Polar, bipolar and copolar varieties: Real solving of algebraic varieties with intrinsic complexity[1]

Bernd Bank [2], Marc Giusti [3], Joos Heintz [4]

November 8, 2012

Abstract

This survey covers a decade and a half of joint work with L. Lehmann, G. M. Mbakop, and L. M. Pardo. We address the problem of finding a smooth algebraic sample point for each connected component of a real algebraic variety, being only interested in components which are generically smooth locally complete intersections. The complexity of our algorithms is essentially polynomial in the degree of suitably defined generalized polar varieties and is therefore intrinsic to the problem under consideration.

1 Introduction

The modern concept of polar varieties was introduced in the 1930's by F. Severi ([34], [33]) and J. A. Todd ([37], [36]), while the intimately related

[1]Research partially supported by the following Argentinian, French and Spanish grants: CONICET PIP 2461/01, UBACYT 20020100100945, PICT–2010–0525, Digiteo DIM 2009–36HD "Magix", ANR-2010-BLAN-0109-04 "LEDA", MTM2010-16051.

[2]Humboldt-Universität zu Berlin, Institut für Mathematik, 10099 Berlin, Germany.
bank@math.hu-berlin.de

[3]CNRS, École Polytechnique, Lab. LIX, 91228 Palaiseau Cedex, France.
marc.giusti@polytechnique.fr

[4]Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Univ., Pab.I, 1428 Buenos Aires, Argentina, and Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, Avda. de los Castros, s/n, E-39005 Santander, Spain.
joos@dc.uba.ar & joos.heintz@unican.es

notion of a reciprocal curve goes back to the work of J.-V. Poncelet in the period of 1813–1829. As pointed out by Severi and Todd, generic polar varieties have to be understood as being organized in certain equivalence classes which embody relevant geometric properties of the underlying algebraic variety S. This view led to the consideration of rational equivalence classes of the generic polar varieties. For historical details we refer to [29, 35].

About 16 years ago (classic) polar varieties became our fundamental tool to tackle the task of real equation solving with a new view. We used them for the design of a pseudo-polynomial computer procedure with an intrinsic complexity bound which finds for a given complete intersection variety S with a smooth compact real trace $S_{\mathbb{R}}$ algebraic sample points for each connected component of $S_{\mathbb{R}}$ if there are such points ([1, 2]).
Actually the geometric resolution of polar varieties, thanks to the algoritm `Kronecker` developed by the TERA-group [16, 18, 19, 24], led directly to a good pseudo–polynomial complexity.
Then we dropped successively the hypothesis on compactness of $S_{\mathbb{R}}$ (leading to dual polar varieties [3, 4]) and eventually the hypothesis on smoothness of $S_{\mathbb{R}}$.
The presence of real singularities of $S_{\mathbb{R}}$ guided us to the introduction of copolar incidence and finally to bipolar varieties ([6, 7]).
.

2 Notations and statement of results

2.1 Notations

Let $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ be the fields of rational, real and complex numbers, respectively, let $X := (X_1, \ldots, X_n)$ be a vector of indeterminates over $\mathbb{C}$ and let $F_1, \ldots, F_p$ be a regular sequence of polynomials in $\mathbb{Q}[X]$ defining a closed, $\mathbb{Q}$–definable subvariety S of the n–dimensional complex affine space $\mathbb{A}^n := \mathbb{C}^n$. Thus S is a non–empty equidimensional affine variety of dimension $n-p$, i.e., each irreducible component of S is of dimension $n-p$. Said otherwise, S is a closed subvariety of $\mathbb{A}^n$ of pure codimension p (in $\mathbb{A}^n$).
Let $\mathbb{A}^n_{\mathbb{R}} \cong \mathbb{R}^n$ be the n–dimensional real affine space. We denote by $S_{\mathbb{R}} := S \cap \mathbb{A}^n_{\mathbb{R}}$ the real trace of the complex variety S. Moreover, we denote by $\mathbb{P}^n$ the n–dimensional complex projective space and by $\mathbb{P}^n_{\mathbb{R}}$ its real counterpart. We shall use also the following notations:

$$\{F_1 = 0, \ldots, F_p = 0\} := S \text{ and } \{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}} := S_{\mathbb{R}}.$$

We call the regular sequence $F_1, \ldots, F_p$ *reduced* if the ideal $(F_1, \ldots, F_p)$ generated in $\mathbb{Q}[X]$ is the ideal of definition of the affine variety S, i.e., if $(F_1, \ldots, F_p)$ is radical. We call $(F_1, \ldots, F_p)$ *strongly reduced* if for any index $1 \leq k \leq p$ the ideal $(F_1, \ldots, F_k)$ is radical. Thus, a strongly reduced regular sequence is always reduced.
A point x of $\mathbb{A}^n$ is called $(F_1, \ldots, F_p)$–*regular* if the Jacobian $J(F_1, \ldots, F_p) := \left[\frac{\partial F_j}{\partial X_k}\right]_{\substack{1 \leq j \leq p \\ 1 \leq k \leq n}}$ has maximal rank p at x. Observe, that for each *reduced* regular sequence $F_1, \ldots, F_p$ defining the variety S, the locus of $(F_1, \ldots, F_p)$–regular points of S is the same. In this case we call an $(F_1, \ldots, F_p)$–regular point of S simply *regular* (or *smooth*) or we say that S is regular (or smooth) at x. The set S_{reg} of regular points of S is called the *regular locus*, whereas $S_{sing} := S \setminus S_{reg}$ is called the *singular locus* of S. Remark that S_{reg} is a non–empty open and S_{sing} a proper closed subvariety of S. We say that a connected component C of $S_{\mathbb{R}}$ is *generically smooth* if C contains a smooth point.
We are going to use the expression *generic* according to Thom's terminology. A property that depends on parameters belonging to a certain configuration space Ω is called *generic* if there exists an Zariski open and dense subset of Ω, where the parameters are taken from, to insure the property.

We suppose now that there are natural numbers d, L and ℓ and an essentially division–free arithmetic circuit β in $\mathbb{Q}[X]$ with p output nodes such that the following conditions are satisfied.

- The degrees $\deg F_1, \ldots, \deg F_p$ of the polynomials $F_1, \ldots, F_p$ are bounded by d.
- The p output nodes of the arithmetic circuit β represent the polynomials $F_1, \ldots, F_p$ by evaluation.
- The size and the non–scalar depth of the arithmetic circuit β are bounded by L and ℓ, respectively.

For the terminology and basic facts concerning arithmetic circuits we refer to [10, 12, 18].

2.2 Statement of the results

For the sake of simplicity we suppose that the variables $X_1, \ldots, X_n$ are in generic position with respect to the variety S. Observe that we allow $S_{\mathbb{R}}$ to have singular points.

In this paper we comment a series of complexity results which concern the computational task to find in each generically smooth connected component of $S_{\mathbb{R}}$ a suitably encoded smooth point.
The most general result we are going to present is the following statement about the *existence* of an algorithm with certain properties (see Theorem 6.2 below).
For each $1 \leq i \leq n-p$ there exists a *non–uniform deterministic* or *uniform probabilistic* procedure Π_i and an invariant δ_i satisfying the following specification.

(*i*) The invariant δ_i is a positive integer depending on $F_1, \ldots, F_p$ and having asymptotic order not exceeding $(n^n\, d)^{O(n)}$. We call δ_i the *degree of the real interpretation of the equation system* $F_1 = 0, \ldots, F_p = 0$.

(*ii*) The algorithm Π_i decides on input β whether the variety S contains a smooth real point and, if it is the case, produces for each generically smooth connected component of S a suitably encoded real algebraic sample point.

(*iii*) In order to achieve this goal, the algorithm Π_i performs on input β a computation in $\mathbb{Q}$ with $\binom{n}{p} L (n\, d)^{O(1)} (\min\{(n\, d)^{c\, n}, \delta_i\})^2$ arithmetic operations (additions, subtractions, multiplications and divisions) which become organized in non–scalar depth $O(n(\ell + \log n\, d) \log \delta_i)$ with respect to the parameters of the arithmetic circuit β (here $c > 0$ is a suitable universal constant).

