JOURNAL OF COMPLEXITY **13,** 5–27 (1997)
ARTICLE NO. CM970432

Polar Varieties, Real Equation Solving, and Data Structures: The Hypersurface Case*

B. Bank†

Humboldt-Universität zu Berlin, Untern den Linden 6, D-10099 Berlin, Germany

M. Giusti‡

GAGE, Centre de Mathématiques, École Polytechnique, F-91228 Palaiseau Cedex, France

J. Heintz§

Department de Matemáticas, Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, E-39071 Santander, Spain

and

G. M. Mbakop||

Humboldt-Universität zu Berlin, Untern den Linden 6, D-10099 Berlin, Germany

Received July 1, 1996

DEDICATED TO SHMUEL WINOGRAD

In this paper we apply for the first time a new method for multivariate equation solving which was developed for complex root determination to the *real* case. Our main result concerns the problem of finding at least one representative point for each connected component of a real compact and smooth hypersurface. The basic algorithm yields a new method for symbolically solving zero-dimensional polynomial equation systems over the complex numbers. One feature of central importance of this algorithm is the use of a problem-adapted data type represented by the data structures arithmetic network and straight-line program (arithmetic circuit). The algorithm finds the complex solutions

*Research partially supported by the Spanish government grant DGICT, PB93-0472-C02-02.
†E-mail address: bank@mathematik.hu-berlin.de.
‡E-mail address: giusti@ariana.polytechnique.fr.
§E-mail address: heintz@matsun1.unican.es.
||E-mail address: mbakop@mathematik.hu-berlin.de.

0885-064X/97 $25.00

of any affine zero-dimensional equation system in nonuniform sequential time that is *polynomial* in the length of the input (given in straight-line program representation) and an adequately defined *geometric degree of the equation system.* Replacing the notion of geometric degree of the given polynomial equation system by a suitably defined *real (or complex) degree* of certain polar varieties associated to the input equation of the real hypersurface under consideration, we are able to find for each connected component of the hypersurface a representative point (this point will be given in a suitable encoding). The input equation is supposed to be given by a straight-line program and the (sequential time) complexity of the algorithm is polynomial in the input length and the degree of the polar varieties mentioned above.

1. INTRODUCTION

The present article is strongly related to the main complexity results and algorithms in [18–20]. Whereas the algorithms developed in these papers concern solving polynomial equation systems over the complex numbers, here we deal with the problem of real solving. More precisely, we consider the particular problem of finding real solutions of a single equation $f(x) = 0$, where f is an n-variate polynomial of degree $d \geq 2$ over the rationals which is supposed to be a regular equation of a compact and smooth hypersurface of $\mathbb{R}^n$. Best known complexity bounds for this problem over the reals are of the form $d^{O(n)}$, counting arithmetic operations in $\mathbb{Q}$ at unit cost (see [1, 6, 22, 23, 26–28, 41, 42, 50]).

Complex root finding methods cannot be applied directly to real polynomial equation solving just by looking at the complex interpretation of the input system. If we want to use a complex root finding method for a problem over the reals, some previous adaptation or preprocessing of the input data becomes necessary. In this paper we show that certain *polar varieties* associated to our input affine hypersurface possess specific geometric properties, which permits us to adapt the complex main algorithm designed in the papers [18–20] to the real case.

This algorithm is of *intrinsic type,* which means that it allows us to distinguish between semantical and syntactical properties of the input system in order to profit from both for an improvement of the complexity estimates compared with more “classical” procedures (as e.g. [5, 6, 8–10, 14, 17, 24, 25, 30–32, 34, 35, 44]). The papers [18–20] show that the *geometric degree of the input system* is associated with the intrinsic complexity of solving the system algorithmically when the complexity is measured in terms of the number of arithmetic operations in $\mathbb{Q}$. The paper [18] is based on the somewhat unrealistic complexity model in which certain *FOR* instructions executable in parallel count at unit cost. This drawback of the complexity model is corrected in the paper [19] at the price of introducing algebraic parameters in the straight-line programs and arithmetic networks occurring there. These algebraic parameters are finally eliminated in the paper [20], which contains a procedure satisfying our complexity requirement and is completely rational.

We show that the algorithmic method of the papers [18–20] is also applicable to the problem of (real) root finding in the case of a compact and smooth hypersurface of $\mathbb{R}^n$, given by an n-variate polynomial f of degree d with rational coefficients which represents a regular equation of that hypersurface. It is possible to design an algorithm of *intrinsic type* using the same data structures as in [20], namely arithmetic networks and straight-line programs over $\mathbb{Q}$ (the straight-line programs—which are supposed to be division-free—are used for the coding of input system, intermediate results, and output). In the complexity estimates the notion of *(geometric) degree of the input system* of [18–20] has then to be replaced by the *(complex or real) degree of the polar varieties* which are associated to the input equation.

The basic computation model used in our algorithm will be that of an arithmetic network with parameters in $\mathbb{Q}$ (compare with [20]). Our first complexity result is the following:

There is an arithmetic network of size $(nd\delta L)^{O(1)}$ with parameters in the field of the rational numbers which finds at least one representative point in every connected component of a smooth compact hypersurface of $\mathbb{R}^n$ given by a regular equation $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree $d \geq 2$. Here L denotes the size of a suitable straight-line program which represents the input of our procedure coding the input polynomial f. Moreover, δ denotes the maximal geometric degree of suitably defined polar varieties associated to the input equation f.

The network size $(nd\delta L)^{O(1)}$ involves the maximal geometric degree of certain *complex* polar varieties associated to the equation f. The answer concerning the algorithmic problem is satisfactory. However, this is not the case with respect to the network size that measures the complexity of the underlying algorithm, because the size depends, besides n, d, and L, on the parameter δ, which is related to complex considerations rather than to real ones. Our second complexity result deals with a procedure showing a complexity that is polynomial only in a suitably defined *real* degree of the associated polar varieties instead of their geometric degree.

The second complexity result relies on two algorithmic assumptions which are very strong in theory, but hopefully not so restrictive in practice. We assume now that a factorization procedure for univariate polynomials over $\mathbb{Q}$ being "polynomial" in a suitable sense (e.g. counting arithmetic operations in $\mathbb{Q}$ at unit cost) is available and that we are able (also at polynomial cost) to localize regions where a given multivariate polynomial has "many" real zeros (if there exist such regions). This second assumption may be replaced by the following more theoretical one (which, however, is simpler to formulate precisely): we suppose that we are able to decide in polynomial time whether a given multivariate polynomial has a real zero (however, we do *not* suppose that we are able to exhibit such a zero if there exists one). We call an arithmetic network *extended* if it uses subroutines of these two types.

Let notations and assumptions be as before. Suppose furthermore that f represents a regular equation of a nonempty smooth and compact real hypersurface. Then there exists an extended arithmetic network which finds at least one representative point for each connected component of the real hypersurface given by f. The size of this arithmetic network is $(nd\delta^* L)^{O(1)}$, where δ^* denotes the suitably defined maximal real degree of the polar varieties mentioned above.

Complexity results in a similar sense for the specific problem of *numerical* polynomial equation solving can be found in [49], following an approach initiated in [45–48] (see also [12, 13]). In the same sense one might also want to mention [7] and [15] as representative contributions for the sparse viewpoint. For more details we refer the reader to [40] and [20] and the references cited therein.

2. POLAR VARIETIES

As usual, let $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the field of rational, real, and complex numbers, respectively. The affine n-spaces over these fields are denoted by $\mathbb{Q}^n$, $\mathbb{R}^n$, and $\mathbb{C}^n$, respectively. Further, let $\mathbb{C}^n$ be endowed with the Zariski topology of $\mathbb{Q}$-definable algebraic sets, where a closed set consists of all common zeros of a finite number of polynomials with coefficients in $\mathbb{Q}$. Let $W \subset \mathbb{C}^n$ be a closed subset with respect to this topology and let $W = C_1 \cup \cdots \cup C_s$ be its decomposition into irreducible components with respect to the same topology. Thus $W, C_1, \ldots, C_s$ are algebraic subsets of $\mathbb{C}^n$. We call W equidimensional if all its irreducible components $C_1, \ldots, C_s$ have the same dimension.

In the following we need the notion of (geometric) degree of an affine algebraic variety. Let W be an equidimensional Zariski closed subset of $\mathbb{C}^n$. If W is zero-dimensional, the *degree* of W, denoted by $\deg W$, is defined as the cardinality of W (neither multiplicities nor points at infinity are counted). If W is of positive dimension r, then we consider the collection $\mathcal{M}$ of all $(n-r)$-dimensional affine linear subspaces, given as the solution set in $\mathbb{C}^n$ of a linear equation system $L_1 = 0, \ldots, L_r = 0$ where for $1 \le k \le r$ the equation L_k is of the form $L_k = \sum_{j=1}^n a_{kj}x_j + a_{k0}$ with a_{kj} being rational. Let $\mathcal{M}_W$ be the subcollection of $\mathcal{M}$ consisting of all affine linear spaces $H \in \mathcal{M}$ such that the affine variety $H \cap W$ satisfies $H \cap W \neq \emptyset$ and $\dim(H \cap W) = 0$. Then the geometric degree of W is defined as $\deg W := \max\{\deg(W \cap H) | H \in \mathcal{M}_W\}$.

For an *arbitrary* Zariski closed subset W of $\mathbb{C}^n$, let $W = C_1 \cup \cdots \cup C_s$ be its decomposition into irreducible components. As in [24] we define its geometric degree as $\deg W := \deg C_1 + \cdots + \deg C_s$. Let W be a Zariski closed subset of $\mathbb{C}^n$ of dimension $n-i$ given by a regular sequence of polynomials $f_1, \ldots, f_i \in \mathbb{Q}[X_1, \ldots, X_n]$.

