

POINT SEARCHING IN REAL SINGULAR COMPLETE INTERSECTION VARIETIES – ALGORITHMS OF INTRINSIC COMPLEXITY¹

BERND BANK, MARC GIUSTI, AND JOOS HEINTZ

Abstract. Let X_1, \dots, X_n be indeterminates over \mathbb{Q} and let $X := (X_1, \dots, X_n)$. Let F_1, \dots, F_p be a regular sequence of polynomials in $\mathbb{Q}[X]$ of degree at most d such that for each $1 \leq k \leq p$ the ideal (F_1, \dots, F_k) is radical. Suppose that the variables X_1, \dots, X_n are in generic position with respect to F_1, \dots, F_p . Further suppose that the polynomials are given by an essentially division-free circuit β in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ .

We present a family of algorithms \mathcal{A}_i and invariants δ_i of F_1, \dots, F_p , $1 \leq i \leq n - p$, such that \mathcal{A}_i produces on input β a smooth algebraic sample point for each connected component of $\{x \in \mathbb{R}^n \mid F_1(x) = \dots = F_p(x) = 0\}$ where the Jacobian of $F_1 = 0, \dots, F_p = 0$ has generically rank p .

The sequential complexity of \mathcal{A}_i is of order $L(nd)^{O(1)}(\min\{(nd)^{cn}, \delta_i\})^2$ and its non-scalar parallel complexity is of order $O(n(\ell + \log nd) \log \delta_i)$. Here $c > 0$ is a suitable universal constant. Thus, the complexity of \mathcal{A}_i meets the already known worst case bounds. The particular feature of \mathcal{A}_i is its pseudo-polynomial and intrinsic complexity character and this entails the best runtime behavior one can hope for. The algorithm \mathcal{A}_i works in the non-uniform deterministic as well as in the uniform probabilistic complexity model. We exhibit also a worst case estimate of order $(n^n d)^{O(n)}$ for the invariant δ_i . The reader may notice that this bound overestimates the extrinsic complexity of \mathcal{A}_i , which is bounded by $(nd)^{O(n)}$.

1. Introduction

Before we start to explain the main results of this article and their motivations, we introduce some basic notions and notations.

Let \mathbb{Q} , \mathbb{R} and \mathbb{C} be the fields of rational, real and complex numbers, respectively, let $X := (X_1, \dots, X_n)$ be a vector of indeterminates over \mathbb{C} and let F_1, \dots, 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).

Received by the editor version of April 19, 2013.

2010 *Mathematics Subject Classification.* Primary 68W30 14B05, 14P05, 14B07 Secondary 68W10.

Key words and phrases. real polynomial equation solving, intrinsic complexity, singularities, polar, copolar and bipolar variety, degree of variety.

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

Let $\mathbb{A}_{\mathbb{R}}^n := \mathbb{R}^n$ be the n -dimensional real affine space. We denote by $S_{\mathbb{R}} := S \cap \mathbb{A}_{\mathbb{R}}^n$ the real trace of the complex variety S . Moreover, we denote by \mathbb{P}^n the n -dimensional complex projective space and by $\mathbb{P}_{\mathbb{R}}^n$ its real counterpart. We shall use also the following notations:

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

We call the regular sequence F_1, \dots, F_p *reduced* if the ideal (F_1, \dots, F_p) generated in $\mathbb{Q}[X]$ is the ideal of definition of the affine variety S , i.e., if (F_1, \dots, F_p) is radical. We call (F_1, \dots, F_p) *strongly reduced* if for any index $1 \leq k \leq p$ the ideal (F_1, \dots, F_k) is radical. Thus, a strongly reduced regular sequence is always reduced.

A point x of \mathbb{A}^n is called (F_1, \dots, F_p) -*regular* if the Jacobian $J(F_1, \dots, F_p) := \begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \dots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_p}{\partial X_1} & \dots & \frac{\partial F_p}{\partial X_n} \end{pmatrix}$ has maximal rank p at x . Observe, that for each *reduced* regular sequence F_1, \dots, F_p defining the variety S , the locus of (F_1, \dots, F_p) -regular points of S is the same. In this case we call an (F_1, \dots, 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 suppose now that there are natural numbers d, L and δ and an essentially division-free arithmetic circuit \mathcal{C} in $\mathbb{Q}[X]$ with p output nodes such that the following conditions are satisfied.

- The degrees $\deg F_1, \dots, \deg F_p$ of the polynomials F_1, \dots, F_p are bounded by d .
- The p output nodes of the arithmetic circuit \mathcal{C} represent the polynomials F_1, \dots, F_p by evaluation.
- The size and the non-scalar depth of the arithmetic circuit \mathcal{C} are bounded by L and δ , respectively.

For the terminology and basic facts concerning arithmetic circuits we refer to [22, 13, 11].

Suppose that the variables X_1, \dots, 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 design for each $1 \leq i \leq n - p$ 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, \dots, 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* $F_1 = 0, \dots, F_p = 0$.
- (ii) The algorithm Π_i decides on input δ_i 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 δ_i a computation in \mathbb{Q} with $L(nd)^{O(1)}(\min\{(nd)^{cn}, \delta_i\})^2$ arithmetic operations (additions, subtractions, multiplications and divisions) which become organized in non-scalar depth $O(n(\delta_i + \log nd) \log \delta_i)$ with respect to the parameters of the arithmetic circuit \mathcal{C} (here $c > 0$ is a suitable universal constant).

This is the outcome of our main result, namely Theorem 14 below and the three remarks following the theorem.

Although we were not able to derive a better worst case bound as $(n^n d)^{O(n)}$ for the invariant δ_i (see Propositions 8 and 12 and Observation 11 below) the worst case complexity of the procedure Π_i meets the already known extrinsic bound of $(nd)^{O(n)}$ for the elimination problem under consideration (compare the original papers [24, 12, 35, 30, 31, 32, 36, 9] and the comprehensive book [10]).

The complexity of the procedure Π_i depends polynomially on the *extrinsic* parameters L, δ, n and d and on the degree δ_i of the real interpretation of the equation system $F_1 = 0, \dots, F_p = 0$ 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 the complexity $L(nd)^{O(1)}(\min\{(nd)^{c_n}, \delta_i\})^2$ 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 [27, 28], 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.

In the case that $S_{\mathbb{R}}$ is smooth and F_1, \dots, F_p is a strongly reduced regular sequence in $\mathbb{Q}[X]$ there exist already pseudo-polynomial algorithms of intrinsic complexity which solve the computational task of item (ii) above (see [1, 3, 4]). The same is true for the singular hypersurface case, namely $p := 1$, where $\{F_1 = 0\}_{\mathbb{R}}$ contains possibly singular points (see [8, 6, 7]). The methods developed in [1, 2, 4] cannot be applied directly when $S_{\mathbb{R}}$ is singular. To overcome this difficulty we consider in Section 3.1 two families of smooth incidence varieties which parametrize the so-called copolar varieties of S introduced in Section 3.2.

For a given full rank matrix $b \in \mathbb{A}^{(n-i) \times n}$, the corresponding copolar variety of S is the Zariski closure of the set of all points x of S such that there exist p rows of b which generate the same linear space as the rows of the Jacobian of the equation system $F_1 = 0, \dots, F_p = 0$ at x .

The procedure Π_i is based on a geometrical and computational analysis of the dual polar varieties of the two families of incidence varieties (see [3, 4, 5] for the notion of a dual polar variety). These geometric objects are called *bipolar varieties* of S . They become introduced in Section 4.1. Important for the worst case complexity of the procedure are the degree estimates for the bipolar varieties developed in Section 4.2.

2. Preliminaries about polar varieties

Let notations be as in the Introduction. Let $F_1, \dots, F_p \in \mathbb{Q}[X]$ 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 $a := [a_{k,i}]_{\substack{1 \leq k \leq n-p-i+1 \\ 0 \leq i \leq n}}$ be a complex $((n-p-i+1) \times (n+1))$ -matrix and suppose that $a_* := [a_{k,i}]_{\substack{1 \leq k \leq n-p-i+1 \\ 1 \leq i \leq n}}$ has maximal rank $n-p-i+1$.

In case $(a_{1,0}, \dots, a_{n-p-i+1,0}) = 0$ we denote by $\underline{K}(a) := \underline{K}^{n-p-i}(a)$ and in case $(a_{1,0}, \dots, a_{n-p-i+1,0}) \neq 0$ 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 $(a_{k,0} : a_{k,1} : \dots : a_{k,n})$. In the first case we shall also use the notations $\underline{K}(a_*)$ and $\underline{K}^{n-p-i}(a_*)$ instead of $\underline{K}(a)$ and $\underline{K}^{n-p-i}(a)$.

The classic and the dual i th polar varieties of S associated with the linear varieties $\underline{K}(a)$ and $\overline{K}(a)$ are defined as the closures of the loci of the (F_1, \dots, F_p) -regular points of S where all $(n-i+1)$ -minors of the respective polynomial $((n-i+1) \times n)$ -matrix

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

and

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

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

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

and

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

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 $F_1 = 0, \dots, F_p = 0$ 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

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

which is supposed to be non-empty.

In Section 4 we shall need this extended definition of polar varieties in order to establish the notion of a bipolar variety of a given 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, \dots, 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 $a = [a_{k,l}]_{\substack{1 \leq k \leq n-p-i+1 \\ 0 \leq l \leq n}}$ with $[a_{k,l}]_{\substack{1 \leq k \leq n-p-i+1 \\ 1 \leq l \leq n}}$ 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 non necessarily smooth) at any of their (F_1, \dots, 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 $F_1 = 0, \dots, F_p = 0$). However, when

a generic $((n - \rho - i + 1) \times (n + 1))$ -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 $((n - \rho - i + 1) \times (n + 1))$ -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 [8], Theorem 8 and Corollary 9).

For our use of the word “generic” we refer to [5], Definition 1.

In case that $S_{\mathbb{R}}$ is smooth and a is a real $((n - \rho - i + 1) \times (n + 1))$ -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 $W_{\overline{K}(a)}(S_{\mathbb{R}})$ may be empty (see [3] and [4], Proposition 2).