Although we were not able to derive a better worst case upper bound as $(n^n\, d)^{O(n)}$ for the invariant δ_i (see Propositions 6.1 and 6.3 below) the worst case complexity of the procedure Π_i meets the already known extrinsic bound of $(n\, d)^{O(n)}$ for the elimination problem under consideration (compare the original papers [20, 11, 30, 25, 26, 27, 31, 8] and the comprehensive book [9]).
The complexity of the procedure Π_i depends polynomially on the *extrinsic* parameters L, ℓ, n and d and on the degree δ_i of the real interpretation of the equation system $F_1 = 0, \ldots, F_p = 0$ which represents an *intrinsic* parameter measuring the input size of our computational task. In this sense we say that the procedure Π_i is of *intrinsic complexity*.
Since for fixed p the complexity $\binom{n}{p} L (n\, d)^{O(1)} (\min\{(n\, d)^{c\, n}, \delta_i\})^2$ is polynomial in all its parameters, including the intrinsic parameter δ_i, we say that the procedure Π_i is *pseudo-polynomial*. In view of the main outcome of [22, 23] intrinsic complexity and pseudo-polynomiality constitute the best runtime

behavior of Π_i that can be expected for elimination algorithms implemented by rules of software engineering.
The above result is the consequence of a reduction to the case that $S_{\mathbb{R}}$ is smooth, where a similar, but somewhat simpler, complexity statement is true (see Theorem 4.1 below). For this reduction we considered in [7] a new type of geometrical objects, called *copolar incidence* and *bipolar* varieties.

First complexity results in this direction were obtained for the case that $S_{\mathbb{R}}$ is smooth and compact using *classic polar varieties* [1, 2]. In order to treat the smooth unbounded case we introduced in [3, 4] the concept of *dual polar varieties*.
In the present paper we put emphasis on the geometrical ideas which together with the `Kronecker` algorithm [16, 18, 19, 24], that solves polynomial equation systems over the complex numbers, lead to our complexity statements.

3 Polar varieties

Let notations be as in Subsection 2.1. Let $F_1, \ldots, F_p \in \mathbb{Q}[X]$ be a reduced regular sequence defining a (non–empty) subvariety S of $\mathbb{A}^n$ of pure codimension p.
Let $1 \leq i \leq n-p$ and let $a := [a_{k,l}]_{\substack{1 \leq k \leq n-p-i+1 \\ 0 \leq l \leq n}}$ be a complex $((n-p-i+1) \times (n+1)$–matrix and suppose that $[a_{k,l}]_{\substack{1 \leq k \leq n-p-i+1 \\ 1 \leq l \leq n}}$ has maximal rank $n-p-i+1$.
In case $(a_{1,0}, \ldots, a_{n-p-i+1,0}) = 0$ we denote by $\underline{K}(a) := \underline{K}^{n-p-i}(a)$ and in case $(a_{1,0}, \ldots, a_{n-p-i+1,0}) \neq 0$ by $\overline{K}(a) := \overline{K}^{n-p-i}(a)$ the $(n-p-i)$–dimensional linear subvarieties of the projective space $\mathbb{P}^n$ which for $1 \leq k \leq n-p-i+1$ are spanned by the points $(a_{k,0} : a_{k,1} : \cdots : a_{k,n})$.
The hyperplane at infinity of $\mathbb{P}^n$ is the set of points whose first coordinate is zero. It determines an embedding of $\mathbb{A}^n$ into $\mathbb{P}^n$. The classic and the dual ith polar varieties of S associated with the linear varieties $\underline{K}(a)$ and $\overline{K}(a)$, respectively, are geometrically defined as the Zariski closures of the set of points of S, where the tangent space of S is not transversal to the affine traces of $\underline{K}(a)$ and $\overline{K}(a)$, respectively.
Algebraically, the classic and the dual ith polar varieties of S associated with the linear varieties $\underline{K}(a)$ and $\overline{K}(a)$, respectively, can be described as the closures of the loci of the smooth points of S where all $(n-i+1)$–minors

of the respective polynomial $((n-i+1)\times n)$–matrix

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1} & \cdots & a_{1,n} \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1} & \cdots & a_{n-p-i+1,n} \end{bmatrix}$$

and

$$\begin{bmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \cdots & \frac{\partial F_p}{\partial X_n} \\ a_{1,1}-a_{1,0}X_1 & \cdots & a_{1,n}-a_{1,0}X_n \\ \vdots & \vdots & \vdots \\ a_{n-p-i+1,1}-a_{n-p-i+1,0}X_1 & \cdots & a_{n-p-i+1,n}-a_{n-p-i+1,0}X_n \end{bmatrix}$$

vanish.

If a is a real $((n-p-i+1)\times(n+1)$–matrix, we denote the real traces of the polar varieties $W_{\underline{K}(a)}(S)$ and $W_{\overline{K}(a)}(S)$ by

$$W_{\underline{K}(a)}(S_{\mathbb{R}}) := W_{\underline{K}^{n-p-i}(a)}(S_{\mathbb{R}}) := W_{\underline{K}(a)}(S)\cap \mathbb{A}^n_{\mathbb{R}}$$

and

$$W_{\overline{K}(a)}(S_{\mathbb{R}}) := W_{\overline{K}^{n-p-i}(a)}(S_{\mathbb{R}}) := W_{\overline{K}(a)}(S)\cap \mathbb{A}^n_{\mathbb{R}}$$

and call them the real polar varieties.

Observe that this definition of classic and dual polar varieties may be extended to the case that there is given a Zariski open subset O of $\mathbb{A}^n$ such that the equations $F_1=0,\ldots,F_p=0$ intersect transversally at any of their common solutions in O and that S is now the locally closed subvariety of $\mathbb{A}^n$ given by

$$S := \{F_1=0,\ldots,F_p=0\}\cap O,$$

which is supposed to be non-empty.

In Section 6 we shall need this extended definition of polar varieties in order to establish the notion of a bipolar variety of a given reduced complete intersection. For the moment let us suppose again that S is the closed subvariety of $\mathbb{A}^n$ defined by the reduced regular sequence $F_1,\ldots,F_p$.

In [3] and [4] we have introduced the notion of dual polar varieties of S (and $S_{\mathbb{R}}$) and motivated by geometric arguments the calculatory definition of these objects. Moreover, we have shown that, for a complex $((n-p-i+1)\times(n+1))$–matrix $a=[a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 0\le l\le n}}$ with $[a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 1\le l\le n}}$ *generic*, the polar varieties $W_{\underline{K}(a)}(S)$ and $W_{\overline{K}(a)}(S)$ are either empty or of pure codimension i in

S. Further, we have shown that $W_{\underline{K}(a)}(S)$ and $W_{\overline{K}(a)}(S)$ are normal and Cohen–Macaulay (but for $1 < p \leq n$ not necessarily smooth) at any of their $(F_1, \ldots, F_p)$–regular points (see [5], Corollary 2 and Section 3.1). This motivates the consideration of the so–called *generic* polar varieties $W_{\underline{K}(a)}(S)$ and $W_{\overline{K}(a)}(S)$, associated with complex $((n-p-i+1) \times (n+1))$–matrices a which are generic in the above sense, as invariants of the complex variety S (independently of the given equation system $F_1 = 0, \ldots, F_p = 0$). However, when a generic $((n-p-i+1) \times (n+1))$–matrix a is real, we cannot consider $W_{\underline{K}(a)}(S_{\mathbb{R}})$ and $W_{\overline{K}(a)}(S_{\mathbb{R}})$ as invariants of the real variety $S_{\mathbb{R}}$, since for suitable real generic $((n-p-i+1) \times (n+1))$–matrices these polar varieties may turn out to be empty, whereas for other real generic matrices they may contain points (see [5], Theorem 1 and Corollary 2 and [6], Theorem 8 and Corollary 9).
In case that $S_{\mathbb{R}}$ is smooth and a is a real $((n-p-i+1) \times (n+1))$–matrix, the real dual polar variety $W_{\overline{K}(a)}(S_{\mathbb{R}})$ contains at least one point of each connected component of $S_{\mathbb{R}}$, whereas the classic (complex or real) polar varieties $W_{\underline{K}(a)}(S)$ and $W_{\underline{K}(a)}(S_{\mathbb{R}})$ may be empty (see [3] and [4], Proposition 2).

