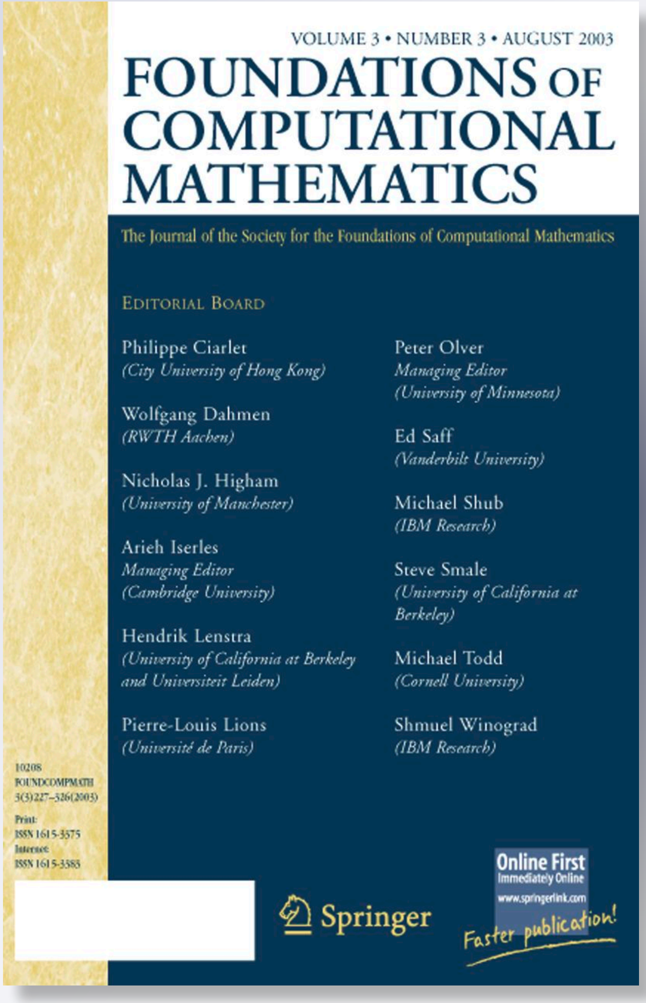
Algorithms of Intrinsic Complexity for Point Searching in Compact Real Singular Hypersurfaces

Bernd Bank, Marc Giusti, Joos Heintz, Lutz Lehmann & Luis Miguel Pardo

Foundations of Computational Mathematics
The Journal of the Society for the Foundations of Computational Mathematics

ISSN 1615-3375
Volume 12
Number 1

Found Comput Math (2012) 12:75-122
DOI 10.1007/s10208-011-9112-6



Springer

Found Comput Math (2012) 12:75–122
DOI 10.1007/s10208-011-9112-6

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Algorithms of Intrinsic Complexity for Point Searching in Compact Real Singular Hypersurfaces

Bernd Bank · Marc Giusti · Joos Heintz ·
Lutz Lehmann · Luis Miguel Pardo

Received: 9 June 2010 / Revised: 26 May 2011 / Accepted: 1 November 2011 /
Published online: 4 January 2012

Abstract For a real square-free multivariate polynomial F, we treat the general problem of finding real solutions of the equation $F = 0$, provided that the real solution

Dedicated to Tomás Recio on the occasion of his 60th birthday.

Communicated by Teresa Krick.

B. Bank · L. Lehmann
Institut für Mathematik, Humboldt-Universität zu Berlin, 10099 Berlin, Germany

B. Bank
e-mail: bank@mathematik.hu-berlin.de

L. Lehmann
e-mail: llehmann@mathematik.hu-berlin.de

M. Giusti
CNRS, Lab. LIX, École Polytechnique, 91228 Palaiseau CEDEX, France
e-mail: Marc.Giusti@Polytechnique.fr

J. Heintz (✉)
Departamento de Computación, Universidad de Buenos Aires and CONICET, Ciudad Univ.,
Pab. I, 1428 Buenos Aires, Argentina
e-mail: joos@dc.uba.ar

J. Heintz · L.M. Pardo
Departamento de Matemáticas, Estadística y Computación, Facultad de Ciencias,
Universidad de Cantabria, 39071 Santander, Spain

J. Heintz
e-mail: heintzj@unican.es

L.M. Pardo
e-mail: luis.pardo@unican.es

set $\{F=0\}_{\mathbb{R}}$ is compact. We allow that the equation $F=0$ may have singular real solutions. We are going to decide whether this equation has a non-singular real solution and, if this is the case, we exhibit one for each generically smooth connected component of $\{F=0\}_{\mathbb{R}}$. We design a family of elimination algorithms of *intrinsic complexity* which solves this problem. In the worst case, the complexity of our algorithms does not exceed the already known *extrinsic* complexity bound of $(nd)^{O(n)}$ for the elimination problem under consideration, where n is the number of indeterminates of F and d its (positive) degree. In the case that the real variety defined by F is smooth, there already exist algorithms of intrinsic complexity that solve our problem. However, these algorithms cannot be used in case when $F=0$ admits F-singular real solutions.

An elimination algorithm of intrinsic complexity presupposes that the polynomial F is encoded by an essentially division-free arithmetic circuit of size L (i.e., F can be evaluated by means of L additions, subtractions and multiplications, using scalars from a previously fixed real ground field, say $\mathbb{Q}$) and that there is given an invariant $\delta(F)$ which (roughly speaking) depends only on the geometry of the complex hypersurface defined by F. The complexity of the algorithm (measured in terms of the number of arithmetic operations in $\mathbb{Q}$) is then *linear* in L and *polynomial* in n, d and $\delta(F)$.

In order to find such a geometric invariant $\delta(F)$, we consider suitable incidence varieties which in fact are algebraic families of dual polar varieties of the complex hypersurface defined by F. The generic dual polar varieties of these incidence varieties are called *bipolar varieties* of the equation $F=0$. The maximal degree of these bipolar varieties then becomes the essential ingredient of our invariant $\delta(F)$.

Keywords Real polynomial equation solving · Intrinsic complexity · Singularities · Polar and bipolar varieties · Degree of varieties

Mathematics Subject Classification (2010) 14P05 · 14B05 · 14B07 · 68W30

1 Introduction

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 $n-p$. Put otherwise, S is a closed subvariety of $\mathbb{A}^n$ of pure codimension p (in $\mathbb{A}^n$).

Let $\mathbb{A}^n_{\mathbb{R}} := \mathbb{R}^n$ 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 also use the following notation:

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

We call the regular sequence $F_1, \ldots, F_p$ *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 $J(F_1, \ldots, F_p) := [\frac{\partial F_j}{\partial X_k}]_{\substack{1 \leq j \leq p \\ 1 \leq k \leq n}}$ 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 $S_{\mathrm{sing}} := S \setminus S_{\mathrm{reg}}$ is called the *singular locus* of S. Notice 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 regular point.

We suppose now that there are given natural numbers d, L and ℓ and an essentially division-free arithmetic circuit σ 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 σ represent the polynomials $F_1, \ldots, F_p$ by evaluation.
- The size and the non-scalar depth of the arithmetic circuit σ are bounded by L and ℓ, respectively.

For the terminology and basic facts concerning arithmetic circuits we refer to [13, 15, 23].

The fundamental algorithmic elimination problem which motivates the outcome of the present paper is the search for an invariant and a *non-uniform deterministic* or *uniform probabilistic* algorithm Π satisfying the following specification.

(i) The invariant is a function which assigns to $F_1, \ldots, F_p$ a positive integer value $\delta := \delta(F_1, \ldots, F_p)$ of asymptotic order not exceeding $(nd)^{O(n)}$, called the *degree of the real interpretation of the equation system* $F_1 = 0, \ldots, F_p = 0$. The value $\delta(F_1, \ldots, F_p)$ depends rather on the resulting variety S and its geometry than on the defining polynomials $F_1, \ldots, F_p$ themselves.

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

(iii) In order to achieve this goal, the algorithm Π performs on input σ a computation in $\mathbb{Q}$ with $L(nd)^{O(1)}\delta^{O(1)}$ arithmetic operations (additions, subtractions, multiplications and divisions) which become organized in non-scalar depth $O(n(\ell + \log nd) \log \delta)$ with respect to the parameters of the arithmetic circuit σ.

The formulation of this problem is somewhat imprecise, because of the requirement (i) that the value $\delta(F_1, \ldots, F_p)$ depends “rather on the resulting variety S and its geometry than on the defining polynomials $F_1, \ldots, F_p$ themselves”. This is due to the fact that in case that $S_{\mathbb{R}}$ is smooth and $F_1, \ldots, F_p$ is strongly reduced, it is possible to exhibit an algorithm that fulfills conditions (ii) and (iii) and that contains a preprocessing which reduces $F_1, \dots, F_p$ to a single (elimination) polynomial P such that P depends only on S and has, in particular, the same degree as S. The remaining part of the algorithm is its main subroutine, which depends only on S (see [4, 5, 50, 51]).

In view of [15, 23] it seems unlikely that the dependence of the degree of the real interpretation of $F_1 = 0, \dots, F_p = 0$ on the given equations can be completely reduced to an exclusive dependence on S. However, the quantity $\delta(F_1, \dots, F_p)$ depends only through $F_1, \dots, F_p$ on the input circuit σ. We therefore consider $\delta(F_1, \dots, F_p)$ as an *intrinsic* complexity parameter measuring the size of the input σ. The quantities n, d, L and ℓ are considered as *extrinsic* parameters measuring the size of σ.

In these terms we may say that we search for algorithms Π of *intrinsic* complexity which solve the algorithmic elimination problem expressed by requirement (ii). Since the complexity $L(nd)^{O(1)}\delta^{O(1)}$ is polynomial in all parameters, including the intrinsic parameter $\delta := \delta(F_1, \dots, F_p)$, we say that the algorithm Π is *pseudo-polynomial*. As already mentioned, in the case that $S_{\mathbb{R}}$ is smooth and $F_1, \dots, F_p$ is a strongly reduced regular sequence, there already exist algorithms which fit in this pattern, i.e., which have pseudo-polynomial intrinsic complexity.

An important issue is the requirement of (i) that the asymptotic order of $\delta(F_1, \dots, F_p)$ does not exceed the extrinsic bound $(nd)^{O(n)}$. This implies that any algorithm Π that satisfies the specification (i), (ii), and (iii) has a worst case complexity that meets the already known extrinsic bound of $(nd)^{O(n)}$ for the elimination problem under consideration (compare the original papers [9, 14, 29, 32–34, 47, 48] and the comprehensive book [10]).

Algorithms of intrinsic complexity for elimination problems over the *complex* numbers (or more generally, over arbitrary algebraically closed fields) were first introduced in [24–27] (see also [35] and the survey [38]). Decisive progress in the direction of computer implementations was made in [28] (see also [36]). This led to the development of the software package “Kronecker” by G. Lecerf [42]. The main procedure of the “Kronecker” software package solves over the complex numbers the multivariate circuit represented polynomial equation systems by a reusable and portable algorithm of intrinsic (bit-) complexity character. This algorithm supports type polymorphism and runs in an exact computer algebra as well as in a numeric environment. In the sequel we shall refer to the underlying theoretical procedure as the “Kronecker algorithm” (see Sect. 4).

The Kronecker software package contains various extensions of its main procedure to other, more ambitious elimination tasks in (complex) algebraic geometry and commutative algebra (see [19, 40, 41] for the theoretical aspects of this extension and [20] for a streamlined presentation of the underlying mathematics).

In the context of wavelet constructions, the Kronecker algorithm and software has been adapted to the real case in [43, 44] for the computation of real solutions of polynomial equation systems.

We now come back to the initial real elimination problem. In [2] we solved this problem first for a smooth and compact real hypersurface given by a square-free equation. For an arbitrary strongly reduced regular sequence $F_1, \dots, F_p \in \mathbb{Q}[X]$ defining a complex affine variety S with *smooth* and *compact* real trace $S_{\mathbb{R}}$, we solved the problem in [3]. Finally, the problem was tackled in [4, 5, 50, 51] under the single assumption that $S_{\mathbb{R}}$ is smooth.

In all these cases the intrinsic invariant which essentially determines the complexity of the algorithm is a combination of the degree of the original equation system $F_1 = 0, \ldots, F_p = 0$ with the maximal degree of the *generic* polar varieties of suitable type, namely *classic* or *dual*, of the complex variety S (see [25, 27] for the notion of system degree and [4, 5, 8] for motivations, definitions and basic properties of classic and dual polar varieties).

The introduction of the (at this moment) new notion of *dual* polar variety became necessary in order to settle the case when $S_{\mathbb{R}}$ is unbounded. In this situation some of the generic *classic* polar varieties of S may have an empty intersection with $S_{\mathbb{R}}$. This makes classic polar varieties inappropriate for algorithmic applications if $S_{\mathbb{R}}$ is unbounded.

The dual polar varieties are the complex counterpart of Lagrange multipliers. In [4, 5] we introduced the notion of a *generalized polar variety* of S associated with a given embedding of S into the projective space $\mathbb{P}^n$ and a given non-degenerate hyperquadric of $\mathbb{P}^n$. These generalized polar varieties form an algebraic family which connects the classic with the dual polar varieties of S.

In case that $S_{\mathbb{R}}$ is smooth, but possibly unbounded, the fundamental issue for our algorithmic method is the fact that the dual polar varieties of S cut each connected component of $S_{\mathbb{R}}$ (compare [8], and Theorem 1 below for the case that $S_{\mathbb{R}}$ is singular).

The *generic* (classic or dual) polar varieties of S, and therefore also their degrees, depend only on S and not on the particular equations which define S. Thus, if the real traces of the generic polar varieties of S are all non-empty, their maximal degree becomes a candidate for an intrinsic invariant which rules over the complexity of an algorithm which satisfies requirement (ii) above. This was the strategy followed in [4, 5], which led to a solution of our algorithmic elimination problem in case that $S_{\mathbb{R}}$ is smooth, but possibly unbounded.

In Theorem 14 of Sect. 4 we shall present a discrete family of algorithms which solves our problem in the particular case of a *compact* real hypersurface containing smooth points and possibly also singularities.

So we start with a square-free polynomial $F \in \mathbb{Q}[X]$ of positive degree d and with an essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ, such that σ has a single output node representing F. Let $S := \{F = 0\}$, and suppose that $S_{\mathbb{R}}$ is compact.

We ask for an invariant $\delta := \delta(F)$ of asymptotic order not exceeding $(nd)^{O(n)}$, called the *degree of the real interpretation of the equation* $F = 0$, and for an algorithm Π satisfying for $p := 1$ the above specification.

Observe that the invariant $\delta(F)$ depends only on the complex hypersurface S, since F is supposed to be square-free. In this sense we consider as automatically satisfied the informal requirement above, namely that $\delta(F)$ depends rather on S than on the defining polynomial F itself.

The methods developed in [2–5, 50, 51] for the case that $S_{\mathbb{R}}$ is smooth (but not necessarily compact) cannot be applied directly when $S_{\mathbb{R}}$ is singular. This becomes clear on observing that in the singular case some of the *generic* polar varieties of S may have empty real traces, even if $S_{\mathbb{R}}$ is compact.

Nevertheless, Corollary 1 of [8] asserts the *existence* of generic *dual* polar varieties which cut $S_{\mathbb{R}}$ in smooth points in case that $(S_{\text{reg}})_{\mathbb{R}}$ is non-empty.

Using suitable algebraic families of *dual* polar varieties of the complex hypersurface S we shall find a way out of this dilemma. We realize these algebraic families by means of *equidimensional* and *smooth* complex incidence varieties which we call *polar incidence varieties of the equation* $F=0$.

It turns out that the degrees of the generic dual polar varieties of the polar incidence varieties of the equation $F=0$, called *bipolar varieties* of the equation $F=0$, furnish appropriate invariants for the design of discrete families of procedures which solve on input σ our algorithmic elimination problem for the compact real hypersurface $S_{\mathbb{R}}$.

The degrees of the polar varieties of the most general type of polar incidence variety of the equation $F=0$ remain invariant under unitary linear transformations of the indeterminates $X_1, \ldots, X_n$. In this sense they are intrinsic invariants of the equation $F=0$.

One may ask, in case $(S_{\text{reg}})_{\mathbb{R}} \neq \emptyset$, what the generic dual polar varieties are that contain smooth points of $S_{\mathbb{R}}$. We deduce from [8], Corollary 1 that such generic polar varieties always exist. If we would be able to exhibit explicit equations for such generic dual varieties, then we could also find real solutions of the equation $F=0$ in the same way as in the case that $S_{\mathbb{R}}$ is smooth.

This leads us to the question of how we could find efficiently (rational or algebraic) witness points for strict polynomial inequalities (see end of Sects. 4 and 6 for motivations and a partial answer).

For the search of generic dual polar varieties which cut $S_{\mathbb{R}}$ in smooth points, we have to investigate how dual polar varieties vary with their parameters. This is done in Theorem 8.

In Sect. 5 we introduce a unified view of the algorithms developed in Sect. 4 for the case that $S_{\mathbb{R}}$ is possibly singular, and of the algorithms of [2, 4, 5, 50, 51] for the case that $S_{\mathbb{R}}$ is smooth. All these algorithms become interpreted as *walks* in suitable graphs. Theorem 17 reflects Theorem 14 in this context. The complex Kronecker algorithm turns out to be a substantial ingredient of our procedures.

We might also consider an avatar of polar incidence varieties based on the pattern of classic polar varieties. The advantage of this construction would be that we get rid of the compactness assumption on $S_{\mathbb{R}}$ for our point finding algorithms.

However, if $S_{\mathbb{R}}$ contains smooth *and* singular points, the higher dimensional *classic* generic polar varieties may all become empty, even if $S_{\mathbb{R}}$ is compact. This makes a statement like Theorem 8 senseless in the classic setting. Hence the geometrical structure of the polar incidence varieties based on the dual pattern is richer than that of their classic counterpart. For this reason, there is still room for future complexity improvements in the dual case, but not in the classic one.

A local version of the complexity statements of Sect. 5 in terms of classic polar varieties is contained in [6] and [7], with a substantially different treatment of the corresponding polar incidence variety of $F=0$.

For another approach, relying on the so-called "critical point method", to find roots in singular real hypersurfaces we refer to [1] and [49].

The reader only interested in the algorithms and their correctness proofs, namely Theorems 14, 17 and 19, may restrict his attention to Propositions 5 and 12 and the estimates of the degrees of distinct types of bipolar variety in Sect. 4.2. The rest of the mathematical results of this paper illustrate the relevance of the general concept of the bipolar variety for algorithmic applications.

We shall make extensive use of the general concept of polar varieties. The modern notion of classic polar varieties was introduced in the 1930s by F. Severi [53, 54] and J.A. Todd [60, 61], while the intimately related 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 the rational equivalence classes of generic classic polar varieties.

Around 1975 a renewal of the theory of classic polar varieties took place with essential contributions due to R. Piene [46] (global theory), B. Teissier, D.T. Lê [39, 58], J.P. Henry and M. Merle [37], A. Dubson [18], Chap. IV (local theory), J. P. Brasselet and others (the list is not exhaustive; see [46, 59] and [12] for a historical account and references). The idea was to use rational equivalence classes of generic classic polar varieties as a tool which allows one to establish numerical formulas in order to classify singular varieties by their intrinsic geometric character [46].

On the other hand, first classic and then dual polar varieties around 12 years ago became a fundamental tool for the design of efficient computer procedures of intrinsic complexity which solve suitable instances of our algorithmic elimination problem [2–5]. The use of polar varieties in the present paper is based on certain geometric facts which are developed in [8]. Of particular relevance is a relative estimate of the degree for polar varieties, namely [8], Theorem 3, which allows us to compare the intrinsic complexities of distinct algorithms.

2 Preliminaries About Polar Varieties

Let the notation be as in the Introduction. Unless stated otherwise, we suppose throughout this section that $F_1, \dots, F_p \in \mathbb{Q}[X]$ is a *reduced* regular sequence defining a (non-empty) subvariety S of $\mathbb{A}^n$ of pure codimension p.

Let $1 \le i \le n - p$ and let $a := [a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 0\le l\le n}}$ be a complex matrix, and suppose that $a_* := [a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 1\le l\le n}}$ 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 $1 \le k \le n-p-i+1$ are spanned by the points $(a_{k,0} : a_{k,1} : \dots : a_{k,n})$.

The classic and the dual ith 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 regular points of S where all $(n-i+1)$-minors of the polynomial $((n-i+1)\times n)$ matrix

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

vanish. We denote these polar varieties by

$$W_{\underline{K}(a)}(S) := W_{\underline{K}^{n-p-i}(a)}(S) \quad \text{and} \quad W_{\overline{K}(a)}(S) := W_{\overline{K}^{n-p-i}(a)}(S),$$

respectively. They are of expected pure codimension i in S and do not depend on the particular choice of the reduced regular sequence defining S. In the sequel we shall restrict our attention to the concept of dual polar varieties only.

If a is a real $((n-p-i+1)\times(n+1))$ matrix, we denote by

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

the real trace of $W_{\overline{K}(a)}(S)$.

Observe that this definition of dual polar varieties may be extended to the case that there is given a Zariski open and dense 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 Sect. 4 we shall need this extended definition of polar varieties in order to establish the notion of a bipolar variety of a given hypersurface. 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 [4] and [5] 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 matrix $a=[a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 0\le l\le n}}$ with $a_* := [a_{k,l}]_{\substack{1\le k\le n-p-i+1\\ 1\le l\le n}}$ *generic*, the dual polar variety $W_{\overline{K}(a)}(S)$ is either empty or of pure codimension i in S. Further, we proved that $W_{\overline{K}(a)}(S)$ is normal and Cohen–Macaulay (but non necessarily smooth) at any of its $(F_1,\dots,F_p)$-regular points (see [8], Corollary 2 and Sect. 3.1). This motivates the consideration of the so-called *generic* dual polar varieties $W_{\overline{K}(a)}(S)$, associated with a complex $((n-p-i+1)\times(n+1))$ matrix a with a_* generic, as an invariant of the complex variety S (independently of the given equation system $F_1 = 0, \dots, F_p = 0$). However, when this matrix a is real, we cannot consider $W_{\overline{K}(a)}(S_{\mathbb{R}})$ as an invariant of the real variety $S_{\mathbb{R}}$, since for a suitable real $((n-p-i+1) \times (n+1))$ matrix a with a_* generic, this polar variety may turn out to be empty, whereas for another real matrix of this kind it may contain points (see [8], Theorem 1 and Corollary 1 and Theorem 8 and Corollary 9 below). For our use of the word "generic" we refer to [8], Definition 1.