Polar varieties have a long story in algebraic geometry which goes back to Severi [39] and Todd [43, 44] in the 1930’s. Originally they were used to establish numerical formulas in order to classify singular algebraic varieties by their intrinsic geometric character or to formulate a manageable local equisingularity criterion which implies the Whitney conditions for analytic varieties. About 10 years ago they became also a fundamental tool for the design of pseudo-polynomial computer procedures with intrinsic complexity bounds which find for a given complete intersection variety S with a smooth real trace $S_{\mathbb{R}}$ algebraic sample points for each connected component of $S_{\mathbb{R}}$. For details we refer to [42] and [5].

3. Copolar incidence varieties

3.1. Two families of copolar incidence varieties. Let d, n, ρ and i be natural numbers with $1 \leq \rho \leq n$ and $1 \leq i \leq n - \rho$ and let $X := (X_1, \dots, X_n)$, $B := [B_{k,l}]_{\substack{1 \leq k \leq n-i \\ 1 \leq l \leq n}}$, $\Lambda := [\Lambda_{r,s}]_{1 \leq r, s \leq \rho}$ and $\Theta := [\Theta_{k,r}]_{\substack{1 \leq k \leq n-i \\ 1 \leq r \leq \rho}}$ be matrices of indeterminates over \mathbb{C} .

We fix for the rest of the paper a strongly reduced regular sequence $F_1, \dots, F_\rho \in \mathbb{Q}[X]$. Let $d := \max\{\deg F_s \mid 1 \leq s \leq \rho\}$, where $\deg F_s$ denotes the degree of the polynomial F_s . We denote by $F := (F_1, \dots, F_\rho)$ the sequence of these polynomials and by $J(F) := \left[\frac{F_s}{X_i} \right]_{\substack{1 \leq s \leq \rho \\ 1 \leq i \leq n}}$ the Jacobian of F . Observe that the rank of $J(F)$ is generically ρ on any irreducible component of the complex variety $S := \{F_1 = \dots = F_\rho = 0\}$. We write $J(F)^T$ for the transposed matrix of $J(F)$ and for any point $x \in \mathbb{A}^n$ we denote by $\text{rk } J(F)(x)$ 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

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

the \mathbb{Q} -definable locally closed incidence variety

$$H_i := \{(x, b, \Lambda, \Theta) \in \mathbb{T}_i \mid x \in S, \text{rk } b = n - i, \text{rk } \Lambda = \rho, J(F)(x)^T + b^T \Theta = 0\}.$$

Observe that the isomorphism class of H_i does not depend on the choice of the generators F_1, \dots, F_ρ of the vanishing ideal of S . The canonical projection of \mathbb{T}_i onto \mathbb{A}^n maps H_i into S .

We are now going to state and prove three facts, namely Lemma 1 and Propositions 2 and 3 below, which will be fundamental in the sequel.

Lemma 1. *Let (x, b, Λ, Θ) be a point of H_i . Then x belongs to S_{reg} and Λ is a regular complex $(\rho \times \rho)$ -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 $(S_{\mathbb{R}})_{\text{reg}}$.*

Proof

Let (x, b, \dots) be a point of H_i . Then b and \dots are complex full rank matrices of size $(n-i) \times n$ and $(n-i) \times p$, respectively. Therefore b^T is a complex full rank matrix of size $n \times p$. From $J(F)(x)^T + b^T = 0$ we deduce that the complex $(n \times p)$ -matrix $J(F)(x)^T$ and the matrix \dots have rank p . This implies that the rank of $J(F)(x)$ is p . Since x belongs to S we conclude that S is smooth at x . Thus we have $x \in S_{\text{reg}}$ and \dots is a regular complex $(p \times p)$ -matrix. By the way we have shown that the canonical projection of \mathbb{T}_i onto \mathbb{A}^n maps H_i into S_{reg} .

Consider now an arbitrary point $x \in S_{\text{reg}}$. Without loss of generality we may assume that the first p columns of $J(F)(x)$ are \mathbb{C} -linearly independent. Let \dots be the $(p \times p)$ -identity matrix I_p . Furthermore, let

$$b := \begin{pmatrix} -J(F)(x) \\ O_{(n-p-i) \times p} \end{pmatrix} \quad \text{and} \quad \dots := \begin{pmatrix} I_p \\ O_{(n-p-i) \times p} \end{pmatrix},$$

where $O_{(n-p-i) \times p}$ denotes the $((n-p-i) \times p)$ -zero matrix.

Then b and \dots are full rank matrices which satisfy the condition $J(F)(x)^T + b^T = 0$. Since x belongs to S , we conclude that (x, b, \dots) is an element of H_i which becomes mapped onto x under the canonical projection of \mathbb{T}_i onto \mathbb{A}^n . In particular, if $x \in (S_{\mathbb{R}})_{\text{reg}}$ then \dots, b and \dots are real matrices and (x, b, \dots) belongs to $(H_i)_{\mathbb{R}}$. This implies that the canonical projection of \mathbb{T}_i onto \mathbb{A}^n maps H_i onto S_{reg} and $(H_i)_{\mathbb{R}}$ onto $(S_{\mathbb{R}})_{\text{reg}}$. \square

Proposition 2. *Let D_i be the closed subvariety of \mathbb{T}_i defined by the conditions $\text{rk } B < n-i$ or $\text{rk } \Theta < p$. Then the polynomial equations*

$$(1) \quad \begin{aligned} &F_1(X) = \dots = F_p(X) = 0, \\ &\Lambda_{r,s} \frac{F_s}{X_l}(X) + \sum_{1 \leq k \leq n-i} B_{k,l} \Theta_{k,r} = 0, \\ &1 \leq r \leq p, 1 \leq l \leq n, \end{aligned}$$

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 (1) outside of the locus D_i .

In particular, H_i is an equidimensional algebraic variety which is smooth and of dimension $n(n-i+1) + p(p-i-1) \geq 0$.

Proof

One sees immediately that a point $(x, b, \dots) \in \mathbb{T}_i$ belongs to H_i if and only if it is a solution of the polynomial equation system (1) outside of the locus D_i . The Jacobian of the system (1) at such a point (x, b, \dots) has the following form

$$\mathcal{L}_x := \begin{pmatrix} J(F)(x) & O_{p \times p} & \dots & O_{p \times p} & O_{p \times (n-i)} & \dots & O_{p \times (n-i)} & O_{p \times n(n-i)} \\ J(F)(x)^T & \dots & O_{n \times p} & b^T & \dots & O_{n \times (n-i)} & D^{(1)} \\ * & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ O_{n \times p} & \dots & J(F)(x)^T & O_{n \times (n-i)} & \dots & b^T & D^{(p)} \end{pmatrix},$$

where $D^{(r)}$, $1 \leq r \leq \rho$, is the complex $(n \times n(n-i))$ -matrix

$$D^{(r)} := \begin{matrix} & \begin{matrix} 1,r & \cdots & n-i,r & \cdots & \end{matrix} & \mathcal{O}_{1 \times (n-i)} \\ \begin{matrix} \vdots \\ \vdots \\ \vdots \end{matrix} & & & & \\ \mathcal{O}_{1 \times (n-i)} & \cdots & \begin{matrix} 1,r & \cdots & n-i,r \end{matrix} & & \end{matrix}.$$

From Lemma 1 we conclude that the $(\rho \times n)$ -matrix $J(F)(x)$ has maximal rank ρ . Since the matrix has full rank we infer that the $(n\rho \times n(n-i))$ -submatrix of \mathcal{L}_x built up by $D^{(1)}, \dots, D^{(\rho)}$ has rank $n\rho$. This implies that the Jacobian \mathcal{L}_x has full rank. Therefore, the $(n+1)\rho$ equations of the system (1) intersect transversally at (x, b, \dots) and the algebraic variety H_i is smooth and of dimension

$$n + (n-i)n + \rho^2 + (n-i)\rho - (n+1)\rho = n(n-i+1) + \rho(\rho-i-1)$$

at this point. Thus H_i is an equidimensional variety which is empty or smooth and of dimension $n(n-i+1) + \rho(\rho-i-1)$ (observe that $1 \leq i \leq n-\rho$ implies $n(n-i+1) + \rho(\rho-i-1) \geq 0$).

Observe that H_i is a \mathbb{Q} -definable closed subvariety of \mathbb{F}_i whose isomorphism class does not depend on the choice of the polynomials F_1, \dots, 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 3. *Let notations and definitions be as before. For the sake of simplicity assume that σ is the identity permutation of $\text{Sym}(n)$. Then the polynomial equations*

$$(2) \quad \begin{aligned} & F_1 = 0, \dots, F_s = 0, \\ & \Lambda_{r,s} \frac{F_s}{X_l}(X) + \delta_{r,l} = 0, \quad 1 \leq r \leq p, 1 \leq l \leq p, \\ & \Lambda_{r,s} \frac{F_s}{X_l}(X) + \Theta_{l,r} = 0, \quad 1 \leq r \leq p, p < l \leq n-i, \\ & \Lambda_{r,s} \frac{F_s}{X_l}(X) + B_{r,l} = 0, \quad 1 \leq r \leq p, n-i < l \leq n \end{aligned}$$

intersect transversally at any of their common solutions in \mathbb{F}_i . Moreover, H_i is exactly the set of solutions of the equation system (2). In particular, H_i is a closed equidimensional algebraic variety which is empty or smooth and of dimension $n-p$.

The image of H_i under the canonical projection of \mathbb{F}_i onto \mathbb{A}^n is the set of (smooth) points of S where Δ does not vanish. For each real point $x \in S$ with $\Delta(x) \neq 0$ there exists a real point (x, b, \dots) of H_i .

Proof

From the matrix identities

$$\mathbf{B}_i \cdot {}^T \Theta_i = \begin{array}{cc} I_p & O_{p \times (n-p-i)} \\ O_{(n-p-i) \times p} & I_{n-p-i} \end{array} \cdot \Theta = \begin{array}{cc} I_p & I_p \\ \Theta & \Theta \end{array} = \begin{array}{ccc} & & \begin{array}{ccc} 1 & \cdots & 0 \\ \vdots & \cdots & \vdots \\ 0 & \cdots & 1 \\ \Theta_{\rho+1,1} & \cdots & \Theta_{\rho+1,p} \\ \vdots & \cdots & \vdots \\ \Theta_{n-i,1} & \cdots & \Theta_{n-i,p} \\ B_{1,n-i+1} & \cdots & B_{\rho,n-i+1} \\ \vdots & \cdots & \vdots \\ B_{1,n} & \cdots & B_{p,n} \end{array} \end{array}.$$

one deduces easily that a point (x, b, \dots) of \mathbb{F}_i belongs to H_i if and only if it is a solution of the polynomial equation system (2).