4 The smooth case

In this section we suppose that $S_{\mathbb{R}}$ is smooth. We choose a generic rational $((n-p) \times n)$–matrix $a := [a_{k,l}]_{\substack{1 \leq k \leq n-p \\ 1 \leq l \leq n}}$. For $1 \leq i \leq n-p$ we consider the $((n-p-i+1) \times (n+1)$–matrices $\underline{a}^{(i)} := \left[\underline{a}^{(i)}_{k,l}\right]_{\substack{1 \leq k \leq n-p-i+1 \\ 0 \leq l \leq n}}$ and $\overline{a}^{(i)} := \left[\overline{a}^{(i)}_{k,l}\right]_{\substack{1 \leq k \leq n-p-i+1 \\ 0 \leq l \leq n}}$ with $\underline{a}^{(i)}_{k,l} = \overline{a}^{(i)}_{k,l} = a^{(i)}_{k,l}$ for $1 \leq k \leq n-p-i+1$ and $1 \leq l \leq n$ and $\underline{a}^{(i)}_{1,0} = \cdots = \underline{a}^{(i)}_{n-p-i+1,0} = 0$ and $\overline{a}^{(i)}_{1,0} = \cdots = \overline{a}^{(i)}_{n-p-i+1,0} = 1$. Then

$$W_{\underline{K}(\underline{a}^{(n-p)})}(S) \subset \cdots \subset W_{\underline{K}(\underline{a}^{(1)})}(S) \subset S$$

and

$$W_{\overline{K}(\overline{a}^{(n-p)})}(S) \subset \cdots \subset W_{\overline{K}(\overline{a}^{(1)})}(S) \subset S$$

form two flags of generic classic and dual polar varieties of S.
If $S_{\mathbb{R}}$ is compact, then, for $1 \leq i \leq n-p$, the classic real polar variety $W_{\underline{K}(\underline{a}^i)}(S_{\mathbb{R}})$ contains a point of each connected component of $S_{\mathbb{R}}$ and, in particular, $W_{\underline{K}(\underline{a}^i)}(S)$ is of pure codimension i in S. The inclusion relations in the first flag are therefore strict and $W_{\underline{K}(\underline{a}^{(n-p)})}(S)$ is a zero–dimensional algebraic variety. Mutatis mutandis the same statement is true for the second flag without the assumption that $S_{\mathbb{R}}$ is compact.

Let

$$\underline{\delta} := \max\{\max\{\deg\{F_1 = 0, \ldots, F_s = 0 | 1 \leq s \leq p\}\}, \\ \max\{W_{\underline{K}(\underline{a}^i)} | 1 \leq i \leq n - p\}\}\}$$

and

$$\overline{\delta} := \max\{\max\{\deg\{F_1 = 0, \ldots, F_s = 0 | 1 \leq s \leq p\}\}, \\ \max\{W_{\overline{K}(\overline{a}^i)} | 1 \leq i \leq n - p\}\}\}.$$

We call $\underline{\delta}$ and $\overline{\delta}$ the degrees of the real interpretation of the equation system

$$F_1 = 0, \ldots, F_p = 0.$$

Our most general complexity result for the case that $S_{\mathbb{R}}$ is smooth is the following.

Theorem 4.1 ([4]) *Let n, p, d, δ, L, ℓ be natural numbers. Let $X_1, \ldots, X_n$ and Z be indeterminates over $\mathbb{Q}$ and let $X := (X_1, \ldots, X_n)$.*
There exists an arithmetic network $\mathcal{N}$ (or arithmetic–boolean circuit) over $\mathbb{Q}$, depending on certain parameters and having size

$$\binom{n}{p} L\,(n\,d)^{O(1)}\,\delta^2 = (n\,d)^{O(n)}$$

and non–scalar depth

$$O(n\,(\ell + \log(n\,d))\log\delta) = O(n^2 \log(d\,n)\,\log d),$$

such that $\mathcal{N}$ satisfies for suitable random specializations of its parameters the following condition:
Let $F_1, \ldots, F_p \in \mathbb{Q}[X]$ be polynomials of degree at most d and assume that $F_1, \ldots, F_p$ are given by an essentially division–free arithmetic circuit β in $\mathbb{Q}[X]$ of size L and non–scalar depth ℓ. Suppose that $F_1, \ldots, F_p$ form a strongly reduced regular sequence in $\mathbb{Q}[X]$, that $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ is empty or smooth and that $\overline{\delta} \leq \delta$ holds.
Then the algorithm represented by the arithmetic network $\mathcal{N}$ starts from the circuit β as input and decides whether the variety $\{F_1 = 0, \ldots, F_p = 0\}$ contains a real point. If this is the case, the algorithm produces a circuit representation of the coefficients of $n + 1$ polynomials $P, G_1, \ldots, G_n \in \mathbb{Q}[Z]$ satisfying for $G := (G_1, \ldots, G_n)$ the following conditions:

- *P is monic and separable,*

- $\deg G < \deg P \leq \delta$*,*

- *the complex affine variety* $\{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$ *is zero–dimensional and contains a smooth real algebraic sample point for each connected component of* $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$*.*

In order to represent these sample points the algorithm returns an encoding "à la Thom" of the real zeros of the polynomial P.

For the terminology of arithmetic network and boolean–arithmetic circuit we refer to [38, 39].
This complexity result has an interpretation in the non–uniform deterministic as well as in the uniform probabilistic computational model. If we add the condition that $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$ must be compact the statement of Theorem 4.1 holds true for $\overline{\delta}$ replaced by $\underline{\delta}$ ([1] and [2]).

Interpretation of Theorem 4.1 for the hypersurface case

We are going to discuss this outcome in the case of a smooth compact real hypersurface given by a regular polynomial equation. So let $p := 1$ and $F := F_1 \in \mathbb{Q}[X]$ be a squarefree polynomial of positive degree d and $S := \{F = 0\}$. For the sake of simplicity we assume that the variables $X_1, \ldots, X_n$ are in generic position with respect to S and that $S_{\mathbb{R}}$ is non-empty, smooth and compact.
Let F be given by an essentially division–free arithmetic circuit β in $\mathbb{Q}[X]$ of size L and depth ℓ. The algebraic version of the Bertini–Sard Theorem (see [14]) and our assumptions imply that for each $1 \leq i < n$ the polynomials $F, \frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_i}$ form a strongly reduced regular sequence in the ring of fractions $\mathbb{Q}[X]_{\frac{\partial F}{\partial X_{i+1}}}$. It is not hard to see that the set

$$F = 0, \frac{\partial F}{\partial X_1} = 0, \ldots, \frac{\partial F}{\partial X_i} = 0, \frac{\partial F}{\partial X_{i+1}} \neq 0$$

is the locus of a generic classic polar variety of S where $\frac{\partial F}{\partial X_{i+1}}$ does not vanish. Therefore, the degree of the Zariski closure of this set is bounded by $\underline{\delta}$. For the same reason

$$\left\{ F = 0, \frac{\partial F}{\partial X_1} = 0 \,, \ldots, \frac{\partial F}{\partial X_{n-1}} = 0 \,, \frac{\partial F}{\partial X_n} \neq 0 \right\}$$

is a finite set that contains a point of each connected component of $S_{\mathbb{R}}$.

