JOURNAL OF COMPLEXITY 11, 174–193 (1995)

Complexity of Finding Irreducible Components of a Semialgebraic Set

ANDRÉ GALLIGO*

Laboratoire de Mathématiques, URA CNRS et l'Université de Nice - Sophia Antipolis, Park Valrose, 06108-Nice Cedex-02, France

AND

NICOLAI VOROBJOV

Steklov Mathematical Institute at St. Petersburg, Russia; and Departments of Mathematics and Computer Science, Pennsylvania State University, University Park, Pennsylvania 16802

Received June 2, 1994

Let $W \subset \mathbf{R}^n$ be a semialgebraic set defined by a quantifier-free formula with k atomic polynomials of the kind $f \in \mathbf{Z}[X_1, \ldots, X_n]$ such that $\deg_{X_1,\ldots,X_n}(f) < d$ and the absolute values of coefficients of f are less than 2^M for some positive integers d, M. An algorithm is proposed for producing the complexification, Zariski closure, and also for finding all irreducible components of W. The running time of the algorithm is bounded from above by $M^{O(1)}(kd)^{n^{O(1)}}$. The procedure is applied to computing a Whitney system for a semialgebraic set and the real radical of a polynomial ideal. © 1995 Academic Press, Inc.

INTRODUCTION

Consider a semialgebraic set W determined by a Boolean combination of k atomic subformulas of the form $f > 0$ or $f = 0$, where the polynomials $f \in \mathbf{Z}[X_1, \ldots, X_n]$, the degrees $\deg_{X_1,\ldots,X_n}(f) < d$, and the maxima of bit lengths of coefficients $l(f) < M$.

Let $\mathbf{F}$ be a subfield of $\mathbf{R}$. The family of all real algebraic varieties defined by polynomials with coefficients in $\mathbf{F}$ defines a Zariski topology on $\mathbf{R}^n$

* Partially supported by EC ESPRIT-BRA project 6846 (POSSO).

0885-064X/95 $6.00

which induces a topology on any subset of $\mathbf{R}^n$, in particular, on any semialgebraic subset.

Let $V = \overline{W} \subset \mathbf{R}^n$ denote the Zariski closure of W in $\mathbf{R}^n$. Note that V actually depends on a choice of a subfield $\mathbf{F}$ and is the smallest real algebraic variety containing W defined by equations with coefficients from $\mathbf{F}$.

Let $V_{\mathbf{C}} \subset \mathbf{C}^n$ be the complexification of W (the smallest *complex* algebraic variety containing W).

A semialgebraic set $U \subset \mathbf{R}^n$ is called irreducible (*over* a subfield $\mathbf{F} \subset \mathbf{R}$ *in* the space $\mathbf{R}^n$) if a representation $U = U_1 \cup U_2$, where U_1, U_2 are Zariski closed subsets *in* U (i.e., w.r.t. Zariski topology induced on U, these subsets are semialgebraic), implies either $U = U_1$ or $U = U_2$. Note, that, unlike the case of complex algebraic varieties, an irreducible real variety is not necessarilly connected w.r.t. Euclidean topology on $\mathbf{R}^n$ or equidimensional.

Obviously U is irreducible iff its Zariski closure $\overline{U}$ is irreducible. Relations between irreducibility in $\mathbf{R}^n$ and in $\mathbf{C}^n$ can be illustrated by the following example.

EXAMPLE. The polynomial $f = (X^2 - 1)^2 + (Y - 1)^2$ is irreducible over $\mathbf{Q}$. Hence (see, e.g., Shafarevich, 1974) the complex variety (curve) $\{f = 0\}_{\mathbf{C}} \subset \mathbf{C}^2$ is irreducible over $\mathbf{Q}$ in $\mathbf{C}^2$. On the other hand, the real variety

$$\{f = 0\}_{\mathbf{R}} = \{f = 0\}_{\mathbf{C}} \cap \mathbf{R}^2 = \{X = 1 \ \& \ Y = 1\} \cup \{X = -1 \ \& \ Y = 1\}$$

consists of two zero-dimensional components irreducible over $\mathbf{Q}$ in $\mathbf{R}^2$.