In case that $S_{\mathbb{R}}$ is *smooth* and a is a real $((n-p-i+1) \times (n+1))$ matrix with full rank submatrix a_*, the real dual polar variety $W_{\overline{K}(a)}(S_{\mathbb{R}})$ contains always a point of each connected component of $S_{\mathbb{R}}$. We are now going to state and prove a technical result about affine linear sections of dual polar varieties. This will be needed in Sects. 4 and 5.

Let $\overline{X} := (X_1, \dots, X_{n-1})$ and let O be a Zariski open and dense subset of $\mathbb{A}^n$ and, let $c \in \mathbb{A}^1$ be a complex number such that the equations $F_1(X) = 0, \dots, F_p(X) = 0$ and the equations $F_1(\overline{X}, c) = 0, \dots, F_p(\overline{X}, c) = 0$ intersect transversally at any of their common zeros that belong to O or to $O_c := \{\overline{x} \in \mathbb{A}^{n-1} \mid (\overline{x}, c) \in O\}$, respectively. Denote by $\mu_c : \mathbb{A}^{n-1} \to \mathbb{A}^n$ the embedding of affine spaces defined for $\overline{x} \in \mathbb{A}^{n-1}$ by $\mu_c(\overline{x}) := (\overline{x}, c)$.

We compare now the dual polar varieties of

$$S := \bigl\{F_1(X) = 0, \dots, F_p(X) = 0\bigr\} \cap O$$

and

$$S_c := \bigl\{F_1\bigl(\overline{X}, c\bigr) = 0, \dots, F_p\bigl(\overline{X}, c\bigr) = 0\bigr\} \cap O_c.$$

Observe that S and S_c are (locally closed) subvarieties of $\mathbb{A}^n$ and $\mathbb{A}^{n-1}$ which we suppose to be non-empty.

Let $1 \leq i < n - p$ and let $a = [a_{k,l}]_{\substack{1 \leq k \leq n-p-i \\ 0 \leq l \leq n}}$ be a complex matrix such that $[a_{k,l}]_{\substack{1 \leq k \leq n-p-i \\ 1 \leq l \leq n}}$ has maximal rank $n - p - i$.

Lemma 1 *Let notation be as above; further let* $a' := [a_{k,l}]_{\substack{1 \leq k \leq n-p-i \\ 0 \leq l \leq n-1}}$ *and* $a'' := \left[\begin{smallmatrix} & a & \\ 0 & \cdots 0 & 1 \end{smallmatrix}\right]$. *Then, in case* $(a_{1,0}, \dots, a_{n-p-i,0}) \neq 0$, *the affine linear map* $\mu_c : \mathbb{A}^{n-1} \to \mathbb{A}^n$ *induces an isomorphism between the dual polar variety* $W_{\overline{K}^{n-p-i}(a')}(S_c)$ *and the closed variety* $W_{\overline{K}^{n-p-i}(a'')}(S) \cap \{X_n - c = 0\}$.

Proof Deleting in the matrices a' and a'' the columns number 0, we obtain full rank matrices. Therefore the dual polar varieties $W_{\overline{K}^{n-p-i}(a')}(S_c)$ and $W_{\overline{K}^{n-p-i}(a'')}(S)$ are well defined. It suffices to show that μ_c induces an isomorphism between $W_{\overline{K}^{n-p-i}(a')}(S_c) \cap O_c$ and $W_{\overline{K}^{n-p-i}(a'')}(S) \cap \{X_n - c = 0\} \cap O$. From our assumptions, we deduce that the mapping μ_c identifies S_c with $S \cap \{X_n - c = 0\}$ and that for each $\overline{x} \in S_c$ the point $\overline{x}$ is $(F_1(\overline{X}, c), \dots, F_p(\overline{X}, c))$-regular and the point $\mu_c(\overline{x}) = (\overline{x}, c)$ is $(F_1, \dots, F_p)$-regular. Let $\overline{x}$ be an arbitrary element of S_c. Then all $(n-i)$-minors of the polynomial $((n-i)\times(n-1))$ matrix

$$L := \begin{bmatrix} \frac{\partial F_1}{\partial X_1}(\overline{X}, c) & \cdots & \frac{\partial F_1}{\partial X_{n-1}}(\overline{X}, c) \\ \vdots & \vdots & \vdots \\ \frac{\partial F_p}{\partial X_1}(\overline{X}, c) & \cdots & \frac{\partial F_p}{\partial X_{n-1}}(\overline{X}, c) \\ a_{1,1} - a_{1,0}X_1 & \cdots & a_{1,n-1} - a_{1,0}X_{n-1} \\ \vdots & \vdots & \vdots \\ a_{n-p-i,1} - a_{n-p-i,0}X_1 & \cdots & a_{n-p-i,n-1} - a_{n-p-i,0}X_{n-1} \end{bmatrix}$$

vanish at $\overline{x}$ if and only if all $(n-i+1)$-minors of the polynomial $((n-i+1)\times n)$ matrix, obtained from L by adding the row $(0,\dots,0,1)$, vanish at $\mu_c(\overline{x})$. This implies that $\overline{x}$ belongs to $W_{\overline{K}^{n-p-i+1}(a')}(S_c)\cap O_c$ if and only if $\mu_c(\overline{x})$ belongs to $W_{\overline{K}^{n-p-i}(a'')}(S)\cap\{X_n - c = 0\}\cap O$. □

3 Polar Incidence Varieties

3.1 Basic Incidence Varieties

Let d, n and i be natural numbers, $1\leq i\leq n-1$, let $X := (X_1,\dots,X_n)$, $\Omega := (\Omega_1,\dots,\Omega_{n-i})$ be row vectors, and let $A := [A_{k,l}]_{\substack{1\leq k\leq n-i\\ 0\leq l\leq n}}$ be a matrix of indeterminates over $\mathbb{C}$. Furthermore, let Λ be a single indeterminate over $\mathbb{C}$ and $F\in\mathbb{R}[X_1,\dots,X_n]$ an n-variate polynomial over $\mathbb{R}$ of positive degree $\deg F = d$. The polynomial F will be fixed for the rest of this paper.

Let $J(F) := (\frac{\partial F}{\partial X_1},\dots,\frac{\partial F}{\partial X_n})$ be the gradient (i.e., the Jacobian) of F. For the sake of simplicity of the exposition we shall from now on assume that F is reduced (i.e., square-free). Thus $J(F)$ does not vanish identically on any irreducible component of the complex hypersurface $\{F=0\}$.

For a complex $((n-i)\times(n+1))$ matrix $a := [a_{k,l}]_{\substack{1\leq k\leq n-i\\ 0\leq l\leq n}}$ and a point $x = (x_1,\dots,x_n)\in\mathbb{A}^n$ we write $A_0 := (A_{1,0},\dots,A_{n-i,0})$, $a_0 := (a_{1,0},\dots,a_{n-i,0})$, $A_* := [A_{k,l}]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}}$ and, as above, $a_* := [a_{k,l}]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}}$. Furthermore, we denote by $A(X)$ and $a(x)$ the $((n-i)\times n)$ matrices $[A_{k,l} - A_{k,0}X_l]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}}$ and $[a_{k,l} - a_{k,0}x_l]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}}$.

Thus, specializing the $((n-i)\times(n+1))$ matrix A to a and the row vector X to x, we obtain a_0, a_*, and $a(x)$ as specializations of A_0, A_* and $A(X)$, respectively. We indicate the rank of a matrix, e.g. of a, by $\mathrm{rk}(a)$. As usual we denote by a^T the transposed matrix of a.

For $(\lambda,\omega_1,\dots,\omega_{n-i})\in\mathbb{A}^{n-i+1}\setminus\{0\}$ and $\omega := (\omega_1,\dots,\omega_{n-i})$ we shall write $(\lambda:\omega) := (\lambda:\omega_1:\cdots:\omega_{n-i})$ for the corresponding point of $\mathbb{P}^{n-i}$.

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

$$\mathbb{M}_i := \mathbb{A}^n\times\mathbb{A}^{(n-i)\times(n+1)}\times\mathbb{P}^{n-i}$$

containing the $\mathbb{R}$-definable locally closed incidence variety

$$E_i := \big\{\big(x, a, (\lambda : \omega)\big) \in \mathbb{M}_i \mid F(x) = 0, \operatorname{rk} a_* = \operatorname{rk} a(x) = n - i,\\ a_0\omega^{\mathrm{T}} \neq 0, J(F)(x)^{\mathrm{T}}\lambda + a(x)^{\mathrm{T}}\omega^{\mathrm{T}} = 0\big\}.$$

Let $(x, a, (\lambda : \omega))$ be an arbitrary point of E_i. From $a_0\omega^{\mathrm{T}} \neq 0$ and $\operatorname{rk} a(x) = n - i$ we deduce first $\omega \neq 0$ and then $J(F)(x) \neq 0$ and $\lambda \neq 0$.

Observation 2 *Let x be a point of $\mathbb{A}^n$ satisfying the conditions $F(x) = 0$ and $J(F)(x) \neq 0$. Then there exists a point $(a, (\lambda : \omega))$ of $\mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{P}^{n-i}$ such that $(x, a, (\lambda : \omega))$ belongs to E_i and in particular, that E_i is non-empty. If x is a real point, then $(a, (\lambda : \omega))$ may be chosen real.*

Proof Since we have by assumption $J(F)(x) \neq 0$ we may choose a complex number $\gamma \in \mathbb{C} \setminus \{0\}$ with $\gamma x - J(F)(x) \neq 0$. Therefore, there exists a complex $((n - i - 1) \times (n - 1))$ matrix b such that the matrices

$$a_* := \begin{bmatrix} \gamma x - J(F)(x) \\ b \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} -J(F)(x) \\ b \end{bmatrix}$$

have maximal rank $n - i$. Let $a_0 \in \mathbb{A}^{n-i}$ with $a_0 := (\gamma, 0, \ldots, 0)$, $a := [a_0^{\mathrm{T}}, a_*]$, $\lambda := 1$ and $\omega \in \mathbb{A}^{n-i}$ with $\omega := (1, 0, \ldots, 0)$. One now easily verifies that the point $(x, a, (\lambda : \omega))$ belongs to E_i. In particular, if x is a real point, then γ and b, and hence also a and $(\lambda : \omega)$, may be chosen real. □

Proposition 3 *Let D_i be the closed subvariety of $\mathbb{M}_i$ defined by the condition* $\operatorname{rk} A_* < n - i$ *or* $\operatorname{rk} A(X) < n - i$ *or* $A_0 \cdot \Omega^{\mathrm{T}} = 0$. *Then the polynomial equations*

$$F(X) = 0, \qquad \frac{\partial F}{\partial X_l}\Lambda + \sum_{1\le k\le n-i} (A_{k,l} - A_{k,0}X_l)\Omega_k = 0, \quad 1 \le l \le n, \tag{1}$$

intersect transversally at any of their common solutions in $\mathbb{M}_i \setminus D_i$. Moreover, E_i is exactly the set of solutions of the polynomial equation system (1) outside of the locus D_i.

The set E_i, interpreted as incidence variety between $\mathbb{A}^n$ and $\mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{P}^{n-i}$, dominates the locus of all regular points of the complex hypersurface $\{F = 0\}$.

In particular, E_i is an equidimensional algebraic variety which is empty or smooth and of dimension $(n - i)(n + 2) - 1$. The real variety $E_{\mathbb{R}}^{(i)} := (E_i)_{\mathbb{R}}$ is non-empty if and only if the hypersurface $\{F = 0\}$ contains a regular real point.

Proof Observe that the succinctly written polynomial equation system $J(F)(X)^{\mathrm{T}}\Lambda + A(X)^{\mathrm{T}}\Omega^{\mathrm{T}} = 0$ is nothing else than a matrix expression for the system

$$\frac{\partial F}{\partial X_l}\Lambda + \sum_{1\le k\le n-i} (A_{k,l} - A_{k,0}X_l)\Omega_k = 0, \quad 1 \le l \le n.$$

Therefore, any point $(x, a, (\lambda : \omega)) \in \mathbb{M}$ which does not belong to D_i and is a solution of the preceding polynomial equation system satisfies the condition

$$\omega \neq 0, \quad \lambda \neq 0 \quad \text{and} \quad J(F)(x) \neq 0.$$

Hence we may suppose without loss of generality that $\lambda := 1$. The polynomial equation system (1) therefore becomes

$$F(X) = 0, \qquad \frac{\partial F}{\partial X_l}(X) + \sum_{1 \leq k \leq n-i} (A_{k,l} - A_{k,0} X_l)\Omega_k = 0, \quad 1 \leq l \leq n. \qquad (2)$$

The Jacobian of this system is the following $((n+1) \times ((n-i)(n+2)+n))$ matrix:

$$\mathcal{L}_i :=$$

$$\left[\begin{array}{cccccccccccccccc}
\frac{\partial F}{\partial X_1} & \cdots & \frac{\partial F}{\partial X_n} & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\
 & & & & & & \Omega_1 & \cdots & \Omega_{n-i} & & 0 & \cdots & 0 & -X_1\Omega_1 & \cdots & -X_1\Omega_{n-i} \\
 & * & & & A(X)^{\mathrm{T}} & & & 0 & & \ddots & & 0 & & \vdots & \vdots & \vdots \\
 & & & & & & 0 & \cdots & 0 & \cdots & \Omega_1 & \cdots & \Omega_{n-i} & -X_n\Omega_1 & \cdots & -X_n\Omega_{n-i}
\end{array}\right].$$

A point $(x, a, (1 : \omega)) \in \mathbb{M}_i$ which does not belong to D_i satisfies the polynomial equation system (1) if and only if $(x, a, \omega) \in \mathbb{A}^n \times \mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{A}^{n-i}$ is a solution of (2). Moreover, in this case we have $J(F)(x) \neq 0$ and $\omega \neq 0$. This implies that the polynomial matrix $\mathcal{L}_i$ has maximal rank $n+1$ at any solution (x, a, ω) of (2) which satisfies the condition $(x, a, (1 : \omega)) \notin D_i$.

Thus the equations of (1) intersect transversally at any of their common solutions in $\mathbb{M}_i \setminus D_i$ and it is also clear from the definitions that these solutions constitute the algebraic variety E_i.

Since the polynomial equation system (2) contains $n+1$ equations in $(n-i) \times (n+2)+n$ unknowns we conclude that E_i is empty or equidimensional of dimension $((n-i)(n+2)+n) - (n+1) = (n-i)(n+2) - 1$.

If the hypersurface $\{F = 0\}$ contains a regular real point, then Observation 2 implies that E_i (or $E_{\mathbb{R}}^{(i)}$) is not empty. If E_i (or $E_{\mathbb{R}}^{(i)}$) is non-empty it contains a (real) point $(x, a, (\lambda : \omega))$ with $F(x) = 0$, $\operatorname{rk} a(x) = n - i$ and $(\lambda : \omega) \in \mathbb{P}^{n-i}$. From $\operatorname{rk} a(x) = n - i$ we deduce $J(F)(x) \neq 0$. Therefore, $\{F = 0\}$ contains a regular real point. This implies that E_i dominates the locus of all regular points of $\{F = 0\}$ and that $E_{\mathbb{R}}^{(i)}$ is non-empty if and only if $\{F = 0\}$ contains a regular real point. □

The final aim of this paper is the development of geometric tools which allow us to design efficient algorithms that find regular real points of the hypersurface $\{F = 0\}$ in case that $\{F = 0\}_{\mathbb{R}}$ is compact. The condition $\Lambda := 1$ in (1) and hence the equation system (2) are not well-suited for this purpose, since in this way we obtain a description of A as a function of X and not the opposite. Therefore, we prefer to fix one of the entries of Ω and to let Λ be unfixed.

We are now going to introduce our next family of polar incidence varieties and to show a result analogous to Proposition 3 about them, namely Proposition 4.

For this purpose we introduce the following mathematical objects and notation.

Let $1 \leq h \leq n-i$ and let $B := [B_{k,l}]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}}$ and $\Theta := (\Theta_1, \dots, \Theta_{n-i})$ be a $((n-i)\times n)$ matrix and a row vector whose entries are new indeterminates $B_{k,l}$ and Θ_k, $1 \leq k \leq n-i$, $1 \leq l \leq n$. We write $B^{(h)}$ for the $((n-i)\times(n+1))$ matrix defined by $(B^{(h)})_0 := (\delta_{k,h})_{1\leq k\leq n-i}$ and $B^{(h)}_* := B$, where $\delta_{k,h}$ denotes the Kronecker symbol given by $\delta_{k,k}=1$ and $\delta_{k,h}=0$ for $k \neq h$. Similarly, for $b \in \mathbb{A}^{(n-i)\times n}$ we denote by $b^{(h)}$ the complex $((n-i)\times(n+1))$ matrix defined by $(b^{(h)})_0 := (\delta_{k,h})_{1\leq k\leq n-i}$ and $(b^{(h)})_* := b$. We introduce a new ambient space, namely

$$\begin{aligned}\mathbb{T}_i^{(h)} := \bigl\{\bigl(x, b, (\lambda : \vartheta)\bigr) \mid x \in \mathbb{A}^n, b \in \mathbb{A}^{(n-i)\times n}, \lambda \in \mathbb{A}^1 \\ \text{and } \vartheta = (\vartheta_1, \dots, \vartheta_{n-i}) \in \mathbb{A}^{n-i} \text{ with } \vartheta_h \neq 0\bigr\}.\end{aligned}$$

Let

$$\begin{aligned}H_i^{(h)} := \bigl\{\bigl(x, b, (\lambda : \vartheta)\bigr) \in \mathbb{T}_i^{(h)} \mid F(x) = 0, \\ \operatorname{rk} b = \operatorname{rk} b^{(h)}(x) = n-i,\ J(F)(x)^{\mathrm{T}}\lambda + b^{(h)}(x)^{\mathrm{T}}\vartheta^{\mathrm{T}} = 0\bigr\}.\end{aligned}$$

Observe that $\mathbb{T}_i^{(h)}$ is an algebraic variety which is isomorphic to the affine space $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^{n-i}$ and that $H_i^{(h)}$ is an $\mathbb{R}$-definable locally closed subvariety of $\mathbb{T}_i^{(h)}$. The ambient space $\mathbb{T}_i^{(h)}$ may be linearly embedded in $\mathbb{M}_i$ and this embedding maps $H_i^{(h)}$ into E_i.

Sometimes we shall tacitly identify $\mathbb{T}_i^{(h)}$ with the affine space $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^{n-i}$. This will always be clear by the context.

For $1 \leq h \leq n-i$ and $1 \leq l_1 < \cdots < l_{n-i} \leq n$, let

$$\begin{aligned}O_{(h;l_1,\dots,l_{n-i})} &:= \bigl\{a \in \mathbb{A}^{(n-i)\times(n+1)} \mid a = [a_{k,l}]_{\substack{1\leq k\leq n-i\\ 0\leq l\leq n}} \text{ with } a_{h,0} \neq 0 \\ &\qquad \text{and } \det[a_{l_k,l_j}]_{1\leq k,j\leq n-i} \neq 0\bigr\}, \\ U_{(l_1,\dots,l_{n-i})} &:= \bigl\{b \in \mathbb{A}^{(n-i)\times n} \mid b = [b_{k,l}]_{\substack{1\leq k\leq n-i\\ 1\leq l\leq n}} \text{ with } \det[b_{l_k,l_j}]_{1\leq k,j\leq n-i} \neq 0\bigr\}, \\ \mathbb{M}^{(i)}_{O_{(h;l_1,\dots,l_{n-i})}} &:= \bigl\{\bigl(x, a, (\lambda : \omega)\bigr) \in \mathbb{M}_i \mid a \in O_{(h;l_1,\dots,l_{n-i})}\bigr\}, \\ \mathbb{T}^{(i,h)}_{U_{(l_1,\dots,l_{n-i})}} &:= \bigl\{\bigl(x, b, (\lambda : \omega)\bigr) \in \mathbb{T}_i^{(h)} \mid b \in U_{(l_1,\dots,l_{n-i})}\bigr\}, \\ E^{(i)}_{O_{(h;l_1,\dots,l_{n-i})}} &:= E_i \cap \mathbb{M}^{(i)}_{O_{(h;l_1,\dots,l_{n-i})}}\end{aligned}$$

and

$$H^{(i,h)}_{U_{(l_1,\dots,l_{n-i})}} := H_i \cap \mathbb{T}^{(i,h)}_{U_{(l_1,\dots,l_{n-i})}}.$$

Observe that $(E^{(i)}_{O_{(h;l_1,\dots,l_{n-i})}})_{\substack{1\leq h\leq n-i\\ 1\leq l_1<,\dots,l_{n-i}\leq n}}$ and $(H^{(i,h)}_{U_{(l_1,\dots,l_{n-i})}})_{\substack{1\leq h\leq n-i\\ 1\leq l_1<,\dots,l_{n-i}\leq n}}$ are coverings of E_i and $H_i^{(h)}$ by open subvarieties.

We are now able to state and prove the next result.