We are now in conditions to apply the `Kronecker` algorithm to the given circuit β in order to find the complex solutions of the system

$$F = 0,\ \frac{\partial F}{\partial X_1} = 0\,, \ldots,\ \frac{\partial F}{\partial X_{n-1}} = 0\,, \frac{\partial F}{\partial X_n} \neq 0$$

Between these solutions we filter out the real ones. We control the complexity of the algoritm computing for $1 \leq i < n$ at its $(i+1)$th step a lifting fiber of the system $F = 0,\ \frac{\partial F}{\partial X_1} = 0\,, \ldots,\ \frac{\partial F}{\partial X_i} = 0\,, \frac{\partial F}{\partial X_{i+1}} \neq 0$. This can be done performing $L\,(n\,d)^{O(1)}\,\underline{\delta}^2 = (n\,d)^{O(n)}$ arithmetic operations in $\mathbb{Q}$ which become organized in non–scalar depth $O(n(\ell + \log(nd)) \log \underline{\delta}) = O(n^2\ \log(n\,d) \log d)$.

5 Tools to handle the singular case

In this section we consider the algorithmic problem of finding for each geometrically smooth connected component of $S_{\mathbb{R}}$ an $(F_1, \ldots, F_p)$–regular point when $S_{\mathbb{R}}$ may be singular. In the next two sections we are going to prepare the geometrical tools for this task.

5.1 Two families of copolar incidence varieties

Let i be a natural numbers with $1 \leq i \leq n - p$ and let $B := [B_{k,l}]_{\substack{1 \leq k \leq n-i \\ 1 \leq l \leq n}}$, $\Lambda := [\Lambda_{r,s}]_{1 \leq r,s \leq p}$ and $\Theta := [\Theta_{k,r}]_{\substack{1 \leq k \leq n-i \\ 1 \leq r \leq p}}$ be matrices of indeterminates over $\mathbb{C}$.
We denote by $F := (F_1, \ldots, F_p)$ the sequence of the given polynomials and by $J(F) := \left[\frac{\partial F_s}{\partial X_l}\right]_{\substack{1 \leq s \leq p \\ 1 \leq l \leq n}}$ the Jacobian of F. Observe that the rank of $J(F)$ is generically p on any irreducible component of the complex variety $S := \{F_1 = \cdots = F_p = 0\}$. We write $J(F)^T$ for the transposed matrix of $J(F)$ and for any point $x \in \mathbb{A}^n$ we denote by rk $J(F)(x)$ the rank of the complex matrix $J(F)(x)$.

We are now going to introduce two families of varieties which we shall call *copolar incidence varieties*. In order to define the first one we consider in the ambient space

$$\mathbb{T}_i := \mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^{p\times p} \times \mathbb{A}^{(n-i)\times p}$$

the $\mathbb{Q}$–definable locally closed incidence variety

$$H_i := \{(x, b, \lambda, \vartheta) \in \mathbb{T}_i |\ \ x \in S,\ \text{rk}\ b = n-i,\ \text{rk}\ \vartheta = p,\ J(F)(x)^T\lambda + b^T\vartheta = 0\}.$$

Observe that the isomorphy class of H_i does not depend on the choice of the generators $F_1, \ldots, F_p$ of the vanishing ideal of S. The canonical projection of $\mathbb{T}_i$ onto $\mathbb{A}^n$ maps H_i into S.
Let us state three facts, namely Lemma 5.1 and Propositions 5.1 and 5.2 below, which will be fundamental in the sequel.

Lemma 5.1 *Let $(x, b, \lambda, \vartheta)$ be a point of H_i. Then x belongs to S_{reg} and λ is a regular complex $(p \times p)$–matrix. Moreover, the canonical projection of $\mathbb{T}_i$ onto $\mathbb{A}^n$ maps H_i onto S_{reg} and $(H_i)_{\mathbb{R}}$ onto $(S_{\mathbb{R}})_{reg}$.*

Proposition 5.1 *Let D_i be the closed subvariety of $\mathbb{T}_i$ defined by the conditions $rk\, B < n - i$ or $rk\, \Theta < p$. Then the polynomial equations*

$$\begin{gathered} F_1(X) = \cdots = F_p(X) = 0, \\ \sum_{1 \le s \le p} \Lambda_{r,s} \frac{\partial F_s}{\partial X_l}(X) + \sum_{1 \le k \le n-i} B_{k,l}\, \Theta_{k,r} = 0, \\ 1 \le r \le p,\ 1 \le l \le n, \end{gathered} \tag{5.1}$$

intersect transversally at any of their common solutions in $\mathbb{T}_i \setminus D_i$. Moreover, H_i is exactly the set of solutions of the polynomial equation system (5.1) outside of the locus D_i.
In particular, H_i is an equidimensional algebraic variety which is smooth and of dimension $n(n - i + 1) + p(p - i - 1) \ge 0$.

For algorithmic applications Proposition 5.1 contains too many open conditions, namely the conditions rk $B = n - i$ and rk $\Theta = p$. By means of a suitable specialization of the matrices B and Θ we are going to eliminate these open conditions. However, we have to take care that these specialization process does not exclude to many smooth points of the variety S. The following result, namely Proposition 5.2 below seems to represent a fair compromise. We shall need it later for the task of finding smooth points of S. For the formulation of this proposition we need some notations.
Let $\mathbf{B}$ and $\mathbf{\Theta}$ be the following matrices

$$\mathbf{B} := \begin{bmatrix} B_{1,n-i+1} & \cdots & B_{1,n} \\ \vdots & \ldots & \vdots \\ B_{p,n-i+1} & \cdots & B_{p,n} \end{bmatrix} \quad \text{and} \quad \mathbf{\Theta} := \begin{bmatrix} \Theta_{p+1,1} & \cdots & \Theta_{p+1,p} \\ \vdots & \ldots & \vdots \\ \Theta_{n-i,1} & \cdots & \Theta_{n-i,p,} \end{bmatrix}.$$

Let σ be a permutation of the set $\{1, \ldots, n\}$ (in symbols, $\sigma \in \mathrm{Sym}\,(n)$) and apply σ to the columns of the $((n - i) \times n)$–matrix

$$\begin{bmatrix} I_p & O_{p \times (n-p-i)} & \mathbf{B} \\ O_{(n-p-i) \times p} & I_{n-p-i} & O_{(n-p-i) \times i} \end{bmatrix}.$$

In this way we obtain a $((n-i)\times n)$–matrix which we denote by $\mathbf{B}_{i,\sigma}$. Furthermore, let

$$\mathbf{\Theta}_i := \begin{bmatrix} I_p \\ \mathbf{\Theta} \end{bmatrix} \qquad \text{and} \qquad \Delta_\sigma := \det \left[\tfrac{\partial F_s}{\partial X_{\sigma(r)}} \right]_{1\leq s,r\leq p}.$$

If we specialize in $\mathbf{B}_{i,\sigma}$ the submatrix $\mathbf{B}$ to $b \in \mathbb{A}^{p\times i}$ and in $\mathbf{\Theta}_i$ the submatix $\mathbf{\Theta}$ to $\vartheta \in \mathbb{A}^{(n-p-i)\times p}$ then the resulting complex matrices become denoted by $b_{i,\sigma}$ and ϑ_i, respectively.

We consider now in the ambient space

$$\mathbb{F}_i := \mathbb{A}^n \times \mathbb{A}^{p\times i} \times \mathbb{A}^{p\times p} \times \mathbb{A}^{(n-p-i)\times p}$$

a copolar incidence variety of more restricted type, namely

$$H_{i,\sigma} := \{(x, b, \lambda, \vartheta) \in \mathbb{F}_i \mid x \in S,\ J(F)(x)^T\lambda + b_{i,\sigma}^T\vartheta_i = 0\}.$$

Observe that $H_{i,\sigma}$ is a $\mathbb{Q}$–definable closed subvariety of $\mathbb{F}_i$ whose isomorphy class does not depend on the choice of the polynomials $F_1, \ldots, F_p$ of the vanishing ideal of S.
In the statement of the next result we make use of the Kronecker symbol $\delta_{r,l}$, $1 \leq r, l \leq p$ which is defined by $\delta_{r,l} := 0$ for $r \neq l$ and $\delta_{r,r} := 1$.

