V(f) \cap \mathbb{R}^n$ is compact, any projection on a line has a critical point on each connected component of $V(f) \cap \mathbb{R}^n$ [4, 5].

Case 2. After dropping the compactness assumption, it is no longer guaranteed for the critical points of the projection on a line to contain one point in each connected component of $V(f) \cap \mathbb{R}^n$. Now, in this non-compact senario, we use the 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. In this paper, it is shown that by computing suitable zero-dimensional sections of higher dimensional critical loci called *polar varieties* (first introduced in the 1930's in order to define characteristic classes [30, 40], and which we will discuss in great detail in Chapter 3), one obtains one point on each connected component.

Case 3. Here we develop an extension of the algorithm used for case 2. The extension involves a different approach for modeling polar varieties in terms of Lagrangian systems, with new Lagrange variables. Solution sets are first computed with these additional Largange variables. Then, one point on each connected component is obtained by computing the projection on the $\boldsymbol{X}$-space.

1.2.3 Background

For this section we only consider case 3 because it is the most general. Recall that we then have S given as $S = V \cap \mathbb{R}^n$, where $V = V(F) \subset \mathbb{C}^n$ is a smooth, complex algebraic set defined by a sequence of polynomials $F = (f_1, \ldots, f_p)$ in $\mathbb{Z}[X_1, \ldots, X_n]$ defining a radical ideal. And suppose that the polynomials $F = (f_1, \ldots, f_p)$ each have total degree at most d, and coefficients of bit-size h.

The algorithm given in [8, Section 13.1] will compute one point in each connected component of $V(F) \cap \mathbb{R}^n$ using $p^{n+1}d^{O(n)}$ operations in $\mathbb{Q}$ (that is, without making additional assumption on F). Furthermore, the output of the algorithm is represented by polynomials of degree $d^{O(n)}$ and with coefficients of bit-size $hd^{O(n)}$. The main idea used in this algorithm originates with [21], where 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 is large, because the algorithm relies on infinitesimal deformations[1] that affect the runtime non-trivially; this makes the algorithm impractical.

In each of the 3 cases, we assume that the V is a *smooth* complex algebraic set. And we place ourselves in the continuation of the line of work initiated by [4], where cases with V smooth and $V \cap \mathbb{R}^n$ compact are dealt with. Here it is also pointed out how polar varieties

[1] Infinitesimal deformations are used as an alternative method for perturbing the input and establishing genericity properties, for randomized algorithms in real algebraic geometry.

(see Chapter 3) can play a role in effective real geometry. This paper was extended in several directions. Firstly, to V being a smooth complete intersection and with $V \cap \mathbb{R}^n$ compact [5]. Then, without the compactness assumption [34, 6]. Finaly, the smoothness assumption was then partly dropped in [2, 3].

For cases 2 and 3, as stated above, we use the algorithm from [34]. If the setting is changed so that V has finitely many singularities, then this algorithm will still work up to some minor modifications. However, if V has infinitely many singularities then the algorithm will most likely not work any longer, although we don't know for sure.

1.3 Main results

To state our main results, we need to define the *height* of a rational number, and of a polynomial with rational coefficients. We provide this now, as well as the data structures we rely on.

1.3.1 Bit size and data structures

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. Note that when f has integer coefficients, this is simply the maximum of the logarithms of the absolute values of these coefficients.

The output of the algorithms is a finite set in $\overline{\mathbb{Q}}^n$. To represent it, we rely on a widely used data structure based on univariate polynomials [27, 28, 16, 19, 1, 17, 18, 31]. Consider a zero-dimensional algebraic set $S \subset \mathbb{C}^n$ defined over $\mathbb{Q}$. A *zero-dimensional parametrization* $\mathscr{Q} = ((q, v_1, \ldots, v_n), \lambda)$ of S consists in polynomials $(q, v_1, \ldots, v_n)$, such that $q \in \mathbb{Q}[T]$ is monic and squarefree, all v_i's 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 parametrization of the coordinates by rational functions having q' as a denominator goes back to [27, 28]: as pointed out in [1], it allows one to control precisely the size of the coefficients of $v_1, \ldots, v_n$.

1.3.2 The compact hypersurface case

Theorem 1.3.1. *Suppose that $f \in \mathbb{Z}[X_1, \ldots, X_n]$ is squarefree, satisfies $\deg(f) \leq d$ and $\mathrm{ht}(f) \leq b$, and that $V(f) \subset \mathbb{C}^n$ is smooth and compact. Also suppose that $0 < \epsilon < 1$.*

There exists a randomized algorithm that takes f and ϵ as input and produces a zero-dimensional parameterization that 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 [19, 17, 18, 4, 34], it would be possible to refine the runtime estimate by assuming that f is given by a *straight-line program*, which 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.

1.3.3 The hypersurface case, without compactness

As it turns out, even after dropping the compactness assumption, by using the algorithm by Safey El Din and Schost in [34], we can achieve the same soft oh complexity as we did for case 1.

Theorem 1.3.2. *Suppose that $f \in \mathbb{Z}[X_1 \ldots, X_n]$ is squarefree, satisfies $\deg(f) \leq d$ and $\mathrm{ht}(f) \leq b$, 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 again assume that f is given as a dense polynomial. And, as was true for case 1, we could again refine the runtime estimate by assuming that f is given by a straight-line program.

1.3.4 The general case

Now we generalize from the hypersurface case, where $V = V(f)$ is defined by the vanishing of a single polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$, to varieties defined by finite sequences of polynomials:

$$V = V(F) = V(f_1, \ldots, f_p) \subset \mathbb{C}^n,$$

where $F = (f_1, \ldots, f_p) \in \mathbb{C}[X_1, \ldots, X_n]^p$ is a sequence of polynomials defining a radical ideal.

Remark 1.3.3. *Even though case 2 is covered by case 3, the techniques are different enough that we decided to document both separately in this thesis.*

Theorem 1.3.4. *Let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1 \ldots, X_n]^p$ be a sequence of polynomials with $\deg(f_i) \leq d$ and $\mathrm{ht}(f_i) \leq b$. Suppose that the ideal $\langle f_1, \ldots, f_p \rangle$ is radical and that $V = V(F) \subset \mathbb{C}^n$ is smooth with $\dim V = n - p$. 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

$$O^{\sim}(d^{3n+2p+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$

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

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

Here we assume that F is given as a sequence of dense polynomials. Again, following references such as [19, 17, 18, 4, 34], it would be possible to refine the runtime estimate by assuming that F is given by a straight-line program. Indeed, given $F = (f_1, \ldots, f_p)$ in $\mathbb{C}[X_1, \ldots, X_n]$, we can build a straight-line program that evaluates each f_i in $O(d^n)$ operations, by computing all monomials of degree up to d, multiplying them by the corresponding coefficients in f_i, and adding results. The number of operations here is thus

$$O(nd^n) = O^{\sim}(d^n).$$

1.3.5 Summary of contributions

As we dicussed in Section 1.1, the algorithms rely on certain geometric properties that hold generically, and which we ensure by applying a carefully chosen change of coordinates $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ to our input variety $V \subset \mathbb{C}^n$. The algorithms also rely on some additional, *lucky*, parameter choices, which we discuss in full detail in Section 3.2. Our main contributions are to analyze precisely what conditions on our parameter choices guarantee success, for each of the 3 cases of the main problem that we consider. This is done by revisiting the key ingredients in the proofs given in [4] and [34], and giving quantitative versions of these results, bounding the degrees of the hypersurfaces we have to avoid. And in doing this work, we have developed techniques that can be used in the analysis of further randomized algorithms in real algebraic geometry, which rely on related types of genericity properties. See the conclusions in Chapter 9 for a specific example.

1.4 Thesis outline

Chapter 2 provides the basic definitions and notation used throughout. Chapter 3 gives the main algorithms along with their genericity properties. Here we give genericity statements, which we prove in subsequent chapters. These statements are the key tools that we use to prove the main results that were given in Section 1.3. We also define polar varieties and discuss their central role in the algorithms. In Chapter 4, we define weak transversality and prove a quantitative version of Thom's weak transversality, specialised to the particular case of transversality to a point. In Chapter 5, we apply this new quantitative transversality result in proving several of our genericity statements. In Chapter 6, we prove some other genericity statements. We prove the remaining genericity statements in Chapter 7; these consist in Noether normalization properties for polar varieties. In Chapter 8, we provide an analysis of the bit complexity and error probability of our algorithms. And we give conclusions in Chapter 9.

Chapter 2

Preliminaries

Let $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ be the fields of rational, real and complex numbers, and $\mathbb{Z}$ the ring of integers. Let $\boldsymbol{X} = (X_1, \ldots, X_n)$ be a sequence of variables, and for $l \in \{1, \ldots, n\}$ let $\boldsymbol{X}_{\leq l}$ be the subsequence of variables $(X_1, \ldots, X_l)$.

2.1 Algebraic sets

Consider a sequence of polynomials $F = (f_1, \ldots, f_p)$ in $\mathbb{C}[X_1, \ldots, X_n]$. An *algebraic set*:

$$\begin{aligned} V = \; & V\big(F\big) = V(f_1, \ldots, f_p) \\ = \; & \{(a_1, \ldots, a_n) \in \mathbb{C}^n \mid f_1(a_1, \ldots, a_n) = \ldots = f_p(a_1, \ldots, a_n) = 0\} \subset \mathbb{C}^n \end{aligned}$$

is the set of common zeros of F. Given an algebraic set $X \subset \mathbb{C}^n$, the set of polynomials in $\mathbb{C}[X_1, \ldots, X_n]$ that vanish at all points of X is called the *ideal of* X, and which we denote by

$$I(X) = \{f \in \mathbb{C}[X_1, \ldots, X_n] \mid (a_1, \ldots, a_n) \in X \Rightarrow f(a_1, \ldots, a_n) = 0\}.$$

2.1.1 Irreducibility

An algebraic set $V \subset \mathbb{C}^n$ is *irreducible* when $V = V_1 \cup V_2$ implies $V = V_1$ or $V = V_2$, for any $V_1, V_2 \subset V$. An algebraic set $V \subset \mathbb{C}^n$ can be uniquely decomposed into a finite union of irreducible algebraic sets:

$$V = V_1 \cup V_2 \cup \ldots V_r,$$

where $V_j, 1 \leq j \leq r$, are called the irreducible components of V.

2.1.2 Dimension

The *dimension* of an algebraic set $V \subset \mathbb{C}^n$, denoted $\dim V$, can be defined in the following ways:

1. The number of generic hyperplanes needed to intersect with V to obtain a finite set.
2. The *Krull dimension* of $\mathbb{C}[X_1, \ldots, X_n]/I(V)$, which is the supremum of the lengths of all chains of prime ideals

The *codimension* of V is $n - \dim V$. An algebraic set is *equidimensional* if each irreducible component has the same dimension. If each component has dimension d then we say the algebraic set is d-equidimensional.

We especially care about zero dimensional algebraic sets; these sets are finite and their degree is equal to their cardinality.

2.1.3 Degree

The *degree* of an irreducible algebraic set is the number of intersection points between itself and $\dim(V)$ generic hyperplanes. And the degree of an arbitrary algebraic set is defined as the sum of the degrees of its irreducible components.

Example 2.1.1. *An algebraic set of dimension zero is a finite set, with degree equal to its cardinality (as mentioned above).*

Example 2.1.2. *An algebraic set of dimension 1 is a curve, with degree equal to the number of intersection points with a generic hyperplane.*

We will often apply Bézout's bound [22, Theorem 1], which tells us the following. Considering a sequence of polynomials $F = (f_1, \ldots, f_p) \in \mathbb{K}[X_1, \ldots, X_n]^p$, with $\mathbb{K}$ a field, if each polynomial in the sequence has degree at most D, then the algebraic set $V(F)$ has degree at most D^p.

2.1.4 Noether position

For $i \in \{1, \ldots, n - p + 1\}$, let π_i denote the projection

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

A d-equidimensional algebraic set $Y \subset \mathbb{C}^n$ is in *Noether position* for the projection π_d when the extension

$$\mathbb{C}[X_1, \ldots, X_d] \to \mathbb{C}[X_1, \ldots, X_n]/I(Y)$$

is integral; here, $I(Y) \subset \mathbb{C}[X_1, \ldots, X_n]$ is the defining ideal of Y. It is then a consequence that, for any $\boldsymbol{x} \in \mathbb{C}^d$, the fiber $Y \cap \pi_d^{-1}(\boldsymbol{x})$ has dimension zero and is thus finite and not empty.

2.1.5 The Zariski topology

Algebraic sets are the closed sets of the *Zariski Topology* on $\mathbb{C}^n$. Let $V \subset \mathbb{C}^n$ be an algebraic set. The Zariski Topology is the set of all sub-varieties of V. Indeed,

1. $V(\mathbb{C}[X_1, \ldots, X_n]) = V(\{0\})$ and $V(\emptyset) = V(\{1\}) = \mathbb{C}^n$;
2. $V(S) \cup V(T) = V(R)$ when $R = \{fg \mid f \in A, g \in B\}$;
3. $\bigcap_{\alpha \in A} V(S_\alpha) = V(\bigcup_{\alpha \in A} S_\alpha)$.

Parts (1) and (3) are easily seen to be true. To prove part (2), first suppose that $x \in V(S) \cup V(T)$, and, without loss of generality, assume that $x \in V(S)$. Then for $f \in S$ and $g \in T$, $f(x) = 0$, which implies that $(fg)(x) = 0$, and thus $x \in V(R)$. Now assume that $x \notin V(S) \cup V(T)$ and choose $f \in S$ and $g \in T$ such that $f(x) \neq 0$ and $g(x) \neq 0$. Then $fg \in R$ but $(fg)(x) \neq 0$, and therefore $x \notin V(R)$.

Example 2.1.3. *Consider the following particular instance of 2 from above:*

$$\begin{aligned}\{(a,b),(c,d)\} &= V(x-a, y-b) \cup V(x-c, y-d) \\ &= V((x-a)(x-c), (x-a)(y-d), (x-c)(y-b), (y-b)(y-d)).\end{aligned}$$

This subsection on the Zariski Topology is inspired from lecture notes written by Stephen New, in the class PMATH 764: Introduction to Algebraic Geometry.

2.2 The Zariski-tangent space and regular / singular points and values

Assume that $V \subset \mathbb{C}^n$ is a d-equidimensional algebraic set. Let $\text{grad}_{\boldsymbol{x}}(f)$ be the evaluation of the gradient vector of $f \in \mathbb{C}[X_1, \ldots, X_n]$ at $\boldsymbol{x} \in \mathbb{C}^n$. The *Zariski-tangent space* to V at

$\boldsymbol{x} \in V$ is the vector space $T_{\boldsymbol{x}}V$ defined by the equations

$$\mathrm{grad}_{\boldsymbol{x}}(g) \cdot \boldsymbol{v} = 0,$$

for all polynomials g that vanish on V (i.e. for all polynomials $g \in I(V)$).

The point $\boldsymbol{x} \in V$ is a *regular point* if $\dim(T_{\boldsymbol{x}}V) = d$. Otherwise $\boldsymbol{x}$ is a *singular point*. We let $\mathrm{reg}(V)$ and $\mathrm{sing}(V)$ respectively denote the regular and singular points of V. The image of a regular point is a *regular value* and the image of a singular point is a *singular value*. When $\mathrm{sing}(V)$ is empty then we say that V is *smooth*.

The following is a direct consequence of [14, Corollary 16.20]

Proposition 2.2.1. *If $V \subset \mathbb{C}^n$ is a d-equidimensional algebraic set with ideal $I(V)$ generated by polynomials*

$$G = (g_1, \ldots, g_p) \in \mathbb{C}[X_1, \ldots, X_n]^p,$$

then at any point $\boldsymbol{x}$ of $\mathrm{reg}(V)$, $\mathrm{jac}_{\boldsymbol{x}}(G)$ has full rank $n - \dim(V)$ and the kernel of $\mathrm{jac}_{\boldsymbol{x}}(G)$ is equal to $T_{\boldsymbol{x}}V$.

2.3 Changes of variables

For a matrix $\boldsymbol{A}$ in $\mathbb{C}^{n\times n}$ and a polynomial g in $\mathbb{C}[X_1, \ldots, X_n]$, we write

$$g^{\boldsymbol{A}} := g(\boldsymbol{AX}) \in \mathbb{C}[X_1, \ldots, X_n],$$

where $\boldsymbol{X}$ is the column vector with entries $X_1, \ldots, X_n$. And for a sequence of polynomials $G = (g_1, \ldots, g_p) \in \mathbb{C}[X_1, \ldots, X_n]^p$, we write

$$G^{\boldsymbol{A}} = \left(g_1^{\boldsymbol{A}}, \ldots, g_p^{\boldsymbol{A}}\right) = (g_1(\boldsymbol{Ax}), \ldots, g_p(\boldsymbol{Ax})) \in \mathbb{C}[X_1, \ldots, X_n]^p.$$

For a variety $Y \subset \mathbb{C}^n$ and a matrix $\boldsymbol{A} \in \mathrm{GL}(n)$, we define $Y^{\boldsymbol{A}}$ as the image of Y by the map $\phi_{\boldsymbol{A}} : \boldsymbol{x} \mapsto \boldsymbol{A}^{-1}\boldsymbol{x}$. Notice that

$$V(G^{\boldsymbol{A}}) = \phi_{\boldsymbol{A}}(V(G)) = V(G)^{\boldsymbol{A}}.$$

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 g as above, we will then define the polynomial $g^{\mathfrak{A}} := g(\mathfrak{A}\boldsymbol{X})$, which we may consider in either $\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]$ or $\mathbb{C}[\mathfrak{A}, X_1, \ldots, X_n]$.