DEFINITION 1. For $1 \le j \le s$, the irreducible component C_j is called a real component of W if the real variety $C_j \cap \mathbb{R}^n$ contains a smooth point of C_j. Let us write

$$I := \{j \in \mathbb{N} | 1 \le j \le s, \quad C_j \textit{ is a real component of } W\}.$$

Then the (complex) affine variety $W^* := \cup_{j \in I} C_j$ is called the *real part* of W. We call $\deg^* W := \deg W^* = \sum_{j \in I} \deg C_j$ the *real degree* of the algebraic set W.

Remark 2.

(i) $\deg^* W = 0$ holds if and only if the real part W^* of W is empty.

(ii) Note that "smooth point of C_j" in Definition 1 is somewhat ambiguous and should be interpreted following the context. Thus "smooth point of C_j" may just mean that the tangent space of C_j is of dimension $(n-i)$ at such a point, or, more restrictively, it may mean that the hypersurfaces defined by the polynomials $f_1, \ldots, f_i$ intersect transversally in such a point.

PROPOSITION 3. *Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a nonconstant and square-free polynomial and let $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ be the set of complex zeros of the equation $f(x) = 0$. Furthermore, consider for any fixed i, $0 \le i < n$, the complex variety*

$$\widetilde{W}_i := \left\{ x \in \mathbb{C}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0 \right\}$$

(here $\widetilde{W}_O$ is understood to be W). Suppose that the variables $X_1, \ldots, X_n$ are in generic position with respect to f. Then any point of $\widetilde{W}_i$ being a smooth point of W is also a smooth point of $\widetilde{W}_i$. More precisely, at any such point the Jacobian of the equation system $f = \partial f(x)/\partial X_1 = \cdots = \partial f(x)/\partial X_i = 0$ has maximal rank, i.e., the hypersurfaces defined by the polynomials f, $\partial f/\partial X_1, \ldots, \partial f/\partial X_i$ intersect transversally in this point.

Proof. Consider the nonsingular linear transformation $x = A^{(i)} y$, where the new variables are $y = (Y_1, \ldots, Y_n)$. Suppose that $A^{(i)}$ is given in the form

$$\begin{pmatrix} I_{i,\,i} & 0_{i,\,n-i} \\ (a_{kl})_{n-i,\,i} & I_{n-i,\,n-i} \end{pmatrix} \tag{1}$$

where $I_{i,\,i}$ and $0_{i,\,(n-i)}$ denote the $i \times i$ unit and the $i \times (n-i)$ zero matrix, respectively, and where a_{kl} are arbitrary complex numbers for $i+1 \le k \le n$ and $1 \le l \le i$. Since the square matrix $A^{(i)}$ has full rank, the transformation

$x = A^{(i)}y$ defines a linear change of coordinates. In the new coordinates, the variety $\widetilde{W}_i$ takes the form

$$\widetilde{W}_i := \left\{ y \in \mathbb{C}^n \,\middle|\, f(y) = \frac{\partial f(y)}{\partial Y_1} + \sum_{j=i+1}^{n} a_{j1} \frac{\partial f(y)}{\partial Y_j} \right. \\ \left. = \cdots = \frac{\partial f(y)}{\partial Y_i} + \sum_{j=i+1}^{n} a_{ji} \frac{\partial f(y)}{\partial Y_j} = 0 \right\}.$$

The coordinate transformation given by $A^{(i)}$ induces a morphism of affine spaces $\Phi_i : \mathbb{C}^n \times \mathbb{C}^{(n-i)i} \to \mathbb{C}^{i+1}$ defined by

$$\Phi_i\,(Y_1, \ldots, Y_i, \ldots, Y_n, a_{i+1,1}, \ldots, a_{n,1}, \ldots, a_{i+1,i}, \ldots, a_{n,i}) \\ = \left(f, \frac{\partial f}{\partial Y_1} + \sum_{j=i+1}^{n} a_{j1} \frac{\partial f}{\partial Y_j}, \ldots, \frac{\partial f}{\partial Y_i} + \sum_{j=i+1}^{n} a_{ji} \frac{\partial f}{\partial Y_j} \right).$$

For the moment let

$$\alpha := (\alpha_1, \ldots, \alpha_{n+(n-i)i}) := (Y_1, \ldots, Y_n, a_{i+1,1}, \ldots, a_{n,i}) \in \mathbb{C}^n \times \mathbb{C}^{(n-i)i}.$$

Then the Jacobian matrix $J(\Phi_i)(\alpha)$ of Φ_i in α is given by

$$J(\Phi_i)(\alpha) = \\ \begin{pmatrix} \frac{\partial f}{\partial Y_1} & \cdots & \frac{\partial f}{\partial Y_n} & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ * & \cdots & * & \frac{\partial f}{\partial Y_{i+1}} & \cdots & \frac{\partial f}{\partial Y_n} & 0 & \vdots & 0 \\ \vdots & & \vdots & \ddots & \ddots & 0 & \cdots & \ddots & 0 \\ * & \cdots & * & 0 & 0 & \cdots & \frac{\partial f}{\partial Y_{i+1}} & \cdots & \frac{\partial f}{\partial Y_n} \end{pmatrix} (\alpha).$$

Suppose that we are given a point $\alpha^0 = (Y_1^0, \ldots, Y_n^0, a_{i+1,1}^0, \ldots, a_{n,i}^0)$ which belongs to the fiber $\Phi_i^{-1}(0)$ and suppose that $(Y_1^0, \ldots, Y_n^0)$ is a point of the hypersurface W in which the equation f is regular (i.e., we suppose that not all partial derivatives of f vanish in that point). Let us consider the Zariski open neighborhood $\mathcal{U}$ of $(Y_1^0, \ldots, Y_n^0)$ consisting of all points of $\mathbb{C}^n$ in which at least one partial derivative of f does not vanish. We claim now that the restricted map

$$\Phi_i : \mathcal{U} \times \mathbb{C}^{(n-i)i} \to \mathbb{C}^{i+1}$$

is transversal to the origin $0 = (0, \ldots, 0)$ of $\mathbb{C}^{i+1}$. In order to prove this assertion we consider an arbitrary point $\alpha = (Y_1, \ldots, Y_n, a_{i+1,1}, \ldots, a_{n,i})$ of $\mathcal{U} \times \mathbb{C}^{(n-i)i}$ which satisfies $\Phi_i(\alpha) = 0$. Thus $(Y_1, \ldots, Y_n)$ belongs to $\mathcal{U} \cap W$ and is therefore a point of the hypersurface W in which the equation f is regular. Let us now show that the Jacobian matrix of Φ_i has maximal rank in α. If this is not the case, the partial derivatives $\partial f/\partial Y_{i+1}, \ldots, \partial f/\partial Y_n$ must vanish in the point $(Y_1, \ldots, Y_n)$. Then the relation $\Phi_i(\alpha) = 0$ implies that the derivatives $\partial f/\partial Y_1, \ldots, \partial f/\partial Y_i$ at the point $(Y_1, \ldots, Y_n)$ vanish, too.

This contradicts the fact that the equation f is regular in that point. Therefore the Jacobian matrix of Φ_i has maximal rank in α, which means that α is a regular point of Φ_i. Since α was an arbitrary point of $\Phi_i^{-1}(0) \cap (\mathcal{U} \times \mathbb{C}^{(n-i)i})$, our claim follows. Applying the algebraic-geometric form of the Weak Transversality Theorem of Thom-Sard (see e.g. [21]) to the diagram

$$\begin{array}{ccc} \Phi_i^{-1}(0) \cap (\mathcal{U} \times \mathbb{C}^{(n-i)i}) & \hookrightarrow & \mathbb{C}^n \times \mathbb{C}^{(n-i)i} \\ & \searrow & \downarrow \\ & & \mathbb{C}^{(n-i)i} \end{array} ,$$

one concludes that the set of all matrices $(a_{kl})_{n-i,\,i} \in \mathbb{R}^{(n-i)i}$ for which transversality holds is Zariski dense in $\mathbb{C}^{(n-i)i}$. More precisely, the affine space $\mathbb{Q}^{(n-i)i}$ contains a nonempty Zariski open set of matrices $A^{(i)}$ such that the corresponding coordinate transformation (1) leads to the desired smoothness of $\widetilde{W}_i$ in points which are smooth in W. ■

The proof of Proposition 3 could also be given using a linear transformation of the variables with a generic nonsingular $n \times n$ matrix instead of the generic one in "triangular form" used here. However, our transformation is sufficiently generic to show Proposition 3 and exhibits the benefit that it invokes only "sparse transformations" of the equations, which is necessary in the following.

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a nonconstant square-free polynomial and let again $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ be the hypersurface defined by f. Let $\Delta \in \mathbb{Q}[X_1, \ldots, X_n]$ be the polynomial $\Delta := \sum_{j=1}^{n} (\partial f/\partial X_j)^2$. Consider the real variety $V := W \cap \mathbb{R}^n$ and suppose that:

- *V is nonempty and bounded (and hence compact),*
- *the gradient of f is different from zero in all points of V (i.e., V is a smooth hypersurface in $\mathbb{R}^n$ and $f = 0$ is its regular equation),*
- *the variables $X_1, \ldots, X_n$ are in generic position.*

Under these assumptions the following problem adapted notion of polar variety is meaningful and remains consistent with the more general definition of the same concept (see e.g. [36]).

