Polar Varieties and Efficient Real Equation Solving: The Hypersurface Case

B. Bank [1], M. Giusti [2], J. Heintz [3],

R. Mandel, G. M. Mbakop [1]

March 21, 1996

Abstract

The objective of this paper is to show how the recently proposed method by Giusti, Heintz, Morais, Morgenstern, Pardo [10] can be applied to a case of real polynomial equation solving. Our main result concerns the problem of finding one representative point for each connected component of a real bounded smooth hypersurface.

The algorithm in [10] yields a method for symbolically solving a zero-dimensional polynomial equation system in the affine (and toric) case. Its main feature is the use of adapted data structure: Arithmetical networks and straight-line programs. The algorithm solves any affine zero-dimensional equation system in non-uniform sequential time that is polynomial in the length of the input description and an adequately defined affine degree of the equation system.

Replacing the affine degree of the equation system by a suitably defined real degree of certain polar varieties associated to the input equation, which describes the hypersurface under consideration, and using straight-line program codification of the input and intermediate results, we obtain a method for the problem introduced above that is polynomial in the input length and the real degree.

Keywords and phrases: Real polynomial equation solving, polar varieties, real degree, straight-line programs, complexity

[1] Humboldt-Universität zu Berlin, Unter den Linden 6, D–10099 Berlin, bank(at)mathematik.hu-berlin.de; mbakop(at)mathematik.hu-berlin.de

[2] GAGE, Centre de Mathématiques. École Polytechnique. F-91228, Palaiseau Cedex. France, giusti(at)ariana.polytechnique.fr

[3] Dept. de Matemáticas, Estadística y Computación. F. de Ciencias. U. Cantabria. E-39071 Santander, Spain, heintz(at)matsun1.unican.es

1 Introduction

The present article is strongly related to the papers [10] and [9]. Whereas the algorithms developed in these references are related to the algebraically closed case, here we are concerned with the real case. Finding a real solution of a polynomial equation $f(x) = 0$ where f is a polynomial of degree $d \geq 2$ with rational coefficients in n variables is for practical applications more important than the algebraically closed case. Best known complexity bounds for the problem we deal with are of the form $d^{O(n)}$ due to [17], [27], [1], [35]. Related complexity results can be found in [3], [14].
Solution methods for the algebraically closed case are not applicable to real equation solving normally. The aim of this paper is to show that certain *polar varieties* associated to an affine hypersurface possess a geometric invariant, *the real degree*, which permits an adaptation of the algorithms designed in the papers mentioned at the beginning. The algorithms there are of "intrinsic type", which means that they are able to distinguish between the semantical and the syntactical character of the input system in order to profit both for the improvement of the complexity estimates. Both papers [10] and [9] show that the *affine degree* of an input system is associated with the complexity when measured in terms of the number of arithmetic operations. Whereas the algorithms in [10] still need algebraic parameters, those proposed in [9] are completely rational.
We will show that, under smoothness assumptions for the case of finding a real zero of a polynomial equation of degree d with rational coefficients and n variables, it is possible to design an algorithm of intrinsic type using the same data structure, namely straight-line programs without essential divisions and rational parameters for codifying the input system, intermediate results and the output, and replacing the affine degree by the real degree of the associated polar varieties to the input equation.
The computation model we use will be an arithmetical network (compare to [10]). Our main result then consists in the following. *There is an arithmetical network of size $(nd\delta^* L)^{O(1)}$ with parameters in the field of rational numbers which finds a representative real point in every connected component of an affine variety given by a non-constant square-free n-variate polynomial f with rational coefficients and degree $d \geq 2$ (supposing that the affine variety contains a smooth real point). L denotes the size of the straight-line program codifying the input and δ^* is the real degree associated to f.*
Close complexity results are the ones following the approach initiated in [29], and further developed in [30], [31], [32], [33], see also [7], [8].
For more details we refer the reader to [10] and [9] and the references cited there.