Let (x, b, \dots) be such a point of H_i . Then the system (2) implies $\Delta(x) \neq 0$ and its Jacobian may be organized as the matrix

$$\mathcal{L}_x^{(i)} := \begin{pmatrix} J(F)(x) & O_{p \times p} & \cdots & O_{p \times p} & O_{p \times (n-p)} & \cdots & O_{p \times (n-p)} \\ & J(F)(x)^T & \cdots & O_{n \times p} & Z & \cdots & O_{n \times (n-p)} \\ * & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ & O_{n \times p} & \cdots & J(F)(x)^T & O_{n \times (n-p)} & \cdots & Z \end{pmatrix},$$

with

$$Z := \begin{pmatrix} O_{p \times (n-p-i)} & O_{p \times i} \\ I_{n-p-i} & O_{(n-p-i) \times i} \\ O_{i \times (n-p-i)} & I_i \end{pmatrix}.$$

From $\Delta(x) \neq 0$ we deduce that $J(F)(x)$ has rank p . Thus $\mathcal{L}_x^{(i)}$ has full rank. Therefore, the $(n+1)p$ equations of the system (2) intersect transversally at (x, b, \dots) and the algebraic variety H_i is smooth and of dimension $n + pi + p^2 + (n - p - i)p - (n+1)p = n - p$ at this point. Thus H_i is an equidimensional variety which is empty or smooth of dimension $n - p$. For any point (x, b, \dots) of H_i we have $\Delta(x) \neq 0$ and, in particular, S is smooth at x .

On the other hand, for $x \in S$ with $\Delta(x) \neq 0$ we may consider

$$a := - \frac{F_s(x)}{X_l}^{-1}_{1 \leq s, l \leq p}, \quad b := - \frac{F_s(x)}{X_l}^T_{\substack{1 \leq s \leq p \\ p < l \leq n-i}}, \quad \text{and} \quad c := - \frac{F_s(x)}{X_l}^T_{\substack{1 \leq s \leq p \\ n-i < l \leq n}}.$$

Then the corresponding point (x, b, \dots) belongs to H_i . Moreover, for x real we have that b, \dots are also real and therefore (x, b, \dots) is a real point of H_i . \square

In the sequel we shall refer to H_i and H_i as the

Proposition 4. *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 $V_b(S) \cap S_{\text{reg}}$ and has (non-negative) dimension $n - (i + 1)\rho$.*

Proof

(Sketch) We consider in the ambient space $\mathbb{F}_i := \mathbb{A}^n \times \mathbb{A}^{(n-i) \times n} \times \mathbb{A}^{(n-i) \times \rho}$ the \mathbb{Q} -definable locally closed incidence variety

$$H_i := \{(x, b, \gamma) \in \mathbb{F}_i \mid x \in S, \text{rk } b = n - i, \text{rk } \gamma = \rho, J(F)(x)^T + b^T \gamma = 0\}$$

Using the same argument as in Proposition 2 we see that H_i is nonempty, equidimensional of dimension $n(n-i+1) - (i+1)\rho \geq 0$ and smooth. Let $\pi : H_i \mapsto \mathbb{A}^{(n-i) \times n}$ be the morphism induced by the canonical projection of \mathbb{F}_i onto $\mathbb{A}^{(n-i) \times n}$. Notice that for any full rank matrix $b \in \mathbb{A}^{(n-i) \times n}$ the b -fiber of π is isomorphic to $V_b(S) \cap S_{\text{reg}}$ as algebraic variety. Suppose now that π is dominating. From Sard's Theorem (see [16, 40]) we deduce that for a generic $b \in \mathbb{A}^{(n-i) \times n}$ the b -fiber of π and hence $V_b(S) \cap S_{\text{reg}}$, are nonempty, equidimensional of dimension $n - (i+1)\rho \geq 0$ and smooth. If π is not dominating, then we see by the same argument that $V_b(S)$ is empty. \square

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 $H_{i, \gamma}$ may be interpreted as suitable algebraic families of copolar varieties. In [8] we considered in the case $\rho := 1$ 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 $\rho := 1$, the copolar varieties are classic polar varieties.

4. Bipolar varieties

4.1. Definition and basic properties of bipolar varieties. In order to measure the complexity of the real point finding procedures of this paper for complete intersection varieties, we consider for $1 \leq \rho \leq n$, $1 \leq i \leq n - \rho$ and $\gamma \in \text{Sym}(n)$ the generic dual polar varieties of the copolar incidence varieties H_i and $H_{i, \gamma}$. In analogy to the hypersurface case tackled in [8], we call them the *large* and the *small* bipolar varieties of S .

Definition 5. *The bipolar varieties $\mathfrak{B}_{(i,j)}$ and $\mathcal{B}_{(i, \gamma)}$ are defined as follows:*

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

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

The bipolar varieties $\mathfrak{B}_{(i,j)}$ and $\mathcal{B}_{(i, \gamma)}$ are well defined geometric objects which depend on the equation system $F_1(X) = \dots = F_\rho(X) = 0$, although the copolar incidence varieties H_i is not closed (compare the definition of the notion of polar variety in Section 2, 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.

From Propositions 2 and 3 and [5], Corollary 2 we deduce that $\mathfrak{B}_{(i,j)}$ and $\mathcal{B}_{(i,j)}$ are empty or equidimensional of dimension $j - 1$ and Cohen-Macaulay and normal at any point of $\mathfrak{B}_{(i,j)} \cap H_i$ and $\mathcal{B}_{(i,j)} \cap H_i$.

Let $1 \leq j \leq n(n-i+1) + \rho(\rho-i-1)$, $a_0 \in \mathbb{A}^j$ with $a_0 \neq 0$, $a_* \in \mathbb{A}^{j \times (n(n-i+1) + \rho(n+\rho-1))}$ generic and $a := [a_0^T, a_*]$. Furthermore, let $T_a^{(i,j)}$ be the polynomial $((n+1)\rho + j) \times (n(n-i+1) + \rho(n+\rho-i))$ -matrix whose first $(n+1)\rho$ rows constitute the Jacobian of the system (1) of Section 3 and whose remaining j rows are built as in Section 2 in order to define the $(n(n-i+1) + \rho(\rho-i-1) - j + 1)$ th dual polar variety of H_i associated with the linear variety $\overline{K}(a)$. Then $\mathfrak{B}_{(i,j)}$ is the Zariski closure in \mathbb{T}_i of the set of all points $(x, b, \dots) \in H_i$ where $T_a^{(i,j)}(x, b, \dots)$ has not full rank.

By $T_a^{(i,j)}$ we denote the polynomial $((n+1)\rho + j - 1) \times (n(n-i+1) + \rho(n+\rho-i))$ -matrix consisting of all rows of $T_a^{(i,j)}$ except the last one.

Observe that the large bipolar varieties of S form a chain of equidimensional varieties

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

The variety $\mathfrak{B}_{(i,1)}$ is empty or zero-dimensional. If $\mathfrak{B}_{(i,1)}$ is nonempty, then the chain is strictly decreasing. We define $\mathfrak{B}_{(i,0)} := \emptyset$.

For $t \in \mathbb{N}^{j-1}$ with $t := (t_1, \dots, t_{j-1})$ and

$$(n+1)\rho < t_1 < \cdots < t_{j-1} \leq n(n-i+1) + \rho(n+\rho-i)$$

we denote by $m_{(i,j;t)}$ the $((n+1)\rho + j - 1)$ -minor of $T_a^{(i,j)}$ which corresponds to the first $(n+1)\rho$ columns and the columns numbered t_1, \dots, t_{j-1} of $T_a^{(i,j)}$. Moreover, for

$$(n+1)\rho < k_1 < \cdots < k_{n(n-i+1) + \rho(\rho-i-1) - j + 1} \leq n(n-i+1) + \rho(n+\rho-i)$$

different from t_1, \dots, t_{j-1} and $1 \leq h \leq n(n-i+1) + \rho(\rho-i-1) - j + 1$ we denote by $M_h^{(i,j;t)}$ the $((n+1)\rho + j)$ -minor of $T_a^{(i,j)}$ which corresponds to the first $(n+1)\rho$ columns of $T_a^{(i,j)}$ and the columns numbered t_1, \dots, t_{j-1} and k_h . Observe $\deg M_h^{(i,j;t)} \leq (n+1)\rho d + j$.

Finally, for $t' \in \mathbb{N}^{n-i}$ and $t'' \in \mathbb{N}^\rho$ with $t' := (t'_1, \dots, t'_{n-i})$, $t'' := (t''_1, \dots, t''_\rho)$ and

$$1 \leq t'_1 < \cdots < t'_{n-i} \leq n \quad \text{and} \quad 1 \leq t''_1 < \cdots < t''_\rho \leq n-i$$

let $B_{(i,t)}$ and $\Theta_{(i,t)}$ be the $(n-i)$ - and ρ -minors of the matrices B and Θ which correspond to the columns t'_1, \dots, t'_{n-i} and rows t''_1, \dots, t''_ρ of B and Θ , respectively. By induction on $n(n-i+1) + \rho(\rho-i-1), \dots, 1$ one sees easily that for any point (x, b, \dots) of $\mathfrak{B}_{(i,j)} \cap H_i \setminus \mathfrak{B}_{(i,j-1)}$ there exist suitable vectors $t \in \mathbb{N}^{j-1}$, $t' \in \mathbb{N}^{n-i}$ and $t'' \in \mathbb{N}^\rho$ with $m_{(i,j;t)} B_{(i,t)} \Theta_{(i,t)}(x, b, \dots) \neq 0$.