Proposition 5.2 *Let notations and definitions be as before. For the sake of simplicity assume that σ is the identity permutation of Sym (n). Then the polynomial equations*

$$\begin{aligned} &F_1 = 0, \ldots, F_s = 0, \\ &\sum_{1\leq s\leq p} \Lambda_{r,s} \frac{\partial F_s}{\partial X_l}(X) + \delta_{r,l} = 0, \quad 1 \leq r \leq p,\ 1 \leq l \leq p, \\ &\sum_{1\leq s\leq p} \Lambda_{r,s} \frac{\partial F_s}{\partial X_l}(X) + \Theta_{l,r} = 0,\ 1 \leq r \leq p,\ p < l \leq n-i, \\ &\sum_{1\leq s\leq p} \Lambda_{r,s} \frac{\partial F_s}{\partial X_l}(X) + B_{r,l} = 0,\ 1 \leq r \leq p,\ n-i < l \leq n \end{aligned} \tag{5.2}$$

intersect transversally at any of their common solutions in $\mathbb{F}_i$. Moreover, $H_{i,\sigma}$ is exactly the set of solutions of the equation system (5.2). In particular, $H_{i,\sigma}$ is a closed equidimensional algebraic variety which is empty or smooth and of dimension $n-p$.
The image of $H_{i,\sigma}$ under the canonical projection of $\mathbb{F}_i$ onto $\mathbb{A}^n$ is the set of (smooth) points of S where Δ_σ does not vanish. For each real point $x \in S$ with $\Delta_\sigma(x) \neq 0$ there exists a real point $(x, b, \lambda, \vartheta)$ of $H_{i,\sigma}$.

In the sequel we shall refer to H_i and $H_{i,\sigma}$ as the *copolar incidence varieties* of $S := \{F_1 = \cdots = F_p = 0\}$ associated with the indices $1 \leq i \leq n-p$ and $\sigma \in \mathrm{Sym}\,(n)$.
The notion of a copolar incidence variety is inspired by the Room-Kempf canonical desingularization of determinantal varieties [28, 32].

5.2 Copolar varieties

Let notations and assumptions be as in previous section and let $b \in \mathbb{A}^{(n-i)\times n}$ be a full rank matrix. We observe that the set

$$\widetilde{V}_b(S) := \{x \in S \mid \exists\,(\lambda, \vartheta) \in \mathbb{A}^{p\times p} \times \mathbb{A}^{(n-p)\times p} \ : \ \mathrm{rk}\ \vartheta = p \ \text{ and } \ (x, b, \lambda, \vartheta) \in H_i\}$$

does not depend on the choice of the generators $F_1, \ldots, F_p$ of the vanishing ideal of S. We call the Zariski closure in $\mathbb{A}^n$ of $\widetilde{V}_b(S)$ the *copolar variety* of S associated with the matrix b and we denote it by $V_b(S)$. Obviously we have $\widetilde{V}_b(S) = V_b(S) \cap S_{\mathrm{reg}}$.
Observe that a point x of S belongs to $\widetilde{V}_b(S)$ if and only if there exist p rows of the $((n-i)\times n)$–matrix b which generate the same affine linear space as the rows of the Jacobian $J(F)$ at x. In case $p := 1$ and $F := F_1$ the copolar variety $V_b(\{F = 0\})$ coincides with the ith classic polar variety $W_{\underline{K}^{n-1-i}(\underline{b})}(\{F = 0\})$ of the complex hypersurface $\{F = 0\}$ (here $\underline{b}$ denotes the $((n-i)\times(n+1))$–matrix whose column number zero is a null-vector, whereas the columns numbered $1, \ldots, n$ are the corresponding columns of b).

Proposition 5.3 *If $b \in \mathbb{A}^{(n-i)\times n}$ is a generic matrix, then the copolar variety $V_b(S)$ is empty or an equidimensional closed subvariety which is smooth at any point of $V_b(S) \cap S_{reg}$ and has (non-negative) dimension $n - (i+1)p$.*

Observe that for a generic $b \in \mathbb{A}^{(n-i)\times n}$ the emptiness or non-emptiness and in the latter case also the geometric degree of the copolar variety $V_b(S)$ is an invariant of the variety S. The incidence varieties H_i and $H_{i,\sigma}$ may be interpreted as suitable algebraic families of copolar varieties. In [6] we considered in the case $p := 1$ three analogous incidence varieties which turned out to be algebraic families of dual polar varieties. Here we have a similar situation since in the hypersurface case, namely in the case $p := 1$, the copolar varieties are classic polar varieties.

6 Bipolar varieties and real point finding in the singular case

In order to measure the complexity of the real point finding procedures of this paper for complete intersection varieties, we consider for $1 \leq p \leq n$, $1 \leq i \leq n-p$ and $\sigma \in \mathrm{Sym}\,(n)$ the generic dual polar varieties of the copolar incidence varieties H_i and $H_{i,\sigma}$. In analogy to the hypersurface case tackled in [6], we call them the *large* and the *small* bipolar varieties of S.

Definition 6.1 *The bipolar varieties $\mathfrak{B}_{(i,j)}$ and $\mathcal{B}_{(i,\sigma,j)}$ are defined as follows:*

- *for $1 \leq j \leq n(n-i+1)+p(p-i-1)$ let $\mathfrak{B}_{(i,j)}$ a $(n(n-i+1)+p(p-i-1)-j+1)$th generic dual polar variety of H_i and,*
- *for $1 \leq j \leq n-p$ and $\sigma \in Sym\,(n)$ let $\mathcal{B}_{(i,\sigma,j)}$ a $(n-p-j+1)$th generic dual polar variety of $H_{i,\sigma}$.*

We call $\mathfrak{B}_{(i,j)}$ the large *and $\mathcal{B}_{(i,\sigma,j)}$ the* small bipolar variety of S*, respectively.*

The bipolar varieties $\mathfrak{B}_{(i,j)}$ and $\mathcal{B}_{(i,\sigma,j)}$are well defined geometric objects which depend on the equation system $F_1(X) = \cdots F_p(X) = 0$, although the copolar incidence variety H_i is not closed (compare the definition of the notion of polar variety in Section 3, where we have taken care of this situation). Moreover, our notation is justified because we are only interested in invariants like the dimension and the degree of our bipolar varieties and these are independent of the particular (generic) choice of the linear projective varieties used to define the bipolar varieties.
Observe that the large bipolar varieties of S form a chain of equidimensional varieties

$$\overline{H_i} \supsetneq \mathfrak{B}_{(i,n(n-i+1)+p(p-i-1))} \supset \cdots \supset \mathfrak{B}_{(i,1)}.$$

The variety $\mathfrak{B}_{(i,1)}$ is empty or zero–dimensional. If $\mathfrak{B}_{(i,1)}$ is nonempty, then the chain is strictly decreasing.
Similarly the small bipolar varieties $\mathcal{B}_{(i,\sigma,j)}$ of S form also a chain of equidimensional varieties

$$\overline{H_{i,\sigma}} \supsetneq \mathcal{B}_{(i,\sigma,n-p)} \supset \cdots \supset \mathcal{B}_{(i,\sigma,1)}.$$