2 Polar Varieties and Algorithms

As usually, 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, 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 $\mathbb{C}^n$. Let $1 \leq j \leq s$, be arbitrarily fixed and consider the irreducible component C_j of W.
In the following we need the notion of degree of an affine algebraic variety. Let $W \subset \mathbb{C}^n$ be an algebraic subset given by a regular sequence $f_1, \cdots f_i \in \mathbb{Q}[x_1, \cdots, x_n]$ of degree at most d. If $W \subset \mathbb{C}^n$ ist zero–dimensional the *degree* of W, $degW$, is defined to be the number of points in W (neither multiplicities nor points at infinity are counted). If $W \subset \mathbb{C}^n$ is of dimension greater than zero (i.e. $dimW = n - i \geq 1$), then we consider the collection $\mathcal{M}$ of all affine varieties of dimension i given as the solution set in $\mathbb{C}^n$ of a linear equation system $L_1 = 0, \cdots, L_{n-i} = 0$ with $L_k = \sum_{j=1}^{n} a_{kj} x_j + a_{k0},\ a_{ki} \in \mathbb{Q}, 1 \leq i \leq n$. Let $\mathcal{M}_W$ be the subcollection of $\mathcal{M}$ formed by all varieties $H \in \mathcal{M}$ such that the affine variety $H \cap W$ satisfies $H \cap W \neq \emptyset$ and $dim(H \cap W) = 0$. Then the affine degree of W is defined as $max\{\delta | \delta = deg(H \cap W),\ H \in M_W\}$.

Definition 1 *The 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.*
If we denote

$$I = \{j \in \mathbb{N} | 1 \leq j \leq s,\ C_j \text{ is a real component of } W\}.$$

then the affine variety $W^* := \bigcup_{j \in I} C_j \subset \mathbb{C}^n$ is called the real part of W. By $deg^* W := degW^* = \sum_{j \in I} degC_j$ we define the real degree of the set W.

Remark 2 Observe that $deg^* W = 0$ holds if and only if the real part W^* of W is empty.

Proposition 3 *Let $f \in \mathbb{Q}[X_1, \cdots, X_n]$ be a non-constant and square-free polynomial and let $\widetilde{V}(f)$ be the set of real zeros of the equation $f(x) = 0$. Assume $\widetilde{V}(f)$ to be bounded. Furthermore, let for every fixed i, $0 \leq i < n$, the real variety*

$$\widetilde{V}_i := \{x \in \mathbb{R}^n \mid f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots, \frac{\partial f(x)}{\partial X_i} = 0\}$$

be non-empty (and $\widetilde{V}_0$ is understood to be $\widetilde{V}(f)$). Suppose the variables to be in generic position. Then any point of $\widetilde{V}_i$ that is a smooth point of $\widetilde{V}(f)$ is also a smooth point of $\widetilde{V}_i$. Moreover, for every such point the Jacobian of the equation system $f = \frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_i} = 0$ has maximal rank.

Proof

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

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

where I and 0 define a unit and a zero matrix, respectively, and
$a_{kl} \in \mathbb{R}$ arbitrary if k, l satisfy $i+1 \leq k \leq n, \;\; 1 \leq l \leq i$.
The transformation $x \longleftarrow A^{(i)}y$ defines a linear change of coordinates, since the square matrix $A^{(i)}$ has full rank.
In the new coordinates, the variety $\widetilde{V}_i$ takes the form

$$\widetilde{V}_i := \{y \in \mathbb{R}^n \mid f(y) = \frac{\partial f(y)}{\partial Y_1} + \sum_{j=i+1}^{n} a_{j1} \frac{\partial f(y)}{\partial Y_j} = \ldots = \frac{\partial f(y)}{\partial Y_i} + \sum_{j=i+1}^{n} a_{ji} \frac{\partial f(y)}{\partial Y_j} = 0\}$$

This transformation defines a map $\Phi_i \; : \mathbb{R}^n \times \mathbb{R}^{(n-i)i} \longrightarrow \mathbb{R}^{i+1}$ given by

$$\Phi_i\left(Y_1, \cdots, Y_i, \cdots, Y_n, a_{i+1,1}, \cdots a_{n1}, \cdots a_{i+1,i}, \cdots, a_{n,i}\right) =$$