Chapter 3

Algorithms

To describe the algorithms, we need to define *polar varieties*.

3.1 Critical points and polar varieties

Let $V = V(F)$ be an equidimensional algebraic set, with $F = (f_1, \ldots, f_p)$ a sequence of polynomials in $\mathbb{C}[X_1, \ldots, X_n]$. Suppose that the ideal $\langle f_1, \ldots, f_p \rangle$ is radical and that V is smooth with $\dim V = n - p$.

Polar varieties are higher dimensional critical loci that were introduced in the 1930's in order to define characteristic classes [30, 40]. They play a central role in each algorithm we consider (in each of the cases 1, 2, and 3). Recall that, for $i \in \{1, \ldots, n - p + 1\}$, we denote by π_i the projection

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

A *critical point* is a singular point on the projection π_i. In other words, the point $\boldsymbol{x} \in V$ is a critical point if the dimension of $\pi_i(T_{\boldsymbol{x}}V)$ is less than 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.

3.1.1 Determinantal modeling of polar varieties

Let $\mathrm{jac}(F, i)$ denote the truncated Jacobian matrix of $F = (f_1, \ldots, f_p)$ with respect to $\boldsymbol{X} = (X_1, \ldots, X_n)$:

$$\begin{bmatrix} \frac{\partial f_1}{\partial X_{i+1}} & \cdots & \frac{\partial f_1}{\partial X_n} \\ \vdots & & \vdots \\ \frac{\partial f_p}{\partial X_{i+1}} & \cdots & \frac{\partial f_p}{\partial X_n} \end{bmatrix}.$$

And let

$$\mathrm{Minors}(F, p) = (M_{i,1}, \ldots, M_{i,S_i})$$

be the minors of size p of $\mathrm{jac}(F, i)$. Notice that

$$S_i = \binom{p}{p}\binom{n-i}{p} = \binom{n-i}{p}.$$

For each i in $\{1, \ldots, n-p+1\}$ and F as above, we will let $\mathfrak{J}(i, F)$ denote the sequence of polynomials

$$\big(F, \mathrm{Minors}(F, p)\big) = \big(f_1, \ldots, f_p, M_{i,1}, \ldots, M_{i,S_i}\big).$$

Proposition 3.1.1. *Consider $F = (f_1, \ldots, f_p)$ in $\mathbb{C}[X_1, \ldots, X_n]$. If the ideal defined by F is radical and $V = V(F)$ is smooth with $\dim V = d$, then the polar variety*

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

is defined by F and Minors(F, p).

To prove Proposition 3.1.1, we will use the following two lemmas.

Lemma 3.1.2. *Let $\widetilde{A} = \begin{bmatrix} A \\ B \end{bmatrix} \in \mathbb{R}^{m \times n}$ be a matrix. Then,*

$$\mathrm{rank}(\widetilde{A}) = \mathrm{rank}(A) + \mathrm{rank}(B|\ker(A)),$$

where $B|\ker(A)$ is the restriction of the linear map defined by B to the kernel of A.

Proof. By the rank nullity theorem, we have that

$$\begin{aligned} \dim\ker(A) &= \mathrm{rank}(B|\ker(A)) + \dim\ker(B|\ker(A)) \\ &= \mathrm{rank}(B|\ker(A)) + \dim(\ker(B \cap \ker(A)) \\ &= \mathrm{rank}(B|\ker(A)) + \dim(\ker(\widetilde{A})) \end{aligned}$$

Therefore,

$$m - \operatorname{rank}(A) = \operatorname{rank}(B|\ker(A)) + m - \operatorname{rank}(\widetilde{A})$$

so that

$$\operatorname{rank}(\widetilde{A}) = \operatorname{rank}(A) + \operatorname{rank}(B|\ker(A)).$$

□

Lemma 3.1.3. *Consider $F = (f_1, \ldots, f_p)$ in $\mathbb{C}[X_1, \ldots, X_n]$ and $\boldsymbol{x} \in V(f_1, \ldots, f_p)$. Let J denote the Jacobian matrix $\operatorname{jac}_{\boldsymbol{x}}(F)$ and let T denote the kernal of J. Assume the dimension of T is equal to d so that the rank of J is equal to $n - d$. Then, for $i \in \{1, \ldots, n - p + 1\}$, the dimension of $\pi_i(T)$ is less than i if and only if the rank of $\operatorname{jac}(F, i)$ is less than $n - d$.*

Proof. Let $\widetilde{J}$ denote the matrix

$$\left[\begin{array}{c|c} \boldsymbol{0}_{p\times i} & \operatorname{jac}(F,i) \\ \hline \boldsymbol{I}_i & \boldsymbol{0}_{i\times n-i} \end{array}\right].$$

Now we can calculate the rank of $\widetilde{J}$ in two different ways. We have

$$\operatorname{rank}(\widetilde{J}) = i + \operatorname{rank}(\operatorname{jac}(F, i)).$$

And, by Lemma 3.1.2,

$$\begin{aligned} \operatorname{rank}(\widetilde{J}) &= \operatorname{rank}(J) + \dim(\pi_i(\ker(J))) \\ &= \operatorname{rank}(J) + \dim(\pi_i T) \\ &= n - d + \dim \pi_i(T). \end{aligned}$$

Equating both we have

$$i + \operatorname{rank}(\operatorname{jac}(F, i)) = n - d + \dim \pi_i(T),$$

which implies that

$$\operatorname{rank}(\operatorname{jac}(F, i)) + (i - \dim \pi_i(T)) = n - d.$$

Therefore, the rank of $\operatorname{jac}(F, i)$ is less than $n - d$ if and only if the dimension of $\pi_i(T)$ is less than i. □

Now Proposition 3.1.1 follows from Lemma 3.1.3 and therefore the polar variety $W(\pi_i, V)$ is defined by the vanishing of F and Minors(F, p). Furthermore, this means that when $V = V(F) = V(f)$ is a hypersurface, then the polar variety $W(\pi_i, V(f))$ is defined by

$$V\left(f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}\right).$$

Consider the following example.

Example 3.1.4. *([36, Example 3.1]) Let $f = X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbb{C}[X_1, X_2, X_3]$ and consider the hypersurface*

$$V = V(X_1^2 + X_2^2 + X_3^2 - 1) \subset \mathbb{C}^3.$$

The critical points of the projection $\pi_2 : (x_1, x_2, x_3) \mapsto (x_1, x_2)$ on $V(f)$ are defined by

$$X_1^2 + X_2^2 + X_3^2 - 1 = X_3 = 0$$

and thus the second polar variety $W(\pi_2, V(f))$ is $V\left(f, \partial f/\partial X_3\right)$.

Now, the critical points of the projection $\pi_1 : (x_1, x_2, x_3) \mapsto (x_1)$ on $V(f)$ are defined by

$$X_1^2 + X_2^2 + X_3^2 - 1 = X_2 = X_3 = 0.$$

and thus the first polar variety $W(\pi_1, V(f))$ is $V\left(f, \partial f/\partial X_2, \partial f/\partial X_3\right)$.

Note the dimensions of the polar varieties: $i - 1$.

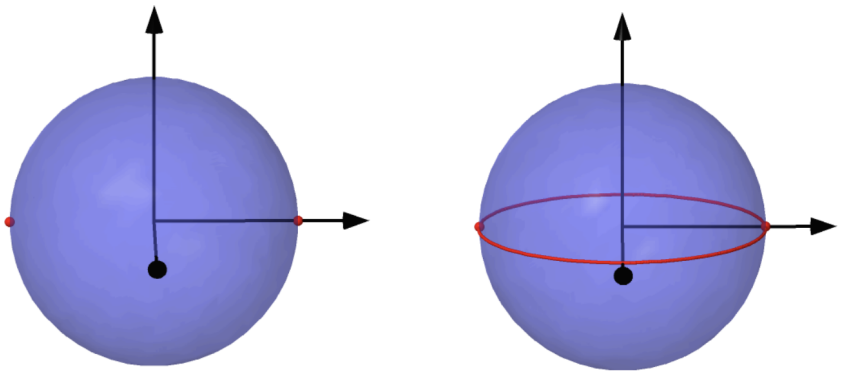

Figure 3.1: The polar varieties $W(0,1,V(f))$ and $W(0,2,V(f))$, where

$$f = X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbb{C}[X_1, X_2, X_3]$$

[36, Example 3.1].

Proposition 3.1.5. *Let $F = (F_1, \ldots, f_p) \in \mathbb{C}[X_1, \ldots, X_n]^p$ be a sequence of polynomials defining a radical ideal and a smooth variety. The degree of $W(\pi_i, V)$ is at most $(nd)^n$.*

Proof. The conclusion follows from [23, Proposition 2.3]. □

3.1.2 Lagrangian modeling of polar varieties

When the algebraic set $V = V(F) = V(f_1, \ldots, f_p)$ is defined by a sequence of polynomials with $n - i \sim 2p$, the length of the sequence of minors $\text{Minors}(F, p)$ is

$$S_i = \binom{n-i}{p} \sim 2^{n-i+1}.$$

The number of equations therefore grows exponentially and the determinantal modeling becomes impractical algorithmically. To avoid this problem, we use an alternative modeling of the polar varieties which involves introducing Lagrange variables.

Definition 1. *Let $\boldsymbol{L} = (L_1, \ldots, L_p)$ be new indeterminants. Then* **Lagrange**$(F, i, (L_1, \ldots, L_p))$ *denotes the entries of the vector*

$$[L_1 \cdots L_p] \cdot \text{jac}(F, i),$$

where the Jacobian is in the variables $(X_{i+1}, \ldots, X_n)$.

Let $\mathscr{W}(\pi_i, V)$ denote the variety

$$V\left(F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p))\right) \subset \mathbb{C}^{n+p}$$

in indeterminants $\boldsymbol{X} = (X_1, \ldots, X_n)$ and $\boldsymbol{L} = (L_1, \ldots, L_p)$. We want to enforce that $\boldsymbol{l} = (0, \ldots, 0)$ is not included in any solutions; we add a linear form $\sum_{i=1}^{p} u_i \cdot L_i - 1$, for a randomly chosen point $\boldsymbol{u} = (u_1, \ldots, u_p) \subset \mathbb{C}^p$. We let $\mathscr{W}_{\boldsymbol{u}}(\pi_i, V)$ denote the variety

$$V\left(F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i \cdot L_i - 1\right) \subset \mathbb{C}^{n+p},$$

again in indeterminants $\boldsymbol{X} = (X_1, \ldots, X_n)$ and $\boldsymbol{L} = (L_1, \ldots, L_p)$. We further let $\mathscr{I}(i, F)$ denote the polynomials

$$(F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p))) \in \mathbb{C}[\boldsymbol{X}, \boldsymbol{L}]^{p+n-i},$$

and for $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbb{C}^p$, we let $\mathscr{I}_{\boldsymbol{u}}(i, F)$ denote the polynomials

$$\left(F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1\right) \in \mathbb{C}[\boldsymbol{X}, \boldsymbol{L}]^{p+n-i+1}.$$

Example 3.1.6. *Consider again* $f = X_1^2 + X_2^2 + X_3^2 - 1 \in \mathbb{C}[X_1, X_2, X_3]$ *and*

$$V(X_1^2 + X_2^2 + X_3^2 - 1) \subset \mathbb{C}^3.$$

Since $\mathrm{jac}(X_1^2 + X_2^2 + X_3^2 - 1, 2) = 2X_3$, *the Lagrangian modeling gives us*

$$V(X_1^2 + X_2^2 + X_3^2 - 1, LX_3, L - 1) = V(X_1^2 + X_2^2 - 1, X_3, L - 1),$$

where the equations on the right hand side are a lexicographically ordered Gröbner basis of the ideal $\langle X_1^2 + X_2^2 + X_3^2 - 1, LX_3, L - 1\rangle$. *Notice that we have only 1 Lagrange multiplier,* L, *and we have* $\boldsymbol{u} = (u) = (1)$, *but any* $u \neq 0$ *would suffice here. We therefore have that*

$$\pi_{\boldsymbol{X}}(V(X_1^2 + X_2^2 - 1, X_3, L - 1))$$

describes the set where

$$X_1^2 + X_2^2 + X_3^2 - 1 = X_3 = 0$$

and therefore describes the polar variety $W(\pi_2, V(f))$.

Proposition 3.1.7. *The degree of $\mathscr{W}_{\boldsymbol{u}}(\pi_i, V)$ is at most d^{p+n}.*

Proof. Let $g_1, \ldots, g_{n-i}$ in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{L}]$ denote the *Lagrange polynomials*:

$$\textbf{Lagrange}(F, i, (L_1, \ldots, L_p)) = [L_1 \cdots L_p] \cdot \mathrm{jac}(F, i).$$

Since each polynomial in the sequence $F = (f_1, \ldots, f_p)$ has degree at most d, the degrees of each g_i are also bound by d. Thus, after adding the linear form $\sum_{i=1}^{p} u_i L_i - 1$, by Bézout's bound, we obtain

$$\deg \mathscr{W}_{\boldsymbol{u}}(\pi_i, V) \leq d^{p+n-i+1} \leq d^{p+n}.$$

□

3.2 Genericity statements

Here we state the genericity properties that each algorithm requires, and we state the key results which are used in the proofs of Theorems 1.3.1, 1.3.2, and 1.3.4. In generic coordinates, polar varieties are smooth, equidimensional, and in Noether position (or empty). The genericity statements given in this section are quantitative versions of these facts.

Recall that an equidimensional algebraic set $Y \subset \mathbb{C}^n$ of dimension d is in *Noether position* for the projection π_d when the extension

$$\mathbb{C}[X_1, \ldots, X_d] \to \mathbb{C}[X_1, \ldots, X_n]/I(Y)$$

is integral, and here, $I(Y) \subset \mathbb{C}[X_1, \ldots, X_n]$ is the defining ideal of Y. And recall that it then follows that, for any $\boldsymbol{x} \in \mathbb{C}^d$, the fiber $Y \cap \pi_d^{-1}(\boldsymbol{x})$ has dimension zero, so it is finite and not empty.

3.2.1 The hypersurfase cases

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 keys to proving Theorems 1.3.1 and 1.3.2 are the following results.

First recall that, for i in $\{1, \ldots, n\}$ and f as above, we let $\mathfrak{J}(i, f)$ denote the sequence of $n - (i-1)$ polynomials

$$\left(f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}\right).$$

As pointed out in the introduction, their zero-set is the i-th polar variety $W(\pi_i, V(f))$.

We say that f satisfies $\mathbf{H}_i$ if

1. For any $\boldsymbol{x}$ in $W(\pi_i, V(f))$, the Jacobian matrix $\mathrm{jac}_{\boldsymbol{x}}(\mathfrak{J}(i, f))$ has full rank $n - (i-1)$ at $\boldsymbol{x}$.

   By the Jacobian Criterion [14, Corollary 16.20], this implies that $W(\pi_i, V(f))$ is either empty or $(i-1)$-equidimensional, and that $\mathfrak{J}(i, f)$ 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

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

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

   By the Jacobian Criterion [14, Corollary 16.20], this implies that there are finitely many solutions to these equations.

The proof of Theorem 1.3.2 requires both $\mathbf{H}_i$ and $\mathbf{H}'_i$ for all i in $\{1, \ldots, n\}$. However, Theorem 1.3.1 only requires $\mathbf{H}_i$ (for the same i in $\{1, \ldots, n\}$).

The input polynomial f may not initially satisfy $\mathbf{H}_i$. However, it will after applying a generic change of variables. The precise statements are the following.

Theorem 3.2.1. *For $i = 1, \ldots, n$, there exists a non-zero polynomial $\mathfrak{h}_i \in \mathbb{C}[\mathfrak{A}]$ of degree at most $5n^2(2d)^{2n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel $\mathfrak{h}_i$, then $\boldsymbol{A}$ is invertible and $f^{\boldsymbol{A}}$ satisfies $\boldsymbol{H}_i$.*

Theorem 3.2.2. *For $i = 1, \ldots, n$, suppose that f satisfies $\boldsymbol{H}_i$, then there exists a non-zero polynomial $\mathfrak{g}_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most d^{2n} such that if $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel $\mathfrak{g}_i$, then f and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{H}'_i$.*

We prove Theorem 3.2.1 in Section 5.1.1 and 7.1. And we prove Theorem 3.2.2 in Section 5.1.2. For the compact hypersurface case, case 1, when proving Theorem 1.3.1, only Theorem 3.2.1 is used. For the hypersurface case, case 2, after removing the compactness assumption, when proving Theorem 1.3.2, both Theorems 3.2.1 and 3.2.2 are used.

3.2.2 The general case

Consider a sequence of polynomials $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$, with degrees at most d, defining a radical ideal $\langle f_1, \ldots, f_p \rangle$ and a smooth variety $V = V(F) \subset \mathbb{C}^n$, and with $\dim V = n - p$.

Establishing correctness for Lagrange systems. We need to prove that for a carefully chosen $\boldsymbol{u} \in \mathbb{C}^p$, we have the inclusion

$$\mathscr{I}_{\boldsymbol{u}}(i, F) \cap \mathbb{C}[X_1, \ldots, X_n] \subset \sqrt{\mathfrak{I}(i, F)}.$$

For $i \in \{1, \ldots, n-p+1\}$, let Z be an irreducible component of the polar variety $W(\pi_i, V)$.