The curve $\{f = 0\}_{\mathbf{C}}$ is *reducible* over the field of complex algebraic numbers $\mathbf{C}_{\text{alg}}$ in $\mathbf{C}^2$ and consists of two one-dimensional components:

$$\{f = 0\}_{\mathbf{C}} = \{X^2 - 1 + \sqrt{-1}(Y - 1) = 0\} \cup \{X^2 - 1 - \sqrt{-1}(Y - 1) = 0\};$$

for each of them its intersection with $\mathbf{R}^2$ is $\{f = 0\}_{\mathbf{R}}$.

The semialgebraic set $W \subset \mathbf{R}^n$ is uniquely representable as a union

$$W = \bigcup_{1 \le i \le s} W_i$$

of its irreducible over $\mathbf{F}$ in $\mathbf{R}^n$ components, i.e., semialgebraic subsets $W_1, \ldots, W_s$ such that:

(1) every W_i, $1 \le i \le s$, is Zariski closed in W and irreducible over $\mathbf{F}$ in $\mathbf{R}^n$;

(2) $W_i \not\subset \bigcup_{j \ne i} W_j$ for $1 \le i \le s$

(see, e.g., Hartshorn, 1977).

Note that if

$$V = \overline{W} = \bigcup_{1 \le i \le s_1} V_i$$

is a decomposition of the Zariski closure V into its irreducible components then $s_1 = s$ and $W_i = V_i \cap W$.

For the semialgebraic set $W \subset \mathbf{R}^n$ the *Krull dimension* is the maximal number p such that there exists a sequence

$$W_1 \subset W_2 \subset \cdots \subset W_{p+1}$$

of distinct irreducible Zariski-closed in W semialgebraic subsets of W. For a sequence of maximal length this definition implies that the Krull dimension of W_i is $i - 1$ for each $1 \le i \le p + 1$.

The *Euclidean dimension* of W is the maximum among the dimensions of coordinate subspaces of $\mathbf{R}^n$ such that the projections of W on them contain open balls in these subspaces.

For the semialgebraic set W its Krull and Euclidean dimensions coincide (Bochnak *et al.*, 1987); we shall denote them both by $\dim_{\mathbf{R}}(W)$.

The (Krull) dimension of a complex algebraic variety $U_{\mathbf{C}}$ in $\mathbf{C}^n$ will be denoted by $\dim_{\mathbf{C}}(U_{\mathbf{C}})$.

The *theorem on the dimension of intersection* is valid which implies that for two Zariski closed in W irreducible subsets W_1, W_2 of $W \subset \mathbf{R}^n$, either

$$\dim_{\mathbf{R}}(W_1 \cap W_2) < \min\{\dim_{\mathbf{R}}(W_1), \dim_{\mathbf{R}}(W_2)\},$$

or $W_1 \subset W_2$, or $W_2 \subset W_1$.

Let $B_a(b)$, with $a \in \mathbf{R}^n$, $0 < b \in \mathbf{R}$, denote an open ball centered at a with radius b.

For a point $x \in W$ denote by $\dim_{\mathbf{R}}(x, W)$ the dimension of $W \cap B_x(r)$ for all sufficiently small $r > 0$.

For an integer $p > 0$ consider the subset of all points $x \in W$ such that $\dim_{\mathbf{R}}(x, W) \le p$. If this subset has the dimension p then denote it by $W^{(p)}$ (hence, in particular, $W^{(m)} = W$, where $m = \dim_{\mathbf{R}}(W)$).

Irreducible over a field $\mathbf{F}$ in $\mathbf{R}^n$ components of semialgebraic sets $W^{(p)}$ for all $0 \le p \le \dim_{\mathbf{R}}(W)$ can be arranged in the form of an oriented acyclic *component graph*. Recall that a vertex A in an oriented graph is called *adjacent to* a vertex B if there is an edge of the graph passing from B to A. The vertices of the component graph are all the components. Vertex $W_i^{(p)}$ with $\dim_{\mathbf{R}}(W_i^{(p)}) = p$, $0 \le p \le \dim_{\mathbf{R}}(W)$, is adjacent to a vertex $W_j^{(l)}$ with $\dim_{\mathbf{R}}(W_j^{(l)}) = l$, $0 < l \le \dim_{\mathbf{R}}(W)$, iff $W_i^{(p)} \subset W_j^{(l)}$ and there is no l', with

$p < l' < l$, and j' such that $W_i^{(p)} \subset W_{j'}^{(l')} \subset W_j^{(l)}$ (note that in this case $p < l$).

It follows that the irreducible components of W are all the vertices in component graph each of which is not adjacent to another vertex.