Proposition 4 *Let $1 \leq h \leq n-i$ and $1 \leq l_1 < \cdots < l_{n-i} \leq n$. The $\mathbb{R}$-definable algebraic variety $E^{(i)}_{O_{(h;l_1,\ldots,l_{n-i})}}$ is isomorphic to $\mathbb{A}^{n-i} \times H^{(i,h)}_{U_{(l_1,\ldots,l_{n-i})}}$. In particular, $H^{(h)}_i$ is an $\mathbb{R}$-definable equidimensional algebraic variety which is empty or smooth and of dimension $(n-i)(n+1)-1$. Let $D_{(i,h)}$ be the closed subvariety of $\mathbb{T}^{(h)}_i$ defined by the condition $\operatorname{rk} B_i < n-i$ or $\operatorname{rk} B^{(h)}_i(X) < n-i$.*

Then the equations of the system

$$F(X)=0, \qquad \frac{\partial F}{\partial X_l}(X)\varLambda + (B_{h,l}-X_l)\varTheta_h + \sum_{\substack{1\leq k\leq n-i\\ k\neq h}} B_{k,l}\varTheta_k = 0, \quad 1 \leq l \leq n, \tag{3}$$

intersect transversally at any of their common solutions in $\mathbb{T}^{(h)}_i \setminus D_{(i,h)}$. The algebraic variety $H^{(h)}_i$ consists exactly of these solutions.

The set $H^{(h)}_i$, interpreted as an incidence variety between $\mathbb{A}^n$ and $\mathbb{A}^{(n-i)\times n} \times \mathbb{P}^{n-i}$, dominates the locus of all regular points of the complex hypersurface $\{F=0\}$. The real variety $(H^{(h)}_i)_{\mathbb{R}}$ is non-empty if and only if $\{F=0\}$ contains a regular real point.

Proof The first part of this proof follows the same line as the proof of Proposition 3. For the sake of completeness we briefly indicate the main arguments.

Observe that the succinctly written polynomial equation system

$$J(F)(X)^{\mathrm{T}}\varLambda + B^{(h)}(X)^{\mathrm{T}}\varTheta^{\mathrm{T}} = 0$$

is in fact

$$\frac{\partial F}{\partial X_l}(X)\varLambda + (B_{h,l}-X_l)\varTheta_h + \sum_{\substack{1\leq k\leq n-i\\ k\neq h}} B_{k,l}\varTheta_k = 0, \quad 1 \leq l \leq n,$$

and that any point $(x, b, (\lambda : \vartheta)) \in \mathbb{T}^{(h)}_i$ with $\vartheta = (\vartheta_1, \ldots, \vartheta_{n-i})$ which does not belong to $D_{(i,h)}$ and is a solution of the polynomial equation system (3) satisfies the condition

$$\vartheta_h \neq 0, \quad \lambda \neq 0 \quad \text{and} \quad J(F)(x) \neq 0.$$

Therefore we may again assume $\lambda = 1$. The Jacobian of the specialized system, obtained from (3) by setting $\varLambda = 1$, is the polynomial $((n+1) \times (n-i)(n+1)+n)$ matrix

$$J_{i,h} := \left[\begin{array}{ccccccccccccc}
\frac{\partial F}{\partial X_1} & \cdots & \frac{\partial F}{\partial X_n} & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\
 & & & & & & \varTheta_1 & \cdots & \varTheta_{n-i} & & 0 & \cdots & 0 \\
 & * & & & B_h(X)^{\mathrm{T}} & & & 0 & & \ddots & & 0 & \\
 & & & & & & 0 & \cdots & 0 & \cdots & \varTheta_1 & \cdots & \varTheta_{n-i}
\end{array}\right],$$

with

$$B_h(X) := \begin{bmatrix} B_{h,1} - X_1 & \cdots & B_{h,n} - X_n \\ B_{1,1} & \cdots & B_{1,n} \\ \vdots & \vdots & \vdots \\ B_{h-1,1} & \cdots & B_{h-1,n} \\ B_{h+1,1} & \cdots & B_{h+1,n} \\ \vdots & \vdots & \vdots \\ B_{n-i,1} & \cdots & B_{n-i,n} \end{bmatrix}.$$

A point $(x, b, (1 : \vartheta))$ of $\mathbb{T}_i{}^{(h)}$ with $\vartheta = (\vartheta_1, \ldots, \vartheta_{n-i})$ which does not belong to $D_{(i,h)}$ satisfies the polynomial equation system (3) if and only if (x, b, ϑ) is a solution of the specialized system. Moreover, we have $J(f)(x) \neq 0$ and $\vartheta \neq 0$ in this case. This implies that the $((n + 1) \times ((n - i)(n + 1) + n))$ matrix $J_{i,h}$ has maximal rank $n + 1$ at (x, b, ϑ).

Thus the equations of (3) intersect transversally at any of their common solutions in $\mathbb{T}_i^{(h)} \setminus D_{(i,h)}$. It is also clear from the definitions that these solutions form the algebraic variety $H_i^{(h)}$. As in the proof of Proposition 3 one sees that $H_i^{(h)}$ is empty or equidimensional of dimension $(n - i)(n + 1) - 1$ and dominates the locus of the regular points of $\{F = 0\}$.

We now are going to construct for $1 \leq h \leq n - i$ and $1 \leq l_1 < \cdots < l_{n-i} \leq n$ an isomorphism from the algebraic variety $E^{(i)}_{O_{(h;l_1,\ldots,l_{n-i})}}$ to $\mathbb{A}^{n-i} \times H^{(i,h)}_{U_{(l_1,\ldots,l_{n-i})}}$.

Without loss of generality we may restrict our attention to the case $h := 1$ and $l_1 := 1, \ldots, l_{n-i} := n - i$. We consider therefore

$$U := U_{(1,\ldots,n-i)} = \left\{ b \in \mathbb{A}^{(n-i)\times n} \mid b = [b_{k,l}]_{\substack{1\leq k\leq n-i \\ 1\leq l\leq n}}, \det[b_{k,l}]_{1\leq k,l\leq n-i} \neq 0 \right\}$$

and

$$O := O_{(1;1,\ldots,n-i)} = \Big\{ a \in \mathbb{A}^{(n-i)\times(n+1)} \mid a = [a_{k,l}]_{\substack{1\leq k\leq n-i \\ 1\leq l\leq n}}, a_{1,0} \neq 0, \\ \det[a_{k,l}]_{1\leq k,l\leq n-i} \neq 0 \Big\}.$$

Further, we consider the $((n - i) \times (n - i))$ matrix

$$Q := \begin{bmatrix} \frac{1}{A_{1,0}} & \frac{-A_{2,0}}{A_{1,0}} & \cdots & \frac{-A_{n-i,0}}{A_{1,0}} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix},$$

whose inverse matrix is

$$Q^{-1}=\begin{bmatrix} A_{1,0} & A_{2,0} & \cdots & A_{n-i,0} \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

Let $A''=[A''_{k,l}]_{\substack{1\le k\le n-i\\1\le l\le n}}$ be the matrix $A'':=Q^{\mathrm{T}}A_*$ and let $\Omega''=(\Omega''_1,\dots,\Omega''_{n-i})$ be the row vector $\Omega'':=\Omega(Q^{\mathrm{T}})^{-1}$. Observing the identity $A_0\cdot Q=(1,0,\dots,0)$ we conclude that $(Q^{\mathrm{T}}A)_0=(1,0,\dots,0)$ and $(Q^{\mathrm{T}}A)_*=A''$ hold. Moreover, we have $\Omega''_1=A_0\cdot\Omega^{\mathrm{T}}$.

The entries $A''_{k,l}$ of A'' are rational functions belonging to $\mathbb{Q}(A)$, all well defined at any point of O, and the same is true for the entries of the $((n-i)\times(n-i))$ matrix Q. On the other hand, the entries $\Omega''_k$of Ω'' are polynomials belonging to $\mathbb{Q}[A,\Omega]$.

Let $(x,a,(\lambda:\omega))$ be a point of $E_O^{(i)}$. Then $q:=Q(a)$, and $A''(a)$ and $\widetilde{A}(a):=q^{\mathrm{T}}a$ are well defined, q is a regular complex $((n-i)\times(n-i))$ matrix and $(x,q^{\mathrm{T}}a,(\lambda:q^{-1}(\omega)))$ satisfies by the previous commentaries the following conditions:

$$\begin{aligned}
&\left(q^{\mathrm{T}}a\right)_0=(1,0,\dots,0),\quad \left(q^{\mathrm{T}}a\right)_*=A''(a),\quad A''(a)\in U,\quad \tilde{A}(a)\in O,\\
&\Omega''_1(a,\omega)\neq 0,\quad \operatorname{rk}A''(a)=\operatorname{rk}\bigl(\widetilde{A}(a)\bigr)(x)=n-i,\\
&J(F)(x)^{\mathrm{T}}\lambda+\bigl(\widetilde{A}(a)\bigr)(x)^{\mathrm{T}}\Omega''(a,\omega)^{\mathrm{T}}=0.
\end{aligned}$$

Therefore, we obtain a morphism of algebraic varieties

$$\varphi_O:E_O^{(i)}\to\mathbb{A}^{n-i}\times H_U^{(i,h)},$$

defined for $(x,a,(\lambda:\omega))$ by

$$\varphi_O\bigl(x,a,(\lambda:\omega)\bigr):=\bigl(a_0,x,A''(a),\bigl(\lambda:\Omega''(a,\omega)\bigr)\bigr).$$

Our argumentation implies that φ_O is an isomorphism of algebraic varieties. For any $1\le h\le n-i$ and $1\le l_1<\cdots<l_{n-i}\le n$ we obtain therefore an isomorphism of algebraic varieties,

$$\varphi_{O_{(h;l_1,\dots,l_{n-i})}}:E^{(i)}_{O_{(h;l_1,\dots,l_{n-i})}}\to\mathbb{A}^{n-i}\times H^{(i,h)}_{U_{(l_1,\dots,l_{n-i})}}.$$

Finally, Proposition 3 implies that $(H_i^{(h)})_{\mathbb{R}}$ is non-empty if and only if $\{F=0\}$ contains a regular real point. □

For algorithmic applications, Propositions 3 and 4 contain too many open conditions, namely the conditions $\operatorname{rk}A_*=\operatorname{rk}A(X)=n-i$, $A_0\Omega^{\mathrm{T}}\neq 0$ or $\operatorname{rk}B=\operatorname{rk}B(X)=n-i$, $\Theta_h\neq 0$. Of course, the condition $\operatorname{rk}B=\operatorname{rk}B(X)=n-i$ may be eliminated by a suitable specialization of the $(n-i)\times n$ matrix B. However, one has to take care that this specialization process does not kill too many regular points of the hypersurface $\{F = 0\}$. On the other side, the algorithmic tools we have at hand require subvarieties of affine spaces with *closed* and *smooth* real traces. In order to satisfy these two requirements, we are going to replace the polynomial equation system (3) by a simpler one, namely the system (4) below.

This leads us to a third family of polar incidence varieties. Proposition 5 below represents a fair compromise between our algorithmic requirements and our geometric intuition. We shall need it later for the task of finding efficiently regular real points of $\{F = 0\}$, in case that $\{F = 0\}_{\mathbb{R}}$ is compact.

We need some notation. Let $1 \le h \le n - i$ and let γ be a non-zero real number. For $b \in \mathbb{A}^i$ with $b = (b_{n-i+1}, \dots, b_n)$ we denote by $b_{(i,h;\gamma)}$ the complex $((n-i) \times n)$ matrix

$$b_{(i,h;\gamma)} := \begin{bmatrix} 1 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\ & \ddots & & & & & \vdots & \\ 0 & \cdots & \gamma & \cdots & 0 & b_{n-i+1} & \cdots & b_n \\ & & & \ddots & & & \vdots & \\ 0 & \cdots & 0 & \cdots & 1 & 0 & \cdots & 0 \end{bmatrix},$$

where the row number h is $(0, \dots, \gamma, \dots, 0, b_{n-i+1}, \dots, b_n)$.

We now introduce the ambient space

$$\mathbb{N}_i{}^{(h)} := \big\{\big(x, b, (\lambda : \vartheta)\big) \,|\, x \in \mathbb{A}^n, b \in \mathbb{A}^i \text{ and } \vartheta = (\vartheta_1, \dots, \vartheta_{n-i}) \in \mathbb{A}^{n-i} \text{with} \vartheta_h \ne 0\big\}$$

and consider the $\mathbb{R}$-definable subvariety $H_i^{(h,\gamma)}$ of $\mathbb{N}_i{}^{(h)}$ given by

$$H_i^{(h,\gamma)} := \big\{\big(x, b, (\lambda : \vartheta)\big) \in \mathbb{N}_i{}^{(h)} \,|\, x = (x_1, \dots, x_n) \in \mathbb{A}^n, F(x) = 0, x_h - \gamma \ne 0,$$
$$J(F)(x)^{\mathrm{T}}\lambda + \big(b^{(h)}_{(i,h;\gamma)}(x)\big)^{\mathrm{T}}\vartheta^{\mathrm{T}} = 0\big\}.$$

Observe that $\mathbb{N}_i{}^{(h)}$ is an algebraic variety which is isomorphic to the affine space $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ and that $H_i^{(h,\gamma)}$ is an $\mathbb{R}$-definable locally closed subvariety of $\mathbb{N}_i{}^{(h)}$. The ambient space $\mathbb{N}_i{}^{(h)}$ may be linearly embedded in $\mathbb{T}_i{}^{(h)}$ and this embedding maps $H_i^{(h,\gamma)}$ into $H_i^{(h)}$. Frequently we shall tacitly identify $\mathbb{N}_i^{(h)}$ with the affine space $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$. This will always be clear by the context. Let $B^*_{n-i+1}, \dots, B^*_n$ be new indeterminates.

Proposition 5 *Let $1 \le h \le n - i$ and let γ be a non-zero real number. Then, outside of the locus given by $\Theta_h(X_h - \gamma) = 0$, the polynomial equations of the system*

$$\begin{aligned} & F(X) = 0, \\ & \frac{\partial F(X)}{\partial X_h}\Lambda + (\gamma - X_h)\Theta_h = 0, \\ & \frac{\partial F(X)}{\partial X_l}\Lambda - X_l\Theta_h + \Theta_l = 0, \\ & \quad 1 \le l \le n - i, l \ne h \end{aligned} \tag{4}$$

$$\begin{gathered}\frac{\partial F(X)}{\partial X_l}\Lambda+\left(B_l^*-X_l\right)\Theta_h=0,\\ n-i<l\le n,\end{gathered}$$

intersect transversally at each of their common solutions in $\mathbb{N}_i{}^{(h)}$. *Moreover, the polynomial equation system* (4) *and the open condition* $\Theta_h(X_h-\gamma)\neq 0$ *define the algebraic variety* $H_i^{(h,\gamma)}$ *which is therefore empty or equidimensional of dimension* $n-1$. *The varieties* $H_i^{(h,\gamma)}$ *and* $(H_i^{(h,\gamma)})_{\mathbb{R}}$ *dominate the locus of all points* $x=(x_1,\ldots,x_n)$ *of* $\{F=0\}$ *and* $\{F=0\}_{\mathbb{R}}$ *satisfying the conditions* $\frac{\partial F}{\partial X_h}(x)\neq 0$ *and* $x_h-\gamma\neq 0$. *In particular,* $(H_i^{(h,\gamma)})_{\mathbb{R}}$ *is non-empty and equidimensional of dimension* $n-1$ *if and only if the hypersurface* $\{F=0\}$ *contains a real point* $x=(x_1,\ldots,x_n)$ *with* $\frac{\partial F}{\partial X_h}(x)\neq 0$ *and* $x_h-\gamma\neq 0$. *The polynomials contained in* (4) *generate in* $\mathbb{R}[X,B_{n-i+1}^*,\ldots,B_n^*,\Lambda,\Theta]_{\Theta_h(X_h-\gamma)}$ *the trivial ideal or form a reduced regular sequence.*

Proof Without loss of generality we may assume $h:=1$. Let $(x,b,(\lambda:\vartheta))$ be a point of $\mathbb{A}^n\times\mathbb{A}^i\times\mathbb{P}^{n-i}$ with $x=(x_1,\ldots,x_n)$, $b=(b_{n-i+1},\ldots,b_n)$, $\vartheta=(\vartheta_1,\ldots,\vartheta_{n-i})$ and $\vartheta_1(x_1-\gamma)\neq 0$ which is a solution of the polynomial equation system (4) in the case $h=1$. Without loss of generality we may suppose $\vartheta_1=1$. Therefore, (x,b,λ,ϑ) represents a solution of the polynomial equation system (4) with Θ_1 replaced by one and satisfies the condition $x_1-\gamma\neq 0$. Observe that the conditions (4), $\Theta_1=1$ and $X_1-\gamma\neq 0$ imply $\frac{\partial F}{\partial X_1}\neq 0$. Therefore we have $\frac{\partial F}{\partial X_1}(x)\neq 0$. The Jacobian $J_{(x,b,\lambda,\vartheta)}$ of the system (4) at the point (x,b,λ,ϑ) is the complex $((n+1)\times 2n)$ matrix

$$J_{(x,b,\lambda,\vartheta)}:=\begin{bmatrix} J(F)(x) & 0 & O_{1\times(n-1)}\\ & \frac{\partial F}{\partial X_1}(x) & O_{1\times(n-1)}\\ * & & \\ & J(F)_{n-1}(x)^{\mathrm{T}} & I_{n-1}\end{bmatrix},$$

with $J(F)_{n-1}(x):=(\frac{\partial F}{\partial X_2}(x),\ldots,\frac{\partial F}{\partial X_n}(x))$. From $\frac{\partial F}{\partial X_1}(x)\neq 0$ we deduce that $J_{(x,b,\lambda,\vartheta)}$ has maximal rank $n+1$.

Therefore, outside of the locus given by $\Theta_1(X_1-\gamma)=0$, the equations of the system (4) intersect transversally at each of their common solutions in $\mathbb{A}^n\times\mathbb{A}^i\times\mathbb{P}^{n-i}$.

Let $x=(x_1,\ldots,x_n)$ be an arbitrary complex or real point of the hypersurface $\{F=0\}$ satisfying the conditions $\frac{\partial F}{\partial X_1}(x)\neq 0$ and $x_1-\gamma\neq 0$ and let

$$\begin{aligned}&\vartheta_1:=1,\quad \lambda:=\frac{x_1-\gamma}{\frac{\partial F}{\partial X_1}(x)},\\ &\vartheta_2:=-\frac{\partial F}{\partial X_2}(x)\lambda+x_2,\quad\ldots,\quad \vartheta_{n-i}:=-\frac{\partial F}{\partial X_{n-i}}(x)\lambda+x_{n-i},\\ &b_{n-i+1}:=-\frac{\partial F}{\partial X_{n-i+1}}(x)\lambda+x_{n-i+1},\quad\ldots,\quad b_n:=-\frac{\partial F}{\partial X_n}(x)\lambda+x_n,\\ &\vartheta:=(\vartheta_1,\ldots,\vartheta_{n-i})\quad\text{and}\quad b:=(b_{n-i+1},\ldots,b_n).\end{aligned}$$

Then the point $(x, b, (\lambda : \vartheta)) \in \mathbb{A}^n \times \mathbb{A}^i \times \mathbb{P}^{n-i}$ represents a solution of the polynomial equation system (4) and satisfies the condition $\vartheta_1(x_1 - \gamma) \neq 0$. Therefore, the solutions $(x, b, (\lambda : \vartheta)) \in \mathbb{A}^n \times \mathbb{A}^i \times \mathbb{P}^{n-i}$ of (4) with $x = (x_1, \dots, x_n)$, $\vartheta := (\vartheta_1, \dots, \vartheta_{n-i})$, $\vartheta_1 = 1$ and $x_1 - \gamma \neq 0$ dominate the locus of all points $x = (x_1, \dots, x_n)$ of $\{F = 0\}$ with $\frac{\partial F}{\partial X_1}(x) \neq 0$ and $x_1 - \gamma \neq 0$. One easily sees from the definitions that the points of the algebraic variety $H^{(1,\gamma)}$ represent exactly the solutions of (4) which satisfy the condition $\Theta_1(X_1 - \gamma) \neq 0$. Therefore, $H^{(1,\gamma)}$ is empty or equidimensional of dimension $n - 1$. It follows from our previous argumentation that $H^{(1,\gamma)}$ and $H_{\mathbb{R}}^{(1,\gamma)}$ dominate the locus of all points $x = (x_1, \dots, x_n)$ of $\{F = 0\}$ and $\{F = 0\}_{\mathbb{R}}$ which satisfy the conditions $\frac{\partial F}{\partial X_1}(x) \neq 0$ and $x_1 - \gamma \neq 0$.

Hence, $H_{\mathbb{R}}^{(1,\gamma)}$ is non-empty (and equidimensional of dimension $n - 1$) if and only if $\{F = 0\}$ contains a real point $x = (x_1, \dots, x_n)$ with $\frac{\partial F}{\partial X_1}(x) \neq 0$ and $x_1 - \gamma \neq 0$. The rest of the statement of Proposition 5 now follows by standard arguments of commutative algebra. □

Observation 6 *Let the notation be as in Proposition* 4 *and* 5. *Then the closures of* $(H_i^{(h)})_{\mathbb{R}}$ *and* $(H_i^{(h,\gamma)})_{\mathbb{R}}$ *in their respective real ambient spaces do not need to be compact*, *even if* $\{F = 0\}_{\mathbb{R}}$ *is so. However, the assumption that* $\{F = 0\}_{\mathbb{R}}$ *is bounded implies that* $(H_i^{(h,\gamma)})_{\mathbb{R}}$ *is compact for sufficiently large* γ.

In the sequel we shall refer for $1 \leq i \leq n - 1$, $1 \leq h \leq n - i$ and $\gamma > 0$ to the equation systems (1), (3), and (4) and the corresponding varieties E_i, $H_i^{(h)}$ and $H_i^{(h,\gamma)}$ as *polar incidence varieties of the equation* $F = 0$.

The varieties E_i and $H_i^{(h)}$ are inspired by the concept of a *generic* ith dual polar variety of the hypersurface $\{F = 0\}$ whereas the variety $H_i^{(h,\gamma)}$ is inspired by the concept of a *meagerly generic* polar variety of $\{F = 0\}$ (see [8], Sect. 4, Example 2).

3.2 A Parametric View of the Generic Dual Polar Varieties of a Real Hypersurface

In [8], Sect. 3.1 we made (without any proof) a comment, saying that generic dual polar varieties of smooth hypersurfaces may become singular. This statement seems to be incorrect as the following result shows.