Lemma 3.2.3. *There exists a non-zero vector of rational functions*

$$\boldsymbol{l} = (l_1, \ldots, l_p) = \left(\frac{N_1}{D_1}, \ldots, \frac{N_p}{D_p}\right) \in \mathbb{C}(Z)^p,$$

and an open and dense subset $Z' \subset Z$ defined by

1. $D_1(\boldsymbol{x}) \cdot D_2(\boldsymbol{x}) \cdots D_p(\boldsymbol{x}) \neq \boldsymbol{0}$,
2. $N_j(\boldsymbol{x}) \neq \boldsymbol{0}$, *for some* $j \in \{1, \ldots, p\}$,

and such that for $\boldsymbol{x} \in Z'$, $\boldsymbol{l}(\boldsymbol{x}) \cdot \mathrm{jac}_{\boldsymbol{x}}(F, i) = \boldsymbol{0}$.

Proof. Recall that for $\boldsymbol{x} \in Z$, the rank of $\mathrm{jac}_{\boldsymbol{x}}(F, i)$ is at most $p - 1$, because $W(\pi_i, V)$ is defined by the vanishing of F and Minors(F, p). Now, at $\boldsymbol{x} \in Z$, consider the Jacobian matrix $\mathrm{jac}_{\boldsymbol{x}}(F, i)$ with entries taken modulo the ideal $I(Z)$, and consider these entries as elements in $\mathbb{C}(Z)$; let $\widetilde{J}$ denote this matrix (note that since Z is irreducible, the function field $\mathbb{C}(Z)$ is well defined). Since the p-minors of $\mathrm{jac}_{\boldsymbol{x}}(F, i)$ are zero over $\boldsymbol{x} \in Z$, the p-minors of $\widetilde{J}$ are also zero at $\boldsymbol{x} \in Z$. And therefore the rank of $\widetilde{J}$ is also at most $p - 1$ at $\boldsymbol{x} \in Z$. Thus, some well defined $\boldsymbol{l} \in \mathbb{C}(Z)^p - \{\boldsymbol{0}\}$ exists with rational entries in $\boldsymbol{x}$. and with $\boldsymbol{l}(\boldsymbol{x}) \cdot \widetilde{J} = \boldsymbol{0}$. Since $\boldsymbol{l}$ is well defined, $D_1(\boldsymbol{x}) \cdot D_2(\boldsymbol{x}) \cdots D_p(\boldsymbol{x}) \neq \boldsymbol{0}$ and since $\boldsymbol{l} \neq \boldsymbol{0}, N_j(\boldsymbol{x}) \neq \boldsymbol{0}$, for some $j \in \{1, \ldots, p\}$. Therefore $\boldsymbol{l}(\boldsymbol{x}) \cdot \mathrm{jac}_{\boldsymbol{x}}(F, i) = \boldsymbol{0}$ as well. □

Using the same notation from the lemma above, let K denote the polynomial

$$K := D_1 \cdots D_p N_j \in \mathbb{C}[X_1, \ldots, X_n] - \{\boldsymbol{0}\}. \tag{3.1}$$

Proposition 3.2.4. *The degree of K is at most $2n^2d$.*

Proof. The degrees of each denominator D_l and numerator $N_k, 1 \leq l, k \leq p$, are bound by the degrees of the polynomials in the sequence Minors(F, p), which are at most nd. Therefore the degree of K is at most

$$(p+1)nd \leq (n+1)nd \leq 2n^2d.$$

□

Now, for Z' as in the proof of the lemma above, let $\boldsymbol{l}_Z$ be the vector of rational functions corresponding to the irreducible component Z. Consider the open set

$$\mathscr{O}_Z := \left\{ \boldsymbol{u} \in \mathbb{C}^p \mid \boldsymbol{u}^T \cdot \boldsymbol{l}_Z \neq \boldsymbol{0} \right\}.$$

We know, trivially, that $\mathscr{O}_Z$ is not empty, because $\boldsymbol{l}_Z \neq \boldsymbol{0}$. Let $\mathscr{O}$ denote the intersection

$$\mathscr{O} := \bigcap_Z \mathscr{O}_Z,$$

which we also know to be open and non-empty because it is a finite intersection of non-empty open sets.

Proposition 3.2.5. *For $\boldsymbol{u} \in \mathscr{O}$, we have the inclusion*

$$\mathscr{I}_{\boldsymbol{u}}(i, F) \cap \mathbb{C}[X_1, \ldots, X_n] \subset \sqrt{\mathfrak{I}(i, F)}.$$

In proving Proposition 3.2.5, we will need the following two lemmas.

Lemma 3.2.6. *Take any $\boldsymbol{u} \in \mathscr{O}$. For all irreducible components Z of $W(\pi_i, V)$, there exists a Zariski open and dense subsets $Z^o \subset Z'$, such that if $\boldsymbol{x} \in Z^o$ then $\boldsymbol{u}^T \cdot \boldsymbol{l}_Z(\boldsymbol{x}) \neq \boldsymbol{0}$.*

Proof. For $\boldsymbol{x} \in Z$, let ψ denote the mapping

$$\begin{aligned} Z &\to \mathbb{C}(Z) \\ \boldsymbol{x} &\mapsto \boldsymbol{u}^T \cdot \boldsymbol{l}_Z(\boldsymbol{x}). \end{aligned}$$

By Lemma 3.2.3, we know ψ is a rational function in $\boldsymbol{x}$. Let us write

$$\psi(\boldsymbol{x}) = \sum_{i=1}^{p} \frac{u_i N_i(\boldsymbol{x})}{D_i(\boldsymbol{x})} = \frac{u_1 N_1(\boldsymbol{x}) D_2(\boldsymbol{x}) \cdots D_p(\boldsymbol{x}) + \ldots + u_p N_p(\boldsymbol{x}) D_1(\boldsymbol{x}) \cdots D_{p-1}(\boldsymbol{x})}{D_1(\boldsymbol{x}) \cdots D_p(\boldsymbol{x})}.$$

Denote by $D(\boldsymbol{x})$ the non-zero product $D_1(\boldsymbol{x})\cdots D_p(\boldsymbol{x})$ and put

$$\begin{aligned} Z^o &:= \{\boldsymbol{x}\in Z \mid D(\boldsymbol{x})\cdot\psi(\boldsymbol{x})\neq \boldsymbol{0}\} \\ &= \{\boldsymbol{x}\in Z \mid u_1N_1(\boldsymbol{x})D_2(\boldsymbol{x})\cdots D_p(\boldsymbol{x}) + \ldots + u_pN_p(\boldsymbol{x})D_1(\boldsymbol{x})\cdots D_{p-1}(\boldsymbol{x})\neq \boldsymbol{0}\}. \end{aligned}$$

Notice that Z^o is not empty becuae $\boldsymbol{u}\in\mathscr{O}$. Hence, Z^o is both open and dense in Z, because $Z^o\neq\emptyset$, Z is irreducible, and $Z^o\subset Z^{'}\subset Z$. By construction we also have that if $\boldsymbol{x}\in Z^o$ then $D(\boldsymbol{x})\psi(\boldsymbol{x}) = D(\boldsymbol{x})(\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x}))\neq\boldsymbol{0}$ so that $\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})\neq\boldsymbol{0}$. □

Lemma 3.2.7. *Let $\boldsymbol{u}\in\mathscr{O}$ and consider the algebraic set $\mathscr{W}_{\boldsymbol{u}}(\pi_i,V)$. For all irreducible components Z of $W(\pi_i,V)$, we have the inclusion*

$$Z^o\subset\pi_{\boldsymbol{X}}\left(\mathscr{W}_{\boldsymbol{u}}(\pi_i,V)\right).$$

Proof. By Lemma 3.2.6, $\boldsymbol{x}\in Z^o$ implies that $\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})\neq\boldsymbol{0}$. Set

$$\boldsymbol{\alpha}_{\boldsymbol{x}} = \left(\boldsymbol{x}, \left(\frac{1}{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}\right)\boldsymbol{l}_Z(\boldsymbol{x})\right).$$

Then $F(\boldsymbol{x})=\boldsymbol{0}$,

$$\left(\frac{1}{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}\right)\boldsymbol{l}_Z(\boldsymbol{x})\cdot\mathrm{jac}_{\boldsymbol{x}}(F,i) = \left(\frac{1}{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}\right)\cdot\boldsymbol{0}=\boldsymbol{0},$$

and

$$\boldsymbol{u}^T\cdot\left(\frac{1}{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}\right)\boldsymbol{l}_Z(\boldsymbol{x}) - 1 = \cdot\left(\frac{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}{\boldsymbol{u}^T\cdot\boldsymbol{l}_Z(\boldsymbol{x})}\right) - 1 = 1-1=0,$$

so that $\boldsymbol{\alpha}_{\boldsymbol{x}}\in\mathscr{W}_{\boldsymbol{u}}(\pi_i,V)$. Therefore $Z^o\subset\pi_{\boldsymbol{X}}\left(\mathscr{W}_{\boldsymbol{u}}(\pi_i,V)\right)$. □

Now take $P\in\mathscr{I}_{\boldsymbol{u}}(i,F)\cap\mathbb{C}[X_1,\ldots,X_n]$, and Z an irreducible component of $W(\pi_i,V)$. Then, for $\boldsymbol{x}\in Z^o$ it follows from Lemma 3.2.7 that there exists $\boldsymbol{\alpha}\in\mathbb{C}^p$ with $(\boldsymbol{x},\boldsymbol{\alpha})\in\mathscr{W}_{\boldsymbol{u}}(\pi_i,V)$. Then

$$P(\boldsymbol{x},\boldsymbol{\alpha}) = P(\boldsymbol{x}) = \boldsymbol{0}.$$

Hence, P is zero on Z^o, and thus P is also zero on Z by the definition of Zariski closure. Therefore, P is zero on $W(\pi_i,V)$, and thus P is in $\sqrt{\mathfrak{I}(i,F)}$. This finishes the proof of Proposition 3.2.5.

Genericity statements. For $i \in \{1, \ldots, n-p+1\}$, we say that F satisfies $\mathbf{G}_i$ if

1. $W(\pi_i, V(F))$ is either empty or $(i-1)$-equidimensional.
2. For any $(\boldsymbol{x}, \boldsymbol{l})$ in $\mathscr{W}(\pi_i, V(F))$, the Jacobian matrix of $\mathscr{I}(i, F)$ has full rank $p+n-i$ at $(\boldsymbol{x}, \boldsymbol{l})$.

   By the Jacobian Criterion [14, Corollary 16.20], this implies that $\mathscr{I}(i, F)$ defines a radical ideal.
3. $W(\pi_i, V(F))$ is either empty or in Noether position for π_{i-1}.

For $i \in \{1, \ldots, n-p+1\}$, assuming that F satisfies $\boldsymbol{G}_i$, given $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1})$ in $\mathbb{C}^{i-1}$, we further say that F and $\boldsymbol{\sigma}$ satisfy $\mathbf{G}'_i$ if

1. For any $(\boldsymbol{x}, \boldsymbol{l})$ in $\mathscr{W}(\pi_i, V(F))$, the Jacobian of the system of polynomials

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p))$$

   has full rank $p+n-1$.

   By the Jacobian Criterion [14, Corollary 16.20], this implies that there are finitely many solutions to these equations.
2. The point $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1})$ is not in $\pi_{i-1}(V(K) \cap W(\pi_i, V))$, where K is the polynomial from 3.1.

Now, let $Z_{i,1}, \ldots, Z_{i,r_i}$ be the irreducible components of $W(\pi_i, V(F))$ so that

$$W(\pi_i, V(F)) = \bigcup_{k=1}^{r_i} Z_{i,k}.$$

We in addition say that $\boldsymbol{u}$ satisfies $\mathbf{G}''_i$ when

1. $\boldsymbol{u} \in \mathscr{O} := \left\{\boldsymbol{u} \in \mathbb{C}^p \mid \boldsymbol{u}^T \cdot \boldsymbol{l}_{Z_{i,1}} \neq 0, \ldots, \boldsymbol{u}^T \cdot \boldsymbol{l}_{Z_{i,r_i}} \neq 0\right\}$.

We prove the following.

Theorem 3.2.8. *For $i = 1, \ldots, n-p+1$, there exists a non-zero polynomial $\Delta_i \in \mathbb{C}[\mathfrak{A}]$ of degree at most $6n^2(2d)^{5n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel Δ_i, then $F^{\boldsymbol{A}}$ satisfies $\boldsymbol{G}_i$.*

Theorem 3.2.9. *For $i = 1, \ldots, n-p+1$, suppose that F satisfies $\boldsymbol{G}_i$, then there exists a non-zero polynomial $\Xi_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most $3n(nd)^{3n}$ such that if $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel Ξ_i, then F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{G}_i'$.*

Theorem 3.2.10. *For $i = 1, \ldots, n-p+1$, there exists a non-zero polynomial $\Upsilon_i \in \mathbb{C}[T_1, \ldots, T_p]$ of degree at most $(nd)^n$ such that if $\boldsymbol{u} \in \mathbb{C}^p$ does not cancel Υ_i, then $\boldsymbol{u}$ satisfies $\boldsymbol{G}_i''$.*

Theorem 3.2.8 is proven in Sections 5.2.1, 5.2.2, and 7.2. Theorem 3.2.9 is proven in Section 5.2.4 and Chapter 6. And Theorem 3.2.10 is proven next.

3.2.3 Proof of Theorem 3.2.10

Recall that after fixing $i \in \{1, \ldots, n-p+1\}$, we define

$$\mathscr{O} = \left\{\boldsymbol{u} \in \mathbb{C}^p \mid \boldsymbol{u}^T \cdot \boldsymbol{l}_{Z_{i,1}} \neq 0, \ldots, \boldsymbol{u}^T \cdot \boldsymbol{l}_{Z_{i,r_i}} \neq 0\right\},$$

where $Z_{i,1}, \ldots, Z_{i,r_i}$ are the irreducible components of $W(\pi_i, V(F))$, and hence the number of defining equations for $\mathscr{O}$ is r_i : the number of irreducible components. Notice that each defining equation is linear with degree equal to 1. We want to avoid $\boldsymbol{u} \in \mathbb{C}^p - \mathscr{O}$; this means that $\boldsymbol{u}$ is *unlucky* when

$$\boldsymbol{u}^T \cdot \boldsymbol{l}_{Z_{i,k}} = 0,$$

for any $1 \leq k \leq r_i$. Since each linear form has degree 1, the polynomial $\Upsilon_i \in \mathbb{C}[T_1, \ldots, T_p]$ defining the complement of $\mathscr{O}$:

$$V(\Upsilon_i) := \mathbb{C}^p - \mathscr{O},$$

has degree bounded above by r_i, which in turn is bounded above by the degree of $W(\pi_i, V(F^{\boldsymbol{A}}))$. Therefore, by Proposition 3.1.5,

$$\deg \Upsilon_i \leq \deg W(\pi_i, V(F)) \leq (nd)^n.$$

3.2.4 Related results in the literature

Some related results appear in the literature. For instance, Lemma 5 in [25] or Proposition 4.5 in [26] are quantitative Noether position statements. However, Theorems 3.2.1 and 3.2.8 do 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. And these two sets are in general different; for instance, their dimensions may vary.

3.3 Main algorithms

3.3.1 The compact hypersurface case

Recall the setting for case 1: S is given as $S = V \cap \mathbb{R}^n$, where $V = V(f) \subset \mathbb{C}^n$ is a smooth and compact, complex hypersurface defined by a squarefree polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$. If $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ is such that $f^{\boldsymbol{A}}$ satisfies $\boldsymbol{H}_1(1)$, then to obtain one point in each connected component it suffices to compute the first polar variety:

$$W\left(\pi_1, V(f^{\boldsymbol{A}})\right) = V\left(f^{\boldsymbol{A}}, \frac{\partial f^{\boldsymbol{A}}}{\partial X_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial X_n}\right) \tag{3.2}$$

which describes the critical points of the projection on a line; and will have dimension zero [4, 5]. To solve the equations (3.2), we use the algorithm in [37], for which a complete bit complexity analysis is available.

3.3.2 The hypersurface case, without compactness

Now recall case 2: S is given as $S = V \cap \mathbb{R}^n$, where $V = V(f) \subset \mathbb{C}^n$ is a smooth, complex hypersurface defined by a squarefree polynomial $f \in \mathbb{Z}[X_1, \ldots, X_n]$. For i in $\{1, \ldots, n\}$, assuming that f satisfies $\boldsymbol{H}_i$, and assuming that f and $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{Q}^{i-1}$ satisfy $\boldsymbol{H}_i'$, it suffices to solve the systems defined by

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, f, \frac{\partial f}{\partial X_{i+1}}, \ldots, \frac{\partial f}{\partial X_n}, \tag{3.3}$$

for $i = 1, \ldots, n$. They all admit finitely many solutions, and Theorem 2 in [34] proves that the union of their solution sets contains one point on each connected component of $V \cap \mathbb{R}^n$. And once again, to solve the equations (3.3), we use the algorithm in [37], for which a complete bit complexity analysis is available.