Now Proposition 2 and Propositions 6 and 8 of [3, 4] imply that the equations of the system (1) and the equations

$$M_1^{(i,j;t)} = 0, \dots, M_{n(n-i+1) + \rho(\rho-i-1) - j + 1}^{(i,j;t)} = 0$$

intersect transversally at (x, b, \dots) . In particular, the corresponding polynomials form a regular sequence in

$$\mathbb{Q}[X, B, \Lambda, \Theta]_{m_{(i,j;t)} B_{(i,t)} \Theta_{(i,t)}}$$

and they define the large bipolar variety $\mathfrak{B}_{(i,j)}$ outside of the locus given by

$$m_{(i,j;t)} B_{(i,t)} \Theta_{(i,t)} = 0.$$

Finally, observe that there exist $\binom{n(n-i+1)+\rho(p-i-1)}{j-1}$, $\binom{n}{n-i}$ and $\binom{n-i}{\rho}$ possible choices of the vectors $t \in \mathbb{N}^{j-1}$, $t' \in \mathbb{N}^{n-i}$ and $t'' \in \mathbb{N}^\rho$, respectively. This yields $\binom{n(n-i+1)+\rho(p-i-1)}{j-1} \binom{n}{n-i} \binom{n-i}{\rho}$ possible choices of vectors $(t, t', t'') \in \mathbb{N}^{j-1} \times \mathbb{N}^{n-i} \times \mathbb{N}^\rho$.

This considerations entail the following statement.

Proposition 6. *Let notations be as above and let $t \in \mathbb{N}^{j-1}$, $t' \in \mathbb{N}^{n-i}$ and $t'' \in \mathbb{N}^\rho$ be suitable vectors. Further, let $D_{(i,j;t,t',t'')}$ be the closed variety of \mathbb{T}_i defined by the condition $m_{(i,j;t)} B_{(i,t)} \Theta_{(i,t)} = 0$. Then the equations of the system (1) and the degree $(n+1)\rho d + j$ equations*

$$M_1^{(i,j;t)} = 0, \dots, M_{n(n-i+1)+\rho(p-i-1)-j+1}^{(i,j;t)} = 0$$

intersect transversally at any of their common solutions in $\mathbb{T}_i \setminus D_{(i,j;t,t',t'')}$. They define $\mathfrak{B}_{(i,j)} \setminus D_{(i,j;t,t',t'')}$ in $\mathbb{T}_i \setminus D_{(i,j;t,t',t'')}$. Moreover, for suitably chosen vectors $(t, t', t'') \in \mathbb{N}^{j-1} \times \mathbb{N}^{n-i} \times \mathbb{N}^\rho$ the union of the sets $\mathbb{T}_i \setminus D_{(i,j;t,t',t'')}$ covers $\mathfrak{B}_{(i,j)} \cap H_i \setminus \mathfrak{B}_{(i,j-1)}$. There exist $\binom{n(n-i+1)+\rho(p-i-1)}{j-1} \binom{n}{n-i} \binom{n-i}{\rho}$ such choices for the vector $(t, t', t'') \in \mathbb{N}^{j-1} \times \mathbb{N}^{n-i} \times \mathbb{N}^\rho$.

Now let $1 \leq j \leq n - \rho$, $a_0 \in \mathbb{A}^j$ with $a_0 \neq 0$, $a_* \in \mathbb{A}^{j \times (n(\rho+1))}$ generic and $a := [a_0^T, a_*]$. Let $\sigma \in \text{Sym}(n)$. For the sake of simplicity of exposition we suppose that σ is the identity permutation. Furthermore, let $T_a^{(i,j)}$ be the polynomial $((n+1)\rho + j) \times n(\rho+1)$ -matrix whose first $(n+1)\rho$ rows constitute the Jacobian of the system (2) of Section 3 and whose remaining j rows are built as in Section 2 in order to define the $(n-\rho-j+1)$ th dual polar variety of H_i , associated with the linear space $\overline{K}(a)$. Then $\mathcal{B}_{(i,j)}$ is the Zariski closure in \mathbb{F}_i of the set of all points $(x, b, \dots) \in H_i$, where $T_a^{(i,j)}(x, b, \dots)$ has not full rank.

By $T_a^{(i,j)}$ we denote the polynomial $((n+1)\rho + j - 1) \times n(\rho+1)$ -matrix consisting of all rows of $T_a^{(i,j)}$ except the last one.

Observe again, that the small bipolar varieties $\mathcal{B}_{(i,j)}$ of S form a chain of equidimensional varieties

$$\overline{H_i} \supseteq \mathcal{B}_{(i, n-\rho)} \supset \dots \supset \mathcal{B}_{(i, 1)}.$$

The variety $\mathcal{B}_{(i, 1)}$ is empty or zero-dimensional. If $\mathcal{B}_{(i, 1)}$ is nonempty, then the chain is strictly decreasing. We define $\mathcal{B}_{(i, 0)} := \emptyset$.

For $t \in \mathbb{N}^{j-1}$ with $t := (t_1, \dots, t_{j-1})$ and

$$(n+1)\rho < t_1 < \dots < t_{j-1} \leq n(\rho+1)$$

we denote by $m_{(i,j;t)}$ the $((n+1)\rho + j - 1)$ -minor of $T_a^{(i,j)}$ which corresponds to the first $(n+1)\rho$ columns and the columns numbered t_1, \dots, t_{j-1} of $T_a^{(i,j)}$. Moreover, for

$$(n+1)\rho < k_1 < \dots < k_{n-\rho-j+1} \leq n(\rho+1)$$

different from t_1, \dots, t_{j-1} and $1 \leq h \leq n - \rho - j + 1$ we denote by $M_h^{(i,j;t)}$ the $((n+1)\rho + j)$ -minor of $T_a^{(i,j)}$ which corresponds to the first $(n+1)\rho$ columns of

$T_a^{(i, j)}$ and the columns numbered t_1, \dots, t_{j-1} and k_n . Observe $\deg M_n^{(i, j; t)} \leq (n+1)\rho d$.

Observe that there exist $\binom{n-\rho}{j-1}$ choices of vectors $t \in \mathbb{N}^{j-1}$.

In the same way as in case of Proposition 6, now one proves the following statement.

Proposition 7. *Let notations be as before and let $t \in \mathbb{N}^{j-1}$ be a suitable vector. Denote by $D_{(i, j; t)}$ the closed subvariety of \mathbb{F}_i defined by the equation $m_{(i, j; t)} = 0$. Then the equations of the system (2) and the degree $(n+1)\rho d$ equations*

$$M_1^{(i, j; t)} = 0, \dots, M_{n-\rho-j+1}^{(i, j; t)} = 0$$

intersect transversally at any of their common solutions in $\mathbb{F}_i \setminus D_{(i, j; t)}$. They define $\mathcal{B}_{(i, j)} \setminus D_{(i, j; t)}$ in $\mathbb{F}_i \setminus D_{(i, j; t)}$. Moreover, for suitably chosen vectors $t \in \mathbb{N}^{j-1}$ the union of the sets $\mathbb{F}_i \setminus D_{(i, j; t)}$ covers $\mathcal{B}_{(i, j)} \cap H_i \setminus \mathcal{B}_{(i, j-1)}$. There exist $\binom{n-\rho}{j-1}$ possible choices of vectors $t \in \mathbb{N}^{j-1}$.

4.2. Degrees of bipolar varieties. We denote by $\deg \mathfrak{B}_{(i, j)}$ and $\deg \mathcal{B}_{(i, j)}$ the geometric degrees of the respective bipolar varieties in their ambient spaces \mathbb{T}_i and \mathbb{F}_i (see [26] 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, \dots, X_n by unitary complex matrices.

From [8], Lemma 1 and [5], Theorem 1 and Theorem 3 we deduce that for $1 \leq j \leq n - \rho$ and $(S_{reg})_{\mathbb{R}} \neq \emptyset$

$$(3) \quad \deg \mathcal{B}_{(i, j)} \leq \deg \mathfrak{B}_{(i, n(n-i)+\rho(p-i)+j)}$$

holds.

Suppose that S contains a regular real point x . Then there exists a permutation

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

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

For $1 \leq r \leq \rho$, $1 \leq l \leq n$ and $\in \text{Sym}(n)$ we are going to analyze in the following closed subvarieties $S_{(r, l)}^{(i)}$ and $S_{(r, l)}^{(i,)}$ 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 $1 \leq r \leq \rho$, $1 \leq l \leq n$.

Let $S_{(r, l)}^{(i)}$ be the Zariski closure of the locally closed subset of \mathbb{T}_i defined by the conditions

$$(4) \quad \begin{aligned} & F_1(X) = \dots = F_{\rho}(X) = 0 \\ & \Lambda_{r, s} \frac{F_s}{X_l} + \sum_{1 \leq k \leq n-i} B_{k, l} \Theta_{k, r} = 0, \\ & 1 \leq r' \leq \rho, 1 \leq l' \leq n, (r', l') \leq (r, l) \text{ and} \\ & \text{rk } B = n - i, \text{rk } \Theta = \rho \text{ and } \text{rk } J(F) = \rho. \end{aligned}$$

Observe that the particular structure of the Jacobian of the equations of system (4) 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 $S_{(r,l)}^{(i)}$ be the locally closed subset of \mathbb{F}_i defined by the conditions

$$\begin{aligned} & F_1(X) = \cdots = F_p(X) = 0, \\ & \Lambda_{r,s} \frac{F_s}{X_l} + \Theta_{r,l} = 0, \quad 1 \leq r' \leq r, \quad 1 \leq l' \leq p, \quad (r', l') \leq (r, l), \\ & \Lambda_{r,s} \frac{F_s}{X_l} + \Theta_{l,r} = 0, \quad 1 \leq r' \leq r, \quad p < l' \leq n - i, \quad (r', l') \leq (r, l), \\ & \Lambda_{r,s} \frac{F_s}{X_l} + B_{r,l} = 0, \quad 1 \leq r' \leq r, \quad n - i < l' \leq n, \quad (r', l') \leq (r, l) \end{aligned} \quad (5)$$

and $\Delta(X) \neq 0$.

Again the particular structure of the Jacobian of the equations of system (5) 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 $\Delta(X) = 0$.

In conclusion, the polynomials of the systems (1) and (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, \dots, F_p is bounded by d (see Section 2).