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

For the moment let

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

Then the Jacobian matrix of $\Phi_i(\alpha)$ is given by
$J\left(\Phi_i(\alpha)\right) = \left(\frac{\partial \Phi_i(\alpha)}{\partial \alpha_j}\right)_{(i+1)\times(n+(n-i)i)} =$

$$\begin{pmatrix} \frac{\partial f}{\partial Y_1} & \cdots & \frac{\partial f}{\partial Y_n} & 0 & \cdots & 0 & \cdots & \cdots & 0 \\ * & \cdots & * & \frac{\partial f}{\partial Y_{i+1}} & \cdots & \frac{\partial f}{\partial Y_n} & 0\cdots & \vdots & 0 \\ \vdots & & \vdots & \ddots & \ddots & 0 & \cdots & \ddots & 0 \\ * & \cdots & * & 0\cdots & 0\cdots & \cdots & \frac{\partial f}{\partial Y_{i+1}} & \cdots & \frac{\partial f}{\partial Y_n} \end{pmatrix}$$

If $\alpha^0 = (Y_1^0, \cdots, Y_n^0, a_{i+1,\,1}^0, \cdots a_{n,\,i}^0)$ belongs to the fibre $\Phi_i^{-1}(0)$, where $(Y_1^0, \cdots, Y_n^0)$ is a point of the hypersurface $\widetilde{V}(f)$ and if there is an index $j \in \{i+1, \cdots, n\}$ such that $\frac{\partial f}{\partial Y_j} \neq 0$ at this point, then the Jacobian matrix $J\left(\Phi_i(\alpha^0)\right)$ has the maximal rank $i+1$.
Suppose now that for all points of $\widetilde{V}(f)$

$$\frac{\partial f(y)}{\partial Y_{i+1}} = \cdots = \frac{\partial f(y)}{\partial Y_n} = 0$$

and let $C := \mathbb{R}^n \setminus \{\frac{\partial f(y)}{\partial Y_1} = \cdots = \frac{\partial f(y)}{\partial Y_n} = 0\}$, which is an open set. Then the restricted map

$$\Phi_i : C \times \mathbb{R}^{(n-i)i} \longrightarrow \mathbb{R}^{i+1}$$

is transversal to the subvariety $\{0\}$ in $\mathbb{R}^{i+1}$.
By weak transversality due to Thom/Sard (see e.g. [13]) applied to the diagram

$$\begin{array}{ccc} \Phi_i^{-1}(0) & \hookrightarrow & \mathbb{R}^n \times \mathbb{R}^{(n-i)i} \\ & \searrow & \downarrow \\ & & \mathbb{R}^{(n-i)i} \end{array}$$

one concludes that the set of all $A \in \mathbb{R}^{(n-i)i}$ for which transversality holds is dense in $\mathbb{R}^{(n-i)i}$.
Since the hypersurface $\widetilde{V}(f)$ is bounded by assumption, there is an open and dense set of matrices A such that the corresponding coordinate transformation leads to the desired smoothness. 2

Let $f \in \mathbb{Q}[X_1, \cdots, X_n]$ be a non–constant squarefree polynomial and let $W := \{x \in \mathbb{C}^n \mid f(x) = 0\}$ be the hypersurface defined by f. Consider the real variety $V := W \cap \mathbb{R}^n$ and suppose:

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

Definition 4 (Polar variety corresponding to a linear space) *Let i, $0 \leq i < n$, be arbitrarily fixed. Further, let $X^i := \{x \in \mathbb{C}^n \mid X_{i+1} = \cdots = X_n = 0\}$ be the corresponding linear subspace of $\mathbb{C}^n$. Then, W_i defined to be the Zariski closure of*

$$\{x \in \mathbb{C}^n \mid f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_i} = 0,\ \Delta(x) := \sum_{j=1}^{n} \left(\frac{\partial f(x)}{\partial X_j}\right)^2 \neq 0\}$$

is called the polar variety of W associated to the linear subspace X^i.
The corresponding real variety of W_i is denoted by $V_i := W_i \cap \mathbb{R}^n$.