DEFINITION 4. Let $0 \leq i < n$. Consider the linear subspace X^i of $\mathbb{C}^n$ corresponding to the linear forms $X_{i+1}, \ldots, X_n$, i.e., $X^i := \{x \in$

$\mathbb{C}^n | X_{i+1}(x) = \cdots = X_n(x) = 0\}$. Then the algebraic subvariety W_i of $\mathbb{C}^n$ defined as the Zariski closure of the set

$$\left\{ x \in \mathbb{C}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0, \quad \Delta(x) \neq 0 \right\}$$

is called the (*complex*) *polar variety* of W associated to the linear subspace X^i of $\mathbb{C}^n$. The respective real variety is denoted by $V_i := W_i \cap \mathbb{R}^n$ and called the *real polar variety* of V associated to the linear subspace $X^i \cap \mathbb{R}^n$ of $\mathbb{R}^n$. Here W_0 is understood to be the Zariski closure of the set $\{x \in \mathbb{C}^n;\, f(x) = 0,\, \Delta(x) \neq 0\}$ and V_0 is understood to be V.

Remark 5. Since by assumption V is a nonempty compact hypersurface of $\mathbb{R}^n$ and the variables $X_1, \ldots, X_n$ are in generic position, we deduce from Proposition 3 and general considerations on Lagrange multipliers (as e.g. in [26]) or Morse Theory (as e.g. in [38]) that the real polar variety V_i is nonempty and smooth for any $0 \leq i < n$. In particular, the complex variety W_i is not empty and the hypersurfaces of $\mathbb{C}^n$ given by the polynomials f, $\partial f / \partial X_1, \ldots, \partial f / \partial X_i$ intersect transversally in some dense Zariski open subset of W_i (observe that any element of $\{x \in \mathbb{C}^n;\, f(x) = 0,\, \Delta(x) \neq 0\}$ is a smooth point of W and apply Proposition 3).

Let us observe that the assumption V *smooth* implies that the polar variety V_i can be written as $V_i = \{x \in \mathbb{R}^n;\, f(x) = \partial f(x)/\partial X_1 = \cdots = \partial f(x)/\partial X_i = 0\}$ for any $0 \leq i \leq n$.

THEOREM 6. *Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a nonconstant square-free polynomial and let $\Delta := \sum_{j=1}^{n} (\partial f / \partial X_j)^2$. Let $W := \{x \in \mathbb{C}^n | f(x) = 0\}$ be the hypersurface of $\mathbb{C}^n$ given by the polynomial f. Further, suppose that $V := W \cap \mathbb{R}^n$ is a nonempty, smooth, and bounded hypersurface of $\mathbb{R}^n$ with regular equation f. Assume that the variables $X_1, \ldots, X_n$ are in generic position. Finally, for any i, $0 \leq i < n$, let the complex polar variety W_i of W and the real polar variety V_i of V be defined as above. With these notations and assumptions we have:*

- *$V_0 \subset W_0 \subset W$, with $W_0 = W$ if and only if f and Δ are coprime;*
- *W_i is a nonempty equidimensional affine variety of dimension $n-(i+1)$ being smooth in all its points which are smooth points of W;*
- *the real part W_i^* of the complex polar variety W_i coincides with the Zariski closure in $\mathbb{C}^n$ of the real polar variety*

$$V_i = \left\{ x \in \mathbb{R}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0 \right\};$$

- *the ideal $(f, \partial f / \partial X_1, \ldots, \partial f / \partial X_i)_\Delta$ is radical.*

Proof. The first statement is obvious, because W_0 is the union of all irreducible components of W on which Δ does not vanish identically.

We show now the second statement. Let $0 \leq i < n$ be arbitrarily fixed. Then the polar variety W_i is nonempty by Remark 5. Moreover, the hypersurfaces of $\mathbb{C}^n$ defined by the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1}$ intersect any irreducible component of W_i transversally in a nonempty Zariski open set. This implies that the algebraic variety W_i is a nonempty equidimensional variety of dimension $n-(i+1)$ and that the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1}$ form a regular sequence in the ring obtained by localizing $\mathbb{Q}[X_1, \ldots, X_n]$ by the polynomials which do not vanish identically on any irreducible component of W_i. More exactly, the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$ form a regular sequence in the localized ring $\mathbb{Q}[X_1, \ldots, X_n]_\Delta$. From Proposition 3 we deduce that W_i is smooth in all points which are smooth points of W and that the hypersurfaces of $\mathbb{C}^n$ defined by the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$ intersect transversally in these points.

Let us show the third statement. The Zariski closure of V_i in $\mathbb{C}^n$ is contained in W_i^* (this is a simple consequence of the smoothness of V_i). One obtains the reverse inclusion as follows: let $x^* \in W_i^*$ be an arbitrary point, and let C be an irreducible component of W_i^* containing this point. Since C is a real component of W_i the set $C \cap \mathbb{R}^n$ is not empty and contained in W_i. The polar variety W_i is contained in the algebraic set $\widetilde{W}_i := \{x \in \mathbb{C}^n | f(x) = \partial f(x)/\partial X_1 = \cdots = \partial f(x)/\partial X_i = 0\}$. Therefore, we have $C \cap V_i \neq \emptyset$. Moreover, the hypersurfaces of $\mathbb{R}^n$ defined by the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$, cut out transversally a dense subset of $C \cap V_i$. Thus we have

$$\begin{aligned} n-(i+1) &= \dim_{\mathbb{R}}(C \cap V_i) = \dim_{\mathbb{R}} R(C \cap V_i) \\ &= \dim_{\mathbb{C}} R((C \cap V_i)') \leq \dim_{\mathbb{C}} C \\ &= n-(i+1). \end{aligned}$$

(Here $R(C \cap V_i)$ denotes the set of smooth points of $C \cap V_i$ and $(C \cap V_i)'$ denotes the complexification of $C \cap V_i$.) Thus, $\dim_{\mathbb{C}}(C \cap V_i)' = \dim_{\mathbb{C}} C = n-(i+1)$ and, hence, $C = (C \cap V_i)'$. Moreover, $(C \cap V_i)'$ is contained in the Zariski closure of V_i in $\mathbb{C}^n$, which implies that C is contained in the Zariski closure of V_i as well.

Finally, we show the last statement. Let us consider again the algebraic set

$$\widetilde{W}_i := \left\{ x \in \mathbb{C}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0 \right\}$$

which contains the polar variety W_i. Let C' be any irreducible component of W_i. Then C' is also an irreducible component of $\widetilde{W}_i$. Moreover, the polynomial Δ does not vanish identically on C'. By Remark 5 there exists now a smooth point x^* of $\widetilde{W}_i$ which is contained in C' and in which the hypersurfaces of $\mathbb{C}^n$ given by the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$ intersect transversally.

Let $x^* = (X_1^*, \ldots, X_n^*) \in \mathbb{C}^n$ be fixed in that way. Consider the local ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ of the point x^* in the variety $\widetilde{W}_i$ (i.e., $\mathcal{O}_{\widetilde{W}_i, x^*}$ is the ring of germs of rational functions of $\widetilde{W}_i$ that are defined in the point x^*). Algebraically the local ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ is obtained by dividing the polynomial ring $\mathbb{C}[X_1, \ldots, X_n]$ by the ideal $(f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i)$, which defines $\widetilde{W}_i$ as an affine variety, and then localizing at the maximal ideal $(X_1 - X_1^*, \ldots, X_n - X_n^*)$ of the point $x^* = (X_1^*, \ldots, X_n^*)$. Using now standard arguments from commutative algebra and algebraic geometry (see e.g. [4]), one infers from the fact that the hypersurfaces of $\mathbb{C}^n$ given by the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$ intersect transversally in x^* the conclusion that $\mathcal{O}_{\widetilde{W}_i, x^*}$ is a regular local ring and, hence, an integral domain. The fact that $\mathcal{O}_{\widetilde{W}_i, x^*}$ is an integral domain implies that there exists a uniquely determined irreducible component of $\widetilde{W}_i$ which contains the smooth point x^* (this holds true for the ordinary, $\mathbb{C}$-defined Zariski topology as well as for the $\mathbb{Q}$-defined one considered here). Therefore, the point x^* is uniquely contained in the irreducible component C' of $\widetilde{W}_i$ (and of W_i).

Since the local ring $\mathcal{O}_{\widetilde{W}_i, x^*}$ is an integral domain, its zero ideal is prime. This implies that the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i$ generate a prime ideal in the local ring $\mathbb{C}[X_1, \ldots, X_n]_{(X_1 - X_1^*, \ldots, X_n - X_n^*)}$. Hence, the isolated primary component of the polynomial ideal $(f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i)$ in $\mathbb{Q}[X_1, \ldots, X_n]$, which corresponds to the irreducible component C', is itself a prime ideal. Since this is true for any irreducible component of W_i and since W_i is defined by discarding from $\widetilde{W}_i$ the irreducible components contained in the hypersurface of $\mathbb{C}^n$ given by the polynomial Δ, we conclude that the ideal $(f, \partial f/\partial X_1, \ldots, \partial f/\partial X_i)_\Delta$ of $\mathbb{Q}[X_1, \ldots, X_n]_\Delta$ is an intersection of prime ideals and, hence, is radical. This completes the proof of Theorem 6. ■

Remark 7. Under the assumptions of Theorem 6, we observe that for any i, $0 \leq i < n$, the following inclusions hold among the different nonempty varieties introduced up to now, namely

$$V_i \subset V \quad \textit{and} \quad V_i \subset W_i^* \subset W_i \subset \widetilde{W}_i.$$

Here V is the bounded and smooth real hypersurface we consider in this paper, W_i and V_i are the polar varieties introduced in Definition 4, W_i^* is the real part of W_i according to Definition 1, and $\widetilde{W}_i$ is the complex affine variety introduced in the proof of Theorem 6. With respect to Theorem 6 our settings and assumptions imply that $n - (i+1) = \dim_{\mathbb{C}} W_i = \dim_{\mathbb{C}} W_i^* = \dim_{\mathbb{R}} V_i$ holds. By our smoothness assumption and the generic choice of the variables we have for the respective sets of smooth points the inclusions

$$V_i = R(V_i) \subset R(W_i) \subset R(\widetilde{W}_i) \subset R(W).$$

(Here W is the affine hypersurface $W = \{x \in \mathbb{C}^n | f(x) 0\}$ of $\mathbb{C}^n$.)