Proposition 8. *Let $1 \leq r \leq p$ and $1 \leq l \leq n$. Then we have the extrinsic estimate*

$$\deg S_{(r,l)}^{(i)} \leq d^{p(n+1)} = d^{O(n^2)}.$$

Proof

Without loss of generality we may suppose $d \geq 2$. Then we deduce from the Bézout Inequality ([26, 18, 45]) that the closed subvariety of \mathbb{T}_i defined by the equations of the system (4) is of degree at most $d^{p(n+1)} = d^{O(n^2)}$. 2

In fact this bound is too coarse, because refined methods, based on the multi-homogeneous Bézout Inequality of [34], yield an estimate $\deg S_{(r,l)}^{(i)} = (n^n d)^{O(n)}$ which is sharper for $d \geq n$. This improvement will not be very relevant in Section 5 where the degree of $S_{(r,l)}^{(i)}$ plays a key role in complexity estimates. More important will be the estimate $\deg S_{(r,l)}^{(i)} = (nd)^{O(n)}$, $\in \text{Sym}(n)$, we are going to derive now.

Lemma 9. *Let $1 \leq r \leq p$, $\Lambda^{(r)} := [\Lambda_{r,s}]_{1 \leq s \leq r}$ and $\Delta := \det[\frac{F_s}{X_l}]_{1 \leq s, l \leq p}$. Then the Zariski closure of the locally closed subvariety \mathfrak{S}_r of $\mathbb{A}^n \times \mathbb{A}^{r \times p}$ defined by the conditions*

$$\begin{aligned} & F_1(X) = \cdots = F_p(X) = 0, \\ & \Lambda_{r,s} \frac{F_s}{X_l} + \Theta_{r,l} = 0, \quad 1 \leq r' \leq r, \quad 1 \leq l' \leq p, \\ & \Delta \neq 0 \end{aligned} \quad (6)$$

is empty or equidimensional of dimension $n - p$. Its geometric degree is bounded by $(2nd)^n$. The polynomials of the system (6) form a reduced regular sequence in $\mathbb{Q}[X, \Lambda^{(r)}]_\Delta$.

Proof

From the equations (6) one deduces easily that for a point $(x, \) \in \mathfrak{S}_r$ with $\Delta(x) \neq 0$ the matrix $[-\frac{F_s}{X_t}]_{\substack{1 \leq s \leq r \\ 1 \leq t \leq p}}$ has maximal rank. This implies that the Jacobian of (6) has full rank at $(x, \)$. Hence the variety \mathfrak{S}_r is smooth and of dimension $n - p$ at $(x, \)$. Thus \mathfrak{S}_r is empty or equidimensional of dimension $n - p$. Moreover, the polynomials of the system (6) form a reduced regular sequence in $\mathbb{Q}[X, \Lambda^{(r)}]_\Delta$.

Observe that for $x \in S$ with $\Delta(x) \neq 0$ there exists exactly one point $\ \in \mathbb{A}^{r \times p}$ such that $(x, \)$ belongs to \mathfrak{S}_r . Thus $\mathfrak{S}_r \cap (S_\Delta \times \mathbb{A}^{r \times p})$ is the graph of a rational map $\ : S \rightarrow \mathbb{A}^{r \times p}$ which is everywhere defined on S_Δ . By Cramer's rule each component of this rational map may be described by a rational expression whose numerator is a polynomial of $\mathbb{Q}[X]$ of degree at most pd and whose denominator is Δ .

Let K_1, \dots, K_{n-p} be generic affine linear polynomials of $\mathbb{Q}[X, \Lambda^{(r)}]$. Then we have $\deg \mathfrak{S}_r = \#(\mathfrak{S}_r \cap \{K_1 = 0, \dots, K_{n-p} = 0\})$, where $\#$ denotes the cardinality of the corresponding set. Without loss of cardinality we may suppose that $\mathfrak{S}_r \cap \{K_1 = 0, \dots, K_{n-p} = 0\}$ is contained in $\mathbb{A}_\Delta^n \times \mathbb{A}^{r \times n}$ (see [26], Remark 2). Replacing in $K_1 = 0, \dots, K_{n-p} = 0$ each indeterminate $\Lambda_{r',s}$, $1 \leq r' \leq r$, $1 \leq s \leq p$ by the given rational expression for the corresponding coordinate of $\$ and cleaning the denominator Δ we obtain together with F_1, \dots, F_p a system of n polynomials of $\mathbb{Q}[X]$ having degree at most $2pd$ which in \mathbb{A}_Δ^n defines a set of the same cardinality as $\mathfrak{S}_r \cap \{K_1 = 0, \dots, K_{n-p} = 0\}$. From the Bézout Inequality we deduce therefore

$$\deg \mathfrak{S}_r \leq (2pd)^n \leq (2nd)^n.$$

2

Proposition 10. *Let $1 \leq r \leq p$ and $1 \leq l \leq n$. Then we have the estimate*

$$\deg S_{(r,l)}^{(i, \)} \leq (2nd^3)^n.$$

Proof

Without loss of generality we may suppose that $\ \in \text{Sym}(n)$ is the identity permutation. Then we have with the notation of the previous lemma $\Delta = \Delta$.

We consider $\mathfrak{S}_{r-1} \times \mathbb{A}^p$ and \mathfrak{S}_r as closed subvarieties of $\mathbb{A}^n \times \mathbb{A}^{r \times p}$ with the convention $\mathfrak{S}_0 := \overline{S_\Delta}$. Let $V_{(r,l)}$ be the Zariski closure of the locally closed subvariety of $\mathbb{A}^n \times \mathbb{A}^{r \times p}$ defined by the conditions

$$\begin{aligned} F_1(X) = \dots = F_p(X) = 0, \\ \Lambda_{r',s} \frac{F_s}{X_l} + \ \substack{r',l} = 0, \quad 1 \leq r' \leq r, \quad 1 \leq l' \leq p, \quad (r', l') \leq (r, l) \\ \text{and } \Delta \neq 0 \end{aligned}$$

Observe that $V_{(r,l)}$ is the intersection of $\mathfrak{S}_{r-1} \times \mathbb{A}^p$ with the subvariety of $\mathbb{A}^n \times \mathbb{A}^{r \times p}$ defined by the equations

$$\Lambda_{r,s} \frac{F_s}{X_l} + \dots = 0, \quad 1 \leq l \leq \min\{l, p\}.$$

From the Bézout Inequality and Lemma 9 we infer

$$\deg V_{(r,l)} \leq d^p \deg \mathfrak{S}_r \leq (2nd)^n.$$

By Lemma 9 the variety \mathfrak{S}_{r-1} is empty or of dimension $n - p$. Since $\mathfrak{S}_{r-1} \times \mathbb{A}^p$ contains $V_{(r,l)}$ we conclude $\dim V_{(r,l)} \leq n$. Observe now that the system (5) describes the graph of a polynomial map with domain $(V_{(r,l)})_\Delta$. The polynomials which constitute this map have degree at most d . In the same way as in the proof of Lemma 9, the Bézout Inequality implies that the system (5) describes a locally closed algebraic subvariety of \mathbb{F}_i whose Zariski closure is of degree at most $d^n \deg V_{(r,l)} \leq (nd)^n$. Since the irreducible components of $S_{(r,l)}^{(i)}$ are irreducible components of this variety we conclude that $\deg S_{(r,l)}^{(i)} \leq (2nd)^n$ holds. \square

Observation 11. *Let $1 \leq r \leq p$ and $1 \leq l \leq n$. Then the estimate of Proposition 8 can be improved to $\deg S_{(r,l)}^{(i)} = (n^n d)^{O(n)}$.*

Proof

(Sketch) Let us first suppose $p \leq l \leq n$ and let $Y := [Y_{r,s}]_{1 \leq r, s \leq p}$ be a matrix of new indeterminates. Consider again $\Delta := \det[\frac{F_s}{X_l}]_{1 \leq s, l \leq p}$. We show $\deg (S_{(r,l)}^{(i)})_\Delta = (nd)^{O(n)}$. For this purpose we add to the equations of (4) the equations

$$(7) \quad Y_{r,s} \frac{F_s}{X_l} = \dots, \quad 1 \leq r', l', 1 \leq r'', l'' \leq p$$

In this way we obtain a closed subvariety W of $\mathbb{T}_i \times \mathbb{A}^{p \times p}$. Taking into account the assumption $p \leq l \leq n$, one sees easily that the Jacobian of the system composed by (4) and (7) has at any point of W full rank. Therefore, W is empty or an equidimensional, smooth variety. The system composed by (4) and (7) contains five types of variables, namely the ones contained in B, Λ, Θ and Y (which occur linearly) and the variables X_1, \dots, X_n (which occur in degree at most d). Intersecting W with $\dim W$ many affine hyperplanes of $\mathbb{T}_i \times \mathbb{A}^{p \times p}$ given by generic affine linear polynomials of $\mathbb{Q}[X, B, \Lambda, \Theta, Y]$, we deduce from the dehomogenized version of the multi-homogeneous Bézout Inequality of [34] or from [15], Corollary 1.12 the estimate $\deg W = (n^n d)^{O(n)}$.