3.3.3 The general case

And finally, recall case 3: S is given as $S = V \cap \mathbb{R}^n$, where $V = V(F) \subset \mathbb{C}^n$ is a smooth, complex algebraic set defined by a sequence of polynomials $F = (f_1, \ldots, f_p)$ in $\mathbb{Z}[X_1, \ldots, X_n]$ defining a radical ideal. For i in $\{1, \ldots, n-p+1\}$, assuming that F satisfies

$\mathbf{G}_i$, and assuming that F and $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ satisfy $\mathbf{G}_i'$, it suffices to solve the systems defined by

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F^{\boldsymbol{A}}, \text{Minors}(F^{\boldsymbol{A}}, p) \tag{3.4}$$

for $i = 1, \ldots, n-p+1$. They all admit finitely many solutions, and Theorem 2 in [34] proves that the union of their solution sets contains one point on each connected component of $V \cap \mathbb{R}^n$. However, since the number of minors can grow exponentially in n (recall that the number of minors equals $S_i \sim \binom{n-i}{p} = 2^{n-i+1}$ when $n - i \sim 2p$) we avoid explicitly solving the equations in (3.4) and instead use the Lagrangian modeling of polar varieties. If in addition we assume that $\boldsymbol{u} \in \mathbb{C}^p$ satisfies $\mathbf{G}_i''$, then we can instead solve the equations

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F^{\boldsymbol{A}}, \textbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1, \tag{3.5}$$

and then compute the projections of each solution set on the $\boldsymbol{X}$-space.

Proposition 3.3.1. *For $i \in \{1, \ldots, n-p+1\}$, assuming that F satisfies $\boldsymbol{G}_i$, F and $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ satisfy $\boldsymbol{G}_i'$, and assuming that $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbb{C}^p$ satisfies $\boldsymbol{G}_i''$, if $\boldsymbol{x} \in \mathbb{C}^n$ is a solution of the system*

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, \mathit{Minors}(F, p)$$

then $\boldsymbol{x}$ is also a solution of the system

$$X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, \textbf{Lagrange}(F, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1$$

after projecting to the $\boldsymbol{X}$-space.

Proof. Recall notation from Section 3.2.2. Since F and $\boldsymbol{\sigma}$ satisfy $\boldsymbol{G}_i'(2)$,

$$\boldsymbol{\sigma} \notin \pi_{i-1}\left(V(K) \cap W(\pi_i, V)\right)$$

(where K is the polynomial from 3.1) and therefore an irreducible component Z of $W(\pi_i, V)$ exists with $\boldsymbol{x}$ in the open set $Z' \subset Z$ (recall definitions from Lemma 3.2.3). Hence, $\boldsymbol{l}_Z(\boldsymbol{x}) \neq (0, \ldots, 0)$. And since $\boldsymbol{u}$ satisfies $\boldsymbol{G}_i''$, we also have that $\boldsymbol{u} \cdot \boldsymbol{l}_Z(\boldsymbol{x}) \neq (0, \ldots, 0)$. Now, by the same argument given in the proof of Lemma 3.2.7, we have that

$$\boldsymbol{x} \in \pi_{\boldsymbol{X}}(\mathscr{W}_{\boldsymbol{u}}(\pi_i, V)).$$

□

Therefore, by computing the solutions of the equations 3.5 and then computing the projection on the $\boldsymbol{X}$-space, we will not miss any points on the polar varieties $W(\pi_i, V)$. Furthermore, in Chapter 5, we prove Proposition 5.2.9, which tells us that for any $\boldsymbol{u} \in \mathbb{C}^p$, assuming that F satisfies $\boldsymbol{G}_i(1)$ and $\boldsymbol{G}_i(2)$, we have the inclusion

$$\sqrt{\mathfrak{J}(i, F)} \subset \mathscr{I}_{\boldsymbol{u}}(i, F).$$

And it therefore follows that,

$$\pi_{\boldsymbol{X}}\left(\mathscr{W}_{\boldsymbol{u}}(\pi_i, V)\right) \subset V\left(\sqrt{\mathfrak{J}(i, F)}\right) = W(\pi_i, V).$$

This means that, if we take any point that satisfies the Lagrangian system 3.5, then its image, by the projection mapping to the $\boldsymbol{X}$ variables, is in the polar variety.

And again, to solve the equations (3.5), we use the algorithm in [37], for which a complete bit complexity analysis is available.

Chapter 4

Transversality

This chapter will require the following definitions and notation.

4.1 Definitions and notation: critical points of polynomials mappings

If $\mathbf{\Psi} : Y \to \mathbb{C}^t$ is a mapping from a smooth algebraic set Y to $\mathbb{C}^t$, with $t \leq \dim(Y)$, a *critical point* of $\mathbf{\Psi}$ is a point $\boldsymbol{y} \in Y$ such that the image of the tangent space $T_{\boldsymbol{y}}Y$ by the differential $d_{\boldsymbol{Y}}\mathbf{\Psi}$ 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 $\mathbf{\Psi}$ having rank less than t at $\boldsymbol{y}$. *Critical values* are the images by $\mathbf{\Psi}$ of critical points; the complement of this set are the *regular values* (so a regular value is not necessarily in the image of $\mathbf{\Psi}$).

4.2 Weak tranversality

Let n, s, and m be positive integers, with $m \leq n$, and denote by $\mathbf{\Phi} : \mathbb{C}^n \times \mathbb{C}^s \to \mathbb{C}^m$ a mapping defined by polynomials in $\mathbb{C}[\boldsymbol{X}, \mathbf{\Theta}]$, where $\boldsymbol{X}$, resp. $\mathbf{\Theta}$, is a set of n, resp. s, indeterminates. And for $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$, consider the induced mapping

$$\begin{aligned} \mathbf{\Phi}_{\boldsymbol{\vartheta}} : \mathbb{C}^n &\to \mathbb{C}^m \\ \boldsymbol{x} &\mapsto \mathbf{\Phi}(\boldsymbol{x}, \boldsymbol{\vartheta}). \end{aligned}$$

Thom's weak transversality theorem, as given for instance in [13], tells us that if $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}$, then for a generic $\boldsymbol{\vartheta} \in \mathbb{C}^s$, $\boldsymbol{0}$ is a regular value of the induced mapping $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$, where here transversality to a point is rephrased entirely in terms of critical and regular values. We have developed the following quantitative version of Thom's weak transversality.

Proposition 4.2.1 (Weak transversality)**.** *Let $\mathscr{O} \subset \mathbb{C}^n$ be a Zariski open set and suppose that $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}$ on $\mathscr{O} \times \mathbb{C}^s$. 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 $\Gamma(\boldsymbol{\vartheta}) \neq 0$ then $\mathbf{0}$ is a regular value of $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$ on $\mathscr{O}$.*

This result allows us to establish the first items in properties $\mathbf{H}_i$ and $\mathbf{G}_i$, as well as properties $\mathbf{H}_i'$ and $\mathbf{G}_i'$.

Thom's weak transversality generalizes Sard's lemma, which states that the set of critical values of a smooth function $\mathbb{R}^n \to \mathbb{R}^m$ has measure zero. In Thom's weak transversality, the *unlucky* parameters show up as the critical values of a smooth function. For us, the unlucky parameters are the changes of variables $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ that don't establish the properties we want, and the points $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ that don't establish the properties we want. One can give *algebraic* versions of Sard's lemma, for semi-algebraic mappings $\mathbb{R}^n \to \mathbb{R}^m$ as in [10, Chapter 9], or polynomial mappings $\mathbb{C}^n \to \mathbb{C}^m$ as in [29, Chapter 3], for which the sets of critical values are contained in strict semi-algebraic, resp. algebraic sets in the codomain.

The following simple example shows this result at work.

Example 4.2.2. *Consider a squarefree polynomial f in $\mathbb{C}[X_1, X_2]$, with degree at most d, defining a smooth curve $V(f)$ 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 full rank two at any point in $\boldsymbol{\Phi}^{-1}(\mathbf{0})$, which is to say that $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}$ and therefore the assumptions of the proposition apply. We then deduce that a non-zero polynomial $\Gamma \in \mathbb{C}[\Theta]$ exists, with degree at most d^4 with the property that, if ϑ in $\mathbb{C}$ does not cancel Γ then $\boldsymbol{0}$ is a regular value of the induced mapping $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$. 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.

Now, if we take a finite subset $S \subset \mathbb{C}$, then for $\boldsymbol{\vartheta} \in S$ chosen randomly, independently and uniformly, it then follows by DeMillo-Lipton-Schwartz–Zippel that

$$\mathbb{P}[\Gamma(\boldsymbol{\vartheta}) = \boldsymbol{0}] \leq \frac{d^4}{|S|}.$$

We will revisit this example in Sections 5.1.2 and 5.2.4 (when proving $\boldsymbol{H}_i'$ and $\boldsymbol{G}_i'(1)$).

4.3 Proof of Proposition 4.2.1 (weak transversality)

The rest of this chapter is devoted to proving the proposition. The proof of [36, Theorem B.3] already shows the existence of Γ; it is essentially the classical proof for smooth mappings [13, Section 3.7], written in an algebraic context. In what follows, we revisit this proof, establishing a bound on the degree of Γ.

As mentioned above, Thom's weak transversality theorem is a generalization of Sard's Lemma, which states that the set of critical values of a smooth function has measure zero; unlucky parameters show up as the critical values of this function. The proof begins by characterizing the critical points of this function.

4.3.1 Characterizing the critical points

Put $V' = \boldsymbol{\Phi}^{-1}(\mathbf{0}) \cap (\mathscr{O} \times \mathbb{C}^s)$, and let V be the Zariski closure of V'. If V is empty, there is nothing to do, since all values $\boldsymbol{\vartheta}$ in $\mathbb{C}^s$ satisfy the conclusion of the proposition. We therefore assume that V is not empty. Take $(\boldsymbol{x}, \vartheta)$ in V'; then by assumption, $\mathrm{jac}_{(\boldsymbol{x},\vartheta)}(\boldsymbol{\Phi})$ has full rank m. Since in a neighborhood of $(\boldsymbol{x}, \vartheta), V$ coincides with $\boldsymbol{\Phi}^{-1}(0) \cap \mathscr{O}$, the Jacobian criterion [14, Corollary 16.20] implies that there is a unique irreducible component $V_{(\boldsymbol{x},\vartheta)}$ of V that contains $(\boldsymbol{x}, \vartheta)$, that $(\boldsymbol{x}, \vartheta)$ is regular on this component, that $\dim V_{(\boldsymbol{x},\vartheta)} = n + s - m$ and that $T_{(\boldsymbol{x},\vartheta)}$ is the nullspace of $\mathrm{jac}_{(\boldsymbol{x},\vartheta)}(\boldsymbol{\Phi})$.

Since every irreducible component of V intersects V', this implies that V itself is equidimensional of dimension $n + s - m$, and thus that V' is contained in $\mathrm{reg}(V)$. Furthermore, it also follows that for $(\boldsymbol{x}, \boldsymbol{\vartheta}) \in V', T_{(\boldsymbol{x},\boldsymbol{\vartheta})}V$ is the nullspace of $\mathrm{jac}_{(\boldsymbol{x},\boldsymbol{\vartheta})}(\Phi)$ in $\mathbb{C}^n \times \mathbb{C}^s$.

We will reuse the following fact, proved in [36]. Consider the projection

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

and let Z be the set of critical points of $\pi_{|V'}$. That is,

$$Z := \{(\boldsymbol{x}, \boldsymbol{\vartheta}) \in V' \mid \dim(\pi(T_{\boldsymbol{x},\boldsymbol{\vartheta}} V')) < s\}.$$

Consider its projection $\pi(Z)$ in $\mathbb{C}^s$. This is the set of critical values of $\pi_{|V'}$. Also let Z' be the critical points of $\pi_{|\operatorname{reg}(V)}$ so that, by the algebraic form of Sard's lemma (see [29, Theorem 3.7] for irreducible V' and [36, Proposition B.2] for general V'), its Zariski closure $\overline{\pi(Z')}$ is a strict closed subset of $\mathbb{C}^s$. Then, since $V' \subset \operatorname{reg}(V)$ and since $Z \subset Z'$, the 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 $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}$ on $\mathscr{O}$.

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

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

Lemma 4.3.1. *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 $\operatorname{jac}_{\boldsymbol{X},\boldsymbol{\Theta}}(\boldsymbol{\Phi})$ 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 $(\boldsymbol{x}, \boldsymbol{\vartheta}) \in V'$ and since $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}$, $\boldsymbol{K}(\boldsymbol{x}, \boldsymbol{\vartheta})$ 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 $\boldsymbol{\Phi}(\boldsymbol{x}, \boldsymbol{\vartheta}) = \mathbf{0}$ 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 4.3.2. *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 $\boldsymbol{\Phi}_{\boldsymbol{\vartheta}}^{-1}(\mathbf{0})$ on $\mathscr{O}$, $(\boldsymbol{x}, \boldsymbol{\vartheta})$ 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.

4.3.2 Bounding the degree of the set of critical values

Our next step is to bound the degree of the critical points Z, from which we can bound the degree of $\overline{\pi(Z)}$, the Zariski closure of the critical values, and prove Proposition 4.2.1. 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 once again introduce Lagrangian systems. 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 denote by $\mathfrak{Z}'$ the algebraic set

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

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 4.3.3. *The critical points Z are contained in $\mu(\mathfrak{Z}')$.*

Proof. Take $(\boldsymbol{x}, \boldsymbol{\vartheta}) \in Z$. Then, there exists $\boldsymbol{l} \neq (0, \ldots, 0) \in \mathbb{C}^n$ and $\boldsymbol{x} \in \mathscr{O}$, with

$$\boldsymbol{l} \cdot \boldsymbol{J}(\boldsymbol{x}, \boldsymbol{\vartheta}) = \boldsymbol{0}.$$

Thus, $(\boldsymbol{x}, \boldsymbol{\vartheta}) \in \mu(\mathfrak{Z}')$ so that $Z \subset \mu(\mathfrak{Z}')$. □

Let Y be an irreducible component of $\mathfrak{Z}'$. There exists an open and dense subset $Y^o \subset Y$ such that for all $(\boldsymbol{x}, \boldsymbol{\vartheta}, \boldsymbol{l}) \in Y^o$, $\boldsymbol{x} \in \mathscr{O}$ and $\boldsymbol{l} \neq \boldsymbol{0}$. It then follows that $\mu(Y^o) \subset Z$ and $\mu(\cup_Y Y^o) \subset Z$; thence,

$$\overline{\mu(\cup_Y Y^o)} \subset \overline{Z}. \tag{4.1}$$

Now put $W := \overline{\mu(\mathfrak{Z}')}$.

Lemma 4.3.4. *The algebraic set $\overline{\pi(Z)}$ is equal to $\overline{\pi(W)}$.*

Proof. Since

$$\overline{\cup_Y Y^o} = \mathfrak{Z}',$$

we get

$$W = \overline{\mu(\mathfrak{Z}')} = \overline{\mu(\overline{\cup_Y Y^o})} = \overline{\mu(\cup_Y Y^o)} \subset \overline{Z},$$

where the last inclusion follows by 4.1 above. Hence, by lemma 4.3.3,

$$Z \subset \mu(\mathfrak{Z}') \subset \overline{\mu(\mathfrak{Z}')} = W \subset \overline{Z}.$$

Then

$$\pi(Z) \subset \pi(W) \subset \pi(\overline{Z}),$$

so that

$$\overline{\pi(Z)} \subset \overline{\pi(W)} \subset \overline{\pi(\overline{Z})} = \overline{\pi(Z)}.$$

And therefore,

$$\overline{\pi(Z)} = \overline{\pi(W)}.$$

□

Corollary 4.3.5. *The degree of $\overline{\pi(Z)}$ 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 bound [22] that $\deg(\mathfrak{Z}) \leq d^{m+n}$, and the same upper bound holds for $\deg(\mathfrak{Z}')$, since it consists of certain irreducible components of $\mathfrak{Z}$. Since degree will not increase after projection or closure,

$$\deg(W) = \deg(\overline{\mu(\mathfrak{Z}')}) \leq \deg(\mathfrak{Z}').$$

And by Lemma 4.3.4,

$$\deg(\overline{\pi(Z)}) = \deg(\overline{\pi(W)}) \leq \deg(W).$$

□

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 4.2.1.

Chapter 5

Applications of weak transversality

5.1 Applications: the hypersurface case

Let $f \in \mathbb{Z}[X_1, \ldots, X_n]$ be squarefree with total degree d, and with $V(f) \subset \mathbb{C}^n$ smooth.

5.1.1 Application: proof of $\mathbf{H}_i(1)$

In what follows, we fix i in $\{1, \ldots, n\}$ and we prove the following: *there exists a non-zero polynomial $\mathfrak{h}_{i,1} \in \mathbb{C}[\mathfrak{A}]$ of degree at most $2nd^{2n}$ such that if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel $\mathfrak{h}_{i,1}$, 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 $\boldsymbol{\Phi} : \mathbb{C}^n \times \mathbb{C}^{n\times n} \to \mathbb{C}^{n-i+1}$ be the mapping defined by the polynomials

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

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

Lemma 5.1.1. ***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 4.2.1 that there exists a non-zero polynomial $\Gamma_i \in \mathbb{C}[\mathfrak{A}]$ of degree at most $d^{2n-i+1} \leq d^{2n}$, with the property that, if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel Γ_i, then the Jacobian matrix of

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

taken with respect to $\boldsymbol{X}$, has full rank $n - i + 1$ at all $\boldsymbol{x}$ that cancels equations. We then define

$$\mathfrak{h}_{i,1} := \Gamma_i \det(\mathfrak{A});$$

this is a non-zero polynomial of degree at most $d^{2n} + n \leq 2nd^{2n}$.

Let us verify that $\mathfrak{h}_{i,1}$ satisfies the claim in the preamble. Take $\boldsymbol{A}$ in $\mathbb{C}^{n\times n}$, such that $\mathfrak{h}_{i,1}(\boldsymbol{A})$ 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

$$\left(f^{\boldsymbol{A}}, \frac{\partial f^{\boldsymbol{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial X_n}\right)$$

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 Chapter 7, 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 Section 2.3, this polynomial satisfies the rank property $\mathbf{H}_i(1)$.