3. ALGORITHMS AND COMPLEXITY

The preceding study of adapted polar varieties enables us to state our first complexity result:

THEOREM 8. *Let n, d, δ, L be natural numbers. Then there exists an arithmetic network $\mathcal{N}$ over $\mathbb{Q}$ of size $(nd\delta L)^{O(1)}$ with the following properties:*

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a nonconstant polynomial of degree at most d and suppose that f is given by a division-free straight-line program β in $\mathbb{Q}[X_1, \ldots, X_n]$ of length at most L. Let $\Delta := \sum_{j=1}^{n} (\partial f/\partial X_j)^2$, $W := \{x \in \mathbb{C}^n | f(x) = 0\}$, $V := W \cap \mathbb{R}^n = \{x \in \mathbb{R}^n | f(x) = 0\}$, and suppose that the variables $X_1, \ldots, X_n$ are in "sufficiently generic" position. For $0 \le i < n$ let W_i be the Zariski closure in $\mathbb{C}^n$ of the set

$$\left\{x \in \mathbb{C}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0,\, \Delta(x) \neq 0\right\}$$

(thus W_i is the polar variety of W associated to the linear space $X^i = \{x \in \mathbb{C}^n | X_{i+1}(x) = \cdots = X_n(x) = 0\}$ according to Definition 4). Let $\delta_i := \deg W_i$ be the geometric degree of W_i and assume that $\delta \ge \max\{\delta_i | 1 \le i < n\}$ holds.

The algorithm represented by the arithmetic network $\mathcal{N}$ starts from the straight-line program β as input and decides first whether the complex algebraic variety W_{n-1} is zero-dimensional. If this is the case the network $\mathcal{N}$ produces a straight-line program of length $(nd\delta L)^{O(1)}$ in $\mathbb{Q}$ which represents the coefficients of $n+1$ univariate polynomials $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ satisfying the following conditions:

(1) $\deg(q) = \delta_{n-1} = \deg W_{n-1}$
(2) $\max\{\deg(p_i) | 1 \le i \le n\} < \delta_{n-1}$
(3) $W_{n-1} = \{(p_1(u), \ldots, p_n(u)) | u \in \mathbb{C},\, q(u) = 0\}$.

Moreover, the algorithm represented by the arithmetic network $\mathcal{N}$ decides whether the semialgebraic set $W_{n-1} \cap \mathbb{R}^n$ is nonempty. If this is the case the network $\mathcal{N}$ produces not more than δ_{n-1} sign sequences of $\{-1, 0, 1\}^{\delta_{n-1}}$ which codify the real zeros of q "à la Thom" ([11]). In this way, $\mathcal{N}$ describes the nonempty finite set $W_{n-1} \cap \mathbb{R}^n$.

From the output of this algorithm we may deduce the following information:

- If the complex variety W_{n-1} is not zero-dimensional or if W_{n-1} is zero-dimensional and $W_{n-1} \cap \mathbb{R}^n$ is empty we conclude that V is not a compact smooth hypersurface of $\mathbb{R}^n$ with regular equation f.
- If V is a compact smooth hypersurface of $\mathbb{R}^n$ with regular equation f, then $W_{n-1} \cap \mathbb{R}^n$ is nonempty and contains for any connected component of V at least one point which the network $\mathcal{N}$ codifies à la Thom as a real zero of the polynomial q.

Remark 9. The hypothesis that the variables $X_1, \ldots, X_n$ are in "sufficiently generic" position is not really restrictive since any $\mathbb{Q}$-linear coordinate change increases the length of the input straight-line program β only by an unessential additive term of $O(n^3)$. Moreover, by [29, Theorem 4.4], any genericity condition which the algorithm might require can be satisfied by adding to the arithmetic network $\mathcal{N}$ an extra number of nodes which is polynomial in the input parameters n, d, δ, L.

Remark 10. From the Bézout Theorem we deduce the estimation $\max\{\delta_i | 0 \leq i < n\} \leq d(d-1)^{n-1} < d^n$. Moreover, f can always be evaluated by a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_n]$ of length d^n. Thus, fixing $\delta := d(d-1)^{n-1}$ and $L := d^n$ one is concerned with a worst-case situation in which the statement of Theorem 8 just reproduces the main complexity results of [1, 6, 22, 23, 26–28, 41, 42] in case of a compact smooth hypersurface of $\mathbb{R}^n$ given by a regular equation of degree d. The interest in Theorem 8 lies in the fact that δ may be much smaller than the "Bézout number" $d(d-1)^{n-1}$ and L smaller than d^n in many concrete and interesting cases.

Proof of Theorem 8. Since by [2] and [39] we may derive the straight-line program β representing the polynomial f in time linear in L, we may suppose without loss of generality that β represents also the polynomial Δ. Applying now the algorithm underlying [19, Proposition 18] together with the modifications introduced by [20, Theorem 28] (compare also [20, Theorem 16 and its proof]), we find an arithmetic network $\mathcal{N}'$ with parameters in $\mathbb{Q}$ of size $(nd\delta L)^{O(1)}$ which decides whether the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1}$ form a secant family avoiding the hypersurface of $\mathbb{C}^n$ defined by the polynomial Δ. This is exactly the case if W_{n-1} is zero-dimensional.

Suppose now that the polynomials $(f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1})$ form such a secant family. Then the arithmetic network $\mathcal{N}'$ which we obtained before applying [19, Proposition 18] and [20, Theorem 28] to the input $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1}$ and Δ produces a straight-line program in $\mathbb{Q}$ which represents the coefficients of polynomials $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ characterizing the part W_{n-1} of the complex variety $\widetilde{W}_{n-1} := \{x \in \mathbb{C}^n | f(x) = \partial f(x)/\partial X_1 = \cdots = \partial f(x)/\partial X_{n-1} = 0\}$ which avoids the hypersurface $\{x \in \mathbb{C}^n | \Delta(x) = 0\}$. More precisely, the output $q, p_1, \ldots, p_n$ of the network $\mathcal{N}'$ satisfies the conditions (1)–(3) in the statement of Theorem 8.

Now applying for example the main (i.e., the only correct) algorithm of [3] (see also [43] for refinements) by adding suitable comparison gates for positiveness of rational numbers, we may extend $\mathcal{N}'$ to an arithmetic network $\mathcal{N}$ of asymptotically the same size $(nd\delta L)^{O(1)}$, which decides whether the polynomial q has any real zero. Moreover, without loss of generality the arithmetic network $\mathcal{N}$ codifies any existing zeros of q à la Thom (see [11, 43]). From general considerations of Morse Theory (see e.g. [38]) or more elementarily from the results and techniques of [26, 28] one sees that in the case where f is a regular equation of a bounded smooth hypersurface V of $\mathbb{R}^n$, the arithmetic network $\mathcal{N}$ codifies for each connected component of V at least one representative point. This finishes the proof of Theorem 8. ■

Roughly speaking, the arithmetic network $\mathcal{N}$ of Theorem 8 decides whether a given polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ is a regular equation of a bounded (i.e., compact) smooth hypersurface V of $\mathbb{R}^n$. If this is the case $\mathcal{N}$ computes for any connected component of V at least one representative point. The size of $\mathcal{N}$ depends polynomially on the number of variables n, the degree d, and the straight-line program complexity L of f, and finally on the degree δ of certain complex polar varieties W_i associated to the equation f.

The nature of the answer the network $\mathcal{N}$ gives us about the algorithmic problem is satisfactory. However, this is not the case for the size of $\mathcal{N}$, which measures the complexity of the underlying algorithm, since this complexity depends on the parameter δ being related rather to the complex considerations than to the real ones. We are going now to describe a procedure whose complexity is polynomial only in the *real* degree of the polar varieties W_i instead of their complex degree. The theoretical (not necessarily the practical) price we have to pay for this complexity improvement is relatively high:

- our new procedure does not decide any more whether the input polynomial is a regular equation of a bounded smooth hypersurface V of $\mathbb{R}^n$. We have to assume that this is already known. Therefore the new algorithm can only be used in order to *solve* the real equation $f = 0$, but not to decide its consistency (*solving* means here that the algorithm produces at least one representative point for each connected component of V).
- our new algorithm requires the support of the following two external subroutines whose theoretical complexity estimates are not really taken into account here although their practical complexity may be considered as "polynomial":

—the first subroutine we need is a factorization algorithm for univariate polynomials over $\mathbb{Q}$. In the bit complexity model the problem of factorizing univariate polynomials over $\mathbb{Q}$ is known to be polynomial ([37]), whereas in the arithmetic model we are considering here this question is more intricate ([16]). In the extended complexity model we are going to consider, the cost of factorizing a univariate polynomial of degree D over $\mathbb{Q}$, (given by its coefficients) is accounted as $D^{O(1)}$.

—the second subroutine allows us to discard nonreal irreducible components of the occurring complex polar varieties. This second subroutine starts from a straight-line program for a single polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ as input and decides whether this polynomial has a real zero (however, without actually exhibiting it if there is one). Again this subroutine is taken into account at polynomial cost.

- We call an arithmetic network over $\mathbb{Q}$ *extended* if it contains extra nodes corresponding to the first and second subroutine.