Let $\pi : \mathbb{T}_i \times \mathbb{A}^{p \times p} \rightarrow \mathbb{T}_i$ be the canonical projection from $\mathbb{T}_i \times \mathbb{A}^{p \times p}$ onto \mathbb{T}_i and observe that $\overline{\pi(W)}$ is birationally equivalent to W and hence empty or an equidimensional subvariety of \mathbb{T}_i . Since the irreducible components of $(S_{(r,l)}^{(i)})_\Delta$ are irreducible components of $\overline{\pi(W)}$ we infer from [26], Lemma 2 and its proof the estimate

$$\deg (S_{(r,l)}^{(i)})_\Delta \leq \deg W = (n^n d)^{O(n)}.$$

In a similar way one sees $\deg (S_{(r,l)}^{(i)})_{\Delta_\sigma} = (n^n d)^{O(n)}$ for any permutation $\sigma \in \text{Sym}(n)$. Since there exist $\binom{n}{p}$ many p -minors of $J(F)$ we conclude $\deg S_{(r,l)}^{(i)} =$

$\binom{n}{p} (n^n d)^{O(n)} = (n^n d)^{O(n)}$. Finally, we consider $S_{(r,l)}^{(i)}$ for $1 \leq r \leq \rho$ and arbitrary $1 \leq l \leq n$. From (4) we conclude that the irreducible components of $S_{(r,l)}^{(i)}$ are irreducible components of the intersection of $S_{(r-1,n)}^{(i)}$ with $l \leq n$ hypersurfaces of \mathbb{T}_i of degree at most $\max\{2, d\}$. Since we have by our previous argumentation $\deg S_{(r-1,l)}^{(i)} = (n^n d)^{O(n)}$, we deduce from the Bézout Inequality $\deg S_{(r,l)}^{(i)} = (n^n d)^{O(n)}$. \square

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

Proposition 12. *For $1 \leq j \leq n(n - i + 1) + \rho(\rho - i - 1)$ one has the extrinsic estimate $\deg \mathfrak{B}_{(i,j)} = (nd)^{O(n^2)}$. In particular, for $n(n - i) + \rho(\rho - i) < j \leq n(n - i + 1) + \rho(\rho - i - 1)$ one has the estimate $\deg \mathfrak{B}_{(i,j)} = (n^n d)^{O(n)}$.*

Proof

From Proposition 8 we deduce that the degree of \overline{H}_i in \mathbb{T}_i is bounded by $d^{\rho(n+1)} = d^{O(n^2)}$. Observation 11 yields the estimate $\deg \overline{H}_i = (n^n d)^{O(n)}$. On the other hand we deduce from Proposition 6 and the Bézout Inequality that $\deg \mathfrak{B}_{(i,j)}$ is bounded by $\deg \overline{H}_i \binom{n(n-i+1)+\rho(\rho-i-1)}{j-1} \binom{n}{n-i} \binom{n-i}{\rho} ((n+1)\rho d + j)^{n(n-i+1)+\rho(\rho-i-1)-j+1}$. This implies for $1 \leq j \leq n(n - i + 1) + \rho(\rho - i - 1)$ the general estimate $\deg \mathfrak{B}_{(i,j)} = (nd)^{O(n^2)}$ and for $n(n - i) + \rho(\rho - i) \leq j \leq n(n - i + 1) + \rho(\rho - i - 1)$ the particular estimate $\deg \mathfrak{B}_{(i,j)} = (n^n d)^{O(n)}$. \square

Proposition 13. *The extrinsic estimate $\deg \mathcal{B}_{(i,j)} = (nd)^{O(n)}$ is valid for any $\mathcal{B}_{(i,j)} \in \text{Sym}(n)$ and $1 \leq j \leq n - \rho$.*

Proof

From Proposition 10 we deduce that the degree of H_i is bounded by $(nd^\beta)^n$. Moreover, Proposition 7 and the Bézout Inequality imply that $\deg \mathcal{B}_{(i,j)}$ is bounded by $\deg H_i \binom{n-\rho}{j-1} ((n+1)\rho d + j)^{n-\rho-j+1} = (nd)^{O(n)}$. \square

We associate now with $1 \leq i \leq n - \rho$, $\mathcal{B}_{(i,j)} \in \text{Sym}(n)$ and the polynomial equation system $F_1 = \dots = F_\rho = 0$ the following discrete parameters, namely

$$\begin{aligned}
 i &:= \max\{\max\{\deg\{F_1 = 0 \dots = F_s = 0\} \mid 1 \leq s \leq \rho\}, \\
 &\quad \max\{\deg S_{(r,l)}^{(i)} \mid 1 \leq r \leq \rho, 1 \leq l \leq n\}, \\
 &\quad \max\{\deg \mathfrak{B}_{i, n(n-i)+\rho(\rho-i)+j} \mid 1 \leq j \leq n - \rho\}\}
 \end{aligned}$$

and

$$\begin{aligned}
 i &:= \max\{\max\{\deg\{F_1 = 0 \dots = F_s = 0\} \mid 1 \leq s \leq \rho\}, \\
 &\quad \max\{\deg S_{(r,l)}^{(i)} \mid 1 \leq r \leq \rho, 1 \leq l \leq n\}, \\
 &\quad \max\{\deg \mathcal{B}_{(i,j)} \mid 1 \leq j \leq n - \rho\}\}.
 \end{aligned}$$

Adapting the terminology of [8], Section 4.2 and taking into account that for $1 \leq j \leq n - \rho$ the degree of $\mathfrak{B}_{(i, n(n-i)+\rho(\rho-i)+j)}$ remains invariant under linear transformations of the coordinates X_1, \dots, X_n by unitary complex matrices, we

call i and i_i the *unitary-independent* and the *unitary-dependent degree of the real interpretation* of the equation system $F_1 = \dots = F_p = 0$ associated with i and

Observe that (3) and the Bézout Inequality imply

$$i_i \leq i \quad \text{for any } i \in \text{Sym}(n).$$

From Propositions 10, 12 and 13, Observation 11 and the Bézout Inequality we deduce the following extrinsic estimates

$$(8) \quad i = (n^n d)^{O(n)}$$

and

$$(9) \quad i_i = (n d)^{O(n)}$$

(compare for the case $p := 1$ the estimates (16) and (17) given in [8], Section 4.2).

For the rest of the paper we fix a family $\{i_1, \dots, i_{\binom{n}{p}}\}$ of permutations from $\text{Sym}(n)$ such that for any choice $1 \leq k_1 < \dots < k_p \leq n$ there exists an index $1 \leq k \leq \binom{n}{p}$ with $i_k(1) = k_1, \dots, i_k(p) = k_p$.

Let $i := \sum_{1 \leq k \leq \binom{n}{p}} i_{i_k}$. From (9) we deduce

$$(10) \quad i = (n d)^{O(n)}.$$

Observe finally that

$$(11) \quad i \leq \frac{n}{p} i$$

holds.

5. Real root finding for $\mathbf{F}_1 = \mathbf{0}, \dots, \mathbf{F}_p = \mathbf{0}$

We are going to present a discrete family of efficient non-uniform (or alternatively uniform probabilistic) procedures Π_i , $1 \leq i \leq n - p$, which satisfy the following specifications. Let Z be a new indeterminate.

Input:

An essentially division-free arithmetic circuit \mathcal{C} in $\mathbb{Q}[X]$ of size L and non-scalar depth d having p output nodes.

Input specification:

The circuit \mathcal{C} represents by its output nodes p polynomials $F_1, \dots, F_p \in \mathbb{Q}[X]$ of maximal degree d . These polynomials form a strongly reduced regular sequence in $\mathbb{Q}[X]$.

Output:

The procedure Π_i accepts the input \mathcal{C} if $S := \{F_1 = 0, \dots, F_p = 0\}$ contains a smooth real point. If this is the case, the procedure returns a circuit representation of the coefficients of $n + 1$ polynomials $P, G_1, \dots, G_n \in \mathbb{Q}[Z]$ satisfying for $G := (G_1, \dots, G_n)$ the following

Output specification:

- P is monic and separable,
- $\deg G < \deg P \leq i$, where $\deg G := \max\{\deg G_1, \dots, \deg G_n\}$,
- the zero-dimensional affine variety

$$\{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$$

contains a smooth real point of each generically smooth connected component of $S_{\mathbb{R}}$. In order to represent these sample points, an encoding “à la Thom” of the real zeros of the polynomial P is returned (see e.g. [14] for this kind of encoding).

We say that Π_i solves the *real root finding problem* for $F_1 = 0, \dots, F_p = 0$.

We fix now $1 \leq i \leq n - p$ and $\sigma \in \text{Sym}(n)$. Without loss of generality we may suppose that σ is the identity permutation. From Proposition 3 we deduce that the equations of the system (2) intersect transversally at any of their real solutions. Moreover, the polynomials of (2) form in $\mathbb{Q}[X, \mathbf{B}, \Lambda, \Theta]$ a strongly reduced regular sequence (see Section 4.2).

Denote by $V := H_i$ the closed algebraic subvariety of \mathbb{F}_i consisting of the common complex solutions of the polynomial equation system (2) and let $V_{\mathbb{R}} := V \cap (\mathbb{F}_i)_{\mathbb{R}}$ be the real trace of V in \mathbb{F}_i . Thus $V_{\mathbb{R}}$ consists of all real solutions of (2) and is therefore closed in the Euclidean topology. Moreover, from Proposition 3 we conclude that V and $V_{\mathbb{R}}$ are empty or smooth of dimension $n - p$ and that the real variety $V_{\mathbb{R}}$ is non-empty if and only if S contains a real point x with $\Delta(x) \neq 0$. More precisely, for any connected component C of $S_{\mathbb{R}}$, where Δ do not vanish identically, there exists a point (x, b, \dots) of $V_{\mathbb{R}}$ with $x \in C$, $\Delta(x) \neq 0$ and $(b, \dots) \in \mathbb{A}_{\mathbb{R}}^{p \times i} \times \mathbb{A}_{\mathbb{R}}^{p \times p} \times \mathbb{A}_{\mathbb{R}}^{(n-p-i) \times p}$.

Therefore, a set of algebraic sample points for the connected components of $V_{\mathbb{R}}$ gives rise to a set of algebraic sample points for the connected components of $S_{\mathbb{R}}$ where Δ does not vanish identically.

Suppose now that S contains a real point x with $\Delta(x) \neq 0$. Then the real variety $V_{\mathbb{R}}$ is smooth and equidimensional of dimension $n - p$. For $1 \leq j \leq n - p$ we infer from [4], Proposition 2 that the real bipolar variety $(\mathcal{B}_{(i, j)})_{\mathbb{R}}$ (and hence the complex variety $\mathcal{B}_{(i, j)}$) contains at least one point of each connected component of $V_{\mathbb{R}}$. Thus $\mathcal{B}_{(i, j)}$ and $(\mathcal{B}_{(i, j)})_{\mathbb{R}}$ are equidimensional of dimension $j - 1$. From Proposition 7 we conclude that for $1 \leq j \leq n - p$ the algebraic variety $\mathcal{B}_{(i, j)} \setminus \mathcal{B}_{(i, j-1)}$ is locally definable by reduced regular sequences. In particular, $\mathcal{B}_{(i, 1)}$ is zero-dimensional and contains for each connected component of $V_{\mathbb{R}}$ an algebraic sample point. The algorithm Π_i proceeds now by deciding for each $1 \leq k \leq \frac{n}{p}$ whether $\mathcal{B}_{(i, k, 1)}$ contains real algebraic points, and, if it is the case, by computing them. The algorithm infers from these data whether S contains smooth real points. If the answer is positive, the set of data furnish also a finite set of smooth real algebraic sample points for the generically smooth connected components of $S_{\mathbb{R}}$.