Theorem 7 *Let* F *be reduced*, $1 \leq i \leq n - 1$ *and let* a *be a complex* $((n - i) \times (n + 1))$ *matrix with generic submatrix* a_*. *Suppose that* $\{F = 0\}$ *contains a regular real point. Then the generic dual polar variety* $W_{\overline{K}(a)}$ *is smooth at any of its* F*-regular points* x *satisfying the condition* $\operatorname{rk} a(x) = n - i$.

Proof Let $\varphi_i : E_i \to \mathbb{A}^{(n-i)\times(n+1)}$ be the morphism of *smooth* algebraic varieties induced by the canonical projection from $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{P}^{n-i}$ onto $\mathbb{A}^{(n-i)\times(n+1)}$, and suppose that the generic polar variety $W_{\overline{K}(a)}$ is not empty.

From [8], Corollaries 1 and 2 we deduce that $W_{\overline{K}(a)}$ is equidimensional of dimension $n - i - 1$ and non-empty. On the other hand Proposition 3 implies that E_i is equidimensional of dimension $(n - i)(n + 2) - 1$.

One sees easily that $\varphi_i^{-1}(a)$ is isomorphic to

$$W^* := \left\{x \in \mathbb{A}^n \mid J(F)(x) \neq 0, x \in W_{\overline{K}(a)}, \operatorname{rk} a(x) = n - i\right\}.$$

Therefore, we conclude from the theorem of Fibers (see e.g. [55]) that the morphism φ_i is dominating (i.e., the constructible set $\varphi_i(E_i)$ is Zariski dense in $\mathbb{A}^{(n-i)\times(n+1)}$). Since by assumption a is a generic element of $\mathbb{A}^{(n-i)\times(n+1)}$, Sard's theorem (see e.g. [17, 57]) implies that a is a regular value of φ_i. Therefore $\varphi_i^{-1}(a)$, and hence W^*, are smooth. This means that the polar variety $W_{\overline{K}(a)}$ is smooth at any of its F-regular points x satisfying the condition $\operatorname{rk} a(x) = n - i$. □

For generic classic polar varieties the counterpart of Theorem 7 is a well-known result on generic classic polar varieties of complex hypersurfaces (see the comments in [8, 46] and [2] for an elementary proof).

We are now going to formulate and prove an avatar of [8], Theorem 1 for the most general type of real polar incidence variety (see Theorem 8 and Corollary 9 below).

Theorem 8 *Suppose that the hypersurface $\{F = 0\}$ contains a regular real point. Let C be a generically regular connected component of $\{F = 0\}_{\mathbb{R}}$. Then there exists a non-empty, open, semialgebraic subset $O_C^{(i)}$ of $\mathbb{A}^{(n-i)\times(n+1)}$ such that any $a \in O_C^{(i)}$ satisfies the following conditions*:

(i) $\operatorname{rk} a_* = n - i, a_0 \neq 0$ *and the dual polar variety $W_{\overline{K}(a)}$ is generic and contains a regular point of C.*

(ii) *For any two points $x \in (W_{\overline{K}(a)})_{\mathbb{R}}$ and $(\lambda : \omega) \in \mathbb{P}_{\mathbb{R}}^{n-i}$ with $z := (x, a, (\lambda : \omega)) \in E_{\mathbb{R}}^{(i)}$ there exists a permutation matrix $M \in \mathbb{Z}^{n\times n}$ such that the linear forms $X_1', \ldots, X_n', A_{k,l}, 1 \leq k \leq n - i, 0 \leq l \leq n$ with $(X_1', \ldots, X_n') := XM$ form a system of local parameters of $E_{\mathbb{R}}^{(i)}$ at z.*

Proof Let us consider the morphism of smooth real varieties $\psi_i : E_{\mathbb{R}}^{(i)} \to \mathbb{A}_{\mathbb{R}}^{(n-i)\times(n+1)}$ induced by the canonical projection from $\mathbb{A}_{\mathbb{R}}^n \times \mathbb{A}_{\mathbb{R}}^{(n-i)\times(n+1)} \times \mathbb{P}_{\mathbb{R}}^{n-i}$ onto $\mathbb{A}_{\mathbb{R}}^{(n-i)\times(n+1)}$. From [8], Theorem 1 and Sard's Theorem we deduce that there exists a non-empty, open, semialgebraic subset $O_C^{(i)}$ of $\mathbb{A}_{\mathbb{R}}^{(n-i)\times(n+1)}$ such that any $a \in O_C^{(i)}$ is a regular value of the smooth mapping ψ_i and satisfies the condition (i) of the theorem. Let us consider an arbitrary real $((n-i)\times(n+1))$ matrix a of $O^{(i)}$ and let $x = (x_1, \ldots, x_n) \in (W_{\overline{K}(a)})_{\mathbb{R}}$ and $(\lambda : \omega) \in \mathbb{P}_{\mathbb{R}}^{n-i}$ with $\omega = (\omega_1, \ldots, \omega_{n-i})$ be arbitrary points. Suppose that $z := (x, a, (\lambda : \omega))$ belongs to $E_{\mathbb{R}}^{(i)}$. Without loss of generality we may assume that $\lambda = 1$ holds. Let $\mathcal{L}_i$ be the Jacobian of the polynomial equation system

$$F(X) = 0, \qquad \frac{\partial F}{\partial X_l}(X) + \sum_{1\leq k\leq n-i} (A_{k,l} - A_{k,0}X_l)\Omega_k = 0, \quad 1 \leq l \leq n.$$

An explicit description of the polynomial $(n+1) \times (n+(n+2)(n-i))$ matrix $\mathcal{L}_i$ was given in the proof of Proposition 3.

The matrix $\mathcal{L}_i$ at the point z takes the form

$$\mathcal{L}_i(z) :=$$

$$\left[\begin{array}{cccccccccccccccc}
\frac{\partial F}{\partial X_1}(x) & \cdots & \frac{\partial F}{\partial X_n}(x) & 0 & \cdots & 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 & 0 & \cdots & 0 \\
 & & & & & & \omega_1 & \cdots & \omega_{n-i} & & 0 & \cdots & 0 & -x_1\omega_1 & \cdots & -x_1\omega_{n-i} \\
 & * & & & a(x)^{\mathrm{T}} & & & 0 & & \ddots & & 0 & & & 0 & \\
 & & & & & & 0 & \cdots & 0 & \cdots & \omega_1 & \cdots & \omega_{n-i} & -x_n\omega_1 & \cdots & -x_n\omega_{n-i}
\end{array}\right].$$

Since a is a regular value of the smooth map ψ_i, we conclude that the indeterminates $A_{k,l}, 1 \leq k \leq n-i, 0 \leq l \leq n$ are local parameters of $E_{\mathbb{R}}^{(i)}$ at z. This implies that the $((n+1) \times (2n-i))$ matrix

$$N := \begin{bmatrix} \frac{\partial F}{\partial X_1}(x) & \cdots & \frac{\partial F}{\partial X_n}(x) & 0 & \cdots & 0 \\ & * & & & a(x)^{\mathrm{T}} & \end{bmatrix}$$

has maximal rank $n+1$. Since z belongs to $E_{\mathbb{R}}^{(i)}$, we have $\operatorname{rk} a(x)^{\mathrm{T}} = \operatorname{rk} a(x) = n-i$. Therefore there are $i+1$ columns among the first n columns of N which together with the columns of the $((n+1) \times (n-i))$ matrix

$$\begin{bmatrix} 0 & \cdots & 0 \\ & a(x)^{\mathrm{T}} & \end{bmatrix}$$

form a non-singular $((n+1) \times (n+1))$ matrix. This implies that there exist $n-i-1$, say $X_1', \ldots, X_{n-i-1}'$, from the indeterminates $X_1, \ldots, X_n$ which together with $A_{k,l}, 1 \leq k \leq n-i, 0 \leq l \leq n$ form a set of local parameters of $E_{\mathbb{R}}^{(i)}$ at z. Since by Proposition 3 we have $\dim E_{\mathbb{R}}^{(i)} = (n-i)(n+2)-1$, we obtain a complete system of local parameters of $E_{\mathbb{R}}^{(i)}$. Observe, finally, that there exists a permutation matrix $M \in \mathbb{Z}^{n \times n}$ such that the first $n-i-1$ entries of XM are the indeterminates $X_1', \ldots, X_{n-i-1}'$. This finishes the proof of the theorem. □

In the case $i = n-1$, Theorem 8 implies the following result.

Corollary 9 *Suppose that the hypersurface* $\{F = 0\}$ *contains a regular real point. Then there exists a non-empty, open, semialgebraic subset* O *of* $\mathbb{A}_{\mathbb{R}}^{n+1}$ *such that any point* $a = (a_0, a_1, \ldots, a_n)$ *of* O *satisfies the following two conditions*:

(i) *$a_0 \neq 0$, $(a_1, \dots, a_n) \neq 0$ and the (locally closed) subvariety W_a of $\mathbb{A}^n \times \mathbb{A}^1$ defined by the system*

$$\begin{aligned} &F(X) = 0, \\ &\frac{\partial F}{\partial X_l}(X)\Lambda + a_l - a_0 X_l = 0, \\ &\quad 1 \leq l \leq n, \\ &\bigvee_{1 \leq l \leq n} a_l - a_0 X_l \neq 0, \end{aligned} \tag{5}$$

is zero-dimensional and of cardinality $\# W_{\overline{K}(a)}$, the equations of (5) intersect transversally at any point of W_a and the real trace $(W_a)_{\mathbb{R}}$ of W_a is non-empty.

(ii) *For any $(x, \lambda) \in (W_a)_{\mathbb{R}}$ the point $z := (x, a, (\lambda : 1))$ belongs to $E_{\mathbb{R}}^{(n-1)}$ and $A_0, A_1, \dots, A_n$ form a system of local parameters of $E_{\mathbb{R}}^{(n-1)}$ at z.*

Proof Since the hypersurface $\{F = 0\}$ contains a regular real point, there exists a generically regular connected component C of $\{F = 0\}_{\mathbb{R}}$. Apply Theorem 8 for the case $i := n - 1$ to C and set $O := O_C^{(n-1)}$. Observing that $a \in O$ implies $W_{\overline{K}(a)}$ generic and $W_a \cong W_{\overline{K}(a)}$, Corollary 9 follows easily from [4, 5], Lemma 7 and Proposition 3. □

We comment on Corollary 9 from an algorithmic point of view.

Let $A = (A_0, \dots, A_n)$ be a row vector of $n + 1$ new indeterminates $A_0, \dots, A_n$.

Suppose $F \in \mathbb{Q}[X]$ and that the hypersurface $\{F = 0\}$ contains a regular real point. Let $1 \leq h \leq n$. From Proposition 3 we conclude that, outside of the locus given by

$$A_0 \cdots A_n (A_h - A_0 X_h) = 0,$$

the polynomial equations

$$\begin{aligned} &F(X) = 0, \\ &\frac{\partial F}{\partial X_l}(X)\Lambda + A_l - A_0 X_l = 0, \\ &\quad 1 \leq l \leq n, \end{aligned} \tag{6}$$

intersect transversally at any of their common solutions. This implies that the polynomial equations

$$\begin{aligned} &F(X) = 0, \\ &-\frac{\partial F}{\partial X_l}(A_h - A_0 X_h) + (A_l - A_0 X_l)\frac{\partial F}{\partial X_h}(X) = 0, \\ &\quad 1 \leq l \leq n, l \neq h, \end{aligned} \tag{7}$$

intersect transversally in any of their solutions $(x, a) \in \mathbb{A}^n \times \mathbb{A}^{n+1}$ not contained in the locus $A_0 \cdots A_n(A_h - A_0X_h) = 0$. Therefore, the polynomials which constitute the system (7) generate in $\mathbb{Q}[A, X]_{A_0\cdots A_n(A_h-A_0X_h)}$ the trivial ideal or form a reduced regular sequence. Hence the ideal $\mathfrak{a}_h$ generated by these polynomials in $\mathbb{Q}(A)[X]_{(A_h-A_0X_h)}$ is trivial or a radical complete intersection ideal of dimension zero.

The hypersurface $\{F = 0\}$ contains by assumption a regular real point. Thus Corollary 9 implies that there exists $1 \leq h \leq n$ such that $\mathfrak{a}_h$ is a radical complete intersection ideal of dimension zero which vanishes on a regular point with coordinates in a suitable real closure K of the field $\mathbb{Q}(A)$. Without loss of generality, we may assume that the variables $X_1, \ldots, X_n$ are in a general position with respect to the ideal $\mathfrak{a}_h$ and that in particular the variable X_1 separates the zeros of $\mathfrak{a}_h$ in $K(i)^n$, where i is an algebraic number with $i^2 + 1 = 0$.

For the sake of simplicity we shall suppose $2 \leq h \leq n$. Hence we conclude that there exist polynomials $\varrho_h \in \mathbb{Q}[A]$ and $P_h, G_2^{(h)}, \ldots, G_n^{(h)} \in \mathbb{Q}[A, X_1]$ with $\varrho_h \neq 0$, $\deg_{X_1} P_h \geq 1$ and $\deg_{X_1} G_j^{(h)} < \deg_{X_1} P_h, 2 \leq j \leq n$, such that P_h is primitive and separable with respect to the variable X_1 and such that

$$P_h, \quad \varrho_h X_2 - G_2^{(h)}, \quad \ldots, \quad \varrho_h X_n - G_n^{(h)}$$

generate the ideal $\mathfrak{a}_h$ in $\mathbb{Q}(A)[X]_{A_h-A_0X_h}$. We then say that the polynomials $P_h, G_2^{(h)}, \ldots, G_n^{(h)}$ form a *geometric solution* over $\mathbb{Q}(A)$ of the equation system (7) and the open condition $A_h - A_0X_h \neq 0$ in the variables $X_1, \ldots, X_n$.

The polynomial P_h is uniquely determined by (7), and ϱ_h may be chosen as the numerator of the discriminant of P_h with respect to the indeterminate X_1. This choice in turn determines $G_2^{(h)}, \ldots, G_n^{(h)}$. From Corollary 9 we deduce that $\deg_{X_1} P_h$ is bounded by the degree, say μ, of the $(n-1)$th generic dual polar variety of $\{F = 0\}$.

Let V_h be the union of all irreducible components of the closed subvariety of $\mathbb{A}^n \times \mathbb{A}^{n+1}$, defined by the polynomial equation system (7) in the unknowns X and A that are not contained in the locus given by $A_0A_1 \cdots A_n(A_h - A_0X_h) = 0$. From [52], Theorem 1, we deduce that the total degree of the polynomials

$$\varrho_h, P_h, G_2^{(h)}, \ldots, G_n^{(h)} \in \mathbb{Q}[A, X_1]$$

is of order $O(\mu \deg V_h)$.

Suppose that F is given by a division-free arithmetic circuit σ of size L in $\mathbb{Q}[X]$ (thus F has rational coefficients). Let $\delta_1 \leq \mu$ be the degree of the system (7) over $\mathbb{Q}(A)$ outside of the locus given by $A_h - A_0X_h = 0$ and $\delta := \delta_1\mu \deg V_h$. Then we have $\delta_1 \leq d^n$ and $\deg V_h \leq (d+1)^n$ and therefore $\delta = d^{O(n)}$.

Then the polynomial $\varrho_h \in \mathbb{Q}[A]$ and the coefficients with respect to X_1 of the polynomials $P_h, G_2^{(h)}, \ldots, G_n^{(h)}$ have a representation by a division-free arithmetic circuit σ^* in $\mathbb{Q}[A]$ of size $L(nd)^{O(1)}\delta^2$. The circuit σ^* may be computed from the input circuit σ in time $L(nd)^{O(1)}\delta^2$ (see the original contributions [25, 27, 28, 36] and the survey [20] for the notions of geometric solution, system degree and details of the algorithm).

Applying now real quantifier elimination to the formula

$$(\exists X_1)\big(P_h(A,X_1)=0\wedge A_0\cdots A_n\big(A_h\varrho_h(A)-A_0G_h^{(h)}(A,X_1)\big)\neq 0\wedge \varrho_h(A)\neq 0\big)$$

we obtain a quantifier-free formula $\Psi_h(A)$ in the variables $A_0,\ldots,A_n$ over the elementary language of ordered fields. The formula $\Psi_h(A)$ describes the image of the semialgebraic set

$$\big\{(a,x_1)\in\mathbb{A}_{\mathbb{R}}^{n+1}\times\mathbb{A}_{\mathbb{R}}^{1}\,|\,a=(a_0,\ldots,a_n),\,P_h(a,x_1)=0,$$
$$a_0\cdots a_n\big(a_h\varrho_h(a)-a_0G_h^{(h)}(a,x_1)\big)\neq 0,\,\varrho_h(a)\neq 0\big\}$$

under the canonical projection $\mathbb{A}_{\mathbb{R}}^{n+1}\times\mathbb{A}_{\mathbb{R}}^{1}\to\mathbb{A}_{\mathbb{R}}^{n+1}$. Thus for $a=(a_0,\ldots,a_n)\in\mathbb{A}_{\mathbb{R}}^{n+1}$ the formula $\Psi_h(a)$ is true if and only if there exists a point $x=(x_1,\ldots,x_n)$ of $\mathbb{A}_{\mathbb{R}}^{n}$ such that (x,a) is a solution of the polynomial equation system (7) with $a_0\cdots a_n(a_h-a_0x_h)\neq 0$. In its turn this implies that $\Psi_h(a)$ is true if and only if there exists a point (x,λ) of $\mathbb{A}_{\mathbb{R}}^{n}\times\mathbb{A}_{\mathbb{R}}^{1}$ with $x=(x_1,\ldots,x_n)$ such that (x,a,λ) is a solution of the polynomial equation system (5) with $a_0\cdots a_n(a_h-a_0x_h)\neq 0$, whence $(x,a,(\lambda:1))\in E_{\mathbb{R}}^{(n-1)}$ and $x\in W_{\overline{K}(a)}$. From the choice of h we see that the semialgebraic subset of $\mathbb{A}_{\mathbb{R}}^{n+1}$ defined by the formula $\Psi_h(A)$ has a non-empty interior, which therefore contains "generic" rational points. Let $a\in\mathbb{Q}^{n+1}$ be such a point. From the inputs a and σ we are now able to construct in time $L(nd)^{O(1)}\delta^2$ a regular real algebraic point $x\in\mathbb{A}_{\mathbb{R}}^{n}$ which belongs to the dual polar variety $x\in W_{\overline{K}(a)}$. By [8], Theorem 3 the point x has degree at most μ and belongs to $\{F=0\}_{\mathbb{R}}$.

The crux with this kind of argumentation is the following:
Although we are able to compute in time $L(nd)^{O(1)}\delta^2$ from the arithmetic circuit σ an arithmetic–boolean circuit with $=$ and $>$ decision gates which represents a nonempty open set M_h of points of $\mathbb{A}_{\mathbb{R}}^{n+1}$ that satisfy the formula Ψ_h, we are generally not able to find *efficiently* sample points of M_h, neither rational nor algebraic ones.

An exception is made by certain well-determined singular curves, whose generic dual polar varieties are never empty [45].

By the way, let us mention that the procedures we have in mind for the elimination of just one real existential quantifier are the most classical ones, which may be adapted to the circuit representation of polynomials. There are no precise references to the subject. For technical aspects see [21], Sect. B.

Fix now an index $1\leq i<n-1$ and suppose that we are able to find a "generic" point $a^*\in\mathbb{Q}^{n+1}$ such that $\Psi_h(a^*)$ holds. Then we may find a $((n-i-1)\times(n+1))$ matrix $a^{**}\in\mathbb{Q}^{(n-i-1)\times(n+1)}$ such that the rational $((n-i)\times(n+1))$ matrix $a:=\left[\begin{smallmatrix}a^*\\a^{**}\end{smallmatrix}\right]$ is generic. Hence $W_{\overline{K}(a)}$ is a generic dual polar variety of $\{F=0\}$. Observe that $W_{\overline{K}(a)}$ contains $W_{\overline{K}(a^*)}$. Since the assertion $\Psi_h(a^*)$ holds, we conclude that $W_{\overline{K}(a^*)}$ contains a regular real point x. Because x is also contained in $W_{\overline{K}(a)}$, the generic dual polar variety $W_{\overline{K}(a)}$ contains regular real points.

This leads to the problem of efficiently finding for a given consistent system of *strict* inequalities of arithmetic-circuit represented polynomials of $\mathbb{Q}[X]$ a rational (or algebraic) point $x\in\mathbb{A}_{\mathbb{R}}^{n}$ which satisfies all these inequalities. We call such a point a rational (or algebraic) *witness* for the given system.

In the next section we are going to design a procedure which decides, under the assumption that $\{F=0\}_{\mathbb{R}}$ is compact, whether the hypersurface $\{F=0\}$ contains a regular real point, and, if this is the case, returns such a point for each connected component of $\{F=0\}_{\mathbb{R}}$.

4 Bipolar Varieties

4.1 Definition and Basic Properties of Bipolar Varieties

In order to estimate the complexity of this procedure we shall now introduce the concept of a *bipolar variety* of the equation $F=0$ in different variants. The maximal degree of all bipolar varieties of the equation $F=0$ will then determine the running time of the procedure. Dual polar varieties represent a complex reflection of the Lagrange multipliers. Therefore, their geometric meaning concerns more real than complex algebraic varieties. Maybe this is the reason why they, motivated by the aim to find *real* solutions of polynomial equation systems, were only recently introduced in (complex) algebraic geometry.

The definition of the dual polar varieties associated with an equidimensional complex algebraic variety S requires that S is represented as a subvariety of a projective space $\mathbb{P}^n$ which is in turn equipped with a distinguished hyperplane H at infinity and with a non-degenerate hyperquadric Q such that $Q \cap H$ is again non-degenerate.

Of particular interest is the case where S is a smooth subvariety of the affine space $\mathbb{A}^n$, suitably embedded in $\mathbb{P}^n$. This leads to the concepts of an affine and a real dual polar variety (see [4, 5] and [8] for details and motivations.)