Fix for the moment the natural numbers n, d, δ^*, and L. We suppose that a division-free straight-line program β in $\mathbb{Q}[X_1, \ldots, X_n]$ of length at most L is given such that β represents a nonconstant polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree at most d. Let again $\Delta := \sum_{j=1}^{n} (\partial f/\partial X_j)^2$ and suppose that f is a regular equation of a (non-empty) bounded smooth hypersurface V of $\mathbb{R}^n$. Let $W := \{x \in \mathbb{C}^n;\, f(x) = 0\}$ be the complex hypersurface of $\mathbb{C}^n$ defined by the polynomial f and suppose that the variables $X_1, \ldots, X_n$ are in generic position. Fix $0 \leq i < n$ arbitrarily. Let as in Definition 4 the complex variety W_i be the Zariski closure in $\mathbb{C}^n$ of the set

$$\left\{x \in \mathbb{C}^n \,\middle|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0, \quad \Delta(x) \neq 0\right\},$$

i.e., W_i is the polar variety of the complex hypersurface W associated to the linear subspace $X^i := \{x \in \mathbb{C}^n | X_{i+1}(x) = 0, \ldots, X_n(x) = 0\}$.

Let $V_i := W_i \cap \mathbb{R}^n$ be the corresponding polar variety of the real hypersurface V. Let δ_i^* be the real degree of the polar variety W_i, i.e., the geometric degree of W_i^* (see Definition 1). By Theorem 6 the quantity δ_i^* is also the geometric degree of the Zariski closure in $\mathbb{C}^n$ of the real variety V_i, i.e., of the complexification of V_i. Let $r := n-(i+1)$. Since the variables $X_1, \ldots, X_n$ are in generic position with respect to all our geometric data, they are also in Noether position with respect to the complex variety W_i, the variables $X_1, \ldots, X_r$ being free (see [18, 19] for details). Finally, suppose that $\delta^* \geq \max\{\delta_i^* | 0 \leq i < n\}$ holds.

With these notations and assumptions, we have the following *real* version of [19, Proposition 17]:

LEMMA 11. *Let n, d, $\delta^* L$ be given natural numbers as before and fix $0 \leq i < n$ and $r := n - (i+1)$. Then there exists an extended arithmetic network $\mathcal{N}$ with parameters in $\mathbb{Q}$ of size $(id\delta^* L)^{O(1)}$ which for any nonconstant polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ satisfying the assumptions above produces a division-free straight-line program β_i in $\mathbb{Q}[X_1, \ldots, X_r]$ such that β_i represents a nonzero polynomial $\varrho \in \mathbb{Q}[X_1, \ldots, X_r]$ and the coefficients with respect to X_{r+1} of certain polynomials $q, p_1, \ldots, p_n \in \mathbb{Q}[X_1, \ldots, X_{r+1}]$ having the following properties:*

(i) *the polynomial q is monic and separable in X_{r+1}, and its degree satisfies* $\deg q = \deg_{X_{r+1}} q = \delta_i^* = \deg W_i^* \leq \delta^*$,

(ii) *the polynomial ϱ is the discriminant of q with respect to the variable X_{r+1} and its degree can be estimated as* $\deg \varrho \leq 2(\delta_i^*)^3$,

(iii) *the polynomials* $p_1, \ldots, p_n$ *satisfy the degree bounds*

$$\max\{\deg_{X_{r+1}} p_k | 1 \le k \le n\} < \delta_i^*,$$
$$\max\{\deg p_k | 1 \le k \le n\} = 2(\delta_i^*)^3,$$

(iv) *the ideal* $(q, \varrho X_1 - p_1, \ldots, \varrho X_n - p_n)_\varrho$ *generated by the polynomials* $q, \varrho X_1 - p_1, \ldots, \varrho X_n - p_n$ *in the localization* $\mathbb{Q}[X_1, \ldots, X_n]_\varrho$ *is the vanishing ideal of the affine variety* $(W_i^*)_\varrho := \{x \in W_i^* | \varrho(x) \neq 0\}$. *Moreover,* $(W_i^*)_\varrho$ *is a dense Zariski open subset of the complex variety* W_i^*.

(v) *the length of the straight-line program* β_i *is of the order* $(id\delta^* L)^{O(1)}$.

Proof. The proof of this lemma follows the general lines of the proof of Theorem 8 and is again based on the algorithm underlying [19, Proposition 17] together with the modifications introduced by [20, Theorem 28]. By Theorem 8 above, we know that the polynomials $f, \partial f/\partial X_1, \ldots, \partial f/\partial X_{n-1}$ form a secant family, avoiding in $\mathbb{C}^n$ the hypersurface defined by Δ, and therefore the algorithm of geometric solving due to [20, Section 3] is applicable. In particular, the *lifting procedure* involved there can be exploited for our purpose.

First we observe that by [2] and [39] we are able to derive the straight-line program β representing the input polynomial f at cost linear in L. Thus we may suppose without loss of generality that β represents both f and Δ.

We show Lemma 11 by the exhibition of a recursive procedure in $0 \le i < n$ under the assumption that the first and second subroutines as introduced before are available. First put $i := 0$ and let β_0 be the straight-line program β which represents f and Δ. Since the variables $X_1, \ldots, X_n$ are in generic position, the polynomials f and Δ are monic with respect to the variable X_n and satisfy the conditions $d \ge \deg f = \deg_{X_n} f$ and $2d \ge \deg \Delta = \deg_{X_n} \Delta$.

Let $R_0 := \mathbb{Q}[X_1, \ldots, X_{n-1}]$ and consider f and Δ as univariate polynomials in X_n with coefficients in R_0. Recall that they are monic. Interpolating them in $2d+1$ arbitrarily chosen distinct rational points, we obtain a division-free straight-line program in $R_0 = \mathbb{Q}[X_1, \ldots, X_{n-1}]$ which represents the coefficients of f and Δ with respect to X_n. This straight-line program has length $Ld^{O(1)}$.

We apply now [19, Lemma 8] in order to obtain the greatest common divisor of f and Δ which is again a monic polynomial in $R_0[X_n]$, which we may suppose to be given by a division-free straight-line program in $R_0 = \mathbb{Q}[X_1, \ldots, X_{n-1}]$ representing its coefficients with respect to X_n. Dividing f by this greatest common divisor in $R_0[X_n]$ as in the Noether normalization procedure in [19], we obtain a polynomial $\overline{q} \in R_0[X_n] = \mathbb{Q}[X_1, \ldots, X_n]$ whose coefficients with respect to the variable X_n are represented by a division-free straight-line program $\overline{\beta}_1$ in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$. The polynomial $\overline{q}$ is monic in X_n, it is square-free, and it is a divisor of f. Moreover, we have that $W_0 = \{x \in \mathbb{C}^n | \overline{q}(x) = 0\}$ and $\overline{q}$ is the minimal polynomial of the hypersurface W_0 of $\mathbb{C}^n$. The degree of the polynomial $\overline{q}$ satisfies the condition $\deg \overline{q} = \deg_{X_n} \overline{q} = \deg W_0$.

The straight-line program $\overline{\beta}_1$ which represents the coefficients of $\overline{q}$ with respect to the variable X_n has length $(dL)^{O(1)}$. In order to finish the recursive construction for the case $i := 0$, it is sufficient to find the factor q of $\overline{q}$ which defines the real part W_0^* of W_0. For this purpose we consider the projection map $\mathbb{C}^n \to \mathbb{C}^{n-1}$ which maps each point of $\mathbb{C}^n$ onto its first $n-1$ coordinates. Since the variables $X_1, \ldots, X_n$ are in generic position, the projection map induces a finite surjective morphism π: $W_0 \to \mathbb{C}^{n-1}$. We choose a generic *lifting point* $t = (t_1, \ldots, t_{n-1}) \in \mathbb{Q}^{n-1}$ with rational coordinates $t_1, \ldots, t_{n-1}$ (this is here a generic point $t \in \mathbb{Q}^{n-1}$ for the hypersurface W_0 of the finite morphism π for which the zero-dimensional fiber $\pi^{-1}(t)$, the *lifting fiber,* contains only smooth points of W_0; for more details see [20, Section 3]). Observe that the irreducible components of W_0 are the hypersurfaces of $\mathbb{C}^n$ defined by the $\mathbb{Q}$-irreducible factors of $\overline{q}$ which we denote by $q_1, \ldots, q_s$.

Without loss of generality we may assume that for $1 \leq m \leq s$ the irreducible polynomials $q_1, \ldots, q_m$ define the real irreducible components of W_0. Thus it is clear that the factor q of $\overline{q}$ we are looking for is $q := q_1 \cdots q_m$. It suffices therefore to find all irreducible factors $q_1, \ldots, q_s$ of $\overline{q}$ and then to discard the factors $q_{m+1}, \ldots, q_s$.

In order to find the polynomials $q_1, \ldots, q_s$, we specialize the variables $X_1, \ldots, X_{n-1}$ into the coordinates $t_1, \ldots, t_{n-1}$ of the rational point $t \in \mathbb{Q}^{n-1}$. We obtain thus the univariate polynomial $\overline{q}(t, X_n) := \overline{q}(t_1, \ldots, t_{n-1}, X_n) \in \mathbb{Q}[X_n]$ which decomposes into $\overline{q}(t, X_n) = q_1(t, X_n) \cdots q_s(t, X_n)$ in $\mathbb{Q}[X_n]$. Since the lifting point t was chosen generically in $\mathbb{Q}^{n-1}$, Hilbert's Irreducibility Theorem (see [33]) implies that the polynomials $q_1(t, X_n), \ldots, q_s(t, X_n)$ are irreducible over $\mathbb{Q}$. Specializing the variables $X_1, \ldots, X_{n-1}$ in the straight-line program $\overline{\beta}_1$ into the values $t_1, \ldots, t_{n-1}$ we obtain an arithmetic circuit in $\mathbb{Q}$ which represents the coefficients of $\overline{q}(t, X_n)$. By a call to the first subroutine we obtain the coefficients of the polynomials $q_1(t, X_n), \ldots, q_s(t, X_n)$. Applying to these polynomials the lifting procedure which we are going to explain below in a slightly more general context, we find a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ of size $(dL)^{O(1)}$ which represents the coefficients of the polynomials $q_1, \ldots, q_s$ with respect to the variable X_n.