Remark 5 Because of the hypotheses that $V \neq \emptyset$ is a smooth hypersurface and that $W_i \neq \emptyset$ by the assumptions above, the real variety $V_i := W_i \cap \mathbb{R}^n$, $0 \leq i < n$, is not empty and by smoothness of V, it has the description

$$V_i = \{x \in \mathbb{R}^n \,|\, f(x) = \frac{\partial f(x)}{\partial X_1} = \ldots = \frac{\partial f(x)}{\partial X_i} = 0\}.$$

(V_0 is understood to be V.)
According to Proposition 3, V_i is smooth if the coordinates are chosen to be in generic position. Definition 4 of a polar variety is slightly different from the one introduced by Lê/Teissier [23].

Theorem 6 *Let $f \in \mathbb{Q}[X_1, \cdots, X_n]$ be a non–constant squarefree polynomial and let $W := \{x \in \mathbb{C}^n \,|\, f(x) = 0\}$ be the corresponding hypersurface. Further, let $V := W \cap \mathbb{R}^n$ be a non–empty, smooth, and bounded hypersurface in $\mathbb{R}^n$ whose regular equation is given by $f = 0$. Assume the variables $X_1, \cdots, X_n$ to be generic. Finally, for every i, $0 \leq i < n$, let the polar varieties W_i of W corresponding to the subspace X^i be defined as above. Then it holds :*

- $W_0 = W$,
- *W_i is a non–empty equidimensional affine variety of dimension $n-(i+1)$ that is smooth in all its points that are smooth points of W,*
- *the real part W_i^* of the polar variety W_i coincides with the Zariski closure in $\mathbb{C}^n$ of*

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

- *for any j, $i < j \leq n$ the ideal*

$$\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}\right)_{\frac{\partial f}{\partial X_j}}$$

is radical.

Proof:
Let $i, 0 \leq i < n$, be arbitrarily fixed. The first item is obvious since $W_0 \subset W$ and W has codimension 1 as hypersurface in $\mathbb{C}^n$.
Then W_i is non-empty by the assumptions. The sequence $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}$ of polynomials of $\mathbb{Q}[X_1, \ldots, X_n]$ forms a local regular sequence with respect to the smooth points of W_i since the affine varieties $\{x \in \mathbb{C}^n | f(x) = \frac{\partial f(x)}{\partial X_1} = \cdots = \frac{\partial f(x)}{\partial X_k} = 0\}$ and $\{x \in \mathbb{C}^n | \frac{\partial f(x)}{\partial X_{k+1}} = 0\}$ are transversal for any $k, 0 \leq k \leq i-1$, by the generic choice of the coordinates, and hence the sequence $f, \frac{\partial f}{\partial X_1}, \cdots, \frac{\partial f}{\partial X_i}$ yields a local complete intersection with respect to the same points. This implies that W_i are equidimensional and $dim_{\mathbb{C}} W_i = n - (i+1)$ holds. We observe that every smooth point of W_i is a smooth point of W, which completes the proof of the second item.
The Zariski closure of V_i is contained in W_i^*, which 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_{j*} be an irreducible component of W_i^* containing this point, and $C_{j*} \cap V_i \neq \emptyset$. Then

$$\begin{aligned} n - i - 1 \quad &= dim_{\mathbb{R}}(C_{j*} \cap V_i) = dim_{\mathbb{R}} R(C_{j*} \cap V_i) = \\ &= dim_{\mathbb{C}} R((C_{j*} \cap V_i)') \leq dim_{\mathbb{C}} C_{j*} = n - i - 1, \end{aligned}$$

where $R(\cdot)$ and $(\ )'$ denote the corresponding sets of smooth points contained in $(\cdot)$ and the associated complexification, respectively. Therefore, $dim_{\mathbb{C}}(C_{j*} \cap V_i)' = dim_{\mathbb{C}} C_{j*} = n - i - 1$ and, hence, $C_{j*} = (C_{j*} \cap V_i)'$, and the latter set is contained in the Zariski closure of V_i.
We define the non-empty affine algebraic set