The bipolar varieties of the equation $F=0$ should be introduced as generic dual polar varieties associated with the smooth incidence varieties E_i or $H_i^{(h)}$, $1 \leq i \leq n-1, 1 \leq h \leq n-i$ (if they are not empty), and should be defined in a "natural" way, only depending on the polynomial F, such that their degree is relevant for the complexity of the problem of finding regular real algebraic points belonging to $\{F=0\}$. We shall see that E_i is not suitable for this task, but that $H_i^{(h)}$ furnishes an appropriate notion of bipolar varieties.

Let us fix $1 \leq i \leq n-1$ and $1 \leq h \leq n-i$ and observe that arbitrary points $(x, a, (\lambda : \omega)) \in E_i$ or $(x, a, (\lambda : \vartheta)) \in H_i^{(h)}$ satisfy the condition $\lambda \neq 0$. Therefore, in principle, we may suppose $\lambda = 1$ and consider E_i and $H_i^{(h)}$ as subvarieties of the respective affine spaces $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{A}^{n-i}$ and $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^{n-i}$.

However, these affine embeddings of E_i and $H_i^{(h)}$ are rather irrelevant for our algorithmic considerations, because we are looking for a description of x as a function of a, λ and ω (or alternatively as a function of b, λ and ϑ) and not for the opposite.

Consider now an arbitrary point $(x, a, (\lambda : \omega))$ of E_i with $\omega = (\omega_1, \ldots, \omega_{n-i}) \in \mathbb{A}^{n-i}$. Then we have $a_0 \cdot \omega^{\mathrm{T}} \neq 0$ and this implies $\omega \neq 0$. Therefore there exists an index $1 \leq h \leq n-i$ with $\omega_h \neq 0$. For any such h we obtain a different embedding of the affine ambient space $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times(n+1)} \times \mathbb{A}^{n-i}$ in $\mathbb{P}^{(n-i)(n+2)+n}$, and it remains undetermined which embedding we should choose in order to define the bipolar varieties of E_i. Different embeddings lead to completely incompatible generic dual polar varieties that cannot be patched together.

The situation looks different in the case of $H_i^{(h)}$. For any point $(x, b, (\lambda : \vartheta))$ of $H_i^{(h)}$ with $\vartheta = (\vartheta_1, \dots, \vartheta_{n-i})$ we have $\vartheta_h \neq 0$. Therefore, by setting $\vartheta_h := 1$ we obtain a canonic embedding of the ambient space $\mathbb{A}^n \times \mathbb{A}^{(n-i)\times n} \times \mathbb{A}^{n-i}$ into the projective space $\mathbb{P}^{(n-i)(n+1)+n}$.

Let us be more precise. We associate with $1 \le h \le n-i$ the hyperplane at infinity

$$\begin{aligned} L_h := \{\Theta_h = 0\} := \big\{&(x : b : \lambda : \vartheta) \in \mathbb{P}^{(n-i)(n+1)+n} \mid x \in \mathbb{A}^n, b \in \mathbb{A}^{(n-i)\times n}, \\ &\lambda \in \mathbb{A}^1, \vartheta \in \mathbb{A}^{n-i}, \vartheta = (\vartheta_1, \dots, \vartheta_{n-i}), \vartheta_h = 0\big\} \end{aligned}$$

and the hyperquadric $\mathcal{Q}$ defined by the equation

$$\sum_{1\le l\le n} X_l^2 + \sum_{\substack{1\le k\le n-i\\ 1\le l\le n}} B_{k,l}^2 + \Lambda^2 + \sum_{1\le k\le n-i} \Theta_k^2 = 0.$$

Then $\mathcal{Q}$ and $\mathcal{Q} \cap L_h$ are non-degenerate and

$$(\mathcal{Q} \cap L_h) \cap \mathbb{A}_{\mathbb{R}}^n \times \mathbb{A}_{\mathbb{R}}^{(n-i)\times n} \times \mathbb{A}_{\mathbb{R}}^{n-i}$$

is positive-definite and induces in $\mathbb{A}_{\mathbb{R}}^n \times \mathbb{A}_{\mathbb{R}}^{(n-i)\times n} \times \mathbb{A}_{\mathbb{R}}^{n-i}$ the Euclidean distance.

Similarly, we associate with $1 \le h \le n-i$ the hyperplane at infinity

$$\begin{aligned} \widetilde{L}_h &:= \{\Theta_h = 0\} \\ &:= \big\{(x : b : \lambda : \vartheta) \in \mathbb{P}^{2n} \mid x \in \mathbb{A}^n, b \in \mathbb{A}^i, \lambda \in \mathbb{A}^1, \vartheta \in \mathbb{A}^{n-i}, \\ &\quad \vartheta = (\vartheta_1, \dots, \vartheta_{n-i}), \vartheta_h = 0\big\} \end{aligned}$$

and the hyperquadric $\mathcal{Q}_h$ defined by the equation

$$\sum_{1\le l\le n} X_l^2 + \sum_{n-i<l\le n} B_l^{*2} + \sum_{1\le k\le n-i} \Theta_k^2 = 0.$$

Again $\mathcal{Q}_h$ and $\mathcal{Q}_h \cap \widetilde{L}_h$ are non-degenerate and

$$\big(\mathcal{Q}_h \cap \widetilde{L}_h\big) \cap \mathbb{A}_{\mathbb{R}}^n \times \mathbb{A}_{\mathbb{R}}^i \times \mathbb{A}_{\mathbb{R}}^{n-i}$$

is positive-definite and induces in $\mathbb{A}_{\mathbb{R}}^n \times \mathbb{A}_{\mathbb{R}}^i \times \mathbb{A}_{\mathbb{R}}^{n-i}$ the Euclidean distance.

This leads us to the following concept.

Definition 10 Let $1 \le i \le n-1$ and $1 \le h \le n-i$ and let γ be a non-zero real number. The bipolar varieties $\mathfrak{B}_{(i,h,j)}$ and $\mathcal{B}_{(i,h,j;\gamma)}$ are defined as follows:

For $1 \le j \le (n-i)(n+1)-1$ let $\mathfrak{B}_{(i,h,j)}$ be a $((n-i)(n+1)-j)$th generic dual polar variety of $H_i^{(h)}$ and for $1 \le j \le n-1$ let $\mathcal{B}_{(i,h,j;\gamma)}$ be a $(n-j)$th generic dual polar variety of $H_i^{(h,\gamma)}$. We call $\mathfrak{B}_{(i,h,j)}$ the *large bipolar variety* of the equation $F=0$ associated with the indices i, h and j. For γ generic, we call $\mathcal{B}_{(i,h,j;\gamma)}$ the *small bipolar variety* of the equation $F=0$ associated with the indices i, h and j.

In the latter case we think of γ as given by the context and use as a shorthand

$$\widetilde{\mathcal{B}}_{(i,h,j)} := \mathcal{B}_{(i,h,j;\gamma)}.$$

This 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 γ and the linear projective varieties we used to define our objects.

The bipolar varieties $\mathfrak{B}_{(i,h,j)}$ and $\mathcal{B}_{(i,h,j;\gamma)}$ are well-defined geometric objects, although the varieties $H_i^{(h)}$ and $H_i^{(h,\gamma)}$ are not closed (compare the definition of the notion of polar variety in Sect. 2, where we have taken care of this situation).

Let us fix again $1 \le i \le n-1$, $1 \le h \le n-i$ and a non-zero real number γ. In the sense of [4, 5] we are now going to study different extrinsic descriptions of the bipolar varieties $\mathfrak{B}_{(i,h,j)}$, $1 \le j \le (n-i)(n+1)-1$ and $\mathcal{B}_{(i,h,j;\gamma)}$, $1 \le j \le n-1$, by means of equations and inequalities.

Let

$$\begin{gathered} \nu = (\nu_1, \ldots, \nu_j), \quad \zeta = (\zeta_1, \ldots, \zeta_j), \\ [\rho_{r,l}]_{\substack{1\le r\le j\\ 1\le l\le n}}, \quad [\mu_{r,k}]_{\substack{1\le r\le j\\ 1\le k\le n-i\\ k\ne h}}, \quad [\beta_{r;k,l}]_{\substack{1\le r\le j\\ 1\le k\le n-i\\ 1\le l\le n}} \end{gathered}$$

be row vectors and matrices of generic real (or rational) numbers.

Further, let us write

$$\begin{gathered} \Theta_1^{(h)} := \Theta_1, \quad \ldots, \quad \Theta_{h-1}^{(h)} := \Theta_{h-1}, \quad \Theta_h^{(h)} := 1, \\ \Theta_{h+1}^{(h)} := \Theta_{h+1}, \quad \ldots, \quad \Theta_{n-i}^{(h)} := \Theta_{n-i} \end{gathered}$$

and

$$\Theta^{(h)} := \big(\Theta_1^{(h)}, \ldots, \Theta_{n-i}^{(h)}\big).$$

We consider now two polynomial matrices $T_{(i,h,j)}$ and $T_{(i,h,j;\gamma)}$.

The first one is the $((n+j+1) \times ((n-i)(n+1)+n))$ matrix

$$T_{(i,h,j)} := \begin{bmatrix} J(F) & 0 & O_{1\times(n-i-1)} & \\ \frac{\partial(J(F)^{\mathrm{T}}\Lambda + B(X)^{\mathrm{T}}\Theta^{(h)^{\mathrm{T}}})}{\partial(X_1,\ldots,X_n)} & J(F)^{\mathrm{T}} & [B_{l,k}]_{\substack{1\le l\le n\\ 1\le k\le n-i\\ k\ne h}} & \mathcal{I} \\ [\rho_{r,l} - \nu_r X_l]_{\substack{1\le r\le j\\ 1\le l\le n}} & \zeta^{\mathrm{T}} - \Lambda\nu^{\mathrm{T}} & [\mu_{r,k} - \nu_r\Theta_k]_{\substack{1\le r\le j\\ 1\le k\le n-i\\ k\ne h}} & \end{bmatrix},$$

where the index j has the range $1 \le j \le (n-i)(n+1)-1$ and $\mathcal{I}$ represents the $((n+j+1) \times (n-i)n)$ submatrix

$$\mathcal{I} := \begin{bmatrix} O_{1\times n} & O_{1\times n} & \cdots & O_{1\times n} & O_{1\times n} & \cdots & O_{1\times n} \\ I_n & \Theta_1 I_n & \cdots & \Theta_{h-1} I_n & \Theta_{h+1} I_n & \cdots & \Theta_{n-i} I_n \\ \mathcal{F}_{(h)} & \mathcal{F}_{(1)} & \cdots & \mathcal{F}_{(h-1)} & \mathcal{F}_{(h+1)} & \cdots & \mathcal{F}_{(n-i)} \end{bmatrix}$$

with

$$\mathcal{F}_{(k)} := [\beta_{r;k,l} - \nu_r B_{k,l}]_{\substack{1\le r\le j\\ 1\le l\le n}} \quad \text{for } 1 \le k \le n-i.$$

The second polynomial matrix $T_{(i,h,j;\gamma)}$ is the $((n+j+1)\times 2n)$ matrix

$$T_{(i,h,j;\gamma)} :=$$

$$\begin{bmatrix} J(F) & 0 & & \\ \frac{\partial(J(F)^{\mathrm{T}}\Lambda + B^{(h)}_{(h,\gamma)}(X)^{\mathrm{T}}\Theta^{(h)^{\mathrm{T}}})}{\partial(X_1,\dots,X_n)} & J(F)^{\mathrm{T}} & \mathcal{C} & \\ [\rho_{r,l} - \nu_r X_l]_{\substack{1\le r\le j\\ 1\le l\le n}} & \zeta^{\mathrm{T}} - \Lambda\nu^{\mathrm{T}} \; [\mu_{r,k} - \nu_r\Theta_k]_{\substack{1\le r\le j\\ 1\le k\le n-i\\ k\ne h}} & [\beta_{r;h,l} - \nu_r B^*_l]_{\substack{1\le r\le j\\ n-i<l\le n}} & \end{bmatrix},$$

where $1 \le j \le n-1$. Here $\mathcal{C}$ denotes the $((n+1)\times n)$ submatrix

$$\mathcal{C} := \begin{bmatrix} 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 1 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ & \ddots & & & & & \ddots & \\ 0 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 & \cdots & 0 \\ & \ddots & & & & & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix},$$

whose first and $(h+1)$th rows consist only of zeros.

One deduces from Definition 10, Propositions 4 and 5 that a point $(x, b, (\lambda : \vartheta))$ of $H_i^{(h)}$ or $H_i^{(h,\gamma)}$ with $\vartheta_h = 1$ belongs to $\mathfrak{B}_{(i,h,j)}$ or $\mathcal{B}_{(i,h,j;\gamma)}$ if and only if all $(n+j+1)$-minors of $T_{(i,h,j)}$ or $T_{(i,h,j;\gamma)}$ vanish at $(x, b, \lambda, \vartheta^{(h)})$ in $\mathbb{A}^n \times \mathbb{A}^{(n-i)n} \times \mathbb{A}^{n-i}$, where $\vartheta^{(h)} := (\vartheta_1, \dots, \vartheta_{h-1}, \vartheta_{h+1}, \dots, \vartheta_{n-i})$.

Further, from [4, 5], Proposition 8 we conclude that the bipolar varieties $\mathfrak{B}_{(i,h,j)}$ and $\mathcal{B}_{(i,h,j;\gamma)}$ are of (local) dimension $j-1$ at any point $(x, b, (\lambda : \vartheta))$ of $H_i^{(h)} \cap \mathfrak{B}_{(i,h,j)}$ and $H_i^{(h,\gamma)} \cap \mathcal{B}_{(i,h,j;\gamma)}$. Thus $\mathfrak{B}_{(i,h,j)}$ and $\mathcal{B}_{(i,h,j;\gamma)}$ are empty or equidimensional of dimension $j-1$.

Moreover, from [8] we infer that these bipolar varieties are normal and Cohen–Macaulay at any point of $H_i^{(h)}$ or $H_i^{(h,\gamma)}$ they contain.

In $T_{(i,h,j)}$ we fix any $n+j$ columns which contain the columns corresponding to at least one of the indeterminates $X_1, \dots, X_n$ and to $B^*_{h,1}, \dots, B^*_{h,n}$. We characterize this choice by a vector $\underline{t} \in \mathbb{N}^{n+j}$ whose entries are the numbers of the selected columns. We denote by

$$M^{(i,h,j,\underline{t})}_{n+j+1}, \quad M^{(i,h,j,\underline{t})}_{n+j+2}, \quad \dots, \quad M^{(i,h,j,\underline{t})}_{(n-i)(n+1)+n}$$

the $(n+j+1)$-minors of $T_{(i,h,j)}$ obtained by adding one by one to the selected columns $\underline{t}$ each of the columns of $T_{(i,h,j)}$, and, for $1 \le s \le j$, we denote by $m_{(i,h,j,\underline{t},s)}$

the $(n+j)$-minor of $T_{(i,h,j)}$ corresponding to the selected columns $\underline{t}$ and all rows except the row numbered $n+s+1$.

Proposition 11 *Let $D_{(i,h,j,\underline{t},s)}$ be the closed subvariety of $\mathbb{T}_i^{(h)}$ defined by the condition*

$$\operatorname{rk} B < n-i \quad or \quad \operatorname{rk} B^{(h)}(X) < n-i \quad or \quad m_{(i,h,j,\underline{t},s)} = 0.$$

Then the polynomial equations of the system

$$F(X)=0, \qquad \frac{\partial F}{\partial X_l}(X)\Lambda + B_{h,l} - X_l + \sum_{\substack{1\le k\le n-i\\ k\ne h}} B_{k,l}\Theta_k = 0, \quad 1\le l\le n,$$

$$M_{n+j+1}^{(i,h,j,\underline{t})}=0, \quad \ldots, \quad M_{(n-i)(n+1)+n}^{(i,h,j,\underline{t})}=0$$

intersect transversally at any of their common solutions in $\mathbb{T}_i^{(h)} \setminus D_{(i,h,j,\underline{t},s)}$. They define $\mathfrak{B}_{(i,h,j)} \setminus D_{(i,h,j,\underline{t},s)}$ in $\mathbb{T}_i^{(h)} \setminus D_{(i,h,j,\underline{t},s)}$.

Proof Obvious by Proposition 4, and Propositions 6 and 8 of [4, 5]. □

Observe that, for i,h fixed, the bipolar varieties are ordered by inclusion as follows:

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

(where $\overline{H_i^{(h)}}$ denotes the Zariski closure of $H_i^{(h)}$). The variety $\mathfrak{B}_{(i,h,1)}$ is empty or zero-dimensional. If $\mathfrak{B}_{(i,h,1)}$ is non-empty the chain is strictly decreasing.

Let us fix again $1\le i\le n-1$, $1\le h\le n-i$ and a non-zero real number γ. From Proposition 5 we deduce that for $\Theta_h=1$ the equations of the system (4) generate in $\mathbb{Q}[X, \Lambda, B^*_{n-i+1}, \ldots, B^*_n, \Theta^{(h)}]_{X_h-\gamma}$ the vanishing ideal of $H_i^{(h,\gamma)}$ (interpreted as affine subvariety of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{(n-i)}$). Therefore, all $(n+j+1)$-minors of $T_{(i,h,j;\gamma)}$ vanish at a point $(x,b,(\lambda:\vartheta))$ of $H_i^{(h,\gamma)}$ with $\vartheta=(\vartheta_1,\ldots,\vartheta_{n-i})$ and $\vartheta_h=1$ if and only if $(x,b,(\lambda:\vartheta))$belongs to the affine variety $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}$, consisting of the elements of $(\mathcal{B}_{(i,h,j;\gamma)})$ which satisfy the condition $X_h-\gamma\ne 0$. In other words, $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}$ is the locus of $H_i^{(h,\gamma)}$, where all $(n+j+1)$-minors of $T_{(i,h,j;\gamma)}$ vanish.

In $T_{(i,h,j;\gamma)}$ we fix any $n+j$ columns which contain the columns corresponding to the indeterminate X_h, to the entries of $\Theta^{(h)}$ and to B^*_l, $n-i<l\le n$. As before let us characterize this selection by a vector $\underline{t}\in\mathbb{N}^{n+j}$. We denote by

$$M_{n+j+1}^{(i,h,j,\underline{t};\gamma)}, \quad M_{n+j+2}^{(i,h,j,\underline{t};\gamma)}, \quad \ldots, \quad M_{2n}^{(i,h,j,\underline{t};\gamma)}$$

the $n+j+1$-minors obtained by adding one by one to the selected columns each column of $T_{(i,h,j;\gamma)}$, and, for $1\le s\le j$, we denote by $m_{(i,h,j,\underline{t},s;\gamma)}$ the $(n+j)$-minor of $T_{(i,h,j;\gamma)}$ corresponding to selected columns $\underline{t}$ and all rows, except the row numbered $n+s+1$.

Proposition 12 *The sequence of polynomials*

$$F(X), \qquad \frac{\partial F}{\partial X_h}(X)\Lambda + \gamma - X_h, \qquad \frac{\partial F}{\partial X_l}(X)\Lambda - X_l + \Theta_l, \quad 1 \le l \le n-i, l \ne h,$$
$$\frac{\partial F}{\partial X_l}(X)\Lambda + B_l^* - X_l, \quad n-i < l \le n, \qquad M_{n+j+1}^{(i,h,j,\underline{t};\gamma)}, \quad \ldots, \quad M_{2n}^{(i,h,j,\underline{t};\gamma)} \tag{8}$$

generates in

$$\mathcal{R} := \mathbb{Q}\big[X, \Lambda, B_{n-i+1}^*, \ldots, B_n^*, \Theta^{(h)}\big]_{m_{(i,h,j,\underline{t},s;\gamma)}(X_h-\gamma)}$$

the trivial ideal or forms a reduced regular sequence. The sequence defines in $\mathcal{R}$ the affine variety $(\mathcal{B}_{(i,h,j;\gamma)})_{m_{(i,h,j,\underline{t},s;\gamma)}(X_h-\gamma)}$ and their entries intersect transversally at any point of $(\mathcal{B}_{(i,h,j;\gamma)})_{m_{(i,h,j,\underline{t},s;\gamma)}(X_h-\gamma)}$.

Proof Obvious from Proposition 5, and Propositions 6 and 8 of [4, 5]. □

Similarly as above, notice that, for i, h, γ fixed, the bipolar varieties $\mathcal{B}_{(i,h,j;\gamma)}$ are ordered by inclusion as follows:

$$\overline{H_i^{(h,\gamma)}} \supsetneq \mathcal{B}_{(i,h,n-1;\gamma)} \supset \cdots \supset \mathcal{B}_{(i,h,1;\gamma)}.$$

The variety $\mathcal{B}_{(i,h,1;\gamma)}$ is empty or zero-dimensional. If $\mathcal{B}_{(i,h,1;\gamma)}$ is non-empty, then the chain strictly decreases.

Observation 13 *Let the notation be as in Propositions 11 and 12 and let $j \ge 2$. The loci of $\mathfrak{B}_{(i,h,j)} \cap H_i^{(h)}$ and $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma} \cap H_i^{(h,\gamma)}$, where, for suitable $\underline{t} \in \mathbb{N}^{n+j}$ and $1 \le s \le j$, all minors of the form $m_{(i,h,j,\underline{t},s)}$ and $m_{(i,h,j,\underline{t},s;\gamma)}$ vanish, coincide with $\mathfrak{B}_{(i,h,j-1)} \cap H_i^{(h)}$ and $\mathcal{B}_{i,h,j-1;\gamma} \cap H_i^{(h,\gamma)}$ and are empty or of pure codimension one. Moreover, for each point z of $\mathfrak{B}_{(i,h,1)} \cap H_i^{(h)}$ and $\mathcal{B}_{(i,h,1;\gamma)} \cap H_i^{(h,\gamma)}$ there exist minors of the form $m_{(i,h,1,\underline{t},1)}$ and $m_{(i,h,1,\underline{t},1;\gamma)}$, $\underline{t} \in \mathbb{N}^{n+1}$, respectively, which do not vanish at z.*

Proof Obvious by [8], Lemma 2. □

4.2 Degrees of Bipolar Varieties

We denote by $\deg \mathfrak{B}_{(i,h,j)}$, $\deg \mathcal{B}_{(i,h,j;\gamma)}$ and $\deg \widetilde{\mathcal{B}}_{(i,h,j)}$ the geometric degrees of the respective bipolar varieties in their respective affine ambient spaces (see [31] for a definition and properties of the geometric degree of a subvariety of an affine space).