The variety $\mathcal{B}_{(i,\sigma,1)}$ is empty or zero–dimensional. If $\mathcal{B}_{(i,\sigma,1)}$ is nonempty, then the chain is strictly decreasing.
We denote by $\deg \mathfrak{B}_{(i,j)}$ and $\deg \mathcal{B}_{(i,\sigma,j)}$ the geometric degrees of the respective bipolar varieties in their ambient spaces $\mathbb{T}_i$ and $\mathbb{F}_i$ (see [21] for a definition and properties of the geometric degree of a subvariety of an affine space).
Observe that $\deg \mathfrak{B}_{(i,j)}$ remains invariant under linear transformations of the coordinates $X_1, \ldots, X_n$ by unitary complex matrices.
From [6], Lemma 1 and [5], Theorem 3 we deduce that for $1 \leq j \leq n-p$

$$\deg \mathcal{B}_{(i,\sigma,j)} \leq \deg \mathfrak{B}_{(i,n(n-i))+p(p-i)+j)} \tag{6.1}$$

holds.
Suppose that S contains a regular real point x. The there exists a permutation $\sigma \in \text{Sym}\ (n)$ with $\Delta_\sigma(x) \neq 0$. From Proposition 5.2 we deduce that $(H_{i,\sigma})_{\mathbb{R}}$ is nonempty. This implies that $H_{i,\sigma}$ is given by a reduced regular sequence of polynomials, namely the polynomials in the equation system (5.2). Moreover, the real variety $(H_{i,\sigma})_{\mathbb{R}}$ is smooth. Therefore we may apply [3, 4], Proposition 2 to conclude that $(\mathcal{B}_{(i,\sigma,j)})_{\mathbb{R}}$ contains for each connected component of $(H_{i,\sigma})_{\mathbb{R}}$ at least one point. This implies

$$1 \leq \deg \mathcal{B}_{(i,\sigma,1)} \leq \deg \mathfrak{B}_{(i,n(n-i))+p(p-i)+1)}.$$

For $1 \leq r \leq p,\ 1 \leq l \leq n$ and $\sigma \in \text{Sym}\ (n)$ we are going to analyze in the following closed subvarieties $S^{(i)}_{(r,l)}$ and $S^{(i,\sigma)}_{(r,l)}$ of the affine subspaces $\mathbb{T}_i$ and $\mathbb{F}_i$, respectively. For this purpose we consider the lexicographical order $<$ of the set of all pairs (r,l) with $1 \leq r \leq p,\ \ 1 \leq l \leq n$.
Let $S^{(i)}_{(r,l)}$ be the Zariski closure of the locally closed subset of $\mathbb{T}_i$ defined by the conditions

$$\begin{gathered} F_1(X) = \cdots = F_p(X) = 0 \\ \sum_{1 \leq s \leq p} \Lambda_{r',s} \frac{\partial F_s}{\partial X_{l'}} + \sum_{1 \leq k \leq n-i} B_{k,l'} \Theta_{k,r} = 0, \\ 1 \leq r' \leq p,\ \ 1 \leq l' \leq n,\ \ (r',l') \leq (r,l)\ \text{ and} \\ \text{rk}\ B = n-i,\ \text{rk}\ \Theta = p\ \text{ and }\ \text{rk}\ J(F) = p. \end{gathered} \tag{6.2}$$

Observe that the particular structure of the Jacobian of the equations of system (6.2) implies that the corresponding polynomials form a reduced regular sequence at any of their common zeros outside of the closed locus given by the conditions

$$\text{rk}\ B < n-i,\ \text{rk}\ \Theta < p\ \text{ or }\ \text{rk}\ J(F) < p.$$

Furthermore, let $S^{(i,\sigma)}_{(r,l)}$ be the locally closed subset of $\mathbb{F}_i$ defined by the conditions

$$
\begin{aligned}
&F_1(X) = \cdots = F_p(X) = 0,\\
&\sum_{1\le s\le p} \Lambda_{r',s}\frac{\partial F_s}{\partial X_{l'}} + \delta_{r',l'} = 0, \;\; 1 \le r' \le r, \quad 1 \le l' \le p, \qquad (r',l') \le (r,l),\\
&\sum_{1\le s\le p} \Lambda_{r',s}\frac{\partial F_s}{\partial X_{l'}} + \Theta_{l',r'} = 0, \;\; 1 \le r' \le r, \;\; p < l' \le n-i, \;\; (r',l') \le (r,l),\\
&\sum_{1\le s\le p} \Lambda_{r',s}\frac{\partial F_s}{\partial X_{l'}} + B_{r',l'} = 0, \quad 1 \le r' \le r, \;\; n-i < l \le n, \;\; (r',l') \le (r,l)\\
&\qquad\qquad \text{and} \quad \Delta_\sigma(X) \neq 0.
\end{aligned}
\tag{6.3}
$$

Again the particular structure of the Jacobian of the equations of system (6.3) implies that the corresponding polynomials form a reduced regular sequence at any of their common zeros outside of the closed locus given by the condition $\Delta_\sigma(X) = 0$.
In conclusion, the polynomials of the systems (5.1) and (5.2) form *strongly reduced* regular sequences at any of their common zeros outside of the corresponding closed loci.
For the next statement recall that the degree of the polynomials $F_1, \ldots, F_p$ is bounded by d (see Section 2.1).

Proposition 6.1 *Let $1 \le r \le p$ and $1 \le l \le n$. Then we have the extrinsic estimate*

$$\deg S^{(i)}_{(r,l)} = (n^n\, d)^{O(n)}.$$

This bound is probably too coarse but this will not be relevant in Theorem 6.2 below which relies on the following result.

Proposition 6.2 *Let $1 \le r \le p$ and $1 \le l \le n$. Then we have the estimate*

$$\deg S^{(i,\sigma)}_{(r,l)} = (nd)^{O(n)}.$$

Let $1 \le i \le n-p$. We proceed now to derive two extrinsic estimates for the degrees of the bipolar varieties $\mathfrak{B}_{(i,j)}$, $1 \le j \le n(n-i+1)+p(p-i+1)$, and $\mathcal{B}_{(i,\sigma,j)}, \sigma \in \mathrm{Sym}\,(n)$, $1 \le j \le n-p$.

Proposition 6.3 *For $1 \le j \le n(n-i+1)+p(p-i-1)$ one has the extrinsic estimate $\deg \mathfrak{B}_{(i,j)} = (n\,d)^{O(n^2)}$. In particular, for $n(n-i)+p(p-i) < j \le n(n-i+1)+p(p-i-1)$ one has the estimate $\deg \mathfrak{B}_{(i,j)} = (n^n\, d)^{O(n)}$.*

Proposition 6.4 *The extrinsic estimate* $\deg \mathcal{B}_{(i,\sigma,j)} = (nd)^{O(n)}$ *is valid for any* $\sigma \in Sym\ (n)$ *and* $1 \leq j \leq n-p$.

We associate now with $1 \leq i \leq n-p,\ \sigma \in \text{Sym } (n)$ and the polynomial equation system $F_1 = \cdots = F_p = 0$ the following discrete parameters, namely

$$\begin{aligned}\delta_i := \max\{\max\{\deg\{F_1 = 0 \cdots = F_s = 0\} \mid 1 \leq s \leq p\},\\ \max\{\deg S^{(i)}_{(r,l)} \mid 1 \leq r \leq p,\ 1 \leq l \leq n\},\\ \max\{\deg \mathfrak{B}_{i,n(n-i)+p(p-i)+j} \mid 1 \leq j \leq n-p\}\}\end{aligned}$$

and

$$\begin{aligned}\delta_{i,\sigma} := \max\{\max\{\deg\{F_1 = 0 \cdots = F_s = 0\} \mid 1 \leq s \leq p\},\\ \max\{\deg S^{(i,\sigma)}_{(r,l)} \mid 1 \leq r \leq p,\ 1 \leq l \leq n\},\\ \max\{\deg \mathcal{B}_{(i,\sigma,j)} \mid 1 \leq j \leq n-p\}\}.\end{aligned}$$

Adapting the terminology of [6], Section 4.2 and taking into account that for $1 \leq j \leq n-p$ the degree of $\mathfrak{B}_{(i,n(n-i)+p(p-i)+j)}$ remains invariant under linear transformations of the coordinates $X_1, \ldots, X_n$ by unitary complex matrices, we call δ_i and $\delta_{i,\sigma}$ the *unitary-independent* and the *unitary-dependent degree of the real interpretation* of the equation system $F_1 = \cdots = F_p = 0$ associated with i and σ.
Observe that (6.1) and the Bézout Inequality imply

$$\delta_{i,\sigma} \leq \delta_i \quad \text{for any} \quad \sigma \in \text{Sym } (n). \tag{6.4}$$

From Propositions 6.2, 6.3 and 6.4 and the Bézout Inequality we deduce the following extrinsic estimates

$$\delta_i = (n^n\, d)^{O(n)} \tag{6.5}$$

and

$$\delta_{i,\sigma} = (n\, d)^{O(n)} \tag{6.6}$$

(compare for the case $p := 1$ the estimates (16) and (17) given in [6], Section 4.2).
For the rest of the paper we fix a family $\{\sigma_1, \ldots, \sigma_{\binom{n}{p}}\}$ of permutations from Sym (n) such that for any choice $1 \leq k_1 < \cdots < k_p \leq n$ there exists an index $1 \leq k \leq \binom{n}{p}$ with $\sigma_k(1) = k_1, \ldots, \sigma_k(p) = k_p$.