EXAMPLES. (1) The elliptic curve $W = W^{(1)} = \{Y^2 = X^2(X - 1)\}$ is irreducible over $\mathbf{R}$ in $\mathbf{R}^2$. The set $W^{(0)}$ is the isolated point, therefore it is irreducible and it is the only vertex adjacent to $W^{(1)}$ in the corresponding component graph.

(2) The *Whitney umbrella* $W = W^{(2)} = \{Z^2X = Y^2\}$ is irreducible over $\mathbf{R}$ in $\mathbf{R}^3$. The line $W^{(1)} = \{Z = Y = 0\}$ is irreducible and is the only vertex adjacent to $W^{(2)}$ in the component graph.

Let $\mathbf{R}_{\text{alg}}$ denote the field of all real algebraic numbers.

We shall construct an algorithm which for a given semialgebraic set W produces its component graph (with respect to components irreducible over $\mathbf{R}_{\text{alg}}$ in $\mathbf{R}^n$). Moreover, for each vertex $W_i^{(p)}$ of this graph the algorithm finds the complexification $V_{i\mathbf{C}}^{(p)}$ and the Zariski closure $\overline{W_i^{(p)}}$.

Every component $W_i^{(p)}$ is presented in a form

$$W_i^{(p)} = W \cap \{g_{i1}^{(p)} = \cdots = g_{il}^{(p)} = 0\},$$

where

$$g_{ij}^{(p)} \in \mathbf{R}_{\text{alg}}[X_1, \ldots, X_n],$$
$$\deg_{X_1,\ldots,X_n}(g_{ij}^{(p)}) < (kd)^{n^{O(1)}}, \qquad 1 \le j \le l,$$
$$1 \le i, l < (kd)^{n^{O(1)}}, \qquad 0 \le p \le \dim_{\mathbf{R}}(W).$$

The complexification $V_{i\mathbf{C}}^{(p)}$ (respectively Zariski closure $\overline{W_i^{(p)}}$) of $W_i^{(p)}$ is defined in $\mathbf{C}^n$ (respectively in $\mathbf{R}^n$) by the same system of equations

$$g_{i1}^{(p)} = \cdots = g_{il}^{(p)} = 0.$$

Real algebraic coefficients of a polynomial $g_{ij}^{(p)}$ are given in the following way. The algorithm produces an irreducible over $\mathbf{Q}$ polynomial $\Phi_{ij}^{(p)} \in \mathbf{Z}[Z]$, together with the sequence of signs of its derivatives of all orders, which (by Thom's lemma, Bochnak *et al.*, 1987) defines the unique real root $\theta = \theta_{ij}^{(p)}$ of $\Phi_{ij}^{(p)}$. Furthermore, the algorithm outputs the expressions

$$\xi_\alpha = \sum_{0 \le \beta < \deg_Z(\Phi_{ij}^{(p)})} a_{\alpha,\beta} Z^\beta, \tag{1}$$

$a_{\alpha,\beta} \in \mathbf{Q}$ for all coefficients (indexed by α) of $g_{ij}^{(p)}$. The coefficient with

index α is equal to ξ_α after substituting the root θ in (1) instead of the variable Z.

Also the following bounds hold:

$$\deg_Z(\Phi_{ij}^{(p)}) < (kd)^{n^{O(1)}};$$
$$l(\Phi_{ij}^{(p)}),\ l(a_{\alpha,\beta}) < M^{O(1)}(kd)^{n^{O(1)}}.$$

The running time of the algorithm is polynomial in M, $(kd)^{n^{O(1)}}$.

Remarks. (1) The algorithm can find components of $W^{(p)}$ irreducible over $\mathbf{Q}$ in $\mathbf{R}^n$, then the corresponding polynomials $g_{ij}^{(p)} \in \mathbf{Z}[X_1, \ldots, X_n]$ and $l(g_{ij}^{(p)}) < M^{O(1)}(kd)^{n^{O(1)}}$.

(2) Using the algorithm as a subroutine one can also find complexifications and Zariski closures of the sets $W^{(p)}$, $0 \le p \le \dim_{\mathbf{R}}(W)$, in particular, of the input set W (see Section 4 below). This implies an effective method for deciding whether a given semialgebraic set is, in fact, a real algebraic variety (i.e., can be defined by a system of polynomial *equations*) by comparing the set with its Zariski closure in $\mathbf{R}^n$.

(3) If the input set W is actually a variety, given by a system of k equations, then all the bounds depend only polynomially on k.