At the beginning, the procedure Π_i generates for each $1 \leq k \leq \frac{n}{p}$ from the input circuit a new division-free circuit κ of size $O(L + np)$ and non-scalar depth $+O(1)$ that represents by its output nodes the polynomials of $\mathbb{Q}[X, \mathbf{B}, \Lambda, \Theta]$ which define as in Section 3 the variety $H_{i, \kappa}$. For the sake of simplicity we fix $\sigma := \kappa$ and suppose that σ is the identity permutation of $\text{Sym}(n)$. Taking the circuit κ as input, the procedure Π_i follows now the pattern of the (non-uniform or probabilistic) procedure described in in [3], Theorem 11 and [4], Theorem 13 in order to decide whether $V_{\mathbb{R}}$ is empty.

If $V_{\mathbb{R}}$ is empty then the procedure Π_i returns the answer that Δ vanishes identically on any connected component of $S_{\mathbb{R}}$.

Suppose that $V_{\mathbb{R}}$ is not empty. Then the procedure Π_i returns the coefficients of $n(p + 1) + 1$ polynomials $P, G_1, \dots, G_n, G_{n+1}, \dots, G_{n(p+1)} \in \mathbb{Q}[Z]$ satisfying for $G := (G_1, \dots, G_{n(p+1)})$ the following conditions:

- P is monic and separable,
- $\deg G < \deg P \leq \deg \mathcal{B}_{(i, \cdot, 1)}$,
- $\mathcal{B}_{(i, \cdot, 1)} = \{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$.

From this representation of the variety $\mathcal{B}_{(i, \cdot, 1)}$ we deduce that for $G := (G_1, \dots, G_n)$ the zero-dimensional variety $\{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$ contains a real algebraic sample point for each connected component of $S_{\mathbb{R}}$ where Δ does not vanish identically. The procedure Π_i collects now this information for any permutation σ , $1 \leq k \leq \frac{n}{\rho}$, in order to construct $n+1$ polynomials $P, G_1, \dots, G_n \in \mathbb{Q}[Z]$ which satisfy the output specifications above.

This is done in the following way. The polynomial P is obtained by taking the product of all polynomials P^k with $V_{\mathbb{R}}^k \neq \emptyset$, $1 \leq k \leq \frac{n}{\rho}$ and making the result squarefree. Then we have $\deg P \leq \rho$. From P the polynomials G_1, \dots, G_n are easily obtained applying a standard algorithm which goes back to Kronecker (see [23] for details). In this way the procedure Π_i produces a set of real algebraic sample points for the generically smooth connected components of $S_{\mathbb{R}}$ from G and the encoding “à la Thom” of the real zeros of P .

The procedure Π_i is based on the original paradigm [21, 20] of a procedure with intrinsic complexity that solves polynomial equation systems over the *complex* numbers (see also [19, 23, 17]).

We are now going to describe *succinctly* the procedure Π_i (Propositions 7 and 10 will play here a key role). For this purpose we shall freely refer to terminology, mathematical results and subroutines of [23], where the first streamlined version of the polynomial equation solver [21, 20] was presented and implemented as “Kronecker-algorithm” (compare also [29]).

In order to simplify the exposition we shall refrain from the presentation of details which ensure only appropriate genericity conditions for the procedure. The following description requires that the reader is acquainted with the details of the Kronecker-algorithm. Although this description may look at first glance intricate, no substantially new idea, which was not explained before, becomes introduced.

As before, we consider the identity permutation $\text{id} \in \text{Sym}(n)$. Recall that the polynomials of (2) generate the trivial ideal or form a strongly reduced regular sequence in $\mathbb{Q}[X, \mathbf{B}, \Lambda, \Theta]_{\Delta_\sigma}$. In this situation the procedure Π_i applies to the system (2) the algorithm “Geometric Solve” of [23] to decide whether $V = H_i$ is empty. In this case the information that $V_{\mathbb{R}}$ does not contain any smooth point is returned. Suppose that this is not the case. Then the algorithm “Geometric Solve” returns a lifting fiber of the variety V .

Next, beginning with $j := n - \rho$, the procedure Π_i decides for any index $1 \leq j \leq n - \rho$ whether the variety $\mathcal{B}_{(i, \cdot, j)}$ is empty or returns a lifting fiber of it. In case that there exists an index $1 \leq j \leq n - \rho$ with $\mathcal{B}_{(i, \cdot, j)} = \emptyset$, the procedure Π_i returns the information that $V_{\mathbb{R}}$ does not contain any smooth point. Suppose that this is not the case.

For $1 \leq j \leq n - \rho$ we fix a vector $t^{(j)} \in \mathbb{N}^{j-1}$ with $t^{(j)} := (t_1^{(j)}, \dots, t_{j-1}^{(j)})$ and $(n+1)\rho < t_1^{(j)} < \dots < t_{j-1}^{(j)} \leq n(\rho+1)$. In the same way as in [8], Section 4.3 one sees that the minor $m_{(i, \cdot, j; t^{(j)})}$ does not vanish identically on any irreducible component of $\mathcal{B}_{(i, \cdot, j)}$.

Following Proposition 7 the equations of the system (2) and the equations

$$M_1^{(i, \cdot, j, t^{(j)})} = 0, \dots, M_{n-\rho-j+1}^{(i, \cdot, j, t^{(j)})} = 0$$

define the variety $(\mathcal{B}_{(i, j)})_{m_{(i, \sigma, j; t^{(j)})}}$ outside of the locus of \mathbb{F}_i given by $m_{(i, j; t^{(j)})} = 0$. Our assumptions imply that this variety is not empty. Therefore, the polynomials of the equations above form a reduced regular sequence in $\mathbb{Q}[\mathcal{X}, \mathbf{B}, \Lambda, \Theta]_{m_{(i, \sigma, j; t^{(j)})}}$ and hence a lifting system in the sense of [23] for the variety $\mathcal{B}_{(i, j)}$. Inductively we suppose that there is given a lifting fiber of $\mathcal{B}_{(i, j)}$ on which $m_{(i, j; t^{(j)})}$ vanishes nowhere.

In this situation Π_i combines the algorithms ‘‘Lifting Curve’’, ‘‘Change Free Variables’’, ‘‘Change Lifting Point’’ and ‘‘Change Primitive Element’’ of [23] in order to produce a Kronecker-parameterization of a suitable curve $\mathcal{C}_{(i, j)}$ in $(\mathcal{B}_{(i, j)})_{m_{(i, \sigma, j; t^{(j)})}}$ which lifts the fiber of a sufficiently generic lifting point with respect to the lifting system and a sufficiently generic Noether position of $\mathcal{B}_{(i, j)}$.

Next the procedure Π_i applies for $1 \leq k \leq n - \rho - j + 1$ the algorithm ‘‘One Dimensional Intersect’’ of [23] to the given Kronecker-parameterization of $\mathcal{C}_{(i, j)}$ and the polynomials $M_k^{(i, j-1, t^{(j-1)})}$ and $m_{(i, j-1, t^{(j-1)})}$ and computes the greatest common divisor of the resulting univariate elimination polynomials. This greatest common divisor is not one since by assumption the variety $\mathcal{B}_{(i, j-1)}$ is not empty. In this way Π_i produces a lifting fiber of $\mathcal{B}_{(i, j-1)}$ on which $m_{(i, j-1, t^{(j-1)})}$ vanishes nowhere.

Finally Π_i produces a geometric solution of the zero-dimensional algebraic variety $\mathcal{B}_{(i, 1)}$. More precisely, the procedure Π_i produces a circuit representation of the coefficients of $n(\rho + 1) + 1$ polynomials $P, G_1, \dots, G_{n(\rho+1)} \in \mathbb{Q}[Z]$ as above.

Running the previous routine for each $k, 1 \leq k \leq \binom{n}{\rho}$, we deduce from the complexity estimates of [23] that Π_i uses

$$\begin{aligned} & \max\{\deg\{F_1 = 0, \dots, F_i = 0\} \mid 1 \leq i \leq \rho\}, \quad 2 \\ L(nd)^{O(1)} \max_{1 \leq k \leq \binom{n}{\rho}} & \max\{\deg S_{(r, l)}^{(i, k)} \mid 1 \leq r \leq \rho, 1 \leq l \leq n\}, \quad = \\ & \max\{\deg \mathcal{B}_{(i, k, j)} \mid 1 \leq j \leq n - \rho\} \\ & = L(nd)^{O(1)} \binom{n}{\rho}^2 \end{aligned}$$

arithmetical operations organized, with respect to the parameters of the arithmetic circuit, in non-scalar depth

$$O(n(\rho + \log(dn)) \log \binom{n}{\rho}).$$

The procedure can easily be translated to the bit model. Let ν_i be the logarithmic height of the polynomials F_1, \dots, F_ρ . In order to estimate the bit complexity of the procedure we consider the maximal logarithmic height, say $\nu_i = O((nd)^\rho)$, of the bipolar varieties $\mathcal{B}_{(i, k, 1)}$, $1 \leq k \leq \binom{n}{\rho}$. It is now straightforward to see that a representation of P as primitive polynomial of $\mathbb{Z}[Z]$ and hence a minimal arithmetic expression of the real zeros of P can be found using $O(L^2(nd)^{O(1)} \binom{n}{\rho} \nu_i^2)$ bit operations (see [25] for the relationship between arithmetic and bit representation of integers).

Let us finally observe that an alternative procedure to Π_i may be obtained applying for $j := 1$ the algorithm ‘‘Geometric Solve’’ of [23] to the equation system of Proposition 7. The complexity estimates for this procedure, which are the same as for Π_i , follow from arguments in [5], Section 4 and especially from Theorem 3 and Example 2.