For each $1 \leq k \leq \binom{n}{p}$ the varieties $\{F_1 = 0, \ldots, F_r = 0\},\ 1 \leq r \leq p,\ S^{(i,\sigma_k)}_{(r,l)}, 1 \leq r \leq p,\ 1 \leq l \leq n$ and $\mathcal{B}_{(i,\sigma_k,j)}, 1 \leq j \leq n-p$ form a descending chain which is strict in case that there exists a real point x of S

with $\Delta_{\sigma_k}(x) \neq 0$. We may now apply a suitably adapted version of the `Kronecker` algorithm (see [7], Section 5) to this chain in order to determine the points of the complex variety $\mathcal{B}_{(i,\sigma_k,1)}$ which is empty or zero-dimensional. Observe that $\mathcal{B}_{(i,\sigma_k,1)}$ contains a point of each connected component of $S_{\mathbb{R}}$ where Δ_{σ_k} does not vanish identically. Therefore we obtain for each such component at least one point.

All this can be done using $L\,(n\,d)^{O(1)}\delta_{i,\sigma_k}^2$ arithmetic operations in $\mathbb{Q}$ organized in non–scalar depth $O(n\,(\ell + \log(nd))\log\delta_{i,\sigma_k})$. Repeating this procedure for each $1 \leq k \leq \binom{n}{p}$ and taking into account the estimate 6.4 and 6.6 we obtain the following result.

Theorem 6.2 *Let n, p, d, i, δ, L, ℓ be natural numbers with $d \geq 1$, $1 \leq i \leq n-p$. Let $X_1, \ldots, X_n$ and Z be indeterminates over $\mathbb{Q}$ and let $X := (X_1, \ldots, X_n)$.*
There exists an arithmetic network $\mathcal{N}$ (or arithmetic–boolean circuit) over $\mathbb{Q}$, depending on certain parameters and having size

$$\binom{n}{p} L\,(n\,d)^{O(1)}\,\delta^2 = (n\,d)^{O(n)}$$

and non–scalar depth

$$O(n\,(\ell + \log(n\,d))\log\delta) = O(n^2\log(d\,n)\,\log d),$$

such that $\mathcal{N}$ satisfies for suitable random specializations of its parameters the following condition:
Let $F_1, \ldots, F_p \in \mathbb{Q}[X]$ be polynomials of degree at most d and assume that $F_1, \ldots, F_p$ are given by an essentially division–free arithmetic circuit β in $\mathbb{Q}[X]$ of size L and non–scalar depth ℓ. Suppose that $F_1, \ldots, F_p$ form a strongly reduced regular sequence in $\mathbb{Q}[X]$ and that $\min\{(n\,d)^{c\,n}, \delta_i\} \leq \delta$ holds for a suitable constant $c > 0$.

Then the algorithm represented by the arithmetic network $\mathcal{N}$ starts from the circuit β as input and decides whether the variety $\{F_1 = 0, \ldots, F_p = 0\}$ contains a smooth real point. If this is the case, the algorithm produces a circuit representation of the coefficients of $n+1$ polynomials $P, G_1, \ldots, G_n \in \mathbb{Q}[Z]$ satisfying for $G := (G_1, \ldots, G_n)$ the following conditions:

- *P is monic and separable,*
- $\deg G < \deg P \leq \delta$,

- *the complex affine variety* $\{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$ *is zero–dimensional and contains a smooth real algebraic sample point for each generically smooth connected component of* $\{F_1 = 0, \ldots, F_p = 0\}_{\mathbb{R}}$.

In order to represent these sample points the algorithm returns an encoding "à la Thom" of the real zeros of the polynomial P.

With respect to the encoding "à la Thom" we refer the reader to [13].

Interpretation of Theorem 6.2 in the hypersurface case

We are going to discuss the geometric aspects of the method which leads to Theorem 6.2 in the case of a hypersurface. Let $p := 1$ and $F := F_1 \in \mathbb{Q}[X]$ be a squarefree polynomial of degree d and $S := \{F = 0\}$. Suppose that F is given by an essentially division–free arithmetic circuit β in $\mathbb{Q}[X]$ and, for the sake of simplicity, that the variables $X_1, \ldots, X_n$ are in generic position with respect to S. For each generically smooth connected component of $S_{\mathbb{R}}$ we wish to find a representative point.

Let $1 \leq i \leq n-1$, $B := [B_{k,l}]_{\substack{1 \leq k \leq n-i \\ 1 \leq l \leq n}}$ be a matrix and $(B_{n-i+1}, , \ldots, B_n)$ and $\Theta = (\Theta_1, \ldots, \Theta_{n-i})$ row vectors of indeterminates over $\mathbb{C}$. Furthermore let Λ be a single indeterminate over $\mathbb{C}$ and let $J(F) = (\frac{\partial F}{\partial X_1}, \ldots, \frac{\partial F}{\partial X_n})$ be the gradient (i.e., the Jacobian) of F. Let $\mathbb{T}_i := \mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^1 \times \mathbb{A}^{n-i}$ and $\mathbb{F}_i := \mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^1 \times \mathbb{A}^{n-i-1}$.
The equations

$$F(X) = 0,$$
$$\Lambda \frac{\partial F}{\partial X_l}(X) + \sum_{1 \leq k \leq n-i} B_{k,l}\, \Theta_k = 0,\ 1 \leq l \leq n,$$

define outside of the locus given by the condition rk $B < n - i$ or $\Theta = \mathbf{0}$ in $\mathbb{T}_i$ the copolar incidence variety H_i of S and intersect transversally at any point of H_i. In particular, H_i is smooth and of dimension $(n-i)(n+1)$.

Since the variables $X_1, \ldots, X_n$ are in generic position with respect to S, the partial derivative $\frac{\partial F}{\partial X_1}$ does not vanish identically on any generically smooth connected component of $S_{\mathbb{R}}$. It suffices therefore to consider $H_{i,\sigma}$ only for the identity permutation σ of $\{1, \ldots, n\}$.

The equations

$$\begin{aligned} F(X) &= 0, \\ \Lambda \frac{\partial F}{\partial X_1}(X) + 1 &= 0, \\ \Lambda \frac{\partial F}{\partial X_l}(X) + \Theta_l &= 0,\ 2 \leq l \leq n-i, \\ \Lambda \frac{\partial F}{\partial X_l}(X) + B_l \Theta_1 &= 0,\ n-i < l \leq n \end{aligned}$$

define in $\mathbb{F}_i$ the copolar incidence variety $H_{i,\sigma}$. In particular $H_{i,\sigma}$ is smooth and of dimension $n-1$. For δ_i and $\delta_{i,\sigma}$ we obtain the estimates $\delta_{i,\sigma} \leq \delta_i = (n\,d)^{O(n)}$.