5.1.2 Application: proof of $\mathbf{H}_i'$

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* $\mathfrak{g}_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ *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* $\mathfrak{g}_i$*, then for any root* $\boldsymbol{x}$ *of*

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

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

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

Lemma 5.1.2. $\boldsymbol{0}$ *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

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

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 4.2.1 that there exists a non-zero polynomial $\mathfrak{g}_i$ in $\mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most d^{2n}, with the following property: if $\mathfrak{g}_i(\boldsymbol{\sigma}) \neq 0$ then at any root $\boldsymbol{x}$ of

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

the Jacobian matrix of these equations has full rank n. Theorem 3.2.2 is proven.

5.2 Applications: the general case

Let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ be a sequence of polynomials defining a radical ideal, and where the degree of each polynomial is at most d. Also, assume that the variety $V(F) \subset \mathbb{C}^n$ is smooth. Recall that $\mathfrak{A}$ denotes the matrix of indeterminates with entries $(\mathfrak{A}_{j,k})_{1 \leq j,k \leq n}$ and let $\mathrm{J}_i(\boldsymbol{X}, \mathfrak{A})$ denote the matrix

$$\begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F) \\ \mathfrak{A}_{1,1} & \cdots & \mathfrak{A}_{1,n} \\ \vdots & & \vdots \\ \mathfrak{A}_{i,1} & \cdots & \mathfrak{A}_{i,n} \end{bmatrix}.$$

Consider elements $\boldsymbol{a} \in \mathbb{C}^{in}$ as vectors of length i of the form $\boldsymbol{a} = (\boldsymbol{a}_1, \ldots, \boldsymbol{a}_i)$ with $\boldsymbol{a}_i \in \mathbb{C}^n$. Then for such an $\boldsymbol{a}$, $\mathrm{J}_i(\boldsymbol{X}, \boldsymbol{a})$ is naturally defined with the indeterminates evaluated at $\boldsymbol{a}$. We say that $\boldsymbol{a}$ has rank i when $\boldsymbol{a}$ is a sequence of linearly independent vectors. Let $\boldsymbol{\Phi}$ define the polynomial mapping

$$\begin{aligned} \mathbb{C}^{n+p+i} \times \mathbb{C}^{in} &\to \mathbb{C}^{p+n} \\ (\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{a}) &\mapsto (F(\boldsymbol{x}), [\lambda_1, \ \cdots, \lambda_c, \vartheta_1, \ \cdots, \vartheta_i] \cdot \mathrm{J}_i(\boldsymbol{x}, \boldsymbol{a})) \end{aligned}$$

and $\boldsymbol{\Phi}_{\boldsymbol{a}}$ the induced mapping

$$\begin{aligned} \mathbb{C}^{n+p+i} &\to \mathbb{C}^{p+n} \\ (\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) &\mapsto \boldsymbol{\Phi}(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{a}). \end{aligned}$$

Let $\mathscr{A}$ be defined by the rank conditions: $\mathrm{rank}(\mathrm{jac}_{\boldsymbol{x}}(F)) = p$ and $\boldsymbol{\lambda} = (\lambda_1, \ldots, \lambda_p) \neq \boldsymbol{0}$. In [7, Section 3.2], it is shown that, for any $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{a})$ in $\mathscr{A}$, the Jacobian matrix $\mathrm{jac}_{(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{a})} \boldsymbol{\Phi}$ has full rank $p + n$, which in particular holds for $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}, \boldsymbol{a})$ in $\boldsymbol{\Phi}^{-1}(\boldsymbol{0})$ and therefore $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}$. It therefore follows by Proposition 4.2.1, there exists a non-zero polynomial $\Gamma_i \in \mathbb{C}[\mathfrak{A}_{1,1}, \ldots, \mathfrak{A}_{i,n}]$ of degree at most

$$d^{(n+p+i)+(p+n)} \leq d^{3n+2n} = d^{5n},$$

such that if $\boldsymbol{a} \in \mathbb{C}^{i \times n}$ does not cancel Γ_i, then $\boldsymbol{0}$ is a regular value of $\boldsymbol{\Phi}_{\boldsymbol{a}}$. Thus, for $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \boldsymbol{\Phi}_{\boldsymbol{a}}^{-1}(\boldsymbol{0})$, the Jacobian matrix $\mathrm{jac}_{(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})}(\boldsymbol{\Phi}_{\boldsymbol{a}})$ has full rank $p + n$.

5.2.1 Application: proof of $\mathbf{G}_i(1)$

In what follows, we fix i in $\{1, \ldots, n - p + 1\}$, and we prove the following: *There exists a non-zero polynomial $\Delta_{i,1} \in \mathbb{C}[\mathfrak{A}]$ of degree at most nd^{5n} such that if $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does*

not cancel $\Delta_{i,1}$, then $\boldsymbol{A}$ is invertible and the polar variety $W(\pi_i, V(F^{\boldsymbol{A}})$ is either empty or $(i-1)$-equidimensional.

Consider $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ such that the first i rows of $\boldsymbol{A}^{-1}$ do not cancel Γ_i, and let $\boldsymbol{b}$ denote the first i rows of $\boldsymbol{A}^{-1}$. Note that $\boldsymbol{b}$ has full rank i. Let $\mathfrak{B} \in \mathbb{C}(\mathfrak{A}) - \mathbb{C}$ denote $\mathfrak{A}^{-1}$ and let $\mathfrak{B}_1 = [\mathfrak{B}_{1,1}, \ldots, \mathfrak{B}_{1,n}], \ldots, \mathfrak{B}_n = [\mathfrak{B}_{n,1}, \ldots, \mathfrak{B}_{n,n}]$ denote the rows of $\mathfrak{B}$. Set

$$\Delta_{i,1} := \Gamma_i(\mathfrak{B}_1, \ldots, \mathfrak{B}_i) \cdot (\det \mathfrak{A})^{\deg \Gamma_i}.$$

By multiplying through by $(\det \mathfrak{A})^{\deg \Gamma_i}$, we cancel all denominators and thus make $\Delta_{i,1}$ a polynomial.

Lemma 5.2.1. *The degree of $\Delta_{i,1}$ is at most nd^{5n}.*

Proof. Assume that

$$\mathfrak{B}_{i,j} = \mathfrak{N}_{i,j}/\mathfrak{D}_{i,j},\ \mathfrak{N}_{i,j}, \mathfrak{D}_{i,j} \in \mathbb{C}[\mathfrak{A}] - \{\mathbb{C}\}.$$

Then, $\deg \mathfrak{N}_{i,j} \leq n-1 \leq n$, and since we have cleared all denominators $\mathfrak{D}_{i,j}$ by multiplying through with $(\det \mathfrak{A})^{\deg \Gamma_i}$, we therefore obtain

$$\deg \Delta_{i,1} \leq n \deg \Gamma_i \leq nd^{5n}.$$

□

Now put

$$Y(\boldsymbol{a}) := \{\boldsymbol{x} \in V(F) \mid \operatorname{rank} \mathrm{J}_i(\boldsymbol{X}, \boldsymbol{a}) < p + i\}.$$

Lemma 5.2.2. *For $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ with $\Delta_{i,1}(\boldsymbol{A}) \neq 0$,*

$$Y^{\boldsymbol{A}}(\boldsymbol{b}) = W\left(\pi_i, V\left(F^{\boldsymbol{A}}\right)\right).$$

Proof. Let $L_1, \ldots, L_p$ and $T_1, \ldots, T_i$ be new indeterminants. First note that if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ satisfies

$$\Delta_{i,1}(\boldsymbol{A}) = \Gamma_i(b_{1,1}, \ldots, b_{i,n}) \cdot (\det \boldsymbol{A})^{d^{5n}} \neq 0,$$

so that

$$\Gamma_i(b_{1,1}, \ldots, b_{i,n}) \neq 0,$$

then we have that, for $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \boldsymbol{\Phi}_{\boldsymbol{b}}^{-1}(\boldsymbol{0})$, the Jacobian of the polynomials

$$(F, [L_1 \cdots L_p\ T_1 \cdots T_i] \cdot \mathrm{J}_i(\boldsymbol{X}, \boldsymbol{b}))$$

at $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$ has full rank $p+n$. We then have that

$$Y^{\boldsymbol{A}}(\boldsymbol{b}) = \left\{ \boldsymbol{x} \in V\left(F^{\boldsymbol{A}}\right) \mid \operatorname{rank} \mathrm{J}_i(\boldsymbol{A}\boldsymbol{x}, \boldsymbol{b}) < p+i \right\}.$$

Consider the identity $\operatorname{jac}(F^{\boldsymbol{A}}) = \operatorname{jac}(F)^{\boldsymbol{A}}\boldsymbol{A}$ and notice that

$$\mathrm{J}_i(\boldsymbol{A}\boldsymbol{x}, \boldsymbol{b}) = \begin{bmatrix} \operatorname{jac}_{\boldsymbol{x}}(F)^{\boldsymbol{A}} \\ \boldsymbol{b} \end{bmatrix} = \begin{bmatrix} \operatorname{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}})\boldsymbol{A}^{-1} \\ \begin{bmatrix} \mathbf{1}_i & \mathbf{0} \end{bmatrix} \boldsymbol{A}^{-1} \end{bmatrix} = \begin{bmatrix} \operatorname{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) \\ \operatorname{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix} \boldsymbol{A}^{-1}$$

and therefore

$$\operatorname{rank} \mathrm{J}_i(\boldsymbol{A}\boldsymbol{x}, \boldsymbol{b}) = \operatorname{rank} \begin{bmatrix} \operatorname{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) \\ \operatorname{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix}.$$

Furthermore, since V is smooth, it follows from [14, Corollary 16.20] that for all $\boldsymbol{x}$ in $V, \operatorname{jac}_{\boldsymbol{x}}(F)$ has full rank $n - \dim V = n - (n-p) = p$, which is a property also established in virtue of the rank conditions on $\mathscr{A}$. Therefore

$$\begin{aligned} Y^{\boldsymbol{A}}(\boldsymbol{b}) &= \left\{ \boldsymbol{x} \in V(F^{\boldsymbol{A}}) \;\middle|\; \operatorname{rank} \operatorname{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) = p \text{ and } \operatorname{rank} \begin{bmatrix} \operatorname{jac}_{\boldsymbol{x}}(^{\boldsymbol{A}}) \\ \operatorname{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix} < p+i \right\} \\ &= W\left(\pi_i, V\left(F^{A}\right)\right). \end{aligned}$$

□

Lemma 5.2.3. *$Y(\boldsymbol{b})$ is the projection of $\mathscr{A} \cap \boldsymbol{\Phi}_{\boldsymbol{b}}^{-1}(0)$ on the $\boldsymbol{X}$-space.*

Proof. An element $\boldsymbol{x} \in V$ belongs to $Y(\boldsymbol{b})$ if and only if $\operatorname{rank} \mathrm{J}_i(\boldsymbol{x}, \boldsymbol{b}) < p+i$, which holds if and only if there exists some non zero vector $[\boldsymbol{\lambda}, \boldsymbol{\vartheta}]$ in the right nullspace. Since $\boldsymbol{b}$ has full rank i, we know that $\boldsymbol{\lambda} \neq 0$. □

Lemma 5.2.4. *The set $\dim Y(\boldsymbol{b})$ is either empty or has dimension $i-1$.*

Proof. The conclusion follows from [36, Lemma B.5, Lemma B.11]. □

It now follows that if $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ with $\Delta_{i,1}(\boldsymbol{A}) \neq 0$, then each irreducible component of the polar variety has dimension $i-1$. Therefore, the polar variety $W(\pi_i, V(F^{\boldsymbol{A}}))$ is either empty or $(i-1)$-equidimensional; hence, $\boldsymbol{G}_i(1)$ is established.

5.2.2 Application: proof of $\mathbf{G}_i(2)$

Here we in addition prove: *if* $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ *does not cancel* $\Delta_{i,1}$*, then for any* $(\boldsymbol{x}, \boldsymbol{l})$ *in* $\mathscr{W}(\pi_i, V(F))$*, the Jacobian matrix of* $\mathscr{I}(i, F)$ *has full rank* $p + n - i$ *at* $(\boldsymbol{x}, \boldsymbol{l})$*.*

Take $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ so that $\Delta_{i,1}(\boldsymbol{A}) \neq 0$, and again let $\boldsymbol{b}$ denote the first i rows of $\boldsymbol{A}^{-1}$.

Proposition 5.2.5. *At any* $(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}(\pi_i, V^{\boldsymbol{A}})$*, the Jacobian of the polynomials*

$$\left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p))\right)$$

has full rank $p + n - i$*.*

Proof. Again, let $L_1, \ldots, L_p$ and $T_1, \ldots, T_i$ be new indeterminants. Recall from the beginning of Section 5.2, that for $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta}) \in \mathscr{A} \cap \boldsymbol{\Phi}_{\boldsymbol{b}}^{-1}(\boldsymbol{0})$, the Jacobian matrix of the polynomials

$$(F, [L_1 \ \cdots \ L_p \ T_1 \ \cdots \ T_i] \cdot \mathrm{J}_i(\boldsymbol{X}, \boldsymbol{b}))$$

has full rank $p + n$. Recall that

$$\mathrm{J}_i(\boldsymbol{A}\boldsymbol{x}, \boldsymbol{b}) = \begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F)^{\boldsymbol{A}} \\ \boldsymbol{b} \end{bmatrix} = \begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}})\boldsymbol{A}^{-1} \\ \begin{bmatrix} \mathbf{1}_i & \mathbf{0} \end{bmatrix} \boldsymbol{A}^{-1} \end{bmatrix} = \begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) \\ \mathrm{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix} \boldsymbol{A}^{-1}$$

and therefore

$$\operatorname{rank} \mathrm{J}_i(\boldsymbol{A}\boldsymbol{x}, \boldsymbol{b}) = \operatorname{rank} \begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) \\ \mathrm{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix}.$$

Consider the Jacobian of the polynomials

$$(F, [L_1 \ \cdots \ L_p \ T_1 \ \cdots \ T_i] \cdot \mathrm{J}_i(\boldsymbol{X}, \boldsymbol{b}))$$

taken with respect to the variables

$$X_1, \ldots, X_n, L_1, \ldots, L_p, T_1, \ldots, T_i,$$

at a point $(\boldsymbol{x}, \boldsymbol{\lambda}, \boldsymbol{\vartheta})$ that cancels equations. This Jacobian has full rank $p + n$. Indeed, it is equal to

$$\left[\begin{array}{c|c|c} \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) & \boldsymbol{0}_{p\times p} & \boldsymbol{0}_{p\times i} \\ * * * & * * * & \boldsymbol{I}_i \\ * * * & * * * & \boldsymbol{0}_{p\times i} \end{array}\right] = \left[\begin{array}{c|c} \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}(F^{\boldsymbol{A}}) & \boldsymbol{0}_{p\times i} \\ \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left([\boldsymbol{\lambda}, \boldsymbol{\vartheta}] \cdot \begin{bmatrix} \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}) \\ \mathrm{jac}_{\boldsymbol{x}}(\pi_i) \end{bmatrix}\right) & \begin{bmatrix} \boldsymbol{I}_i \\ \boldsymbol{0}_{p\times i} \end{bmatrix} \end{array}\right]$$

$$= \left[\begin{array}{c|c} \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}(F^{\boldsymbol{A}}) & \boldsymbol{0}_{p\times i} \\ * * * & I_i \\ \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left(\boldsymbol{l} \cdot \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i)\right) & \boldsymbol{0}_{p\times i} \end{array}\right].$$

Therefore, after rearranging blocks and after removing i columns, we can see that

$$\mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left(F^{\boldsymbol{A}}, \boldsymbol{l}\cdot\mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}},i)\right) = \begin{bmatrix} \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}(F^{\boldsymbol{A}}) \\ \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left(\boldsymbol{l}\cdot\mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}},i)\right) \end{bmatrix} \tag{5.1}$$

has full rank $p+n-i$. Now, recall that

$$\boldsymbol{l}\cdot\mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}},i) = \mathbf{Lagrange}(F^{\boldsymbol{A}},i,(L_1,\ldots,L_p)),$$

and therefore it becomes clear that, at any

$$(\boldsymbol{x},\boldsymbol{l}) \in V(\mathscr{I}(i,F^{\boldsymbol{A}})) = \mathscr{W}(\pi_i, V^{\boldsymbol{A}}),$$

the Jacobian of the polynomials

$$\left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}},i,(L_1,\ldots,L_p))\right)$$

has full rank $p+n-i$. □

This establishes $\boldsymbol{G}_i(2)$.

5.2.3 Additional statements for Lagrangian systems

Again assume that $\boldsymbol{A}\in\mathbb{C}^{n\times n}$ has the property that $\Delta_{i,1}(\boldsymbol{A})\neq 0$.