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

Let $j, i < j \leq n$, be arbitrarily fixed. Then one finds a smooth point x^* in $\widetilde{W_i}$ such that $\frac{\partial f(x^*)}{\partial X_j} \neq 0$; let x^* be fixed in that way. The hypersurface $W = \{x \in \mathbb{C}^n | f(x) = 0\}$ contains x^* as a smooth point, too. Consider the local ring $\mathcal{O}_{W,x^*}$ of x^* on the hypersurface W. (This is the ring of germs of functions on W that are regular at x^*. The local ring $\mathcal{O}_{W,x^*}$ is obtained by dividing the ring $\mathbb{C}[X_1, \ldots, X_n]$ of polynomials by the principal ideal (f), which defines W as an affine variety, and then by localizing at the maximal ideal $(X_1 - X_1^*, \ldots, X_n - X_n^*)$, of the point $x^* = (X_1^*, \ldots, X_n^*)$ considered as a single point affine variety.) Using now arguments from Commutative Algebra and Algebraic Geometry, see e.g. Brodmann [2], one arrives at the fact that $\mathcal{O}_{W,x^*}$ is an integral regular local ring.
The integrality of $\mathcal{O}_{W,x^*}$ implies that there is a uniquely determined irreducible

component Y of W containing the smooth point x^* and locally this component corresponds to the zero ideal of $\mathcal{O}_{W,x^*}$, which is radical. Since the two varieties $\widetilde{W}_i \cap Y$ and $W \cap Y$ coincide locally, the variety $\widetilde{W}_i \cap Y$ corresponds locally to the same ideal. Thus, the desired radicality is shown. This completes the proof. 2

Remark 7 If one localizes with respect to the function $\Delta(x) = \sum_{j=1}^{n} \left(\frac{\partial f(x)}{\partial X_j}\right)^2$, then one obtains, in the same way as shown in the proof above, that the ideal

$$(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i})_\Delta$$

is also radical.

Remark 8 Under the assumptions of Theorem 6, for any i, $0 \leq i < n$, we observe the following relations between the different non-empty varieties introduced up to now.

$$V_i \subset V, \quad V_i \subset W_i^* \subset W_i \subset \widetilde{W}_i,$$

where V is the considered real hypersurface, V_i defined as in Remark 5, W_i the polar variety due to Definition 4, W_i^* its real part according to Definition 1, and $\widetilde{W}_i$ the affine variety introduced in the proof of Theorem 6. With respect to Theorem 6 our settings and assumptions imply that $n - i - 1 = dim_{\mathbb{C}} \widetilde{W}_i = dim_{\mathbb{C}} W_i = dim_{\mathbb{C}} W_i^* = dim_{\mathbb{R}} V_i$ holds. By our smoothness assumption and the generic choice of the variables we have for the respective sets of smooth points (denoted as before by $R(\cdot)$)

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

where W is the affine hypersurface.

For the following we use the notations as before, fix an i arbitrarily, $0 \leq i < n$, denote by δ_i^* the real degree of the polar variety W_i (compare with Definition 1, by smoothness one has that the real degree of the polar variety W_i is equal to the real degree of the affine variety $\widetilde{W}_i$), put $\delta^* := \max\{\delta_k^* | 0 \leq k \leq i\}$ and let $d := \deg f$. Finally, we write for shortness $r := n - i - 1$.

We say that the variables $X_1, \ldots, X_n$ are in Noether position with respect to a variety $\{f_1 = \cdots = f_s = 0\}$ in $\mathbb{C}^n$, $f_1, \ldots, f_s \in \mathbb{Q}[X_1, \ldots, X_n]$, if, for each

$r < k \leq n$, there exists a polynomial of $\mathbb{Q}[X_1, \ldots, X_r, X_k]$ that is monic in X_k and vanishes on $\{f_1 = \cdots = f_s = 0\}$.

Then one can state the next, technical lemma according to [10], [9], where the second reference is important in order to ensure that the occurring straight-line programs use parameters in $\mathbb{Q}$ only.