In order to finish the case $i = 0$ we have to identify algorithmically the polynomials $q_1, \ldots, q_m$ that define the irreducible real components of W_0 and, hence, those of W^*. Then, the product $q = q_1 \cdots q_m$ is easily obtained. Observe that q is the minimal polynomial of the hypersurface W_0. From the assumption that $V = W \cap \mathbb{R}^n$ is a smooth real hypersurface one deduces that $V_0 = W_0^* \cap \mathbb{R}^n = W_0 \cap \mathbb{R}^n$ holds. Since f is a regular equation of V and since the polynomials $\overline{q}$ and q are factors of f, one sees immediately that $\overline{q}$ and q are also regular equations of V. This implies that each of the polynomials $q_1, \ldots, q_s$ admitting a real zero $u \in \mathbb{R}$ has a nonvanishing gradient in u. Thus, any polynomial of $q_1, \ldots, q_s$ admitting a real zero belongs to $q_1, \ldots, q_m$. Hence, by a call to the second subroutine, we are able to find the polynomials $q_1, \ldots, q_m$, and therefore the polynomial $q = q_1 \cdots q_m$.

Now we extend the division-free straight-line program representing the polynomials $q_1, \ldots, q_s$ to a circuit in $\mathbb{Q}[X_1, \ldots, X_n]$ of size $(dL)^{O(1)}$ which computes the polynomial $q = q_1 \cdots q_s$. Interpolating q in the variable X_n as before, this circuit provides a division-free straight-line program β_1 in $\mathbb{Q}[X_1, \ldots, X_n]$ of size $(dL)^{O(1)}$ which represents the coefficients of q with respect to the variable X_n. Without changing its order of complexity we extend β_1 to a division-free circuit in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ that computes also the discriminant ϱ of q with respect to the variable X_n and the polynomials $\varrho X_1, \ldots, \varrho X_{n-1}$.

Let $p_1 := \varrho X_1, \ldots, p_{n-1} := \varrho X_{n-1}, p_n := \varrho X_n \in \mathbb{Q}[X_1, \ldots, X_{n-1}, X_n]$. One sees immediately that the polynomials $\varrho \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$ and $q, p_1, \ldots, p_n \in \mathbb{Q}[X_1, \ldots, X_{n-1}, X_n]$ satisfy the conditions (i)–(iv) of Lemma 11 for $i = 0$. Furthermore, β_1 is a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ of size $(dL)^{O(1)}$ which computes ϱ and the coefficients of $q, p_1, \ldots, p_n$ with respect to the variable X_n. By construction the output circuit β_1 can be produced from the input circuit β by an extended arithmetic network over $\mathbb{Q}$ of size $(dL)^{O(1)}$. This finishes the description of the first stage in our recursive procedure.

We consider now the case of $0 < i < n$ and set $r := n-(i+1)$. Suppose that there is given a division-free straight-line program β_{i-1} in $\mathbb{Q}[X_1, \ldots, X_{r+1}]$ of size Λ_{i-1} that represents a nonzero polynomial $\varrho' \in \mathbb{Q}[X_1, \ldots, X_{r+1}]$ and the coefficients with respect to X_{r+2} of certain polynomials $q', p'_1, \ldots, p'_n \in \mathbb{Q}[X_1, \ldots, X_{r+1}, X_{r+2}]$. These polynomials have the following properties: q' is monic and separable in X_{r+2} and satisfies the degree condition $\deg q' = \deg_{X_{r+2}} q' = \delta^*_{i-1}$, ϱ' is the discriminant of q' with respect to X_{r+2}, the polynomials $p'_1, \ldots, p'_n$ satisfy the degree bound $\max\{\deg_{X_{r+2}} p'_k | 1 \le k \le n\} < \delta^*_{i-1}$, and the ideal $(q', \varrho' X_1 - p'_1, \ldots, \varrho' X_n - p'_n)_{\varrho'}$ of the localized ring $\mathbb{Q}[X_1, \ldots, X_n]_{\varrho}$ is the vanishing ideal of the affine variety $(W^*_{i-1})_{\varrho'}$. Observe that $(W^*_{i-1})_{\varrho'}$ is a Zariski open dense subset of (W^*_{i-1}). Let Z be the Zariski closure in $\mathbb{C}^n$ of $\{x \in W^*_{i-1} | (\partial f(x)/\partial X_i) = 0, \Delta(x) \neq 0\}$. We have $W^*_i \subset Z \subset W_i$ and that Z is at least the union of all real irreducible components of W_i. In particular, all irreducible components of Z are irreducible components of W_i. Moreover, we have $\deg Z \le d\delta^*_{i-1}$.

Now we apply the procedure underlying [19, Proposition 15] to the straight-line programs β_{i-1} and β representing the polynomials $\varrho', q', p'_1, \ldots, p'_n$ and $\partial f/\partial X_i$ in order to produce an explicit description of the algebraic variety $\{x \in W^*_{i-1} | (\partial f(x)/\partial X_i) = 0\}$. By means of the algorithm of [19, Subsection 5.1.3], we clear out the irreducible components of this variety contained in the hypersurface $\{x \in \mathbb{C}^n | \Delta(x) = 0\}$. Finally, we obtain a division-free straight-line program $\overline{\mu}$ in $\mathbb{Q}[X_1, \ldots, X_r]$ of size $i(L+\Lambda_{i-1})(d\delta^*_{i-1})$ which represents a nonzero polynomial $\overline{\varrho} \in \mathbb{Q}[X_1, \ldots, X_r]$ and the coefficients with respect to X_{r+1} of certain polynomials $\overline{q}, \overline{p}_1, \ldots, \overline{p}_n \in \mathbb{Q}[X_1, \ldots, X_{r+1}]$. The latter polynomials have the following properties: $\overline{q}$ is monic and separable with respect to X_{r+1} and satisfies the degree condition $\deg \overline{q} = \deg_{X_{r+1}} \overline{q} = \deg Z$, $\overline{\varrho}$ is the discriminant of $\overline{q}$ with respect to X_{r+1}, the polynomials $\overline{p}_1, \ldots, \overline{p}_n$ satisfy the degree bound $\max\{\deg_{X_{r+1}} \overline{p}_k | 1 \leq k \leq n\} < \deg Z$, and the ideal $(\overline{q}, \overline{\varrho}X_1 - \overline{p}_1, \ldots, \overline{\varrho}X_n - \overline{p}_n)_{\overline{\varrho}}$ of the localized ring $\mathbb{Q}[X_1, \ldots, X_n]_{\overline{\varrho}}$ is the vanishing ideal of the affine variety $Z_{\overline{\varrho}}$. Observe again the $Z_{\overline{\varrho}}$ is a Zariski open dense subset of Z. By [19, Proposition 15 and Subsection 5.1.3], there exists an arithmetic network $\mathcal{N}_i$ with parameters in $\mathbb{Q}$ which produces from the input circuits β_{i-1} and β the output circuit $\overline{\mu}$ and has size $i(d\delta_{i-1}^* L\Lambda_{i-1})^{O(1)}$.

Let $q_1, \ldots, q_s \in \mathbb{Q}[X_1, \ldots, X_{r+1}]$ be the $\mathbb{Q}$-irreducible factors of $\overline{q}$. Since $\overline{q}$ is monic and separable in X_{r+1}, we have $\overline{q} = q_1 \cdots q_s$. From the assumption that the variables $X_1, \ldots, X_n$ are in generic position we deduce that each irreducible component of the algebraic variety Z is represented by exactly one of the irreducible polynomials $q_1, \ldots, q_s$. This means that Z has s irreducible components, say $C_1, \ldots, C_s$, such that for $1 \leq l \leq s$ the irreducible component C_l is identical with the Zariski closure in $\mathbb{C}^n$ of the set

$$\begin{aligned}\{x = (X_1, \ldots, X_n) \in \mathbb{C}^n | \, &\overline{\varrho}(X_1, \ldots, X_r)X_1 - \overline{p}_1(X_1, \ldots, X_{r+1}) = 0,\\ &\ldots, \overline{\varrho}(X_1, \ldots, X_r)X_n - \overline{p}_n(X_1, \ldots, X_{r+1}) = 0,\\ &q_l(X_1, \ldots, X_r) = 0, \overline{\varrho}(X_1, \ldots, X_r) \neq 0\}.\end{aligned}$$

Now suppose that the real irreducible components of Z (and hence, the one of W_i) are represented in this way by the polynomials $q_1, \ldots, q_m$ and let $q := q_1 \ldots q_m$. The polynomial q is monic and separable in X_{r+1} and satisfies the degree condition $\deg q = \deg_{X_{r+1}} q = \delta_i^*$. Moreover, we have $W_i^* = C_1 \cup \cdots \cup C_m$.