Corollary 5.2.6. *The ideal defined by* $\mathscr{I}(i,F^{\boldsymbol{A}}) = \left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}},i,(L_1,\ldots,L_p))\right)$ *is radical.*

Proof. Given Proposition 5.2.5, the claim now follows from the Jacobian Criterion [14, Corollary 16.20]. □

Proposition 5.2.7. *Let* $\boldsymbol{u}=(u_1,\ldots,u_p)\in\mathbb{C}^p$ *be any complex point. Then, for any*

$$(\boldsymbol{x},\boldsymbol{l}) \in \mathscr{W}_{\boldsymbol{u}}\left(\pi_i, V(F^{\boldsymbol{A}})\right) \subset \mathbb{C}^{n+p},$$

the Jacobian matrix of the polynomials

$$\left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}},i,(L_1,\ldots,L_p)), \sum_{i=1}^{p} u_i L_i - 1\right)$$

has full rank $p+n-i+1$ *at* $(\boldsymbol{x},\boldsymbol{l})$.

Proof. Note that $(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}_{\boldsymbol{u}}(\pi_i, V(F^{\boldsymbol{A}}))$ implies that $(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}(\pi_i, V(F^{\boldsymbol{A}}))$; thus, by Proposition 5.2.5, the Jacobian of the polynomials

$$\mathscr{J}(i, F^{\boldsymbol{A}}) = (F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)))$$

has full rank $p + n - i$ at $(\boldsymbol{x}, \boldsymbol{l})$. The conclusion therefore holds if $[\boldsymbol{0} \mid \boldsymbol{u}]$ is not in the row space of the Jacobian of the polynomials

$$\left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right),$$

for any $(\boldsymbol{x}, \boldsymbol{l})$ that cancels equations. This matrix is equal to

$$\left[\begin{array}{c|c|c} \frac{\partial f_1^{\boldsymbol{A}}}{\partial X_1}(\boldsymbol{x}) \ldots \frac{\partial f_1^{\boldsymbol{A}}}{\partial X_n}(\boldsymbol{x}) & \boldsymbol{0}_{1\times p} & \boldsymbol{0}_{1\times p} \\ \ddots & \ddots & \ddots \\ \frac{\partial f_p^{\boldsymbol{A}}}{\partial X_1}(\boldsymbol{x}) \ldots \frac{\partial f_p^{\boldsymbol{A}}}{\partial X_n}(\boldsymbol{x}) & \boldsymbol{0}_{1\times p} & \boldsymbol{0}_{1\times p} \\ \ddots & \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i)^T & \boldsymbol{0}_{n-i+1\times p} \\ \boldsymbol{0}_{1\times p} & u_1 \ldots u_p & l_1 \ldots l_p \end{array}\right];$$

consider the upper left block

$$\left[\begin{array}{c|c} A & \boldsymbol{0}_{p\times p} \\ B & C \end{array}\right] := \left[\begin{array}{c|c} \frac{\partial f_1^{\boldsymbol{A}}}{\partial X_1}(\boldsymbol{x}) \ldots \frac{\partial f_1^{\boldsymbol{A}}}{\partial X_n}(\boldsymbol{x}) & \boldsymbol{0}_{1\times p} \\ \ddots & \ddots \\ \frac{\partial f_p^{\boldsymbol{A}}}{\partial X_1}(\boldsymbol{x}) \ldots \frac{\partial f_p^{\boldsymbol{A}}}{\partial X_n}(\boldsymbol{x}) & \boldsymbol{0}_{1\times p} \\ \ddots & \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i)^T \end{array}\right],$$

and suppose for contradiction that $[\boldsymbol{0} \mid \boldsymbol{u}]$ is in the row-space. Then

$$[\boldsymbol{0} \mid \boldsymbol{u}] = \lambda[A \mid \boldsymbol{0}] + \mu[B \mid C]$$

and

$$\boldsymbol{u} = \mu \cdot C = \mu \cdot \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i)^T$$

so that

$$\boldsymbol{u}^T = \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i) \cdot \mu^T.$$

Now we have a contradiction because, $(\boldsymbol{x}, \boldsymbol{l})$ is such that

$$\begin{aligned} & \boldsymbol{l} \cdot \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i) = 0 \\ \Rightarrow\ & \boldsymbol{l} \cdot \mathrm{jac}_{\boldsymbol{x}}(F^{\boldsymbol{A}}, i)\mu^T = 0 \\ \Rightarrow\ & \boldsymbol{l} \cdot \boldsymbol{u}^T = 0, \end{aligned}$$

when by assumption $\boldsymbol{l} \cdot \boldsymbol{u}^T = 1$. □

Corollary 5.2.8. *Let* $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbb{C}^p$ *be any complex point. Then, for any*

$$(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}_{\boldsymbol{u}}(\pi_i, V(F^{\boldsymbol{A}})) \subset \mathbb{C}^{n+p}$$

the ideal defined by $\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})$:

$$\left(F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right)$$

is radical.

Proof. Given Proposition 5.2.7, the conclusion now follows from the Jacobian Criterion [14, Corollary 16.20]. □

Proposition 5.2.9. *Let* $\boldsymbol{u} = (u_1, \ldots, u_p) \in \mathbb{C}^p$ *be any complex point. Then, for any*

$$(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}_{\boldsymbol{u}}(\pi_i, V(F^{\boldsymbol{A}})) \subset \mathbb{C}^{n+p}$$

we have the inclusion

$$\sqrt{\mathfrak{I}(i, F^{\boldsymbol{A}})} \subset \mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}).$$

Proof. First note that $\mathfrak{I}(i, F^{\boldsymbol{A}}) \subset \sqrt{\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})}$. Indeed, let $f \in \mathfrak{I}(i, F^{\boldsymbol{A}})$ and

$$\boldsymbol{\alpha} = (\boldsymbol{x}, \boldsymbol{l}) \in V(\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})) = \mathscr{W}_{\boldsymbol{u}}(\pi_i, V^{\boldsymbol{A}}).$$

Then $\sum_{i=1}^{p} u_i l_i = 1$, so that $\boldsymbol{l} \neq (0, \ldots, 0)$ is in the left null space and therefore the rank of $\mathrm{jac}_{\boldsymbol{x}}(F, i)$ is less than p. Therefore all minors are zero at $\boldsymbol{x}$ and $f(\boldsymbol{\alpha}) = f(\boldsymbol{x}, \boldsymbol{l}) = f(\boldsymbol{x}) = 0$, so that $f \in \sqrt{\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})}$ and $\mathfrak{I}(i, F^{\boldsymbol{A}}) \subset \sqrt{\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})}$.

Now, since by Corollary 5.2.8, $\sqrt{\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})} = \mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})$, we have the inclusion

$$\sqrt{\mathfrak{I}(i, F^{\boldsymbol{A}})} \subset \sqrt{\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})} = \mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}).$$

□

5.2.4 Application: proof of $\mathbf{G}_i'(1)$

Again let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ define a radical ideal and a smooth variety, and let $i \in \{1, \ldots, n-p+1\}$. We now assume that F satisfies $\mathbf{G}_i$, and we prove the following: *there exists a non-zero polynomial*

$$\Xi_{i,1} \in \mathbb{C}[S_1, \ldots, S_{i-1}]$$

of degree at most d^{3n} *such that if* $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ *does not cancel* $\Xi_{i,1}$*, then for any* $(\boldsymbol{x}, \boldsymbol{l}) \in \mathscr{W}(\pi_i, V(F))$*, the Jacobian of the system of polynomials*

$$(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p)))$$

has full rank $p + n - 1$*.*

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

$$(X_1 - S_1, \ldots, X_{i-1} - S_{i-1}, F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p)))\,.$$

Lemma 5.2.10. $\boldsymbol{0}$ *is a regular value of* $\boldsymbol{\Psi}$*.*

Proof. At all zeros $(\boldsymbol{x}, \boldsymbol{l}, \boldsymbol{\sigma})$ of $\boldsymbol{\Psi}$, the Jacobian matrix of $\boldsymbol{\Psi}$ has full rank $n+p-1$. Indeed, indexing columns by

$$X_1, \ldots, X_n, L_1, \ldots, L_p, S_1, \ldots, S_{i-1},$$

this matrix is equal to

$$\begin{bmatrix} \mathbf{I}_{i-1} & \boldsymbol{0}_{(i-1)\times(n+p-i+1)} & -\mathbf{I}_{i-1} \\ \mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left(F, \boldsymbol{l} \cdot \mathrm{jac}_{\boldsymbol{x}}(F, i)\right) & \boldsymbol{0}_{(p+n-i)\times(i-1)} \end{bmatrix}.$$

Recall that by $\boldsymbol{G}_i(2)$, the Jacobian matrix $\mathrm{jac}_{(\boldsymbol{x},\boldsymbol{l})}\left(F, \boldsymbol{l} \cdot \mathrm{jac}_{\boldsymbol{x}}(F, i)\right)$ has full rank $p + n - i$ at any zero $(\boldsymbol{x}, \boldsymbol{l})$. Hence, the entire matrix must have full rank $p + n - 1$. 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 4.2.1 that there exists a non-zero polynomial $\Xi_{i,1}$ in $\mathbb{C}[S_1, \ldots, S_{i-1}]$ of degree at most $d^{(n+p)+(n)} \leq d^{3n}$, with the property that, if $\Xi_{i,1}(\boldsymbol{\sigma}) \neq 0$ then at any root $(\boldsymbol{x}, \boldsymbol{l})$ of

$$(X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F, \mathbf{Lagrange}(F, i, (L_1, \ldots, L_p)))\,,$$

the Jacobian matrix of these equations has full rank $n + p - 1$.

Chapter 6

Proof of $\mathbf{G}_i'$

Let $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ define a radical ideal and a smooth variety, and let $i \in \{1, \ldots, n-p+1\}$.

6.1 Proof of $\mathbf{G}_i'(2)$

We assume that F satisfies $\mathbf{G}_i$, and we prove the following: *there exists a non-zero polynomial*

$$\Xi_{i,2} \in \mathbb{C}[S_1, \ldots, S_{i-1}]$$

of degree at most $2n(nd)^{n+1}$ *such that if* $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ *does not cancel* $\Xi_{i,2}$*, then*

$$\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \notin \pi_{i-1}(V(K) \cap W(\pi_i, V)),$$

where K *is the polynomial from 3.1.*

By Propositions 3.2.4 and 3.1.5, respectively, the degree of K is at most $2n^2d$ and the degree of $W(\pi_i, V)$ is at most $(nd)^n$. Therefore, by Bézout's bound,

$$\deg V(K) \cap W(\pi_i, V)) \leq 2n^2d(nd)^n = 2n(nd)^{n+1}.$$

Since degree will not increase after projection or closure,

$$\begin{aligned} \deg \overline{\pi_{i-1}(V(K) \cap W(\pi_i, V)))} &\leq \deg \pi_{i-1}(V(K) \cap W(\pi_i, V))) \\ &\leq \deg V(K) \cap W(\pi_i, V). \end{aligned}$$

Now take $\Xi_{i,2} \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ as any non-zero polynomial of degree at most $2n(nd)^{n+1}$ that vanishes on

$$\overline{\pi_{i-1}(V(K) \cap W(\pi_i, V)))}.$$

Then, since

$$\pi_{i-1}(V(K) \cap W(\pi_i, V))) \subset \overline{\pi_{i-1}(V(K) \cap W(\pi_i, V)))},$$

we have that if $\Xi_{i,2}(\sigma_1, \ldots, \sigma_{i-1}) \neq 0$ then

$$(\sigma_1, \ldots, \sigma_{i-1}) \notin \pi_{i-1}(V(K) \cap W(\pi_i, V)),$$

and $\boldsymbol{G}_i^{'}(2)$ is satisfied.

6.2 Proof of $\mathbf{G}_i^{'}$

Take $\Xi_{i,1}$ from Section 5.2.4 and $\Xi_{i,2}$ from Section 6.1 and put

$$\Xi_i := \Xi_{i,1}\Xi_{i,2} \in \mathbb{C}[S_1, \ldots, S_{i-1}].$$

The degree of Ξ_i is at most

$$\begin{aligned} \deg \Xi_{i,1} + \deg \Xi_{i,2} &\leq d^{3n} + 2n(nd)^{n+1} \\ &\leq (nd)^{3n} + 2n(nd)^{3n} \\ &\leq 3n(nd)^{3n}. \end{aligned}$$

And if we choose $\boldsymbol{\sigma} = (\sigma_1, \ldots, \sigma_{i-1}) \in \mathbb{C}^{i-1}$ with $\Xi_i(\boldsymbol{\sigma}) \neq 0$ then $\Xi_{i,1}(\boldsymbol{\sigma}) \neq 0$ and $\Xi_{i,2}(\boldsymbol{\sigma}) \neq 0$, so that, by Sections 5.2.4 and 6.1, respectively, F and $\boldsymbol{\sigma}$ satisfy both $\boldsymbol{G}_i^{'}(1)$ and $\boldsymbol{G}_i^{'}(2)$. Theorem 3.2.9 is now proven.

Chapter 7

Noether position

7.1 The hypersurface case: proof of $\mathbf{H}_i(2)$

Consider a squarefree polynomial $f \in \mathbb{C}[X_1, \ldots, X_n]$ and fix $i \in \{1, \ldots, n\}$. We prove that there exists a non-zero polynomial $\mathfrak{h}_i$ in n^2 variables and of degree at most $5n^2(2d)^{2n}$ such that if $\boldsymbol{A}$ does not cancel $\mathfrak{h}_i$, then $\boldsymbol{A}$ is invertible and satisfies both conditions in $\mathbf{H}_i$.

Consider again the matrix of indeterminates $\mathfrak{A} = (\mathfrak{A}_{j,k})_{1 \leq j,k \leq n}$ and the field $\mathbb{C}(\mathfrak{A})$, and define

$$f^{\mathfrak{A}} \in \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]$$

as $f(\mathfrak{A}\boldsymbol{X})$. In Section 5.1.1, we saw that $f^{\mathfrak{A}}$ satisfies $\mathbf{H}_i(1)$, so that $\mathfrak{I}(i, f^{\mathfrak{A}})$ defines a radical ideal, and $W(\pi_i, V(f^{\mathfrak{A}}))$ is equidimensional of dimension $i-1$. We now point out that $f^{\mathfrak{A}}$ also satisfies $\mathbf{H}_i(2)$.

Lemma 7.1.1. *The extension*

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

is integral.

Proof. Let $(\mathfrak{P}_\ell)_{1 \leq \ell \leq L}$ be the prime components of the radical ideal $\mathfrak{I}(i, f^{\mathfrak{A}})$. By [34, 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,

$$Q_j := \prod_{1 \leq \ell \leq L} q_{\ell,j}$$

is monic in X_j and satisfies $Q_j \in \mathfrak{I}(i, f^{\mathfrak{A}})$, 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 7.1.2. *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 $\mathfrak{I}(i, f^{\mathfrak{A}})$, and such that $\deg(\overline{P_j}) \leq (2d)^n$.*

Proof. We let $\mathfrak{L}^{\mathfrak{A}}$ denote the extension of $\mathfrak{I}(i, f^{\mathfrak{A}})$ given by

$$\mathfrak{L}^{\mathfrak{A}} := \mathfrak{I}(i, f^{\mathfrak{A}}) \cdot \mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1})[X_i, \ldots, X_n].$$

Then,

$$\mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1}) \to \mathbb{C}(\mathfrak{A}, X_1, \ldots, X_{i-1})[X_i, \ldots, X_n]/\mathfrak{L}^{\mathfrak{A}} \tag{7.1}$$

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

$$\mathbb{C}(\mathfrak{A})[X_1, \ldots, X_{i-1}] \to \mathbb{C}(\mathfrak{A})[X_1, \ldots, X_n]/\mathfrak{I}(i, f^{\mathfrak{A}}) \tag{7.2}$$

is integral; from this, Proposition 3.3.1 in [20] implies that it is actually a free module. Any basis of the latter is also a basis of (7.1); as a consequence, for j in $i, \ldots, n$, the characteristic polynomials of X_j in (7.1) or (7.2) are the same. Let P_j be the minimal polynomial of X_j in (7.1). The previous discussion implies that the characteristic polynomial χ_j of X_j in (7.1), 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 $\mathfrak{I}(i, f^{\mathfrak{A}})$ 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 $\mathfrak{I}(i, f^{\mathfrak{A}})$. Since the latter ideal is radical, we conclude that P_j is in $\mathfrak{I}(i, f^{\mathfrak{A}})$. This implies that $\overline{P_j}$ is in $\mathfrak{I}(i, f^{\mathfrak{A}})$ as well.

Now, consider the sequence of polynomials

$$\left(f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n} \right) \in \mathbb{C}[\mathfrak{A}, X_1, \ldots, X_n]^{n-i+1},$$

let $\mathfrak{W}$ be their zero-set, and let $\deg(\mathfrak{W})$ be its degree, in the sense of [22]. Proposition 1 in [33] 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 [22] gives

$$\deg(\overline{P_j}) \leq (2d)^{n-i+1} \leq (2d)^n.$$

□

Our next step is to give degree bounds on the coefficients appearing in the membership equality $\overline{P_j} \in \mathfrak{I}(i, f^{\mathfrak{A}})$. 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

$$\alpha_j = \sum_{\ell=1}^{n-i+1} C_{j,\ell} G_\ell + B_j(1 - \overline{P_j}T), \quad G_\ell \in \left\{ f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n} \right\}. \tag{7.3}$$

Let us then define

$$\mathfrak{h}_i := \mathfrak{h}_{i,1} \alpha_i \cdots \alpha_n D_i \cdots D_n,$$

where $\mathfrak{h}_{i,1}$ was defined in Section 5.1.1 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, $\mathfrak{h}_i$ is a non-zero polynomial in $\mathbb{C}[\mathfrak{A}]$; we will estimate its degree below.