We have therefore proven the following complexity statement (compare [3], Theorem 11, [4], Theorem 13 and [8], Theorem 14).

Theorem 14. *Let $n, p, d, i, \ell, L, \delta$ be natural numbers with $d \geq 1, 1 \leq i \leq n - p$. Let X_1, \dots, X_n and Z be indeterminates over \mathbb{Q} and let $X := (X_1, \dots, X_n)$.*

There exists an arithmetic network \mathcal{N} (or arithmetic-boolean circuit) over \mathbb{Q} , depending on certain parameters and having size

$$O(L(nd)^{O(1-\delta)} + (nd)^{O(n)})$$

and non-scalar depth

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

such that \mathcal{N} satisfies for suitable random specializations of its parameters the following condition:

Let $F_1, \dots, F_p \in \mathbb{Q}[X]$ be polynomials of degree at most d and assume that F_1, \dots, F_p are given by an essentially division-free arithmetic circuit in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ . Suppose that F_1, \dots, F_p form a strongly reduced regular sequence in $\mathbb{Q}[X]$ and that $\delta \leq \ell$ holds.

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

- P is monic and separable,
- $\deg G < \deg P \leq \ell$,
- 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 $\{F_1 = 0, \dots, F_p = 0\}_{\mathbb{R}}$.

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 [46, 47].

Three remarks on the formulation of Theorem 14 are at order.

The statement of Theorem 14 remains true if we replace ℓ by $\binom{n}{p} \ell$. This is a direct consequence of the estimate (11). Hence the combinatorial factor $\binom{n}{p}$ occurs hidden in the invariant ℓ . In terms of extrinsic complexity, our bounds therefore are comparable with those of [9]. An improvement can be obtained in case that the variables X_1, \dots, X_n are in generic position with respect to the variety $\{F_1 = \dots = F_p = 0\}$. In this case the factor $\binom{n}{p}$ in this complexity estimate may be dropped. In order to see this, observe that for the identity permutation $\text{id} \in \text{Sym}(n)$ the variety H_{id} contains for each generically smooth connected component C of $\{F_1 = \dots = F_p = 0\}_{\mathbb{R}}$ a point (x, b, \dots) such that x belongs to C . Hence the same is true for $\mathcal{B}_{(i, \text{id})}$. It suffices therefore to apply the subroutine of Π_i which corresponds to id in order to find real algebraic sample points for the generically smooth connected components of $\{F_1 = \dots = F_p = 0\}_{\mathbb{R}}$.

Next we remark that by (9) the condition $\delta \leq \ell$ is always satisfied for $\delta := \min\{(nd)^{c/n}, \ell\}$, where $c > 0$ is a suitable universal constant (independent of n and d). This illustrates that the estimates of Proposition 8 and Observation 11 implying

the estimate (8) (i.e., $\tau_i = (nd)^{O(n)}$) are not very relevant in this context. The worst case bound of Theorem 14 is only $(nd)^{O(n)}$.

Our third remark is the following statement.

Observation 15. *Theorem 14 asserts only the existence of a computation that, for given n -variate input polynomials F_1, \dots, F_p of degree at most d and circuit size and non-scalar depth L and τ_i , solves the real root finding problem for $F_1 = 0, \dots, F_p = 0$ in sequential and non-scalar parallel time $O(L(nd)^{O(1)}(\tau_i)^2)$ and $O(n(\tau_i + \log(nd))\log \tau_i)$, respectively.*

Theorem 14 refers therefore to the non-uniform complexity model. In order to realize such a computation in terms of the uniform complexity model within the same order of sequential and parallel time, probabilistic methods have to be used (see [29] and [23]). This is achieved by choosing randomly the parameters of the arithmetic network \mathcal{N} of Theorem 14.

In [8], Section 5 we developed a common view for the procedures Π_i , $1 \leq i \leq n - p$, solving the task of finding smooth points in possibly singular, real compact hypersurfaces, and for the algorithm of [1] which solves the same task in the smooth case.

When we have to solve a concrete polynomial equation system $F_1 = 0, \dots, F_p = 0$, sometimes the procedures Π_i , $1 \leq i \leq n - p$ and algorithms of [2, 3, 4] may be combined in order to improve the complexity. However, such improvements depend on ad hoc methods and do not lead to a general algorithm. Moreover, the hypersurface case treated in [8] does not differ substantially from that of an arbitrary complete intersection. Therefore, we do not enter into details here and refer the reader to the mentioned paper.

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, and L. M. Pardo, *On the intrinsic complexity of point finding in real singular hypersurfaces*, Inf. Proc. Letters, 109 (2009), 1141-1144. MR2552931 (2010j:68036)
- [7] B. Bank, M. Giusti, J. Heintz, and L. M. Pardo, *Bipolar varieties and real solving of a singular polynomial equation*, Jaen J. Approximation 2, 1 (2010), 65-77. MR2789520 (2012e:14111)
- [8] B. Bank, M. Giusti, J. Heintz, L. Lehmann, and L. M. Pardo, *Algorithms of intrinsic complexity for point searching in compact real singular hypersurfaces*, Found. Comput. Math. 12, no. 1, 75-122 (2012). MR2886157
- [9] 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)
- [10] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in real algebraic geometry*, (2. ed.) Springer Verlag, Berlin etc. 2006. MR2248869 (2007b:14125)
- [11] 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)

- [12] J.F. Canny, *Some algebraic and geometric computations in PSPACE*, ACM Symposium on Theory of Computing (STOC) (1988), 460-467.
- [13] 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)
- [14] 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)
- [15] C. D' Andrea, T. Krick, and M. Sombra, *Heights of varieties in multi-projective spaces and arithmetic Nullstellensätze*, Manuscript, Universidad de Buenos Aires (2011)
- [16] M. Demazure, *Catastrophes et bifurcations*, Ellipses, Paris 1989.
- [17] C. Durvy, G. Lecerf, *A concise proof of the Kronecker polynomial system solver from scratch*, Expo. Math. 26 (2008), no.2, 101-139. MR2413831 (2009c:14119)
- [18] W. Fulton, *Intersection theory (2nd ed.)*, *Ergebnisse der Mathematik und ihrer Grenzgebiete 3 Folge 2*, Springer Verlag, Berlin etc. 1998. MR1644323 (99d:14003)
- [19] 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)
- [20] 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)
- [21] 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)
- [22] 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)
- [23] M. Giusti, G. Lecerf, and B. Salvy, *A Gröbner free alternative for polynomial system solving*, J. Complexity 17 (2001), 154-211. MR1817612 (2002b:68123)
- [24] 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)
- [25] K. Hägele and J. L. Montaña, *Polynomial random test for the equivalence of integers given by arithmetic circuits*, Depto. de Matematicas, Estadística y Computacion, Universidad de Cantabria, 4 (1997)
- [26] J. Heintz, *Definability and fast quantifier elimination in algebraically closed fields*, Theor. Comput. Sci. 24 (1983), 239-277. MR0716823 (85a:68062)
- [27] J. Heintz, B. Kuijpers, A. Rojas Paredes, *Software Engineering and complexity in effective algebraic geometry*, J. Complexity 28 (2012), to appear.
- [28] J. Heintz, B. Kuijpers, A. Rojas Paredes, *On the intrinsic complexity of elimination problems in effective algebraic geometry*, arXiv:1201.4344v3.
- [29] 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)
- [30] 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.
- [31] 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)
- [32] 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)
- [33] G. Kempf, *On the geometry of a theorem of Riemann*, Ann. Math. (2) 98 (1973), 178-185. MR0349687 (50 #2180)
- [34] A.P. Morgan, and A. J. Sommese, *A homotopy for solving general polynomial systems that respects m-homogeneous structures*, Appl. Math. Comput., 24, (1987), 101-113. MR0914806 (88j:65110)
- [35] 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.

- [36] 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)
- [37] T. G. Room, *The geometry of determinantal loci*, Cambridge Univ. Press (1938).
- [38] F. Severi, *Sulle intersezioni delle varietà algebriche e sopra i loro caratteri e singolarità proiettive*, Torino Mem. (2) 52 (1903), 61-118.
- [39] 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.
- [40] M. Spivak, *Calculus on manifolds. A modern approach to classical theorems of advanced calculus*, W. A. Benjamin, Inc., New York-Amsterdam, 1965. MR0209411 (35 #309)
- [41] B. Teissier, *Variétés polaires II., Multiplicités polaires, sections planes, et conditions de Whitney*, in: Algebraic geometry, Proc. int. Conf., La Rabida/Spain 1981, Lect. Notes Math. 961, 1982, pp. 314-491. MR0708342 (85i:32019)
- [42] 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)
- [43] J.A. Todd, *The geometrical invariants of algebraic loci*, Proc. London Math. Soc. S2-43 (1937), 127-138. MR1575589
- [44] J. A. Todd, *The arithmetical invariants of algebraic loci*, Proc. London Math. Soc. S2-43 (1937) no.3, 190-225. MR1575915
- [45] W. Vogel, *Lectures on results on Bézout's theorem*. Notes by D. P. Patil, Lectures on Mathematics and Physics, Mathematics, 74, Tata Institute of Fundamental Research, Springer Verlag, Berlin etc., 1984. MR0743265 (86f:14003)
- [46] 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
- [47] J. von zur Gathen, *Parallel linear algebra*, in Synthesis of parallel algorithms (J. H. Reif, ed.), Kaufmann, San Mateo, CA., 1993, pp. 573-617.

Prof. Dr. Bernd Bank – Institut für Mathematik – Humboldt-Universität zu Berlin
 – Unter den Linden 6 – D-10099 Berlin – Germany
E-mail address: bank@mathematik.hu-berlin.de

Prof. Dr. Marc Giusti – CNRS, École Polytechnique – Lab. LIX – F-91228 Palaiseau
 – Cedex France
E-mail address: marc.giusti@polytechnique.fr

Prof. Dr. Joos Heintz – Departamento de Computación – Universidad de Buenos Aires – CONICET – Ciudad Universitaria – Pabellón I – 1428 Buenos Aires – Argentina,
 –Departamento de Matemáticas, Estadística y Computación – Facultad de Ciencias – Universidad de Cantabria – Avda. de los Castros – E-39005 Santander, Spain
E-mail address: joos@dc.uba.ar