Lemma 9 *Let the assumptions of Theorem 6 be satisfied. Further, suppose that the polynomials $f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i} \in \mathbb{Q}[X_1, \ldots, X_n]$ are given by a straight-line program β in $\mathbb{Q}[X_1, \ldots, X_n]$ without essential divisions, and let L be the size of β. Then there is an arithmetical network with parameters in $\mathbb{Q}$ that constructs the following items from the input β*

- *a regular matrix of $\mathbb{Q}^{n\times n}$ given by its elements that transforms the variables $X_1, \ldots, X_n$ into new ones $Y_1, \ldots, Y_n$*
- *a non-zero linear form $U \in \mathbb{Q}[Y_{r+1}, \ldots, Y_n]$*
- *a division-free straight-line program γ in $\mathbb{Q}[Y_1, \ldots, Y_r, U]$ that represents non-zero polynomials $\varrho \in \mathbb{Q}[Y_1, \ldots, Y_r]$ and $q, p_1, \ldots, p_n \in \mathbb{Q}[Y_1, \ldots, Y_r, U]$.*

These items have the following properties:

(i) The variables $Y_1, \ldots, Y_n$ are in Noether position with respect to the variety W^*_{n-r}, the variables $Y_1, \ldots, Y_r$ being free

(ii) The non-empty open part $(W^*_{n-r})_\varrho$ is defined by the ideal $(q, \varrho X_1 - p_1, \ldots, \varrho X_n - p_n)_\varrho$ in the localization $\mathbb{Q}[X_1, \ldots, X_n]_\varrho$.

(iii) The polynomial q is monic in u and its degree is equal to $\delta^*_{n-r} = \deg^* W_{n-r} = \deg W^*_{n-r} \leq \delta^*$.

(iv) $\max\{\deg_u p_k | 1 \leq k \leq n\} < \delta^*_{n-r}$, $\max\{\deg p_k | 1 \leq k \leq n\} = (d\delta^*)^{0(1)}$, $\deg \varrho = (d\delta^*)^{0(1)}$.

(v) The nonscalar size of the straight-line program γ is given by $(sd\delta^* L)^{0(1)}$.

The proof of Lemma 9 can be performed in a similar way as in [10], [9] for establishing the algorithm. For the case handled here, in the i-th step one has to apply the algorithm to the localized sequence $\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_i}\right)_\Delta$ as input. The only point we have to take care of is the process of cleaning extranious $\mathbb{Q}$-irreducible components. Whereas in the proofs of the algorithms we refer to it suffices to clean out components lying in a prefixed hypersurface (e.g. components at infinity), the cleaning process we need here is more subtile. We have to clean out all non-real $\mathbb{Q}$-irreducible components that appear during our algorithmic process. The idea of doing this is roughly as follows. Due to the generic position of the variables $X_1, \ldots, X_n$ all $\mathbb{Q}$-irreducible components of the variety $\widetilde{W}_{n-r}$ can be visualized as $\mathbb{Q}$-irreducible factors of the polynomial $q(X_1, \ldots, X_r, U)$. If we specialize *generically* the variables $X_1, \ldots, X_r$ to *rational* values $\eta_1, \ldots, \eta_r$, then by Hilbert's Irreducibility Theorem (in the version of [22]) the $\mathbb{Q}$-irreducible factors of the *multivariate* polynomial $q(\eta_1, \ldots, \eta_r, U)$ correspond to the $\mathbb{Q}$-irreducible factors of the *one–variate* polynomial $q(\eta_1, \ldots, \eta_r, U) \in \mathbb{Q}[U]$. In order to explain our idea simpler, we assume that we are able to choose our specialization of $X_1, \ldots, X_r$ into $\eta_1, \ldots, \eta_r$ in such a way that the hyperplanes $X_1 - \eta_1 = 0, \ldots, X_r - \eta_r = 0$ cut any *real* component of $\widetilde{W}_{n-r}$ (This condition is open in the strong topology and doesn't represent a fundamental restriction on the correctness of our algorithm. Moreover, our assumption doesn't affect the complexity). Under these assumptions the $\mathbb{Q}$-irreducible factors of $q(X_1, \ldots, X_r, U)$, which correspond to the real components of $\widetilde{W}_{n-r}$, reappear as $\mathbb{Q}$-irreducible factors of $q(\eta_1, \ldots, \eta_r, U)$ which contain a real zero. These $\mathbb{Q}$-irreducible factors of $q(\eta_1, \ldots, \eta_r, U)$ can be found by a factorization procedure and by a real zero test of standard features of polynomial complexity character. Multiplying these factors and applying to the result the lifting-fibre process of [10], [9] we find the product q^* of the $\mathbb{Q}$-irreducible factors of $q(X_1, \ldots, X_r, U)$, which correspond to the union of the real components of the variety $\widetilde{W}_{n-r}$, i.e. to the real part of $\widetilde{W}_{n-r}$. The ideal $(q^*, \varrho X_1 - p_1, \ldots, \varrho X_n - p_n)_\varrho$ describes the localization of the real part of $\widetilde{W}_{n-r}$ at ϱ. All we have pointed out is executible in polynomial time if a factorization of univariate polynomials over $\mathbb{Q}$ in polynomial time is available and if our geometric assumptions on the choice of the specialization is satisfied.