Lemma 7.1.3. *Suppose that $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel $\mathfrak{h}_i$. Then $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_i$.*

Proof. By assumption, $\mathfrak{h}_{i,1}(\boldsymbol{A})$ 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 (7.3). 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 $\mathfrak{h}_i$, 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 [11], for which we first need to determine degree bounds, separately in $\boldsymbol{X}, T$ and $\mathfrak{A}$, of the polynomials in the membership relationship:

$$\begin{aligned}
\deg_{\boldsymbol{X},T}\left\{f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n}\right\} &\leq d;\\
\deg_{\mathfrak{A}}\left\{f^{\mathfrak{A}}, \frac{\partial f^{\mathfrak{A}}}{\partial X_{i+1}}, \ldots, \frac{\partial f^{\mathfrak{A}}}{\partial X_n}\right\} &\leq d;\\
\deg_{\boldsymbol{X},T}(1 - T\overline{P_j}) &\leq (2d)^n + 1;\\
\deg_{\mathfrak{A}}(1 - T\overline{P_j}) &\leq (2d)^n.
\end{aligned}$$

For each $j \in \{i, \ldots, n\}$, a direct application of [11, 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 5.1.1 that $\mathfrak{h}_{i,1}$ has degree at most $2nd^{2n}$, and all D_j's have degree at most $(2d)^n$. This gives the upper bound

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

This completes the proof of Theorem 3.2.1.

7.2 The general case: proof of $\mathbf{G}_i(3)$

Now let $F = (f_1, \ldots, f_p) \in \mathbb{C}[X_1, \ldots, X_n]^p$ define a radical ideal and a smooth variety, and fix $i \in \{1, \ldots, n-p+1\}$. We prove that there exists a non-zero polynomial Δ_i in $\mathbb{C}[\mathfrak{A}]$ of degree at most $6n^2(2d)^{5n}$ such that if $\boldsymbol{A}$ does not cancel Δ_i, then $F^{\boldsymbol{A}}$ satisfies $\mathbf{G}_i$.

Recall that we let $\boldsymbol{X} = (X_1, \ldots, X_n)$ be a sequence of variables, and for $l \in \{1, \ldots, n\}$ we let $\boldsymbol{X}_{\leq l}$ be the subsequence of variables $(X_1, \ldots, X_l)$. Consider again the $n \times n$ matrix of indeterminates

$$\mathfrak{A} = (\mathfrak{A}_{j,k})_{1 \leq j,k \leq n}$$

and the field $\mathbb{C}(\mathfrak{A})$, and define $F^{\mathfrak{A}} = (f_1^{\mathfrak{A}}, \ldots, f_p^{\mathfrak{A}})$ as

$$(f_1(\mathfrak{A}\boldsymbol{X}), \ldots, f_p(\mathfrak{A}\boldsymbol{X})) \in \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]^p.$$

7.2.1 Degree bounds for the integral dependence relationship

Lemma 7.2.1. *The extension*

$$\mathbb{C}(\mathfrak{A})[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]/\sqrt{\mathfrak{I}(\pi_i, F^{\mathfrak{A}})}$$

is integral.

Proof. Let $(\mathfrak{P}_\ell)_{1 \leq \ell \leq L}$ be the prime components of $\sqrt{\mathfrak{I}(\pi_i, F^{\mathfrak{A}})}$. By [34, Proposition 1], for all ℓ,

$$\mathbb{C}(\mathfrak{A})[\mathbf{X}_{\leq i-1}] \to \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]/\mathfrak{P}_\ell$$

is integral. Therefore polynomials $q_{\ell,j} \in \mathbb{C}(\mathfrak{A})[\mathbf{X}_{\leq i-1}, X_j]$ exist, all monic in X_j, with $q_{\ell,j}(X_j) \in \mathfrak{P}_\ell$ for each j in $\{i, \ldots, n-p+1\}$. Thence,

$$Q_j := \prod_{1 \leq \ell \leq L} q_{\ell,j}$$

is monic in X_j and satisfies $Q_j \in \sqrt{\mathfrak{I}(\pi_i, F^{\mathfrak{A}})}$, for each $j \in \{i, \ldots, n-p+1\}$. This proves our claim. □

Now let $\boldsymbol{u} \in \mathbb{C}^p$ be any complex number.

Corollary 7.2.2. *The extension*

$$\mathbb{C}(\mathfrak{A})[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]/(\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}) \cap \mathbb{C}(\mathfrak{A})[\boldsymbol{X}])$$

is integral.

Proof. By Lemma 7.2.1, polynomials $P_j \in \mathbb{C}(\mathfrak{A})[\boldsymbol{X}_{\leq i-1}, X_j]$ exist, all monic in X_j, with $P_j(X_j) \in \sqrt{\mathfrak{I}(\pi_i, F^{\mathfrak{A}})}$ for each j in $\{i, \ldots, n-p+1\}$. By Proposition 5.2.9,

$$\sqrt{\mathfrak{I}(\pi_i, F^{\mathfrak{A}})} \subset \mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}),$$

and therefore $P_j(X_j) \in \mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}})$ for each j in $\{i, \ldots, n-p+1\}$ and

$$\mathbb{C}(\mathfrak{A})[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]/(\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}) \cap \mathbb{C}(\mathfrak{A})[\boldsymbol{X}])$$

is integral. □

If P is any polynomial in $\mathbb{C}(\mathfrak{A})[\boldsymbol{X}]$, 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 $\mathbb{C}[\mathfrak{A}, \boldsymbol{X}]$.

Lemma 7.2.3. *For each $j \in \{i, \ldots, n-p+1\}$, there exists P_j in $\mathbb{C}(\mathfrak{A})[\boldsymbol{X}_{\leq i-1}, X_j]$, monic in X_j, with $\overline{P_j}$ in $\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}})$, and such that* $\deg(\overline{P_j}) \leq (2d)^{2n}$.

Proof. We let $\mathfrak{L}^{\mathfrak{A}}$ denote the extension of $\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}) \cap \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]$ given by

$$\mathfrak{L}^{\mathfrak{A}} = (\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}) \cap \mathbb{C}(\mathfrak{A})[\boldsymbol{X}]) \cdot \mathbb{C}(\mathfrak{A}, \boldsymbol{X}_{\leq i-1})[X_i, \ldots, X_n].$$

Then,

$$\mathbb{C}(\mathfrak{A}, \boldsymbol{X}_{\leq i-1}) \to \mathbb{C}(\mathfrak{A}, \boldsymbol{X}_{\leq i-1})[X_i, \ldots, X_n]/\mathfrak{L}^{\mathfrak{A}} \tag{7.4}$$

is an algebraic extension. Let $P_j \in \mathbb{C}(\mathfrak{A})(\mathbf{X}_{\leq i-1})[X_j]$ be the minimal polynomial of X_j in (7.4), and note that P_j is monic in X_j. By Corollary 7.2.2, $Q_j \in \mathbb{C}(\mathfrak{A})[\mathbf{X}_{\leq i-1}, X_j]$, exists, monic in X_j, with

$$Q_j(X_j) \in \mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}}) \cap \mathbb{C}(\mathfrak{A})[\boldsymbol{X}].$$

Hence, Q_j is also in the extension $\mathfrak{L}^{\mathfrak{A}}$, and thus P_j divides Q_j in $\mathbb{C}(\mathfrak{A})(\mathbf{X}_{\leq i-1})[X_j]$. We can therefore write

$$Q_j = P_j R_j, \qquad P_j, R_j \in \mathbb{C}(\mathfrak{A})(\mathbf{X}_{\leq i-1})[X_j] - \mathbb{C}(\mathfrak{A})(\mathbf{X}_{\leq i-1}).$$

It then follows by Gauss's lemma that

$$Q_j = p_j r_j, \qquad p_j, r_j \in \mathbb{C}(\mathfrak{A})[\mathbf{X}_{\leq i-1}][X_j] - \mathbb{C}(\mathfrak{A}),$$

and such that $\mu_j \in \mathbb{C}(\mathfrak{A})(\boldsymbol{X}_{\leq i-1})$ exists with

$$P_j = \mu_j p_j, \qquad R_j = \mu_j^{-1} r_j.$$

Since Q_j is monic in X_j, p_j and r_j must also be monic in X_j, and μ_j must be the coefficient of the highest degree term of P_j in X_j. Since P_j is monic in X_j, $\mu_j = 1$ and hence

$$P_j = 1 \cdot p_j = p_j \in \mathbb{C}(\mathfrak{A})[\mathbf{X}_{\leq i-1}][X_j].$$

Now, consider the polynomials $\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}})$:

$$\left(F^{\mathfrak{A}}, \mathbf{Lagrange}(F^{\mathfrak{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right)$$

in $\mathbb{C}[\mathfrak{A}, \boldsymbol{X}, \boldsymbol{L}]$, let $\mathfrak{W}$ be their zero-set, and let $\deg(\mathfrak{W})$ be its degree, in the sense of [22]. Proposition 1 in [33] implies that $\overline{P_j}$ has degree at most $\deg(\mathfrak{W})$. Since all polynomials defining $\mathfrak{W}$, seen in $\mathbb{C}[\mathfrak{A}, \boldsymbol{X}, \boldsymbol{L}]$, have degree at most $2d$, the Bézout inequality of [22] gives

$$\deg(\overline{P_j}) \leq (2d)^{p+n-i+1} \leq (2d)^{2n}.$$

□

7.2.2 Applying the effective Nullstellensatz

Now we apply the Nullstellensatz for $\overline{P_j}$ with the ideal membership for $\mathscr{I}_{\boldsymbol{u}}(i, F^{\mathfrak{A}})$. Let T be a new variable; applying the Nullstellensatz in $\mathbb{C}(\mathfrak{A})[\boldsymbol{X}, \boldsymbol{L}][T]$, and clearing denominators, we obtain the existence of α_j in $\mathbb{C}[\mathfrak{A}] - \{0\}$ and $C_{j,\ell}, B_j$ in $\mathbb{C}[\mathfrak{A}][\boldsymbol{X}, \boldsymbol{L}][T]$, such that

$$\alpha_j = \sum_{\ell=1}^{p+n-i+1} C_{j,\ell} G_\ell + B_j(1 - \overline{P_j} T),$$

$$G_\ell \in \left\{ F^{\mathfrak{A}}, \mathbf{Lagrange}(F^{\mathfrak{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right\}.$$

Let us then define

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

Lemma 7.2.4. *Suppose that $\boldsymbol{A} \in \mathbb{C}^{n \times n}$ does not cancel Δ_i. Then $F^{\boldsymbol{A}}$ satisfies $\boldsymbol{G}_i(1)$ and $\boldsymbol{G}_i(2)$, and the extension*

$$\mathbb{C}[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}[\boldsymbol{X}]/(\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}) \cap \mathbb{C}[\boldsymbol{X}])$$

is integral.

Proof. By assumption, $\Delta_{i,1}(\boldsymbol{A})$ is non-zero so that $\boldsymbol{A}$ is invertible, the ideal defined by $\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})$ is radical (this follows from Corollary 5.2.8, with $\boldsymbol{u} \in \mathbb{C}^p$ any complex point) and $W(\pi_i, V(F^{\boldsymbol{A}})$ is either empty or $(i-1)$-equidimensional. By Proposition 5.2.7 and the Jacobian Criterion [14, Corollary 16.20], we have that $\mathscr{W}_{\boldsymbol{u}}(\pi_i, V^{\boldsymbol{A}})$ is also either empty or $(i-1)$-equidimensional. Now, if it is empty, we are done. Otherwise, for $j = i, \ldots, n-p+1$, evaluate all indeterminates in $\mathfrak{A}$ at the corresponding entries of $\boldsymbol{A}$. This gives us an equality in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{L}, T]$ of the form

$$a_j = \sum_{\ell=1}^{p+n-i+1} c_{j,\ell} g_\ell + b_j(1 - p_j T), \quad g_\ell \in \left\{ F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right\},$$

for a_j in $\mathbb{C}$, polynomials $c_{j,\ell}$ and b_j in $\mathbb{C}[\boldsymbol{X}, \boldsymbol{L}, T]$ and p_j in $\mathbb{C}[\boldsymbol{X}_{\leq i-1}, X_j]$. 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

$$p_j{}^k \in \mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}) \cap \mathbb{C}[\boldsymbol{X}],$$

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, which implies that $\mathscr{W}_{\boldsymbol{u}}(\pi_i, V^{\boldsymbol{A}})$ is not empty). Since $\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})$ is radical, p_j is in $\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}})$. Repeating this for all j proves that

$$\mathbb{C}[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}[\boldsymbol{X}]/(\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}) \cap \mathbb{C}[\boldsymbol{X}])$$

is integral. □

To estimate the degree of Δ_i, what remains is to give an upper bound on the degrees of $\alpha_i, \ldots, \alpha_n$. This will come as an application of the effective Nullstellensatz given in [11], for which we first need to determine degree bounds, separately in $\boldsymbol{X}, \boldsymbol{L}, T$ and $\mathfrak{A}$, of the polynomials in the membership relationship. We have

$$\deg_{\boldsymbol{X},\boldsymbol{L},T} \left\{ F^{\mathfrak{A}}, \mathbf{Lagrange}(F^{\mathfrak{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right\} \leq d, \ \deg_{\boldsymbol{X},\boldsymbol{L},T}(1 - T\overline{P_j}) \leq (2d)^{2n} + 1,$$

and we have

$$\deg_{\mathfrak{A}} \left\{ F^{\mathfrak{A}}, \mathbf{Lagrange}(F^{\mathfrak{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right\} \leq d, \text{ and } \deg_{\mathfrak{A}}(1 - T\overline{P_j}) \leq (2d)^{2n}.$$

For each $j \in \{i, \ldots, n-p+1\}$, a direct application of [11, Theorem 0.5], gives

$$\deg(\alpha_j) \leq (2n+2)d^{2n+1}((2d)^{2n}+1);$$

we will use the slightly less precise bound

$$\deg(\alpha_j) \leq 4n(2d)^{4n}.$$

Since $\Delta_{i,1}$ has degree at most nd^{5n} and all D_j's have degree at most $(2d)^{2n}$, this gives the upper bound

$$\deg(\Delta_i) \leq nd^{5n} + 4n^2(2d)^{4n} + n(2d)^{2n} \leq 6n^2(2d)^{5n}.$$

7.2.3 Proof of $\mathbf{G}_i(3)$

Now assume that $\boldsymbol{u} \in \mathbb{C}^p$ satisfies $\boldsymbol{G}_i''$. It remains to show that if $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel Δ_i then

$$\mathbb{C}[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}[\boldsymbol{X}]/\mathfrak{I}(i, F^{\boldsymbol{A}})$$

is integral. By Lemma 7.2.4, the extension

$$\mathbb{C}[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}[\boldsymbol{X}]/(\mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}) \cap \mathbb{C}[\boldsymbol{X}])$$

is integral, and thus polynomials

$$Q_j \in \mathbb{C}[\boldsymbol{X}_{\leq i-1}, T]$$

exists, monic in T, for each $j \in \{i, \ldots, n-p+1\}$, with

$$Q_j(X_1, \ldots, X_{i-1}, X_j) \in \mathscr{I}_{\boldsymbol{u}}(i, F^{\boldsymbol{A}}) \cap \mathbb{C}[\boldsymbol{X}].$$

Since we are assuming that $\boldsymbol{u} \in \mathbb{C}^p$ satisfies $\boldsymbol{G}_i''$, by Proposition 3.2.5, $Q_j \in \sqrt{\mathfrak{I}(i, F^{\boldsymbol{A}})}$. Hence, there exists some $k \in \mathbb{N} - \{0\}$ with $Q_j^k \in \mathfrak{I}(i, F^{\boldsymbol{A}})$, where Q_j^k is monic in X_j, and therefore

$$\mathbb{C}[\boldsymbol{X}_{\leq i-1}] \to \mathbb{C}[\boldsymbol{X}]/\mathfrak{I}(i, F^{\boldsymbol{A}})$$

is integral.

This completes the proof of Theorem 3.2.8.

Chapter 8

Analysis of algorithms

In what follows, we now use the genericity statements proven in previous sections; they help us analyze the bit complexity and error probability of our algorithms by allowing us to quantify the various random parameter choices.

In each algorithm, we use [37, 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. 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.

8.1 The hypersurface cases

8.1.1 Bounding the degrees of the genericity polynomials

Let $\mathfrak{h}_i \in \mathbb{C}[\mathfrak{A}]$ be the polynomials from Theorem 3.2.1. Put $\mathfrak{h} := \prod_{i=1}^{n} \mathfrak{h}_i$ and note that

$$\deg \mathfrak{h} \leq \sum_{i=1}^{n} \deg \mathfrak{h}_i \leq 5n^3(2d)^{2n}. \tag{8.1}$$

If $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel $\mathfrak{h}$, 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 $\mathfrak{g}_i \in \mathbb{C}[S_1, \ldots, S_{i-1}]$ be the polynomials from

Theorem 3.2.2 applied to $f^{\boldsymbol{A}}$. Denote by $\mathfrak{g} := \prod_{i=1}^{n} \mathfrak{g}_i$, and note that

$$\deg \mathfrak{g} \leq \sum_{i=1}^{n} \deg \mathfrak{g}_i \leq nd^{2n}. \tag{8.2}$$

If $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel $\mathfrak{g}$, then $f^{\boldsymbol{A}}$ and $\boldsymbol{\sigma}$ satisfy $\mathbf{H}_i'$ for all $i \in \{1, \ldots, n\}$.