Now we try to find a straight-line program μ whose length is of order $(id\delta_i^* L)^{O(1)}$ (hence, independent of the length Λ_{i-1} of the circuit β_{i-1}) and which represents the coefficients of the polynomials $q_1, \ldots, q_s$ and, finally, the polynomial q. Adding to the arithmetic network $\mathcal{N}_i$ order of $(id\delta_i^* L\Lambda_{i-1})^{O(1)}$ extra nodes we find as in the proof of [20, Proposition 30], a "sufficiently generic" lifting point $t = (t_1, \ldots, t_r) \in \mathbb{Q}^r$ for the algebraic variety Z (see [20, Definition 19], for the notion of a lifting point). By the generic choice of the point t we deduce from Hilbert's Irreducibility Theorem that $q_1(t, X_{r+1}, \ldots, q_s(t, X_{r+1})$ are irreducible polynomials of $\mathbb{Q}[X_{r+1}]$. Thus the identity $\overline{q}(t, X_{r+1} = q_1(t, X_{r+1}) \cdots q_s(t, X_{r+1})$ represents the decomposition of the polynomial $\overline{q}(t, X_{r+1}) \in \mathbb{Q}[X_{r+1}]$ into its irreducible factors.

Specializing in the straight-line program $\overline{\mu}$ the variables $X_1, \ldots, X_r$ into the values $t_1, \ldots, t_r$ we obtain an arithmetic circuit in $\mathbb{Q}$ that represents the coefficients of the univariate polynomial $\overline{q}(t, X_{r+1})$. Adding some extra nodes to the arithmetic network, without changing its asymptotic size, we may suppose that $\mathcal{N}_i$ represents the nonzero rational number $\overline{\varrho}(t)$ and the coefficients of the univariate polynomials $\overline{q}(t, X_{r+1}), \overline{p}_1(t, X_{r+1}), \ldots, \overline{p}_n(t, X_{r+1})$. Observe that $\deg \overline{q}(t, X_{r+1}) = \deg_{X_{r+1}} \overline{q} = \deg \overline{q} \le d\delta^*_{i-1}$ holds. Therefore we are able to find the irreducible factors $q_1(t, X_{r+1}), \ldots, q_s(t, X_{r+1})$ of $\overline{q}(t, X_{r+1})$ by a call to the first subroutine at a supplementary cost of $(d\delta^*_{i-1})^{O(1)}$. Adding some extra nodes to the arithmetic network $\mathcal{N}_i$, without changing its asymptotic complexity, we may suppose that $\mathcal{N}_i$ represents for each $1 \le l \le s$ the rational number $\overline{\varrho}(t)$ and the coefficients of the polynomials $q_l(t, X_{r+1}), \overline{p}_1(t, X_{r+1}), \ldots, \overline{p}_n(t, X_{r+1})$. Observe that $\mathcal{N}_i$ is now an *extended* arithmetic network. For a fixed l, $1 \le l \le s$, the set $C_l \cap (\{t\} \times \mathbb{C}^{n-r})$ is the lifting fiber of the point t in the irreducible component C_l of Z. The polynomials $q_l(t, X_{r+1}), (1/\overline{\varrho}(t))\,\overline{p}_1(t, X_{r+1}), \ldots, (1/\overline{\varrho}(t))\,\overline{p}_n(t, X_{r+1})$ represent a geometric solution of this lifting fiber. This means that the identity

$$C_l \cap (\{t\} \times \mathbb{C}^{n-r}) = \left\{ \left(\frac{\overline{p}_1(t, u)}{\overline{\varrho}(t)}, \ldots, \frac{\overline{p}_n(t, u)}{\overline{\varrho}(t)} \right) \middle| \, u \in \mathbb{C},\, q_l(t, u) = 0 \right\}$$

holds.

Applying the algorithm underlying [20, Theorem 28] to the input $\beta, t = (t_1, \ldots, t_r), \overline{\varrho}(t), q_l(t, X_{r+1}), \overline{p}_1(t, X_{r+1}), \ldots, \overline{p}_n(t, X_{r+1})$, we obtain a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_r]$ having a length of order $(id \deg C_l L)^{O(1)}$ representing the coefficients of the polynomial q_l with respect to X_{r+1}. Doing this for each l, $1 \le l \le s$, again we have to add to the extended arithmetic network $\mathcal{N}_i$ some extra nodes which do not change its asymptotic size. Then we may suppose that $\mathcal{N}_i$ produces a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_r]$ representing the coefficients of the polynomials $q_1, \ldots, q_s$ with respect to the variable X_r. As in the case of $i = 0$ we discard by a call to the second subroutine the polynomials $q_{m+1}, \ldots, q_s$ which do not have any zero in $\mathbb{R}^n$. From the remaining polynomials $q_1, \ldots, q_m$ we generate $q = q_1 \cdots q_m$. The additional costs of discarding $q_{m+1}, \ldots, q_s$ and producing q is of order $(\sum_{l=1}^{s} id \deg C_l L)^{O(1)} = (id \deg ZL)^{O(1)} = (id\delta^*_{i-1} L)^{O(1)}$. Thus, without loss of generality, we may suppose that the extended arithmetic network $\mathcal{N}_i$ produces a division-free straight-line program in $\mathbb{Q}[X_1, \ldots, X_r]$ of size $(\sum_{l=1}^{s} id \deg C_l L)^{O(1)} = (id\delta^*_{i-1} L)^{O(1)}$ which represents the coefficients of the polynomial q with respect to the variable X_r. We observe that the point $t \in \mathbb{Q}^r$ is a lifting point of the algebraic variety $W_i^* = \cup_{l=1}^{s} C_l$, too. Therefore, the lifting fiber of t in W_i^* is given by the rational number $\overline{\varrho}(t)$ and the coefficients of the polynomials $q(t, X_{r+1})$ and $\overline{p}_1(t, X_{r+1}), \ldots, \overline{p}(t, X_{r+1})$, which, in principle, have already been computed by the arithmetic network $\mathcal{N}_i$. Again applying the procedure underlying [20, Theorem 28] to the input $\beta, t = (t_1, \ldots, t_r), \overline{\varrho}(t), q(t, X_{r+1}), \overline{p}_1(t, X_{r+1}), \ldots, \overline{p}_n(t, X_{r+1})$, we obtain a division-free straight-line program β_i in $\mathbb{Q}[X_1, \ldots, X_r]$ of size $\Lambda_i = (id\delta_i^* L)^{O(1)}$. The straight-line program β_i represents a nonzero polynomial $\varrho \in \mathbb{Q}[X_1, \ldots, X_r]$ and the coefficients with respect to X_{r+1} of the polynomial q and certain other polynomials $p_1, \ldots, p_n$ of $\mathbb{Q}[X_1, \ldots, X_r, X_{r+1}]$ having the properties (i)–(iv) stated in Lemma 11.

The extended arithmetic network $\mathcal{N}_i$ over $\mathbb{Q}$ which produces this output β_i from the input β_{i-1} and β has size $(id\delta_{i-1}^* L\Lambda_{i-1})^{O(1)}$.

Observe that the length Λ_i of the straight-line program β_i is independent of the length Λ_{i-1} of the input circuit β_{i-1}. More precisely, we have $\Lambda_i = (id\delta_i^* L)^{O(1)}$. Taking into account that $\delta_i^* \le d\delta_{i-1}^*$ and $\Lambda_{i-1} = ((i-1)d\delta_{i-1}^* L)^{O(1)}$ holds, we conclude that the size of the extended arithmetic network $\mathcal{N}_i$ which produces from the input circuits β_{i-1} and β the output circuits is of order $(id\delta_i^* L)^{O(1)}$. Concatenating the networks $\mathcal{N}_1, \ldots, \mathcal{N}_i$ we finally obtain an extended arithmetic network $\mathcal{N}$ over $\mathbb{Q}$ which produces the straight-line program β_i from the input circuit β. The network $\mathcal{N}$ is of size $(id\delta^* L)^{O(1)}$. ■

From Lemma 11 one now easily deduces our main result.

THEOREM 12. *Let n, d, δ^*, L be natural numbers. Then there exists an extended arithmetic network $\mathcal{N}$ over $\mathbb{Q}$ of size $(nd\delta^* L)^{O(1)}$ with the following properties:*

Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ be a nonconstant polynomial of degree at most d and suppose that f is given by a division-free straight-line program β in $\mathbb{Q}[X_1, \ldots, X_n]$ of length at most L. Let $\Delta := \sum_{i=1}^n (\partial f/\partial X_i)^2$, $W := \{x \in \mathbb{C}^n | f(x) = 0\}$, $V := W \cap \mathbb{R}^n = \{x \in \mathbb{R}^n | f(x) = 0\}$, and suppose that the variables $X_1, \ldots, X_n$ are in "sufficiently generic" position. Furthermore, suppose that V is a (nonempty) bounded smooth hypersurface of $\mathbb{R}^n$ with regular equation f. For $0 \le i \le n$, let W_i be the Zariski closure of the set $\{x \in \mathbb{C}^n | f(x) = \partial f(x)/\partial X_1 = \cdots = \partial f(x)/\partial X_i = 0, \Delta(x) \ne 0\}$ and $W_i^* := W_i \cap \mathbb{R}^n$.

Let $\delta_i^* := \deg^* W_i := \deg W_i^*$ be the real degree of the complex variety W_i and assume that $\delta^* \ge \max\{\delta_i^* | 0 \le i < n\}$ holds.

The algorithm represented by the extended arithmetic network $\mathcal{N}$ starts from the straight-line program β as input and produces a straight-line program in $\mathbb{Q}$ of size $(nd\delta^* L)^{O(1)}$. This straight-line program represents the coefficients of $n+1$ univariate polynomials $q, p_1, \ldots, p_n \in \mathbb{Q}[X_n]$ satisfying the following conditions:

(i) $\deg q = \delta_{n-1}^*$
(ii) $\max\{\deg p_i | 1 \le i \le n\} < \delta_{n-1}^*$
(iii) *Any connected component of the real hypersurface V has at least one point contained in the set*

$$P := \{(p_1(u), \ldots, p_n(u)) | u \in \mathbb{R}, q(u) = 0\}.$$

Moreover, the extended algorithmic network $\mathcal{N}$ codifies each real zero u of the polynomial q (and hence, the elements of P) "à la Thom."