The algorithmic considerations are now similar as in the general complete intersection case and yield the statement of Theorem 6.2 for $p := 1$ and $\delta_i \leq \delta$.

References

[1] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, *Polar varieties, real equation solving, and data structures: The hypersurface case,* J. Complexity 13 (1997), 5-27, Best paper award. MR1449757 (98h:68123)

[2] B. Bank, M. Giusti, J. Heintz, and G. M. Mbakop, *Polar varieties and efficient real elimination,* Math. Z. 238 (2001) 115-144. MR1860738 (2002g:14084)

[3] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties and an efficient real elimination procedure,* Kybernetika 40 (2004), 519-550. MR2120995 (2006e:14078)

[4] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Generalized polar varieties: geometry and algorithms,* J. Complexity 21 (2005), 377-412. MR2152713 (2006f:14068)

[5] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and E. Schost, *On the geometry of polar varieties,* Appl. Algebra Eng. Commun. Comput. 21 (2010), 33-83. MR2585564 (2011c:68065)

[6] B. Bank, M. Giusti, J. Heintz, L. Lehmann, and L. M. Pardo, *Algorithms of intrinsic complexity for point searching in compact real sin-*

gular hypersurfaces, Found. Comput. Math. 12, no. 1, 75-122 (2012). MR2886157

[7] B. Bank, M. Giusti, and J. Heintz, *Point searching in real singular complete intersection varieties - algorithms of intrinsic complexity*, accepted by Math. Comp. (2012)

[8] S. Basu, R. Pollack, and M.-F. Roy, *On the combinatorial and algebraic complexity of quantifier elimination,* J.ACM 43, (1996) 1002-1045. MR1434910 (98c:03077)

[9] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in real algebraic geometry, (2. ed.)* Springer Verlag, Berlin etc. 2006. MR2248869 (2007b:14125)

[10] P. Bürgisser, M. Clausen, and M. A. Shokrollahi, *Algebraic complexity theory. With the collaboration of Thomas Lickteig,* Grundlehren der Mathematischen Wissenschaften 315, Springer Verlag, Berlin etc. 1997. MR1440179 (99c:68002)

[11] J. F. Canny, *Some algebraic and geometric computations in PSPACE,* ACM Symposium on Theory of Computing (STOC) (1988), 460-467.

[12] D. Castro, M. Giusti, J. Heintz, G. Matera, and L. M. Pardo, *The hardness of polynomial equation solving.* Found. Comput. Math. 3 (2003), 347-420. MR2009683 (2004k:68056)

[13] M. Coste, and M.-F. Roy, *Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets,* J. Symbolic Comput. 5 (1988), no 1-2, 121-129. MR0949115 (89g:12002)

[14] M. Demazure, *Catastrophes et bifurcations,* Ellipses, Paris 1989.

[15] M. Giusti, J. Heintz, J. E. Morais, and L. M. Pardo, *When polynomial equation systems can be "solved" fast?* in Cohen, Gérard et al. (ed.) , Applied algebra, algebraic algorithms and error-correcting codes. 11th international symposium, AAECC-11, Paris, France, July 17-22, 1995. Proceedings. Berlin: Springer LNCS 948, pp. 205-231 (1995). MR1448166 (98a:68106)

[16] M. Giusti, J. Heintz, K. Hägele, J. E. Morais, J. L. Montaña, and L. M. Pardo, *Lower bounds for diophantine approximations,* J. Pure Appl. Algebra 117-118 (1997), 277-317. MR1457843 (99d:68106)

[17] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L. M. Pardo, *Straight–line programs in geometric elimination theory,* J. Pure Appl. Algebra 124 (1998), 101-146. MR1600277 (99d:68128)

[18] M. Giusti, and J. Heintz, *Kronecker's smart, little black boxes,* in Foundations of computational mathematics (Oxford 1999 , R. A. DeVore et al., eds.), Lond. Math. Soc. Lecture Note Ser., 284, Cambridge University Press, Cambridge 2001, 69-104. MR1836615 (2002e:65075)

[19] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving,* J. Complexity 17 (2001), 154-211. MR1817612 (2002b:68123)

[20] D. Yu. Grigoriev, and N. N. Vorobjov, Jr. *Solving systems of polynomial inequalities in subexponential time,* J. Symb. Comput. 5 (1988), no.1-2, 37-64. MR0949112 (89h:13001)

[21] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields,* Theor. Comput. Sci. 24 (1983), 239-277. MR0716823 (85a:68062)

[22] J. Heintz, B. Kuijpers, A. Rojas Paredes, *Software Engineering and complexity in effective algebraic geometry,* J. Complexity 28 (2012), to appear.

[23] J. Heintz, B. Kuipers, A. Rojas Paredes, *On the intrinsic complexity of elimination problems in effective algebraic geometry,* arXiv:1201.4344v3.

[24] J. Heintz, G. Matera, and A. Waissbein, *On the time-space complexity of geometric elimination procedures,* Appl. Algebra Eng. Commun. Comput. 11 (2001), 239-296. MR1818975 (2002c:68108)

[25] J. Heintz, M.-F. Roy, and P. Solernó, *On the complexity of semialgebraic sets,* in IFIP Information Processing 89 (G. X. Ritter , ed.), Elsevier, 1989, pp. 293-298.

[26] J. Heintz, M.-F. Roy, and P. Solernó, *Complexité du principe de Tarski–Seidenberg,* C.R.Acad.Sci. Paris Sér. I Math. 309 (1989), 825–830. MR1055203 (92c:12012)

[27] J. Heintz, M.-F. Roy, and P. Solernó, *Sur la complexité du principe de Tarski–Seidenberg,* Bull. Soc. Math. France, 118 (1990), 101–126. MR1077090 (92g:03047)

[28] G. Kempf, *On the geometry of a theorem of Riemann,* Ann. Math. (2) 98 (1973), 178-185. MR0349687 (50 #2180)

[29] R. Piene, *Polar classes of singular varieties,* Ann. Scient. Éc. Norm. Sup. 4. Série, t. 11, (1978) 247-276. MR0510551 (80j:14051)

[30] J. Renegar, *A faster PSPACE algorithm for the existential theory of the reals,* in Proc. 29th Annual IEEE Symposium on the Foundation of Computer Science, 1988, pp. 291-295.

[31] J. Renegar, *On the computational complexity and geometry of the first order theory of the reals,* J. Symbolic Comput.,13 (1992), no.3, 255-352. MR1156882 (93h:03011a), MR1156883 (93h:03011b), MR1156884 (93h:03011c)

[32] T. G. Room, *The geometry of determinantal loci,* Cambridge Univ. Press (1938).

[33] F. Severi, *Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarita proiettive,* Torino Mem. (2) 52 (1903), 61-118.

[34] F. Severi, *La serie canonica e la teoria delle serie principali di gruppi di punti sopra una superficie algebrica,* Comment. Math. Helv. 4 (1932), 268-326.

[35] B. Teissier, *Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours,* Séminaire d'Analyse, Univ. Blaise Pascal 1987-1988, Exp. No. 4, 12pp. Clermont-Ferrand II, Clermont-Ferrand, 1990. MR1088966 (91m:14001)

[36] J. A. Todd, *The geometrical invariants of algebraic loci,* Proc. London Math. Soc. S2-43 (1937), l27-l38. MR1575589

[37] J. A. Todd, *The arithmetical invariants of algebraic loci,* Proc. London Math. Soc. S2-43 (1937) no.3, 190-225. MR1575915

[38] J. von zur Gathen, *Parallel arithmetic computations: A survey. Mathematical foundations of computer science,* in Proc. 12th Symp., Bratislava/Czech. 1986, Lect. Notes Comput. Sci. 233, 1986, 93-112. MR0874591

[39] J. von zur Gathen, *Parallel linear algebra,* in Synthesis of parallel algorithms (J. H. Reif, ed.), Kaufmann, San Mateo, CA., 1993, pp. 573–617.