8.1.2 Algorithm analysis: the compact hypersurface case

Algorithm 1: CompactHypersurfaceCase

Input: $f \in \mathbb{Z}[X_1, \ldots, X_n]$ of degree at most d and height at most b with $V(f) \subset \mathbb{C}^n$ smooth and compact, and $0 < \epsilon < 1$

Output: a zero-dimensional parameterization that 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

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

and randomly choose $\boldsymbol{A} \in S^{n^2}$;

2 Build a straight-line program Γ_i that computes the equations

$$\left\{ f^{\boldsymbol{A}}, \frac{\partial f^{\boldsymbol{A}}}{\partial X_2}, \ldots, \frac{\partial f^{\boldsymbol{A}}}{\partial X_n} \right\}$$

3 Run [37, Algorithm 2] $k \geq \lg(2/\epsilon) + 1$ times with input Γ_i;

4 **return** the highest cardinality zero-dimensional parameterization from step 3.

Pseudocode. Algorithm 1 requires that the input system be given by a straight-line program. We build it (at Step 2) 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 [9]; this gives Γ_i.

If $f^{\boldsymbol{A}}$ satisfies $\mathbf{H}_1(1)$, then by the Jacobian criterion [14, Corollary 16.20], the parameterizations returned in step 4 are zero-dimensional. Then, correctness of Algorithm 1 is established in [4, 5].

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

1. We defined $S := \{1, 2, \ldots, \lceil 2\epsilon^{-1} 5n^3 (2d)^{2n} \rceil\}$ and therefore the height of any $a_{i,j} \in S$ is at most
$$\log 2/\epsilon + \log(5n^3(2d)^{2n}) \in O^{\sim}(\log 1/\epsilon + n \log d).$$
2. 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
$$O^{\sim}(b + d \log 1/\epsilon + dn).$$
All integer coefficients appearing in Γ_i satisfy the same bound.
3. As a result, after applying [37, Algorithm 2] $k = O(\log(1/\epsilon))$ times, the total boolean cost of the algorithm is
$$O^{\sim}(d^{3n+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$
where the polynomials in the output have degree at most d^n, and height at most
$$O^{\sim}(d^{n+1}(b + \log 1/\epsilon)).$$

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

Error probability. As we argued above, the algorithm is guaranteed to succeed, as long as our call to Algorithm 2 in [37] succeeds. Now, by construction of
$$S := \left\{1, 2, \ldots, \lceil 2\epsilon^{-1} 5n^3 (2d)^{2n} \rceil\right\}$$
where $\boldsymbol{A} \in S^{n^2}$ is randomly chosen, we have
$$\mathbb{P}[\mathfrak{h}(\boldsymbol{A}) = 0] \leq \frac{\deg \mathfrak{h}}{|S|} = \epsilon/2.$$

Let $\mathscr{E}$ be the event that the parameterization returned in step 4 of Algorithm 1 is correct. Then, the probability of success is at least

$$\mathbb{P}[\mathfrak{h}(\boldsymbol{A}) \neq 0] \times \mathbb{P}[\mathscr{E} \mid \mathfrak{h}(\boldsymbol{A}) \neq 0].$$

Set $k = \lg(2/\epsilon) + 1$ so that

$$1 - 2^{-k} \geq 1 - \epsilon/2,$$

and therefore

$$\begin{aligned}
\mathbb{P}[\text{success}] &\geq (1 - \epsilon/2)\mathbb{P}[\mathscr{E} \mid \mathfrak{h}(\boldsymbol{A}) \neq 0] \\
&\geq (1 - \epsilon/2)(1 - 2^{-k}) \\
&\geq (1 - \epsilon/2)(1 - \epsilon/2) \\
&\geq 1 - \epsilon.
\end{aligned}$$

This finishes the proof of theorem 1.3.1.

8.1.3 Algorithm analysis: the hypersurface case, without compactness

Algorithm 2: HypersurfaceCase

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 Γ_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 [37, Algorithm 2] $k \geq \lg(3n/\epsilon)$ times with input Γ_i;

5 Let $\mathscr{Q}_i$ be the highest cardinality zero-dimensional parameterization returned in step 4 ;

6 **return** $[\mathscr{Q}_1, \ldots, \mathscr{Q}_n]$.

Pseudocode. 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 [34] establishes correctness for Algorithm 2.

Bit complexity. The following lists the costs for each step of Algorithm 2:

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 $\sigma_k \in T$ is at most the same.

2. 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
$$O^{\sim}(b + d \log 1/\epsilon + dn).$$

All integer coefficients appearing in Γ_i satisfy the same bound.

3. As a result, after applying [37, Algorithm 2] k times for each index i, with $k = O(\log n + \log 1/\epsilon)$, the total boolean cost of the algorithm is

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

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

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

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

Error probability. Algorithm 2 (HypersurfaceCase) is also guaranteed to succeed, as long as our call to Algorithm 2 in [37] succeeds. 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

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

and

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

Let $\mathscr{E}$ now be the event that the parameterizations $[\mathscr{Q}_1, \ldots, \mathscr{Q}_n]$ returned in step 6 of Algorithm 2 are correct. Then, the probability of success is equal to

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

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

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

by Bernoulli's inequality. Therefore,

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

This finishes the proof of Theorem 1.3.2.

8.2 The general case

8.2.1 Bounding the degrees of the genericity polynomials

Let $\Delta_i \in \mathbb{C}[\mathfrak{A}]$ be the polynomials from Theorem 3.2.8. Denote by $\Delta := \prod_{i=1}^{n-p+1} \Delta_i$, and note that

$$\deg \Delta \leq \sum_{i=1}^{n-p+1} \deg \Delta_i \leq 6n^3(2d)^{5n}. \tag{8.3}$$

If $\boldsymbol{A} \in \mathbb{C}^{n\times n}$ does not cancel Δ, then $\boldsymbol{A}$ is invertible and $F^{\boldsymbol{A}}$ satisfies $\mathbf{G}_i$ for all i in $\{1,\ldots,n-p+1\}$. 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 3.2.9 applied to $F^{\boldsymbol{A}}$. Denote by $\Xi := \prod_{i=1}^{n-p+1} \Xi_i$, and note that

$$\deg \Xi \leq \sum_{i=1}^{n-p+1} \deg \Xi_i \leq 3n^2(nd)^{3n}. \tag{8.4}$$

If $\boldsymbol{\sigma} \in \mathbb{C}^{i-1}$ does not cancel Ξ, then $F^{\boldsymbol{A}}$ and $\boldsymbol{\sigma}$ satisfy $\mathbf{G}_i^{'}$ for all $i \in \{1,\ldots,n-p+1\}$. And finaly, denote by $\Upsilon := \prod_{i=1}^{n-p+1} \Upsilon_i$, and note that

$$\deg \Upsilon \leq \sum_{i=1}^{n-p+1} \deg \Upsilon_i \leq n(nd)^n. \tag{8.5}$$

If $\boldsymbol{u} \in \mathbb{C}^p$ does not cancel Υ, then $\boldsymbol{u}$ satisfies $\mathbf{G}_i^{''}$ for all $i \in \{1,\ldots,n-p+1\}$.

8.2.2 Analysis of the algorithm

Pseudocode. Algorithm 3 (GeneralCase) also requires that the input system be given by a straight-line program. And we again build it (at Step 3) in the straightforward manner: given $F = (f_1,\ldots,f_p)$ in $\mathbb{C}[X_1,\ldots,X_n]$, we can build a straight-line program that evaluates each f_i in $O(d^n)$ operations, by computing all monomials of degree up to d, multiplying them by the corresponding coefficients in f_i, and adding results. And as said already, to obtain a straight-line program for $f_i^{\boldsymbol{A}}$, we add $O(n^2)$ steps corresponding to the application of the change of variables $\boldsymbol{A}$. The number of operations here is thus

$$O(nd^n + n^2) = O^{\sim}(d^n).$$

From this, we can compute and evaluate the required partial derivatives in the Jacobian of $F^{\boldsymbol{A}}$ in

$$O(n^2 d^n) = O^{\sim}(d^n)$$

operations [9]. Then, the matrix vector product with the vector of Lagrange multipliers adds a cost that is polynomial in n, and which we can therefore neglect in the soft oh notation. Finally, we add the linear equations $X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}$; this gives Γ_i, and the total cost for computing the straight line program is $O^{\sim}(d^n)$.

Algorithm 3: GeneralCase

Input: $F = (f_1, \ldots, f_p) \in \mathbb{Z}[X_1, \ldots, X_n]^p$ with $\deg(f_i) \leq d$ and $\mathrm{ht}(f_i) \leq b$, 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 at least $1 - \epsilon$

1 Construct

$$S := \{1, 2, \ldots, \lceil 4\epsilon^{-1} 6n^3 (2d)^{5n} \rceil\},$$

$$T := \{1, 2, \ldots, \lceil 4\epsilon^{-1} 3n^2 (nd)^{3n} \rceil\},$$

and

$$R := \{1, 2, \ldots, \lceil 4\epsilon^{-1} (nd)^n \rceil\},$$

and randomly choose $\boldsymbol{A} \in S^{n^2}, \boldsymbol{\sigma} \in T^{n-1}$, and $\boldsymbol{u} \in R^p$;

2 **for** $i \leftarrow 1$ **to** n **do**

3 Build a straight-line program Γ_i that computes the equations

$$\left\{ X_1 - \sigma_1, \ldots, X_{i-1} - \sigma_{i-1}, F^{\boldsymbol{A}}, \mathbf{Lagrange}(F^{\boldsymbol{A}}, i, (L_1, \ldots, L_p)), \sum_{i=1}^{p} u_i L_i - 1 \right\}$$

4 Run [37, Algorithm 2] $k \geq \lg(4n/\epsilon)$ times with input Γ_i;

5 Let $\mathscr{Q}_i$ be the highest cardinality zero-dimensional parameterization returned in step 4;

6 Compute a parameterization of the projection of $\mathscr{Q}_i$ onto the $\boldsymbol{X}$-space, and let $\mathscr{Q}_i'$ denote this new parameterization ;

7 **return** $[\mathscr{Q}_1', \ldots, \mathscr{Q}_n']$.

If $F^{\boldsymbol{A}}$ satisfies $\mathbf{G}_i$ and $F^{\boldsymbol{A}}$ and $\boldsymbol{\sigma}$ satisfy $\mathbf{G}_i'$ then Theorem 2 in [34] tells us that the parameterizations returned in step 5 are zero dimensional. Then, if $\boldsymbol{u}$ satisfies $\boldsymbol{G}_i''$ for all

$i \in \{1, \ldots, n-p+1\}$, Proposition 3.3.1 gives us that the polar varieties are contained in the projections of the Lagrangian systems, and therefore Theorem 2 in [34] also establishes that the parameterizations returned in step 7 will contain one point on each connected component of $V \cap \mathbb{R}^n$.

Bit complexity. The following lists the costs for each step of Algorithm 3:

(1) We defined $S := \{1, 2, \ldots, \lceil 4\epsilon^{-1} 6n^3 (2d)^{5n} \rceil\}$ and therefore the height of any $a_{i,j} \in S$ is at most

$$\log 4/\epsilon + \log(6n^3(2d)^{5n}) \in O^\sim(\log 1/\epsilon + n \log d).$$

Since $|R| < |T| < |S|$, we also have that the height of any $\sigma_k \in T$ and $u_l \in R$ is at most the same.

(3) After computing the partial derivatives in the Jacobian matrix, the height grows by at most another factor of $\log d$. Thus, all polynomials in the system considered at Step 3 have height

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

All integer coefficients appearing in Γ_i satisfy the same bound.

(4) As a result, after applying [37, Algorithm 2] k times for each index i, with $k = O(\log n + \log 1/\epsilon)$, the total boolean cost of the algorithm is

$$O^\sim(d^{3n+2p+1}(\log 1/\epsilon)(b + \log 1/\epsilon))$$

where the polynomials in the output have degree at most d^{n+p}, and height at most

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

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

Error probability. As we argued above, Algorithm 3 is guaranteed to succeed, as long as our call to Algorithm 2 in [37] succeeds. Now, by construction of

$$S := \{1, 2, \ldots, \lceil 4\epsilon^{-1} 6n^3 (2d)^{5n} \rceil\},$$

$$T := \{1, 2, \ldots, \lceil 4\epsilon^{-1} 3n^2 (nd)^{3n} \rceil\},$$

and

$$R := \{1, 2, \ldots, \lceil 4\epsilon^{-1} n (nd)^{n} \rceil\},$$

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

$$\mathbb{P}[\Delta(\boldsymbol{A}) = 0] \leq \frac{\deg \Delta}{|S|} = \epsilon/4,$$

$$\mathbb{P}[\Xi(\boldsymbol{\sigma}) = 0] \leq \frac{\deg \Xi}{|T|} = \epsilon/4$$

and

$$\mathbb{P}[\Upsilon(\boldsymbol{u}) = 0] \leq \frac{\deg \Upsilon}{|R|} = \epsilon/4.$$

Let $\mathscr{E}$ be the event that the parameterizations $[\mathscr{Q}_1', \ldots, \mathscr{Q}_n']$ returned in step 7 of Algorithm 3 are correct. Then, the probability of success is equal to

$$\begin{aligned}&\mathbb{P}[\Delta(\boldsymbol{A}) \neq 0] \times \mathbb{P}[\Xi(\boldsymbol{\sigma}) \neq 0 \mid \Delta(\boldsymbol{A}) \neq 0] \times \mathbb{P}[\Upsilon(\boldsymbol{u}) \neq 0 \mid \Delta(\boldsymbol{A})\Xi(\boldsymbol{\sigma}) \neq 0] \\ &\times \mathbb{P}[\mathscr{E} \mid \Delta(\boldsymbol{A})\Xi(\boldsymbol{\sigma})\Upsilon(\boldsymbol{u}) \neq 0].\end{aligned}$$

Set $k = \lg(4n/\epsilon)$ so that

$$(1 - 2^{-k})^n = (1 - \epsilon/(4n))^n \geq 1 - \epsilon/4,$$

by Bernoulli's inequality. Therefore,

$$\begin{aligned}\mathbb{P}[\text{success}] &\geq (1 - \epsilon/4)(1 - \epsilon/4)(1 - \epsilon/4)\mathbb{P}[\mathscr{E} \mid \Delta(\boldsymbol{A})\Xi(\boldsymbol{\sigma})\Upsilon(\boldsymbol{u}) \neq 0] \\ &\geq (1 - \epsilon/4)(1 - \epsilon/4)(1 - \epsilon/4)(1 - 2^{-k})^n \\ &\geq (1 - \epsilon/4)(1 - \epsilon/4)(1 - \epsilon/4)(1 - \epsilon/4) \\ &\geq 1 - \epsilon.\end{aligned}$$

This finishes the proof of theorem 1.3.4.

Chapter 9

Conclusions

9.1 Contributions

Our main contributions were to analyze precisely what conditions on our parameter choices guarantee success. And we accomplished this by revisiting key ingredients in the proofs given in [4] and [34], and giving quantitative versions of these results, bounding the degrees of the hypersurfaces we have to avoid.

9.2 Further work

This work should be seen as a step toward the analysis of further randomized algorithms in real algebraic geometry. In particular, randomized algorithms for deciding *connectivity queries* on smooth and bounded algebraic sets have been developed in a series of papers [35, 38], and could be revisited using the techniques introduced here. Indeed, we have accomplished some of the work that is needed for these references; these algorithms require Noether position for polar varieties and transversality for algebraic sets.

References

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

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

[3] B. Bank, M. Giusti, J. Heintz, L. Lehmann, and L.-M. Pardo. Algorithms of intrinsic complexity for point searching in compact real singular hypersurfaces. *Foundations of Computational Mathematics*, 12:75–122, 2012.

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

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

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

[7] B. Bank, M. Giusti, and M. Safey El Din E. Schost Heintz, J. On the geometry of polar varieties. *Communication and Computing*, 21(1):33–83, 2010.

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

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

[10] J. Bochnak, M. Coste, and M.-F. Roy. *Real algebraic geometry*. Ergebnisse der Mathematik und ihrer Grenzgebite. Springer-Verlag, 1998.

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

[12] J. Canny. *On the complexity of robot motion planning*. The MIT Press, 1987.

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

[14] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1st. edition, 1995.

[15] J. Elliott and E. Schost. Bit complexity for critical point computation in smooth and compact real hypersurfaces. *ACM Communications in Computer Algebra*, 55(3):114–117, Dec. 2019.

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

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

[18] 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.

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

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

[21] D. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Comput.*, 5:37–64, 1988.

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

[23] J. Heintz and C.P. Schnorr. Testing polynomials which are easy to compute. *STOC '80: Proceedings of the twelfth annual ACM symposium on Theory of computing*, 1980.

[24] M. Giesbrecht J. Elliott and E. Schost. On the bit complexity of finding points in connected components of a smooth real hypersurface. *ISSAC*, page 170–177, July 2020.

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

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

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

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

[29] D. Mumford. *Algebraic Geometry 1 : complex algebraic varieties*. Classics in Mathematics. Springer, 1976.

[30] R. Piene. Polar classes of singular varieties. In *Annales Scientifiques de l'École Normale Supérieure*, volume 11, pages 247–276, 1978.

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

[32] 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.

[33] E. Schost. Computing parametric geometric resolutions. *Applicable Algebra in Engineering, Communication and Computing*, 5:349–393, July 2002.

[34] E. Schost and M. Safey El Din. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. *ISSAC*, pages 224–231, Aug 2003.

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

[36] E. Schost and M. Safey El Din. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of the ACM*, 63(6):1–48, February 2017.

[37] E. Schost and M. Safey El Din. Bit complexity for multi-homogeneous system solving application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, May 2018.

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

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

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