Proof. Just apply Lemma 11, setting $i := n - 1$. The remaining arguments are the same as in the proof of Theorem 8. ■

REFERENCES

1. Basu, S., Pollack, R., and Roy, M.-F. On the combinatorial and algebraic complexity of quantifier elimination, *in* "Proc. 35th IEEE Symposium on Foundations of Computer Science," to appear.
2. Baur, W., and Strassen, V. The complexity of partial derivatives, *Theoret. Comput. Sci.* **22** (1982), 317–330.
3. Ben-Or, M., Kozen, D., and Reif, J. The complexity of elementary algebra and geometry, *J. Comput. System Sci.* **32** (1986), 251–264.
4. Brodmann, M. "Algebraische Geometrie," Birkhäuser-Verlag, Basel/Boston/Berlin, 1989.
5. Buchberger, B. Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, *Aequationes Math.* **4** (1970), 371–383.
6. Canny, J. F. Some algebraic and geometric computations in PSPACE, *in* "Proc. 20th ACM Symposium on Theory of Computing," pp. 460–467, Assoc. Computing Machinery, 1988.
7. Canny, J. F., and Emiris, I. Z. Efficient incremental algorithms for the sparse resultant and the mixed volume, preprint, 1995.
8. Caniglia, L., and Heintz, J. Some new effectivity bounds in computational geometry, *in* "Proc. AAECC-6," (T. Mora, Ed.), Lecture Notes in Computer Science, Vol. 357, pp. 131–152, Springer-Verlag, New York/Berlin, 1989.
9. Chistov, A. L. Polynomial-time computation of the dimension of components of algebraic varieties in zero-characteristic, preprint, Universtité Paris XII, 1995.
10. Chistov, A. L., and Grigor'ev, D. J. Subexponential time solving systems of algebraic equations, LOMI Preprints E-9-83, E-10-83, Leningrad, 1983.
11. Coste, M., and Roy, M.-F. Thom's Lemma, the coding of real algebraic numbers and the computation of the topology of semialgebraic sets, *J. Symbolic Comput.* **5** (1988), 121–130.
12. Dedieu, J.-P. Estimations for the separation number of a polynomial system, preprint, Univ. Paul Sabatier, Toulouse, 1995.
13. Dedieu, J.-P. Approximate solutions of numerical problems, condition number analysis and condition number theorems, preprint, Univ. Paul Sabatier, Toulouse, 1995.
14. Dickenstein, A., Fitchas, N., Giusti, M., and Sessa, C. The membership problem of unmixed ideals is solvable in single exponential time, *Discrete Appl. Math.* **33** (1991), 73–94.
15. Emiris, I. Z. "On the Complexity of Sparse Elimination," Report UCB/CSD-94/840, Univ. of California, 1994.
16. von zur Gathen, J., and Seroussi, G. Boolean circuits versus arithmetic circuits, *Inform. and Comput.* **91,** No. 1 (1991), 142–154.

17. Giusti, M., and Heintz, J. La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial, *in* "Computational Algebraic Geometry and Commutative Algebra, Proceedings of the Cortona Conference on Computational Algebraic Geometry and Commutative Algebra, Istituto Nazionale di Alta Matematica," (D. Eisenbud and L. Robbiano,Eds.), Symposia Matematica, Vol. 34, Cambridge Univ. Press, Cambridge, 1993.

18. Giusti, M., Heintz, J., Morais, J. E., and Pardo, L. M. When polynomial equation systems can be "solved" fast?, *in* "Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, 1995," (G. Cohen, M. Giusti, and T. Mora, Eds.), Lecture Notes in Computer Science, Vol. 948, pp. 205–231, Springer-Verlag, New York/Berlin, 1995.

19. Giusti, M., Heintz, J., Morais, J. E., Morgenstern, J., and Pardo, L. M. Straight-line programs in geometric elimination theory, *Pure Appl. Algebra,* to appear.

20. Giusti, M., Heintz, J., Hägele, K., Morais, J. E., Montaña, J. L. and Pardo, L. M. Lower bounds for Diophantine approximations, Preprint 4/1996. Departamento de Matemáticas, Estadistica y Computación, Universidad de Cabtabria, Spain; accepted for publication, MEGA, 1996.

21. Golubitsky, M., and Guillemin, V. "Stable Mappings and Their Singularities," Springer-Verlag, New York, 1986.

22. Grigor'ev, D. Complexity of deciding Tarski Algebra, *J. Symbolic Comput.* **3** (1987), 65–108.

23. Grigor'ev, D., and Vorobjov, N. Solving systems of polynomial inequalities in subexponential time, *J. Symbolic Comput.* **5** (1988), 37–64.

25. Hermann, G. Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, *Math. Ann.* **95** (1926), 736–788.

26. Heintz, J., Roy, M.-F., and Solernó P. On the complexity of semialgebraic sets, *in* "Proc. Information Processing '89 (IFIP 89), San Francisco, CA, 1989," (G. X. Ritter, Ed.), pp. 293–298, North–Holland, Amsterdam, 1989.

27. Heintz, J., Roy, M.-F., and Solernó, P. Complexité du principe de Tarski–Seidenberg, *C. R. Acad. Sci. Paris, Ser. I* **309** (1989), 825–830.

28. Heintz, J., Roy, M.-F., and Solernó, P. Sur la complexité du principe de Tarski–Seidenberg, *Bull. Soc. Math. France* **118** (1990), 101–126.

29. Heintz, J., and Schnorr, C. P. Testing polynomials which are easy to compute, *in* "Proc. 12th Annual ACM Symposium on Computing, 1980," pp. 262–268; also in "Logic and Algorithmic, An International Symposium held in Honour of Ernst Specker," l'Enseignement de Mathématiques, Monograph 30, pp. 237–254, Genève, 1982.

30. Heintz, J., and Wüthrich, R. An efficient quantifier elimination algorithm for algebraically closed fields of any characteristic, *SIGSAM Bull.* **9,** No. 4, (1975).

31. Krick, T., and Pardo, L. M. A computational method for Diophantine approximation, *in* "Algorithms in Algebraic Geometry and Applications, MEGA '94," (L. Gonzales-Vega and T. Recio, Eds.), Progress in Mathematics, Vol. 143, pp. 193–254, Birkhäuser, Basel, 1996.

32. Krick, T., and Pardo, L. M. Une approche informatique pour l'approximation diophantienne, *C. R. Acad. Sci. Paris Sér. I,* **318,** No. 5 (1994), 407–412.

33. Lang, S. "Diophantine Geometry," Interscience/Wiley, New York/London, 1962.

34. Lazard, D. Algèbre linéaire sur $K[X_1, \ldots, X_n]$ et élimination, *Bull. Soc. Math. France* **105** (1977), 165–190.

35. Lazard, D. Résolution des systèmes d'équations algébriques, *Theoret. Comput. Sci.* **15** (1981), 77–110.

36. Lê, D. T., and Teissier, B. Variétés polaires locales et classes de Chern des variétés singuliéres, *Ann. of Math.* **114** (1981), 457–491.

37. Lenstra, A. K. Lenstra, H. W., Jr., and Lovász, L. Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 534–543.

38. Milnor, M. On the Betti numbers of real algebraic varieties, *Proc. Amer. Math. Soc.* **15** (1964), 275–280.

39. Morgenstern, J. How to compute fast a function and all its derivatives, Prepublication 49,Université de Nice, 1984.

40. Pardo, L. M. How lower and upper complexity bounds meet in elimination theory, *in* "Proc. 11th International Symposium Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, 1995," (G. Cohen, M. Giusti, and T. Mora, Eds.), Lecture Notes in Computer Science, Vol. 948, pp. 33–69, Springer-Verlag, New York/Berlin, 1995.

41. Renegar, J. A faster PSPACE algorithm for the existential theory of the reals, *in* "Proc. 29th Annual IEEE Symposium on the Foundation of Computer Science (FOCS)," 1988, pp. 291–295.

42. Renegar, J. On the computational complexity and geometry of the first order theory of the reals, *J. Symbolic Comput.* **13,** No. 3 (1992), 255–352.

43. Roy, M.-F., and Szpirglas, A. Complexity of computation with real algebraic numbers, *J. Symbolic Comput.* **10** (1990), 39–51.

44. Seidenberg, A. Constructions in algebra, *Trans. Amer. Math. Soc.* **197** (1974), 273–313.

45. Shub, M., and Smale, S. Complexity of Bezout's theorem. I. Geometric aspects, *J. Amer. Math. Soc.* **6** (1993), 459–501.

46. Shub, M., and Smale, S. Complexity of Bezout's theorem II: Volumes and probabilities, *in* "Proceedings, Effective Methods in Algebraic Geometry, MEGA'92, Nice, 1992," (F. Eyssette and A. Galligo, Eds.), Progress in Mathematics, Vol. 109, pp. 267–285, Birkhäuser, Basel, 1993.

47. Shub, M., and Smale, S. Complexity of Bezout's theorem. III. Condition number and packing. *J. Complexity* **9** (1993), 4–14.

48. Shub, M., and Smale, S. Complexity of Bezout's theorem. IV. Probability of success, extensions, *SIAM J. Numer. Anal.*, to appear.

49. Shub, M., and Smale, M. Complexity of Bezout's theorem. V. Polynomial time, *Theoret. Comput. Sci.* **133** (1994).

50. Solernó, P. "Complejidad de conjuntos semialgebraicos," thesis, Univ. de Buenos Aires, 1989.