Theorem 10 *Let the notations and assumptions be as in Theorem 6. Suppose that the polynomial f is given by a straight-line program β without essential divisions in $\mathbb{Q}[X_1, \ldots, X_n]$, and let L be the nonscalar size of β. Further, let $\delta_i^* := \deg^* W_i$, $\delta^* := \max\{\delta_i^* | 0 \le i < n\}$ be the corresponding real degrees of the polar varieties in question, and let $d := \deg f$. Then there is an arithmetical network of size $(nd\delta^* L)^{0(1)}$ with parameters in $\mathbb{Q}$ which produces, from the input β, the coefficients of a non-zero linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$ and non-zero polynomials $q, p_1, \ldots, p_n \in \mathbb{Q}[U]$ showing the following properties:*

1. *For any connected component C of V there is a point $\xi \in C$ and an element $\tau \in \mathbb{R}$ such that $q(\tau) = 0$ and $\xi = (p_1(\tau), \ldots, p_n(\tau))$*
2. $\deg(q) = \delta_{n-1}^* \le \delta^*$
3. $\max\{\deg(p_i) | 1 \le i \le n\} < \delta_{n-1}^*$.

References

[1] S. Basu, R. Pollack, M.-F. Roy: On the Combinatorial and Algebraic Complexity of Quantifier Elimination. Proc. 35th IEEE Symp. on Foundations of Computer Science (to appear)

[2] M. Brodmann: Algebraische Geometrie, Birkhäuser Verlag, Basel-Boston-Berlin (1989).

[3] J.F. Canny: Some Algebraic and Geometric Computations in PSPACE, Proc. Twentieth ACM Symp. on Theory of Computing (1988), 460-467.

[4] J. F. Canny, I.Z. Emiris: Efficient Incremental Algorithms for the Sparse Resultant and the Mixed Volume, Preprint (1995)

[5] A.L. Chistov: Polynomial-time Factoring of Polynomials and Finding Compounds of a Variety within the Subexponential Time. Notes of SCi Seminars of Leningrad Department of Math. Steklov Inst. 137, 124-188 (in Russian, English transl. to appear in J. Soviet Math.)

[6] A.L. Chistov, D. Yu. Grigor'ev: Subexponential Time solving Systems of Algebraic Equations. LOMI Preprints E-9-83, E-10-83, Leningrad (1983)

[7] J.-P. Dedieu, Estimations for the Separation Number of a Polynomial System, Preprint, Univ. Paul Sabatier, Toulouse (1995)

[8] J.-P. Dedieu, Approximate Solutions of Numerical Problems, Condition Number Analysis and Condition Number Theorems, Preprint, Univ. Paul Sabatier, Toulouse (1995)

[9] M. Giusti, J. Heintz, K. Hägele, J.E. Morais, J.L. Montaña, L.M. Pardo: Lower Bounds for Diophantine Approximations, Preprint (March 1996).