From Lemma 1 and [8], Theorem 13 we deduce that for $1 \le j \le n-1$

$$\deg \mathcal{B}_{(i,h,j;\gamma)} \le \deg \widetilde{\mathcal{B}}_{(i,h,j)} \le \deg \mathcal{B}_{(i,h,(n-i)n-i+j)} \tag{9}$$

holds.

Suppose that $\{F = 0\}_{\mathbb{R}}$ is compact and contains a regular point. Then Observation 6, Proposition 5, Lemma 1 and [8], Corollary 1 imply that $(\widetilde{\mathcal{B}}_{(i,h,j)})_{\mathbb{R}}$ and $(\mathfrak{B}_{(i,h,j)})_{\mathbb{R}}$ are non-empty. This implies $1 \leq \deg \widetilde{\mathcal{B}}_{(i,h,1)} \leq \deg \mathfrak{B}_{(i,h,(n-i)(n+1)-i+1)}$.

For $d \geq 2$ and $1 \leq j \leq (n-i)(n+1)-1$ we infer from the Bézout inequality [22, 31, 62] the following extrinsic bounds for these degrees (see [5] for details):

$$\deg \mathfrak{B}_{(i,h,j)} \leq d^{n+1}(nd+j)^{(n-i)(n+1)-j} = (nd)^{O((n-i)n)} \tag{10}$$

whence, in particular,

$$\deg \mathfrak{B}_{(n-1,h,j)} \leq \frac{(nd^2+dj)^{n+1}}{(nd+j)^j} \leq \big(nd(d+1)\big)^{n+1} = (nd)^{O(n)}. \tag{11}$$

Similarly we have for $1 \leq j \leq n-1$

$$\deg \mathcal{B}_{(i,h,j;\gamma)} \leq \deg \widetilde{\mathcal{B}}_{(i,h,j)} \leq d^{n+1}(nd+j)^{(n-j)} \leq d\big(nd(d+1)\big)^{n} = (nd)^{O(n)}. \tag{12}$$

In view of the subsequent algorithmic considerations we notice that the estimates (11) and (12) of the degree are of order $(nd)^{O(n)}$.

We now fix only $1 \leq i \leq n-1$, $1 \leq k \leq n-i$ and a non-zero real number γ.

For $1 \leq l \leq n$ we are going to consider the following closed subvarieties of the affine ambient spaces $\mathbb{T}_i{}^{(h)}$ and $\mathbb{N}_i{}^{(h)}$, which we denote by $S_l{}^{(i,h)}$ and $S_l{}^{(i,h;\gamma)}$.

Let $S_l{}^{(i,h)}$ be the Zariski closure of the locally closed subset of $\mathbb{N}_i{}^{(h)}$ defined by the conditions

$$F(X)=0, \qquad \frac{\partial F}{\partial X_{t'}}(X)\varLambda + (B_{h,t'} - X_{t'})\varTheta_h + \sum_{\substack{1\leq k\leq n-i\\ k\neq h}} B_{k,t'}\varTheta_k = 0, \quad 1 \leq t' \leq l,$$

$$\operatorname{rk} B = \operatorname{rk} B^{(h)}(X) = n-i \quad \text{and} \quad J(F) \neq 0$$

and let $S_l{}^{(i,h;\gamma)}$ be the Zariski closure of the locally closed subset of $\mathbb{N}_i{}^{(h)}$ defined by the conditions

$$\begin{aligned}
&F(X)=0,\\
&\frac{\partial F}{\partial X_h}(X)\varLambda + (\gamma - X_h)\varTheta_h = 0,\\
&\frac{\partial F}{\partial X_{t'}}(X)\varLambda - X_{t'}\varTheta_h + \varTheta_{t'} = 0,\\
&\quad 1 \leq t' \leq \min\{l, n-i\},\ t' \neq h,\\
&\frac{\partial F}{\partial X_{t'}}(X)\varLambda + \big(B^*_{t'} - X_{t'}\big)\varTheta_h = 0,\\
&\quad n-i < t' \leq l,\\
&\quad X_h - \gamma \neq 0.
\end{aligned}$$

Observe that the particular structure of the Jacobian of the system (3) implies that the polynomials of the equations defining $S_l^{(i,h)}$ form outside of the closed locus given by the conditions $\operatorname{rk} B < n-i$, $\operatorname{rk} B(X) < n-i$ or $J(F)=0$ locally a reduced regular sequence. The same is true for the polynomials of the equations defining $S_l^{(i,h;\gamma)}$ outside of the locus $X_h - \gamma = 0$. In particular, this implies that the polynomials of the systems (3) and (4) form outside of these closed loci locally strongly reduced regular sequences.

From the Bézout Inequality we deduce the estimates

$$\deg {S_l}^{(i,h)} \leq d^{l+1} \tag{13}$$

and

$$\deg {S_l}^{(i,h;\gamma)} \leq d^{l+1}. \tag{14}$$

We associate now with i, h, γ and the real interpretation of the polynomial equation $F=0$ the following discrete parameters:

$$\delta_{(i,h)} := \max\Bigl\{\bigl\{\deg S_l^{(i,h)} \mid 1 \leq l \leq n\bigr\}, \max\bigl\{\deg \mathfrak{B}_{(i,h,(n-i)n-i+j)} \mid 1 \leq j \leq n-1\bigr\}\Bigr\}$$

and

$$\delta_{(i,h;\gamma)} := \max\Bigl\{\bigl\{\deg S_l^{(i,h;\gamma)} \mid 1 \leq l \leq n\bigr\}, \max\bigl\{\deg \overline{(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}} \mid 1 \leq j \leq n-1\bigr\}\Bigr\}.$$

For generically chosen γ we write

$$\tilde{\delta}_{(i,h)} := \delta_{(i,h;\gamma)}.$$

We observe that the parameter $\max\{\deg \mathfrak{B}_{(i,h,j)} | 1 \leq j \leq (n-i)(n+1)-1\}$ remains invariant under linear transformations of the coordinates $X_1, \ldots, X_n$ by unitary complex $(n \times n)$ matrices, whereas the parameter $\max\{\deg \overline{(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}} \mid 1 \leq j \leq n-1\}$ is coordinate-dependent even for such special linear transformations. Therefore, we call $\delta_{(i,h)}$ the *unitary-independent degree* of the real interpretation of the equation $F=0$ associated with i and h. In the same vein we call $\delta_{(i,h;\gamma)}$ and $\tilde{\delta}_{(i,h)}$ the *unitary-dependent degrees* of the real interpretation of $F=0$ associated with i, h, γ and with i, h, respectively.

In the light of the geometric underpinning of the notion of dual polar varieties exposed in [4, 5], Sect. 2, the limitation to unitary complex matrices makes sense. The definition of dual polar varieties in intrinsic terms requires as ingredients a non-degenerate hyperquadric and a hyperplane at infinity in the corresponding projective ambient space such that the restriction of the given hyperquadric to the hyperplane at infinity remains non-degenerate. If the chosen hyperquadric represents in the associated real affine space the Euclidean norm, then only unitary matrices leave the given geometric situation invariant. For details we refer to [4, 5], Sects. 2 and 3.1. Taking into account the estimates (13) and (9) we conclude that

$$\delta_{(i,h;\gamma)} \leq \tilde{\delta}_{(i,h)} \leq \delta_{(i,h)} \tag{15}$$

and that

$$\delta_{(i,h)} = (nd)^{O(n)} \tag{16}$$

holds. This implies

$$\delta_{(i,h;\gamma)} = (nd)^{O(n)} \tag{17}$$

and

$$\tilde{\delta}_{(i,h)} = (nd)^{O(n)}. \tag{18}$$

4.3 The Real Root Finding Problem for F

We finish Sect. 4 with the design of a discrete family of efficient, non-uniform deterministic (or alternatively uniform probabilistic) procedures $\Pi_{(i,h)}$, $1 \le i \le n-1$, $1 \le h \le n-i$, which satisfy the following specification. Let Z be a new indeterminate.

Input: An essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ having a single output node.

Input Specification: The circuit σ represents a polynomial $F \in \mathbb{Q}[X]$ of positive degree d and logarithmic height at most η. The semialgebraic set $\{F = 0\}_{\mathbb{R}}$ is compact and the indeterminates $X_1, \ldots, X_n$ are in general position with respect to the complex hypersurface $\{F = 0\}$.

Output: The procedure $\Pi_{(i,h)}$ accepts the input σ if $\{F = 0\}$ contains a real regular point. If this is the case, the procedure returns 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 output specification:

- P is monic and separable.
- $\deg G < \deg P \le \deg \widetilde{\mathcal{B}}_{(i,h,1)} \le \delta_{(i,h)}$ with $\deg G := \max\{\deg G_1, \ldots, \deg G_n\}$.
- The zero-dimensional complex affine variety, $\{G(z) \mid z \in \mathbb{A}^1, P(z) = 0\}$ contains a smooth, real algebraic sample point of each generically smooth connected component of $\{F = 0\}_{\mathbb{R}}$. 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. [16] for this kind of encoding).

We say that $\Pi_{(i,h)}$ solves the *real root finding problem for F*. We fix now $1 \le i \le n-1$ and $1 \le h \le n-i$.

Design of the Procedure $\Pi_{(i,h)}$ Let σ be an essentially division-free circuit in $\mathbb{Q}[X]$ of size L having a single output node which represents a polynomial $F \in \mathbb{Q}[X]$ satisfying the input specification of the procedure $\Pi_{(i,h)}$. Let d be the (positive) degree of F and η its logarithmic height. We consider the function

$$\|\cdot\| : \{F = 0\}_{\mathbb{R}} \to \mathbb{R}$$

induced by the Euclidean norm on $\mathbb{R}^n$. Observe that $\|\cdot\|$ is continuous and semialgebraic. Since by assumption $\{F = 0\}_{\mathbb{R}}$ is compact, the function $\|\cdot\|$ is bounded by a positive constant, say K, which we suppose to be minimal with respect to this property. From the effective Lojasiewicz Inequality (see [56], Theorem 3) we deduce that there exists a universal constant $c > 0$ (not depending on L, ℓ, d, n or η) which satisfies the condition $\log(\max\{1, K\}) \le \eta d^{cn^2}$.

Let us choose a positive integer γ with $\log\gamma > \eta d^{cn^2}$ which is representable by a division-free arithmetic circuit in $\mathbb{Z}$ of size and non-scalar depth $O(\log\eta + n^2\log d)$ and observe that $\gamma > K$ holds.

Therefore, any real point $x = (x_1, \ldots, x_n)$ of the hypersurface $\{F = 0\}$ satisfies the condition $x_h - \gamma \neq 0$. Since by assumption the indeterminates $X_1, \ldots, X_n$ are in general position with respect to $\{F = 0\}$, we may suppose without loss of generality that any generically regular connected component of $\{F = 0\}_{\mathbb{R}}$ contains also a point x with $\frac{\partial F}{\partial X_h}(x) \neq 0$.

From Proposition 5 and the choice of γ we deduce that the (polynomial) equations of the system

$$\begin{aligned}
&F(X) = 0,\\
&\frac{\partial F}{\partial X_h}(X)\Lambda + \gamma - X_h = 0,\\
&\frac{\partial F}{\partial X_l}(X)\Lambda - X_l + \Theta_l = 0,\\
&\quad 1 \le l \le n - i, l \neq h,\\
&\frac{\partial F}{\partial X_l}(X)\Lambda + B_l^* - X_l = 0,\\
&\quad n - i < l \le n,
\end{aligned} \tag{19}$$

intersect transversally at each of their real solutions. Moreover, the polynomials of (19) generate the trivial ideal or form a strongly reduced regular sequence in $\mathbb{Q}[X, B^*_{n-i+1}, \ldots, B^*_n, \Lambda, \Theta^*]_{X_n-\gamma}$ (see Sect. 4.2).

Denote by $V := S_n^{(i,h;\gamma)}$ the locally closed algebraic subvariety of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ consisting of the common (complex) solutions of the polynomial equation system (19) which satisfy the condition $X_h - \gamma \neq 0$ and let $V_{\mathbb{R}} := V \cap (\mathbb{A}^n_{\mathbb{R}} \times \mathbb{A}^i_{\mathbb{R}} \times \mathbb{A}^{n-i}_{\mathbb{R}})$ be the real trace of V. Our choice of γ implies that $V_{\mathbb{R}}$ consists of all real solutions of (19) and is therefore closed. Moreover, from our assumptions and Proposition 5 we deduce that V and $V_{\mathbb{R}}$ are empty or smooth of dimension $n - 1$, and that the real variety $V_{\mathbb{R}}$ is non-empty if and only if $\{F = 0\}_{\mathbb{R}}$ contains a smooth point. More precisely, for any generically smooth connected component C of $\{F = 0\}_{\mathbb{R}}$ there exists a point $(x, b, \lambda, \vartheta)$ of $V_{\mathbb{R}}$ with $x \in C$, $\frac{\partial F}{\partial X_h}(x) \neq 0$ and $(b, \lambda, \vartheta) \in \mathbb{A}^i_{\mathbb{R}} \times \mathbb{A}^{n-i}_{\mathbb{R}}$. 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 generically smooth connected components of $\{F = 0\}_{\mathbb{R}}$.

Suppose now that the hypersurface $\{F = 0\}$ contains a smooth real point. Then the real variety $V_{\mathbb{R}}$ is smooth and equidimensional of dimension $n - 1$. For $1 \le j \le n - 1$ we deduce from [5], Proposition 2 that the real bipolar variety $(\mathcal{B}_{(i,h,j;\gamma)})_{\mathbb{R}}$ (and hence the complex variety $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}$ contains at least one point of each connected component of $V_{\mathbb{R}}$. Therefore, $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}$ and $(\mathcal{B}_{(i,h,j;\gamma)})_{\mathbb{R}}$ are equidimensional of dimension $j - 1$. From Proposition 12 and Observation 13 we conclude that for $2 \le j \le n - 1$ the algebraic variety $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma} \setminus (\mathcal{B}_{(i,h,j-1;\gamma)})_{X_h-\gamma}$ is locally definable by reduced regular sequences.

In the same way one sees that the complex variety $(\mathcal{B}_{(i,h,1;\gamma)})_{X_h-\gamma}$ is zero-dimensional and contains for each connected component of $V_{\mathbb{R}}$ an algebraic sample point.

The algorithm $\Pi_{(i,h)}$ proceeds now by deciding whether $(\mathcal{B}_{(i,h,1;\gamma)})_{X_h-\gamma}$ contains real algebraic points, and, if this is the case, by computing them. The algorithm infers from these data whether the hypersurface $\{F=0\}_{\mathbb{R}}$ contains smooth points. If the answer is positive, the data furnish also a finite set of smooth real algebraic sample points for the generically smooth connected components of $\{F=0\}_{\mathbb{R}}$.

At the beginning, the procedure $\Pi_{(i,h)}$ transforms the input circuit σ and the chosen encoding of γ into an essentially division-free arithmetic circuit σ_1 in $\mathbb{Q}[X, B^*_{n-i+1}, \dots, B^*_n, \Lambda, \Theta^{(h)}]$ of size $O(L+n^2\log d+\log\eta)$ and non-scalar depth $O(\ell+n^2\log d+\log\eta)$ such that σ_1 represents the equation system (19) and the polynomial $X_n-\gamma$. Taking the circuit σ_1 as input, the procedure $\Pi_{(i,h)}$ now follows the pattern of the (non-uniform deterministic or probabilistic) procedure described in the proofs of [5], 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 $\Pi_{(i,h)}$ returns the answer that the hypersurface $\{F=0\}$ does not contain any smooth real point.

If $V_{\mathbb{R}}$ is non-empty, the procedure $\Pi_{(i,h)}$ produces a circuit representation of the coefficients of $2n+1$ polynomials $P, G_1, \dots, G_n, G_{n+1}, \dots, G_{2n} \in \mathbb{Q}[Z]$ satisfying for $\widetilde{G} := (G_1, \dots, G_{2n})$ the following output specification:

- P is monic and separable.
- $\deg \widetilde{G} < \deg P \leq \deg(\mathcal{B}_{(i,h,1;\gamma)})_{X_h-\gamma} \leq \deg \mathcal{B}_{(i,h,1;\gamma)}$.
- $(\mathcal{B}_{(i,h,1;\gamma)})_{(X_n-\gamma)} = \{\widetilde{G}(z) | z \in \mathbb{A}^1, P(z)=0\}$.

From this representation of the variety $(\mathcal{B}_{(i,h,1;\gamma)})_{(X_n-\gamma)}$ we deduce that for $G := (G_1, \dots, G_n)$ the zero-dimensional variety $\{G(z) \,|\, z \in \mathbb{A}^1, P(z)=0\}$ contains a smooth real algebraic sample point for each generically smooth connected component of $\{F=0\}_{\mathbb{R}}$. Finally, one obtains a set of real algebraic sample points for the generically smooth connected components of $\{F=0\}_{\mathbb{R}}$ from G and the Thom encoding of the real zeros of P. If P has no real zeros, the procedure $\Pi_{(i,h)}$ returns the information that $\{F=0\}_{\mathbb{R}}$ does not contain any smooth point.

The procedure from [4] and [5], called by $\Pi_{(i,h)}$, is based on the original paradigm [25, 27] of a procedure with intrinsic complexity that solves polynomial equation systems over the *complex* numbers (see also [20, 24, 28]).

We are now going to describe *succinctly* how this procedure is applied to the task of real root finding (Proposition 12 and Observation 13 will here play a key role).

For this purpose we shall freely refer to terminology, mathematical results and subroutines of [28], where the first streamlined version of this procedure was presented and implemented as the "Kronecker algorithm" (compare also [36]).

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 the reader to be acquainted with the details of the Kronecker algorithm. Although this description may look at first glance intricate, no substantially new idea, nor one that has not been explained before, is introduced. Recall that the polynomials of (19) generate the trivial ideal or form a strongly reduced regular sequence in $\mathbb{Q}[X, B^*_{n-i+1}, \dots, B^*_n, \Lambda, \Theta^{(h)}]_{X_h-\gamma}$. In this situation the procedure $\Pi_{(i,h)}$

applies to the system (19) the algorithm "Geometric Solve" of [28] to decide whether V is empty. If V is empty, the information that $\{F=0\}_{\mathbb{R}}$ does not contain any regular 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 $j := n-1$, the procedure $\Pi_{(i,h)}$ decides for any index $1 \leq j \leq n-1$ whether the variety $\mathcal{B}_{(i,h,j;\gamma)}$ is empty or returns a lifting fiber of it. In case that there exists an index $1 \leq j \leq n-1$ with $\mathcal{B}_{(i,h,j;\gamma)} = \emptyset$, the procedure $\Pi_{(i,h)}$ returns the information that $\{F=0\}_{\mathbb{R}}$ does not contain any regular point. Suppose that this is not the case.

For $1 \leq j \leq n-1$ we fix a vector of column numbers $\underline{t}^{(j)} \in \mathbb{N}^{n+j}$ of $T_{(i,h,j;\gamma)}$ corresponding to the indeterminate X_h, to the entries of $\Theta^{(h)}$, to $B_l^*, n-i < l \leq n$ and to j other columns of $T_{(i,h,j;\gamma)}$.

We claim that $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}$ does not vanish identically on any irreducible component of $\mathcal{B}_{(i,h,j;\gamma)}$.

Let M be the $((n+1)\times(n+1))$ submatrix of the Jacobian of the equation system (19) which corresponds to the indeterminate X_h, to the entries of $\Theta^{(h)}$ and to $B_l^*, n-i < l \leq n$ (thus we have $\det M = m_{(i,h,j,\underline{t}^{(1)},1;\gamma)}$).

Observe that $\det M$ vanishes nowhere on V. Let $1 \leq j \leq n-1$. The matrix which gives rise to $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}$ contains M as submatrix. From the genericity of the rows number $n+2,\ldots,n+j$ of this matrix and the determinant structure of $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}$ one easily deduces that the hypersurface of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ defined by the equation $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)} = 0$ cuts V properly. Let W be the resulting intersection and let $\underline{t} \in \mathbb{N}^{n+j}$ be a suitable vector. In a similar way as before we see that the hypersurfaces of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ defined by

$$M_{n+j+1}^{(i,h,j,\underline{t};\gamma)} = 0, \quad \ldots, \quad M_{2n}^{(i,h,j,\underline{t};\gamma)} = 0 \tag{20}$$

cut $W_{m_{(i,h,j,\underline{t},1;\gamma)}}$ properly. Thus the hypersurfaces of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ defined by (20) and $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)} = 0$ cut V properly outside of the locus given by $m_{(i,h,j,\underline{t},1;\gamma)} = 0$ (compare [8], Sect. 3 for this kind of argumentation).

Let C be an irreducible component of $\mathcal{B}_{(i,h,j;\gamma)}$. From [5], Proposition 8 we deduce that there exists a suitable vector $\underline{t} \in \mathbb{N}^{n+j}$ such that the minor $m_{(i,h,j,\underline{t},1;\gamma)}$ does not vanish identically on C. Outside of the locus of $\mathbb{A}^n \times \mathbb{A}^i \times \mathbb{A}^{n-i}$ defined by this minor, the irreducible component C is the intersection of V with the variety given by the system (20). Since the codimension of C in V is $n-j$, our claim follows.