[10] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo: Straight–line programs in Geometric Elimination Theory, to appear in Journal of Pure and Applied Algebra

[11] M. Giusti, J. Heintz, J.E. Morais, L.M. Pardo: 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., Springer LNCS **948** (1995) 205–231.

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

[13] M. Golubitsky, V. Guillimin: Stable Mappings and their Singularities, Springer-Verlag, New York (1986).

[14] D. Grigor'ev, N. Vorobjov: Solving Systems of Polynomial Inequalities in Subexponential Time, J. Symbolic Comput. (1988), 5: 37-64.

[15] D. Grigor'ev, N. Vorobjov: Counting commected Components of a Semi-algebraic Set in Subexponential Time, Comput. Complexity (1992), 2: 133-186

[16] J. Heintz, J. Morgenstern: On the intrinsic complexity of elimination theory, J. of Complexity **9** (1993) 471–498.

[17] J. Heintz, M.-F. Roy, R. Solerno: Sur la complexité du principe de Tarski-Seidenberg. Bull. Soc. Math. France 118 (1990), 101-126

[18] J. Heintz, C.P. Schnorr: Testing polynomials which are easy to compute, Proc. 12th Ann. ACM Symp. on Computing (1980) 262–268; also in Logic and Algorithmic. An International Symposium held in Honour of Ernst Specker, Monographie No. **30** de l'Enseignement de Mathématiques, Genève (1982) 237–254.

[19] J. Kollár: Sharp Effective Nullstellensatz, J. of A.M.S. **1** (1988) 963-975.

[20] T. Krick, L.M. Pardo: A Computational Method for Diophantine Approximation, to appear in Proc. MEGA'94, Birkhäuser Progress in Mathematics.

[21] T. Krick, L.M. Pardo: Une approche informatique pour l'approximation diophantienne, C. R. Acad. Sci. Paris, t. **318**, Série I, no. 5 , (1994) 407–412.

[22] S. Lang: Diophantine Geometry, Interscience Publishers John Wiley & Sons, New York, London (1962)

[23] Lê, D.T., B. Teissier: Variété polaires locales et classes de Chern des vairétés singulieres, Annals of Mathematics, 114 (1981), 457-491

[24] M. Mignotte: Mathématiques pour le Calcul Formel, Presses Universitaires de France (1989).

[25] J.L. Montaña, L.M. Pardo: Lower Bounds for Arithmetic Networks, Applicable Algebra in Engineering Communications and Computing (AAECC), vol. **4** (1993), 1–24.

[26] L.M. Pardo: 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., Springer LNCS **948** (1995) 33–69.

[27] J. Renegar: On the Computational Complexity and Geometry of the first Order theory of the Reals. J. of Symbolic Computat. (1992), 13(3): 255-352.

[28] J. Sabia, P. Solernó: Bounds for traces in complete intersections and degrees in the Nullstellensatz, Applicable Algebra in Engineering Communications and Computing (AAECC), vol. **6** (1996) 353–376.

[29] M. Shub, S. Smale: Complexity of Bezout's theorem I: Geometric aspects, J. Amer. Math. Soc. **6** (1993), 459-501

[30] M. Shub, S. Smale: 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, Birkhäuser, Basel, (1993) 267-285

[31] M. Shub, S. Smale: Complexity of Bezout's theorem III: Condition number and packing, J. of Complexity **9** (1993) 4-14

[32] M. Shub, S. Smale: Complexity of Bezout's theorem IV: Probability of Success, Extensions, SIAM J. Numer. Anal. to appear

[33] M. Shub, S. Smale: Complexity of Bezout's theorem V: Polynomial time, Theoretical Comp. Sci. **133** (1994)

[34] M. Shub, S. Smale: On the intractability of Hilbert's Nullstellensatz and an algebraic version of NP $\neq$ P?, IBM Research Report, Yorktown Heights (1994)

[35] P. Solernó: Complejidad de conjuntos semialgebraicos. Thesis Univ. de Buenos Aires (1989)

[36] V. Strassen: Vermeidung von Divisionen, Crelle J. Reine Angew. Math. **264** (1973) 184-202.