From Proposition 12 we deduce that the system

$$\begin{aligned}
&F(X) = 0, \qquad \frac{\partial F}{\partial X_h}(X)\Lambda + \gamma - X_h = 0,\\
&\frac{\partial F}{\partial X_l}(X)\Lambda - X_l + \Theta_l = 0, \quad 1 \leq l \leq n-i, l \neq h,\\
&\frac{\partial F}{\partial X_l}(X)\Lambda + B_l^* - X_l = 0, \quad n-i < l \leq n,\\
&M_{n+j+1}^{(i,h,j,\underline{t}^{(j)};\gamma)} = 0, \quad \ldots, \quad M_{2n}^{(i,h,j,\underline{t}^{(j)};\gamma)} = 0,\\
&m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}(X_h - \gamma) \neq 0
\end{aligned} \tag{21}$$

defines the variety

$$(\mathcal{B}_{(i,h,j;\gamma)})_{m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}(X_n-\gamma)}.$$

The assumption $\mathcal{B}_{(i,h,j;\gamma)} \neq \emptyset$ implies that this variety is not empty. Therefore the polynomials of the equations of the system (21) form a reduced regular sequence in

$$\mathbb{Q}\big[X, \Lambda, B^*_{n-i+1}, \ldots, B^*_n, \Theta^{(h)}\big]_{m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}(X_h-\gamma)}$$

and hence a lifting system in the sense of [28] for the variety $\mathcal{B}_{(i,h,j;\gamma)}$. Inductively we suppose that there is given a lifting fiber of $\mathcal{B}_{(i,h,j;\gamma)}$ on which $m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}(X_h-\gamma)$ nowhere vanishes.

In this situation $\Pi_{(i,h)}$ combines the algorithms "Lifting Curve", "Change Free Variables", "Change Lifting Point" and "Change Primitive Element" of [28] in order to produce a Kronecker parameterization of a suitable curve $\mathcal{C}_{(i,h,j;\gamma)}$ in $(\mathcal{B}_{(i,h,j;\gamma)})_{m_{(i,h,j,\underline{t}^{(j)},1;\gamma)}(X_h-\gamma)}$ which lifts the fiber of a sufficiently generic lifting point with respect to the lifting system (21) and a sufficiently generic Noether position of $\mathcal{B}_{(i,h,j;\gamma)}$.

Next the procedure $\Pi_{(i,h)}$ applies for $n+j \leq k \leq 2n$ the algorithm "One Dimensional Intersect" of [28] to the given Kronecker parameterization of $\mathcal{C}_{(i,h,j;\gamma)}$ and the polynomials $M_k^{(i,h,j-1,\underline{t}^{(j-1)};\gamma)}$ and $m_{(i,h,j-1,\underline{t}^{(j-1)},1;\gamma)}(X_h-\gamma)$ and computes the greatest common divisor of the resulting univariate elimination polynomials. This greatest common divisor is not one, since by assumption the variety $\mathcal{B}_{(i,h,j-1;\gamma)}$ is not empty. In this way $\Pi_{(i,h)}$ produces a lifting fiber of $\mathcal{B}_{(i,h,j-1;\gamma)}$ on which $m_{(i,h,j-1,\underline{t}^{(j-1)},1;\gamma)}$ vanishes nowhere.

At the end $\Pi_{(i,h)}$ produces a geometric solution of the zero-dimensional algebraic variety $\mathcal{B}_{(i,h,1;\gamma)}$. More precisely, the procedure $\Pi_{(i,h)}$ produces a circuit representation of the coefficients of $2n+1$ polynomials $P, G_1, \ldots, G_{2n} \in \mathbb{Q}[Z]$ as above.

From the complexity estimates of [28] we deduce that $\Pi_{(i,h)}$ runs using

$$\begin{aligned}(L+\log\eta)(nd)^{O(1)}\Big(\max\Big\{&\max\big\{\deg S_l^{(i,h;\gamma)} | 1 \leq l \leq n\big\},\\ &\max\big\{\deg \mathcal{B}_{(i,h,j,\underline{t};\gamma)} \mid 1 \leq j \leq n-1\big\}\Big\}\Big)^2\\ = (L+\log\eta)(nd)^{O(1)}&(\delta_{(i,h;\gamma)})^2\end{aligned}$$

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

$$O\big(n^3\big(\ell+\log(dn\eta)\big)\log\delta_{(i,h;\gamma)}\big).$$

The procedure can easily be translated to the bit model. In order to estimate its bit complexity we consider the logarithmic height, say $\varkappa_{(i,h;\gamma)} = O((nd)^n\eta)$, of the bipolar variety $\mathcal{B}_{(i,h,1,\gamma)}$. 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 $O(L^2(nd\eta)^{O(1)}(\delta_{(i,h;\gamma)}\varkappa_{(i,h;\gamma)})^2)$ bit operations (see [30] for the relationship between arithmetic and bit representation of integers).

An alternative procedure to $\Pi_{(i,h)}$ may be obtained applying for $j := 1$ the algorithm "Geometric Solve" of [28] to the system (8). The complexity estimates for this procedure, which are the same as for $\Pi_{(i,h)}$, follow from arguments in [8], Sect. 4 and especially from Theorem 3 and Example 2.

We have therefore proven the following complexity statement (compare [4], Theorem 11 and [5], Theorem 13).

Theorem 14 *Let $n, d, \eta, i, h, \delta, L, \ell$ be natural numbers with $d \geq 1$, $1 \leq i \leq n-1$ and $1 \leq h \leq n-i$. 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*

$$O\big((L + \log \eta)(nd)^{O(1)}\delta^2\big) = (nd)^{O(n)} \log \eta$$

and non-scalar depth

$$O\big(n^3\big(\ell + \log(nd\eta)\big)\log \delta\big) = O\big(n^4 \log(dn\eta) \log d\big),$$

such that $\mathcal{N}$ satisfies for suitable specializations of its parameters the following condition: Let $F \in \mathbb{Q}[X]$ be a polynomial of degree d and (logarithmic) height η and assume that F is given by an essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ. Suppose that $\{F = 0\}_{\mathbb{R}}$ is compact, that the variables $X_1, \ldots, X_n$ are in general position with respect to the complex hypersurface $\{F = 0\}$, and that the unitary-dependent generic degree of the real interpretation of $F = 0$ associated with i and h is bounded by δ (in symbols: $\tilde{\delta}_{(i,h)} \leq \delta$). Then the algorithm represented by the arithmetic network $\mathcal{N}$ starts from the circuit σ as input and decides whether the hypersurface $\{F = 0\}$ 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 output specification:

- *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 $\{F = 0\}_{\mathbb{R}}$.*

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 [63, 64].

Four remarks on the formulation of Theorem 14 are in order.

- If we limit our attention to arithmetic input circuits σ in $\mathbb{Z}[X]$ which depend only on the parameters 0, 1, then we may replace in the statement of Theorem 14 the quantity $\log \eta$ by ℓ.

- The upper bound $O(n^3(\ell+\log(nd\eta))\log\delta)$ for the non-scalar depth of the arithmetical network $\mathcal{N}$ is far from being optimal, because it depends on the factor n^3. Only a single factor n is justified by our recursive method, whereas the coarse estimate in the effective Lojasiewicz Inequality [56] contributes with an extra factor of n^2. In any case, it would be desirable, but maybe difficult to achieve, to have an upper bound of $O(n(\ell+\log(nd\eta))\log\delta)$ for the non-scalar depth of $\mathcal{N}$.

We state the third remark in the following way:

Observation 15 *The statement of Theorem 14 remains true if we drop the hypothesis that the indeterminates $X_1,\dots,X_n$ are in a general position with respect to the complex hypersurface $\{F=0\}$ and if we assume that the condition $\delta_{(i,h)}\le\delta$ is satisfied. This is always the case for $\delta=(nd)^{O(n)}$.*

Proof In the design of the procedure $\Pi_{(i,h)}$ the genericity assumption on the variables was only used in order to guarantee that the partial derivative $\frac{\partial F}{\partial X_h}$ does not vanish identically on any generically regular connected component of $\{F=0\}_{\mathbb{R}}$. It is easy to see that this can be achieved by an orthogonal matrix $M\in\mathbb{A}_{\mathbb{R}}^{n\times n}$ which transforms $X=(X_1,\dots,X_n)$ into $Y=(Y_1,\dots,Y_n):=XM$. Let us denote by $\tilde{\delta}_{(i,h)}(Y)$ and $\delta_{(i,h)}(Y)$ the unitary-dependent and unitary-independent degrees, respectively, of the real interpretation of the equation $F(YM^{\mathrm{T}})=0$, which are associated with the indices $1\le i\le n-1$ and $1\le h\le n-i$. Then Theorem 14 may be applied to $F(YM^{\mathrm{T}})$. From (15) we deduce the estimate $\tilde{\delta}_{(i,h)}(Y)\le\delta_{(i,h)}(Y)$. Since the degree $\delta_{(i,h)}$ is unitary-independent, we have $\delta_{(i,h)}(Y)=\delta_{(i,h)}$, where $\delta_{(i,h)}$ is defined with respect to the original variables $X_1,\dots,X_n$. According to (16) we have $\delta_{(i,h)}=(nd)^{O(n)}$. This implies the statement of Observation 15. □

The fourth remark is the following statement.

Observation 16 *Theorem 14 asserts only the* existence *of a computation that, for a given n-variate input polynomial F of degree d, logarithmic height η and circuit size and non-scalar depth L and ℓ, with variables in general position and $\{F=0\}_{\mathbb{R}}$ compact, solves the real root finding problem for F in sequential and non-scalar parallel time $O((L+\log\eta)(nd)^{O(1)}\tilde{\delta}^2_{(i,h)})$ and $O(n^3(\ell+\log(nd\eta))\log\tilde{\delta}_{(i,h)})$, respectively, where $\tilde{\delta}_{(i,h)}$ denotes the unitary-dependent generic degree of the real interpretation of the equation $F=0$ associated with $1\le i\le n-1$ and $1\le h\le n-i$.*

Theorem 14 therefore refers 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* [36] *and* [28]). *This is achieved by choosing randomly the parameters of the arithmetic network $\mathcal{N}$ of Theorem 14. The same remark applies mutatis mutandis to Observation 15.*

Let us finally comment that the algorithm $\Pi_{(i,h)}$ can be reinterpreted as the following simple minded procedure, inspired by the well-known trick of Rabinowitsch.

Let $F \in \mathbb{Q}[X]$ be a polynomial satisfying the input specification of the procedure $\Pi_{(i,h)}$ and let γ be an integer such that any real point $x = (x_1, \dots, x_n)$ of the hypersurface $\{F = 0\}$ satisfies the condition $x_h \neq \gamma$. Since $\{F = 0\}_{\mathbb{R}}$ is by assumption compact, such an integer γ exists (recall the beginning of the design of the procedure $\Pi_{(i,h)}$).

Consider now the polynomial equation system

$$\begin{aligned} &F(X) = 0, \\ &\frac{\partial F}{\partial X_h}(X)\Lambda + \gamma - X_h = 0 \end{aligned} \tag{22}$$

and observe that it admits only smooth solutions in $\mathbb{A}^n \times \mathbb{A}^1$ and that its equations generate in $\mathbb{R}[X, \Lambda]$ the trivial or a radical complete intersection ideal. Moreover, observe that the connected components of the real solutions of (22) correspond to the generically regular connected components of $\{F = 0\}_{\mathbb{R}}$.

By means of the already mentioned algorithm of [4], Theorem 11 and [5], Theorem 13 we may find for each connected component of

$$\left\{(x, \lambda) \in \mathbb{R}^n \times \mathbb{R} \mid F(x) = 0, \frac{\partial F}{\partial X_h}(x)\lambda + \gamma - x_h = 0\right\}$$

a real algebraic sample point and therefore also for each generically regular connected component of $\{F = 0\}_{\mathbb{R}}$.

For given $1 \leq i \leq n - 1$ and $1 \leq h \leq n - i$ the equations in (22) form part of the system (19), which is solved by the procedure $\Pi_{(i,h)}$. Without the larger context of the incidence varieties $H_i^{(h,\gamma)}$ and $H_i^{(h)}$ and their real traces, this procedure seems to be arbitrary and depending on the position of the variables $X_1, \dots, X_n$ and its complexity behavior appears as completely unrelated to the geometry of the complex hypersurface $\{F = 0\}$ and the real variety $\{F = 0\}_{\mathbb{R}}$.

Thanks to the notion of bipolar varieties we now become aware that this is not the case (see Theorem 14 and Observation 15).

5 Walks

We are now going to develop a common view for the procedures $\Pi_{(i,h)}$, $1 \leq i \leq n - 1, 1 \leq h \leq n - i$ described in Sect. 4 for the task of finding smooth points in possibly singular, real compact hypersurfaces, and the algorithms developed in [2–4] and [5] for the case of smooth real complete intersection varieties.

Let us fix a polynomial $F \in \mathbb{Q}[X]$ and suppose without loss of generality that the hypersurface $\{F = 0\}$ contains a regular real point.

Let $1 \leq i \leq n - 1, 1 \leq h \leq n - i$ and a suitable integer $\gamma \in \mathbb{N}$ be given. We first analyze the procedure $\Pi_{(i,h)}$ on input σ, where σ is an essentially division-free arithmetic circuit in $\mathbb{Q}[X]$ representing the polynomial F, while $\{F = 0\}_{\mathbb{R}}$ is supposed to be compact with $\{F = 0\}_{\mathbb{R}} = (\{F = 0\}_{X_h - \gamma})_{\mathbb{R}}$.

On input σ we may interpret $\Pi_{(i,h)}$ as a computation which starts with the variety $H_i^{(h,\gamma)}$ defined by the system (4) and "walks down" through the localized bipolar varieties $(\mathcal{B}_{(i,h,j;\gamma)})_{X_h-\gamma}$, beginning with $j := n-1$ and ending with $j := 1$.

In view of Lemma 1 we may interpret the procedure $\Pi_{(i,h)}$ on input σ, alternatively, as a computation that starts with the variety $H_i^{(h)}$ defined by the system (3) and walks in reverse mode through the *non-generic* dual polar varieties of $H_i^{(h)}$ defined for $1 \leq j \leq n-1$ as follows: We replace in the $(((n-i)(n+1)+j+1) \times ((n-i)(n+1)+n))$ matrix $T_{(i,h,(n-i)n-i+j)}$ introduced at the beginning of Sect. 4 the rows numbered $n+j+1, \dots, (n-i)(n+1)+j$ by unit vectors whose entries are all zero, except one entry of value 1 at the place of the column of $T_{(i,h,(n-i)n-i+j)}$ which corresponds to one of the indeterminates $B_{k,l}$, $1 \leq k \leq n-i$, $1 \leq l \leq n$ with $(k,l) \notin \{(h,n-i+1), \dots, (h,n)\}$. The points of $(H_i^{(h)})$, where the rank of this new matrix is not maximal, form a dual polar variety of $(H_i^{(h)})$ which is non-generic (in fact, *meagerly generic* in the sense of [8]). The computation, which represents the alternative interpretation of the procedure $\Pi_{(i,h)}$ on input σ, cuts $(H_i^{(h)})_{X_h-\gamma}$ and the intersections of $(H_i^{(h)})_{X_h-\gamma}$ with the dual polar varieties obtained in this way, by the affine hyperplanes $\{B_{k,l} - \beta_{k,l} = 0\}$ with $1 \leq k \leq n-i, 1 \leq l \leq n$, $(k,l) \notin \{(h,n-i+1), \dots, (h,n)\}$, where $\beta_{k,l}$ is defined as $\beta_{k,l} := 0$ for $k \neq l$, $\beta_{k,k} := 1$ for $k \neq h$ and $\beta_{h,h} := \gamma$.

This construction yields algebraic varieties which are by Lemma 1 isomorphic to

$$\bigl(H_i^{(h;\gamma)}\bigr)_{X_h-\gamma}, \quad (\mathcal{B}_{(i,h,n-1;\gamma)}) \cap \bigl(H_i^{(h;\gamma)}\bigr)_{X_h-\gamma}, \quad \dots, \quad (\mathcal{B}_{(i,h,1;\gamma)}) \cap \bigl(H_i^{(h;\gamma)}\bigr)_{X_h-\gamma}.$$

We are now going to analyze the main algorithm of [4, 5] in an analogous way.

First, let us choose for each $1 \leq i \leq n-1$ a generic matrix $b_i = [b_{k,l}]_{\substack{1 \leq k \leq n-i \\ 1 \leq l \leq n}}$ of $\mathbb{Q}^{(n-i)\times n}$ such that all these matrices become "nested", i.e., for $1 < i \leq n-1$ the matrix b_i forms the first $n-i$ rows of the $((n-i+1) \times n)$ matrix b_{i-1}. The genericity condition for the matrices b_i, $1 \leq i \leq n-1$, will become clear by the context.

Suppose now again that F is given by an essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$. Under the assumption that the polynomial F is reduced and $\{F = 0\}_\mathbb{R}$ is non-empty and smooth, this algorithm starts on input σ with the complex hypersurface $\{F = 0\}$ and walks down for $h := 1$ through the generic dual polar varieties

$$W_{\overline{K}(b_1^{(1)})} \supset \cdots \supset W_{\overline{K}(b_{n-1}^{(1)})}$$

associated with the rational matrices $b_1^{(1)}, \dots, b_{n-1}^{(1)}$ (observe that $h := 1$ is the only choice of h which satisfies the condition $1 \leq h \leq n-i$ for any index $1 \leq i \leq n-1$).

Alternatively, we may interpret this algorithm as a procedure that cuts the variety $H_{n-1}^{(1)}$ first with the hyperplanes $\{B_{k,l} - b_{k,l} = 0\}$, $1 \leq k \leq n-1$, $1 \leq l \leq n$, and then successively with the hyperplanes $\{\Theta_{n-1} = 0\}, \dots, \{\Theta_2 = 0\}$.

Observe that for $1 < i \leq n-1$ the (locally closed) variety

$$\left\{ \bigl(x, b', (\lambda : \vartheta), b''\bigr) \in \bigl(H_i^{(1)} \times \mathbb{A}^{(i-1)\times n}\bigr) \mid \operatorname{rk} \begin{bmatrix} b' \\ b'' \end{bmatrix} = \operatorname{rk} \begin{bmatrix} b' \\ b'' \end{bmatrix}^{(1)} (x) = n-1 \right\}$$

is isomorphic to

$$H_{n-1}^{(1)} \cap \{\Theta_{n-1} = 0, \dots, \Theta_{n-i+1} = 0\}$$

and that

$$H_i^{(1)} \cap \big\{B_{k,l} - b_{k,l} = 0 \,|\, 1 \le k \le n-i, 1 \le l \le n\big\}$$

is isomorphic to $W_{\overline{K}(b_i^{(1)})}$.

This shows that we have two different interpretations of essentially the same procedure.

We are now going to generalize this view as walks in the set

$$\Gamma_n := \big\{(i,h,j) \,|\, 1 \le i \le n-1, 1 \le h \le n-i, 1 \le j \le (n-i)(n+1)\big\}.$$

Roughly speaking, a walk $\mathcal{W}$ is given by a sequence

$$\big((i_1,h,j_1),\dots,(i_m,h,j_m)\big)$$

of "nodes" of Γ_n and a series of affine linear cuts. These cuts become subdivided in m disjoint packets. The first packet of cuts precedes node (i_1,h,j_1). The packet number $2 \le k \le m$ becomes inserted between node (i_{k-1},h,j_{k-1}) and (i_k,h,j_k). The cuts fix arbitrary rational values for some (or none) of the indeterminates $B_{k,l}$, $1 \le k \le n-i_1$, $1 \le l \le n$, and value zero for some (or none) of the indeterminates $\Theta_2,\dots,\Theta_{n-i_1}$.

For $1 \le l \le n$, let $S_l^{(i_1,h)}(\mathcal{W})$ be the variety obtained by intersecting $S_l^{(i_1,h)}$ with the cuts of $\mathcal{W}$ preceding the node (i_1,h,j_1). We require that these cuts be transversal, that these varieties be non-empty and equidimensional and that for $1 < l \le n$ the condition

$$\dim S_{l-1}^{(i_1,h)}(\mathcal{W}) = \dim S_l^{(i_1,h)}(\mathcal{W}) + 1$$

be satisfied.

The walk $\mathcal{W}$ now is interpreted by the following semantics:

The node (i_1,h,j_1) is interpreted as the variety $S_n^{(i_1,h)}(\mathcal{W})$. For $1 < k \le m$ the node (i_k,h,j_k) becomes interpreted as the closed variety $\mathcal{W}_{(i_k,h,j_k)}$ which we are going to describe now.

For $j_k = (n-i_k)(n+1)$ let $W_{(i_k,h,j_k)} := H_{i_k}^{(h)}$ and for $1 \le j_k < (n-i_k)(n+1)$ let $W_{(i_k,h,j_k)}$ be an appropriate, possibly non-generic dual polar variety of $H_{i_k}^{(h)}$, defined by the non-maximality of the rank of the $((n+j_k+1) \times ((n-i_k)(n+1)+n))$ matrix which we obtain similarly as before by replacing in $T_{(i_k,h,j_k)}$ suitable rows by suitable $(n-i_k)(n+1)+n)$ unit vectors, all compatible according to Lemma 1 with the cuts of $\mathcal{W}$ up to the node (i_k,h,j_k). Then $\mathcal{W}_{(i_k,h,j_k)}$ is obtained by intersecting $W_{(i_k,h,j_k)}$ with the cuts of $\mathcal{W}$ up to the node (i_k,h,j_k) and taking the closure of this intersection in the corresponding ambient space.

We ask the walk $\mathcal{W}$ to fulfill the following requirements:

- $j_1 = (n-i_1)(n+1)$.
- $1 \le i_1 \le \cdots \le i_m \le n-1$.
- For $1 < k \le m$ the variety $\mathcal{W}_{(i_k,h,j_k)}$ is non-empty and equidimensional.

- For $1 < k \leq m$ the variety $\mathcal{W}_{(i_{k-1},h,j_{k-1})}$ contains $\mathcal{W}_{(i_k,h,j_k)}$ and satisfies the condition $\dim \mathcal{W}_{(i_{k-1},h,j_{k-1})} = \dim \mathcal{W}_{(i_k,h,j_k)} + 1$.
- $\dim \mathcal{W}_{(i_m,h,j_m)} = 0$.
- For $1 < k \leq m$ the cuts $\mathcal{W}$ between the nodes (i_{k-1}, h, j_{k-1}) and (i_k, h, j_k) are transversal to $\mathcal{W}_{(i_{k-1},h,j_{k-1})}$ and define $\mathcal{W}_{(i_k,h,j_k)}$ as a subvariety of $\mathcal{W}_{(i_{k-1},h,j_{k-1})}$.

The varieties $\mathcal{W}_{(i_k,h,j_k)}$, $1 \leq k \leq m$, of the walk $\mathcal{W}$ possibly have to be localized by a suitable polynomial in order to satisfy these requirements.

For $1 \leq i \leq n-1$ and $1 \leq h \leq n-i$ the procedure $\Pi_{(i,h)}$ produces on input σ a walk which we denote by $\mathcal{W}_{(i,h)}(F)$ (in fact, there are several, algorithmically equivalent, candidates for $\mathcal{W}_{(i,h)}(F)$).

Similarly, in case that F is reduced and $\{F = 0\}_{\mathbb{R}}$ is smooth, the main algorithm of [4, 5] produces on input σ a characteristic walk which we denote by $\mathcal{W}_n(F)$.

Let $\mathcal{W}$ be an arbitrary walk in Γ_n with node sequence $((i_1, h, j_1), \ldots, (i_m, h, j_m))$. The (dual) degree $\delta(\mathcal{W})$ of $\mathcal{W}$ is defined as

$$\delta(\mathcal{W}) := \max\bigl\{\max\bigl\{\deg S_l^{(i,h)}(\mathcal{W}) \mid 1 \leq l \leq n\bigr\}, \max\bigl\{\deg \mathcal{W}_{(i_k,h,j_k)} \mid 1 \leq k \leq m\bigr\}\bigr\}.$$

Suppose that $\{F = 0\}$ contains a regular real point. We say that the walk $\mathcal{W}$ solves the real root finding problem for F if the canonical projection of $(\mathcal{W}_{(i_m,h,j_m)})_{\mathbb{R}}$ into $\mathbb{A}^n_{\mathbb{R}}$ is a (finite) set of real algebraic sample points for the generically regular connected components of $\{F = 0\}_{\mathbb{R}}$.

Suppose that the polynomial F is represented by an essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ.

Applying the Kronecker algorithm to this situation we obtain the following result.

Theorem 17 *Let the notation and assumptions be as before and suppose that the walk $\mathcal{W}$ solves the real root finding problem for F. Then $\mathcal{W}$ represents a computation in $\mathbb{Q}$ which starts from σ and uses $O(L(nd)^{O(1)}\delta(\mathcal{W})^2)$ arithmetic operations, organized with respect to the parameters of the arithmetic circuit σ, in non-scalar depth $O(n(\ell + \log(nd)) \log \delta(\mathcal{W}))$ and whose output encodes a finite set of real algebraic sample points for the generically regular connected components of $\{F = 0\}_{\mathbb{R}}$. The number and degree of these sample points is bounded by $\delta(\mathcal{W})$.*

Proof The walk $\mathcal{W}$ represents a computation in $\mathbb{Q}$ that calculates from σ first a representation of (complex) algebraic points of $S_n^{(i_1,h)}(\mathcal{W})$ using $O(L(nd)^{O(1)}\delta(\mathcal{W})^2)$ arithmetic operations organized in non-scalar depth $O(n(\ell+\log(nd)) \log \delta(\mathcal{W}))$. The number and degree of these points is bounded by $\delta(\mathcal{W})$. The assumption that $\mathcal{W}$ solves the real root finding problem for F is then used to extend this computation to a representation of a finite set of real algebraic sample points for the generically regular connected components of $\{F = 0\}_{\mathbb{R}}$. The number and degree of these sample points is bounded by $\delta(\mathcal{W})$. □

Here, two remarks are in order:

- For $1 \leq i \leq n-1, 1 \leq h \leq n-i$ and $\{F = 0\}_{\mathbb{R}}$ compact, containing a regular point, Theorem 14, Observation 15 and Theorem 17 applied to $\mathcal{W}_{(i,h)}(F)$ are compatible with Theorem 17 if we consider the constant γ, produced by the procedure $\Pi_{(i,h)}$ on input σ, as precomputed. Observe that we have under this condition $\delta(\mathcal{W}_{(i,h)}(F)) = \delta_{(i,h;\gamma)}$.

Similarly Theorem 17 is compatible with [4], Theorem 11 and [5], Theorem 13, if we identify $\delta(\mathcal{W}_n(F))$ with the degree of the real interpretation of F in [4] and [5].

- We have no general criterion at hand to decide which real point finding algorithms for hypersurfaces are of best intrinsic complexity. However, if we limit our attention to the algorithms $\Pi_{(i,h)}$, $1 \le i \le n-1, 1 \le h \le n-i$, then [8], Theorem 13 implies that $\Pi_{(n-1,1)}$ has the best intrinsic sequential complexity which in the worst case is of order $d^{O(n)}$. This means that for $\{F=0\}_{\mathbb{R}}$ compact, the Rabinowitsch trick inspired algorithm, which consists of solving the polynomial equation system (21) subject to the open condition $X_h - \gamma \neq 0$ for suitable $\gamma \in \mathbb{N}$, has a fairly good intrinsic complexity despite its coordinate-dependent, extrinsic aspect.

  On the other hand, the algorithm $\Pi_{(n-1,1)}$ comes very close to the "critical point method" applied to point finding in real hypersurfaces (see [1] and [49]).

6 Witnesses for Real Inequalities

At the end of Sect. 3 we addressed the problem of how to efficiently find for a given consistent system of strict inequalities of arithmetic circuit-represented polynomials of $\mathbb{Q}[X]$ a rational witness, i.e., a point $x \in \mathbb{Q}^n$ which satisfies all these inequalities.

In this section we focus on this problem in case of a single inequality. Moreover, since the problem of finding rational witnesses even for a single inequality involves subtle height estimates from Diophantine geometry, we limit our attention to the simpler problem of finding a *real algebraic* witness for a given consistent polynomial inequality.

For this purpose let us consider a square-free polynomial $F \in \mathbb{Q}[X]$ of positive degree d. We suppose that F is given by an essentially division-free arithmetic circuit σ in $\mathbb{Q}[X]$ of size L and non-scalar depth ℓ and that $\{F=0\}_{\mathbb{R}}$ is compact. We shall make use of the following fact.

Proposition 18 *The following two conditions for the polynomial F are equivalent*:

(i) *The polynomial F changes its sign in $\mathbb{A}^n_{\mathbb{R}}$, i.e., there exist points $u, v \in \mathbb{A}^n_{\mathbb{R}}$ such that $F(u)F(v) < 0$ holds.*
(ii) *The real variety $\{F=0\}_{\mathbb{R}}$ contains a regular point.*

Proof For F irreducible, Proposition 18 is an immediate consequence of [11], Theorem 4.5.1. This implies the equivalence of conditions (i) and (ii) for an arbitrary square-free polynomial $F \in \mathbb{Q}[X]$ □

For the next result we recall from Sect. 4 that $\delta_{(n-1,1)}$ denotes the unitary-independent degree of the equation $F=0$ associated with $i := n-1$ and $h := 1$.

Theorem 19 *Let the notation and assumptions be as before. In the non-uniform deterministic or the uniform probabilistic complexity model there exists an algorithm which on input σ decides whether F changes its sign in $\mathbb{A}^n_{\mathbb{R}}$ and, if this is the case, produces the Thom encoding of two real algebraic witness points $u, v \in \mathbb{A}^n_{\mathbb{R}}$ satisfying the conditions $F(u) > 0$ and $F(v) < 0$.*

The algorithm uses $L(nd)^{O(1)}(\delta_{(n-1,1)})^2 = (nd)^{O(n)}$ arithmetic operations in $\mathbb{Q}$ organized in non-scalar depth $O(n(\ell + \log(nd)) \log \delta_{(n-1,1)})$.

Proof Since $\{F = 0\}_{\mathbb{R}}$ is supposed to be compact, we may apply the algorithm $\Pi_{(n-1,1)}$ of Sect. 4 to the input circuit σ which represents the polynomial F.

The algorithm decides first whether $\{F = 0\}_{\mathbb{R}}$ contains a regular point. From Proposition 18 we know that this is the case if and only if the polynomial F changes its sign in $\mathbb{A}^n_{\mathbb{R}}$.

Suppose we get a positive answer. Then the algorithm $\Pi_{(n-1,1)}$ produces the Thom encoding of a regular real algebraic point $x = (x_1, \dots, x_n)$ of $\{F = 0\}_{\mathbb{R}}$ such that the degree of x over $\mathbb{Q}$ is at most $\delta_{(n-1,1)}$. We then determine the signs of $\frac{\partial F}{\partial X_1}(x), \dots, \frac{\partial F}{\partial X_n}(x)$. Since x is regular we may suppose without loss of generality that $\frac{\partial F}{\partial X_1}(x) > 0$.

We consider the univariate polynomial $G(X_1) \in \mathbb{R}[X_1]$, $G(X_1) := F(X_1, x_2, \dots, x_n)$. From $F(x) = 0$ and $\frac{\partial F}{\partial X_1}(x) > 0$ we deduce that $G(x_1) = 0$ and $\frac{dG}{dX_1}(x_1) > 0$. In other words, $G(X_1)$ changes its sign at x_1. Applying any of the most classic procedures for the real root finding of univariate polynomials over $\mathbb{R}$ to this situation, we may decide whether $G(X_1)$ has zeros in the intervals $(-\infty, x_1)$ and (x_1, ∞). If for example $G(X_1)$ has no zero in (x_1, ∞), we put $u := (x_1 + 1, x_2, \dots, x_n)$. Similarly, we put $v := (x_1 - 1, x_2, \dots, x_n)$ if $G(X_1)$ has no zero in $(-\infty, x_1)$. For the sake of simplicity let us suppose that $G(X_1)$ has zeros in $(-\infty, x_1)$ as well as in (x_1, ∞). Then we compute the roots $a < x_1 < b$ of $G(X_1)$ which come closest to x_1 and put $u := (\frac{x_1+b}{2}, x_2, \dots, x_n)$ and $v := (\frac{x_1+a}{2}, x_2, \dots, x_n)$. Observe that in any case we have $F(u) > 0$ and $F(v) < 0$.

For the decision whether the polynomial F changes its sign in $\mathbb{A}^n_{\mathbb{R}}$, the algorithm requires $L(nd)^{O(1)}(\delta_{(n-1,1)})^2$ arithmetic operations in $\mathbb{Q}$ organized in non-scalar depth $O(n(\ell + \log(nd)) \log \delta_{(n-1,1)})$. If this is the case, the procedure $\Pi_{(n-1,1)}$ produces the real algebraic points u and v as witnesses for the strict inequalities $F > 0$ and $F < 0$. The degrees of u and v over $\mathbb{Q}$ are at most $\delta_{(n-1,1)}$. This implies that we can find u and v using at most $L(nd)^{O(1)}(\delta_{(n-1,1)})^2$ arithmetic operations in $\mathbb{Q}$, organized with respect to the parameters of the arithmetic circuit σ, in non-scalar depth $O(n(\ell + \log(nd)) \log \delta_{(n-1,1)})$. This yields the complexity bounds of the theorem. □

Acknowledgements 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.

References

1. P. Aubry, F. Rouillier, M. Safey El Din, Real solving for positive dimensional systems, *J. Symb. Comput.* **34**, 543–560 (2002).

2. B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties, real equation solving, and data structures: the hypersurface case, *J. Complex.* **13**, 5–27 (1997).
3. B. Bank, M. Giusti, J. Heintz, G.M. Mbakop, Polar varieties and efficient real elimination, *Math. Z.* **238**, 115–144 (2001).
4. B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Generalized polar varieties and an efficient real elimination procedure, *Kybernetika* **40**, 519–550 (2004).
5. B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Generalized polar varieties: geometry and algorithms, *J. Complex.* **21**, 377–412 (2005).
6. B. Bank, M. Giusti, J. Heintz, L.M. Pardo, On the intrinsic complexity of point finding in real singular hypersurfaces, *Inf. Process. Lett.* **109**, 1141–1144 (2009).
7. B. Bank, M. Giusti, J. Heintz, L.M. Pardo, Bipolar varieties and real solving of a singular polynomial equation, *Jaen J. Approx.* **2**(1), 65–77 (2010).
8. B. Bank, M. Giusti, J. Heintz, M. Safey El Din, E. Schost, On the geometry of polar varieties, *Appl. Algebra Eng. Commun. Comput.* **21**, 33–83 (2010).
9. S. Basu, R. Pollack, M.-F. Roy, On the combinatorial and algebraic complexity of quantifier elimination, *J. ACM* **43**, 1002–1045 (1996).
10. S. Basu, R. Pollack, M.-F. Roy, *Algorithms in Real Algebraic Geometry*, 2nd edn. (Springer, Berlin, 2006).
11. J. Bochnak, M. Coste, M.-F. Roy, *Géométrie Algébrique Réelle* (Springer, Berlin, 1987).
12. J.P. Brasselet, Milnor classes via polar varieties, in *Singularities in Algebraic and Analytic Geometry*, ed. by C.G. Melles et al., Contemp. Math., vol. 266 (AMS, Providence, 2000), pp. 181–187.
13. P. Bürgisser, M. Clausen, M.A. Shokrollahi, *Algebraic Complexity Theory*, with the collaboration of Thomas Lickteig. Grundlehren der Mathematischen Wissenschaften, vol. 315 (Springer, Berlin, 1997).
14. J.F. Canny, Some algebraic and geometric computations in PSPACE, in *ACM Symposium on Theory of Computing (STOC)* (1988), pp. 460–467.
15. D. Castro, M. Giusti, J. Heintz, G. Matera, L.M. Pardo, The hardness of polynomial equation solving, *Found. Comput. Math.* **3**, 347–420 (2003).
16. M. Coste, M.-F. Roy, Thom's lemma, the coding of real algebraic numbers and the computation of the topology of semi-algebraic sets, *J. Symb. Comput.* **5**, 121–129 (1988).
17. M. Demazure, *Catastrophes et Bifurcations* (Ellipses, Paris, 1989).
18. A. Dubson, Courants sous-analytiques, théorie d'intersection des ensembles analytiques, invariants numériques des singularités et applications. Thèse d'État, Université Paris VII (1982).
19. C. Durvye, Evaluation techniques for zero-dimensional primary decomposition, *J. Symb. Comput.* **44**, 1089–1113 (2009).
20. C. Durvye, G. Lecerf, A concise proof of the Kronecker polynomial system solver from scratch, *Expo. Math.* **26**, 101–139 (2008).
21. N. Fitchas, A. Galligo, J. Morgenstern, Algorithmes rapides en séquentiel et en parallèle pour l'élimination des quantificateurs en géométrie élémentaire, *Publ. Math. Univ. Paris VII* **32**, 103–145 (1990). Structures algébriques ordonnées, Volume I, Sélect. Expos. Sémin., Paris, 1984–1987.
22. W. Fulton, *Intersection Theory* (2nd edn.) Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 3. (Springer, Berlin, 1998). Folge 2
23. M. Giusti, J. Heintz, Kronecker's smart, little black boxes, in *Foundations of Computational Mathematics*, Conference, Oxford, GB, July 18–28, 1999, ed. by R.A. DeVore et al., Lond. Math. Soc. Lect. Note Ser., vol. 284 (Cambridge University Press, Cambridge, 2001), pp. 69–104.
24. M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, When polynomial equation systems can be "solved" fast? in *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, ed. by G. Cohen, M. Giusti, T. Mora, LNCS, vol. 948 (Springer, Berlin, 1995), pp. 205–231.
25. M. Giusti, J. Heintz, K. Hägele, J.E. Morais, J.L. Montaña, L.M. Pardo, Lower bounds for Diophantine approximations, *J. Pure Appl. Algebra* **117–118**, 277–317 (1997).
26. M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo, Le rôle des structures de données dans les problèmes d'élimination, *C.R. Acad. Sci. Paris Sér. I Math.* **325**, 1223–1228 (1997).
27. M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, *J. Pure Appl. Algebra* **124**, 101–146 (1998).
28. M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, *J. Complex.* **17**, 154–211 (2001).
29. D. Grigor'ev, N. Vorobjov, Solving systems of polynomial inequalities in subexponential time, *J. Symb. Comput.* **5**, 37–64 (1988).

30. K. Hägele, J.L. Montaña, Polynomial random test for the equivalence of integers given by arithmetic circuits. Depto. de Matematicas, Estadistica y Computacion, Universidad de Cantabria, 4 (1997).
31. J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, *Theor. Comput. Sci.* **24**, 239–277 (1983).
32. J. Heintz, M.-F. Roy, P. Solernó, On the complexity of semialgebraic sets, in *IFIP Information Processing*, vol. 89, ed. by G.X. Ritter (Amsterdam, Elsevier, 1989), pp. 293–298.
33. J. Heintz, M.-F. Roy, P. Solernó, Complexité du principe de Tarski–Seidenberg, *C.R. Acad. Sci., Paris, Sér. I Math* **309**, 825–830 (1989).
34. J. Heintz, M.-F. Roy, P. Solernó, Sur la complexité du principe de Tarski–Seidenberg, *Bull. Soc. Math. Fr.* **18**, 101–126 (1990).
35. J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, *J. Complex.* **16**, 70–109 (2000).
36. J. Heintz, G. Matera, A. Waissbein, On the time-space complexity of geometric elimination procedures, *Appl. Algebra Eng. Commun. Comput.* **11**, 239–296 (2001).
37. J.P.G. Henry, M. Merle, Limites d'espaces tangents et transversalité de variétés polaires, in *Algebraic Geometry, Proc. Int. Conf., La Rabida/Spain 1981*. Lect. Notes Math., vol. 961 (1982), pp. 189–199.
38. T. Krick, Straight-line programs in polynomial equation solving, in *Foundations of Computational Mathematics: Minneapolis 2002 (FoCM 2002)*, ed. by F. Cucker et al., London Mathematical Society Lecture Note Ser., vol. 312 (Cambridge University Press, Cambridge, 2004), pp. 96–136.
39. D.T. Lê, B. Teissier, Variétés polaires locales et classes de Chern des variétés singulières, *Ann. Math. (2)* **114**, 457–491 (1981).
40. G. Lecerf, Quadratic Newton iteration for systems with multiplicity, *Found. Comput. Math.* **2**, 247–293 (2002).
41. G. Lecerf, Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers, *J. Complex.* **19**, 564–596 (2003).
42. G. Lecerf, Kronecker software package. http://www.math.uvsq.fr/~lecerf/software/index.html.
43. L. Lehmann, Wavelet-Konstruktion als Anwendung der algorithmischen reellen algebraischen Geometrie. Dissertation, Humboldt-Universität zu Berlin, Mathematisch-Naturwissenschaftliche Fakultät II (2007). http://edoc.hu-berlin.de/docviews/abstract.php?lang=ger&id=27952.
44. L. Lehmann, A. Waissbein, Wavelets and semi-algebraic sets, in *WAIT 2001, Anales JAIIO*, vol. 30, ed. by M. Frias, J. Heintz (2001), pp. 139–155.
45. H.C. Mork, R. Piene, Polars of real singular plane curves, in *Algorithms in Algebraic Geometry*, based on the workshop, Minneapolis, MN, USA, September 18–22, 2006, ed. by A. Dickenstein et al., The IMA Volumes in Mathematics and Its Applications, vol. 146 (Springer, New York, 2008), pp. 99–115.
46. R. Piene, Polar classes of singular varieties, *Ann. Sci. Éc. Norm. Supér. (4)* **11**, 247–276 (1978).
47. 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.
48. J. Renegar, On the computational complexity and geometry of the first order theory of the reals, *J. Symb. Comput.* **13**, 255–352 (1992).
49. M. Safey El Din, Finding sampling points on real hypersurfaces is easier in singular situations. Preprint Université Paris VII (2005).
50. M. Safey El Din, E. Schost, Polar varieties and computation of one point in each connected component of a smooth real algebraic set, in *Proc. ISSAC 2003*, ed. by J.R. Sendra (ACM, New York, 2003), pp. 224–231.
51. M. Safey El Din, E. Schost, Properness defects and projections and computation of at least one point in each connected component of a real algebraic set, *J. Discrete Comput. Geom.* **32**, 417–430 (2004).
52. E. Schost, Computing parametric geometric resolutions, *Appl. Algebra Eng. Commun. Comput.* **13**, 349–393 (2003).
53. F. Severi, Sulle intersezioni delle varieta algebriche e sopra i loro caratteri e singolarità proiettive, *Torino Mem. (2)* **52**, 61–118 (1903).
54. F. Severi, La serie canonica e la teoria delle serie principali di gruppi di punti sopra una superficie algebrica, *Comment. Math. Helv.* **4**, 268–326 (1932).
55. I.R. Shafarevich, *Basic Algebraic Geometry. 1: Varieties in Projective Space* (Springer, Berlin, 1994).
56. P. Solernó, Effective Lojasiewicz inequalities in semialgebraic geometry, *Appl. Algebra Eng. Commun. Comput.* **2**, 1–14 (1991).
57. M. Spivak, *Calculus on Manifolds. A Modern Approach to Classical Theorems of Advanced Calculus*, (Benjamins, Amsterdam, 1965).

58. 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., vol. 961 (1982), pp. 314–491.
59. B. Teissier, Quelques points de l'histoire des variétés polaires, de Poncelet à nos jours, *Sémin. Anal.*, Univ. Blaise Pascal 1987–1988, 4 (1988), 12 pp.
60. J.A. Todd, The geometrical invariants of algebraic loci, *Proc. Lond. Math. Soc.* **43**, 127–138 (1937).
61. J.A. Todd, The arithmetical invariants of algebraic loci, *Proc. Lond. Math. Soc.* **43**, 190–225 (1937).
62. W. Vogel, *Lectures on Results on Bézout's Theorem*. Lectures on Mathematics and Physics, vol. 74. Notes by D.P. Patil, published for Tata Institute of Fundamental Research (Springer, Berlin, 1984).
63. 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., vol. 233 (1986), pp. 93–112.
64. J. von zur Gathen, Parallel linear algebra, in *Synthesis of Parallel Algorithms*, ed. by J.H. Reif (Morgan Kaufmann, San Mateo, 1993), pp. 573–617.