A special case of a problem (real planar curves) was considered in Kaltofen (1990), where a polynomial time algorithm for producing real algebraic components was constructed. Our general plan will be as follows.

The algorithm constructs the component graph for W using the recursion on p, beginning with $p = \dim_{\mathbf{R}}(W) = m$.

Suppose that $\dim_{\mathbf{R}}(W) = m \le n - 1$ (the case $m = n$ is trivial).

We start with constructing a system of polynomial equations with integer coefficients which defines:

- in $\mathbf{R}^n$: a real algebraic variety $V^{(1)}$ containing the Zariski closure $\overline{W}$ of W in $\mathbf{R}^n$ with

$$\dim_{\mathbf{R}}(V^{(1)}) = \dim_{\mathbf{R}}(\overline{W}) = m;$$

- in $\mathbf{C}^n$: a complex algebraic variety $V_{\mathbf{C}}^{(1)}$, such that for every irreducible over the field $\mathbf{C}_{\text{alg}}$ (of all complex algebraic numbers) in $\mathbf{C}^n$ component $U_{\mathbf{C}}$ of $V_{\mathbf{C}}^{(1)}$ with $\dim_{\mathbf{R}}(U_{\mathbf{C}} \cap \mathbf{R}^n) = m$, the dimension $\dim_{\mathbf{C}}(U_{\mathbf{C}}) = m$.

We shall prove that each m-dimensional irreducible component U of $\overline{W}$ is contained in a complex component of the kind $U_{\mathbf{C}}$ which turns out to be the complexification of U, in particular, $U = U_{\mathbf{C}} \cap \mathbf{R}^n$. After that the fundamental procedure from Chistov (1984) and Grigoriev (1984) for finding all complex components can be used to produce $U_{\mathbf{C}}$ and, therefore, U.

In order to find all the vertices of the component graph we shall first define the subset $W^{(p)}$ by a formula of first-order theory of $\mathbf{R}$ (with quantifers). Eliminating quantifiers, we reduce the problem to the case of the components of the maximal dimension.

1. Preliminaries

We start with formulating some propositions describing the fundamental procedures used as subroutines in our algorithm.

Proposition 1 (Heintz *et al.*, 1990; Renegar, 1992). *Let Π be a formula of the first-order theory of reals in the prenex form, with q quantifier alternations, and the quantifier-free part in a disjunctive normal form, having r atomic subformulas of the kind $h \geq 0$, where $h \in \mathbf{Z}[Y_1, \ldots, Y_s]$, $\deg_{Y_1,\ldots,Y_s}(h) < t$, $l(h) < N$, for some positive integers q, r, s, t, N. Let $Y_1, \ldots, Y_{s_1}$, $0 \leq s_1 \leq s$ be free variables (i.e., variables not affected by quantifiers). There is an algorithm which for a given Π outputs a quantifier-free formula Π_1 equivalent to Π (i.e., $\{\Pi_1\} = \{\Pi\}$). The atomic subformulas of Π_1 are of the kind $h_1 \geq 0$, where $h_1 \in \mathbf{Z}[Y_1, \ldots, Y_{s_1}]$, $\deg_{Y_1,\ldots,Y_{s_1}}(h_1) < (rt)^{s^{O(q)}}$, $l(h_1) < N^{O(1)}(rt)^{s^{O(q)}}$, and the number of subformulas does not exceed $(rt)^{s^{O(q)}}$. The running time of the procedure is less than $N^{O(1)}(rt)^{s^{O(q)}}$.*

Remark. Renegar (1992) gives a more precise description of the bounds. The most important particular case of the Proposition 1 (for $s_1 = 0$), which is a principal step in the whole procedure, was proved earlier by Grigoriev (1988).

Let a polynomial $h \in \mathbf{C}_{\text{alg}}[Y_1, \ldots, Y_s]$. We say that h is given in a *standard representation* with the *degree* t and the *bit length* N for some positive integers t, N, if the following data is provided:

(i) a polynomial $\Phi \in \mathbf{Z}[Z]$, where Z is a new variable;

(ii) a polynomial $\tilde{h} \in \mathbf{Z}[Z][Y_1, \ldots, Y_s]$, where each coefficient from $\mathbf{Z}[Z]$ is of the kind

$$\xi_\eta = \sum_{0 \leq \mu < \deg(\Phi)} \beta_{\eta\mu} Z^\mu, \tag{2}$$

with $1 \leq \eta \leq (\deg_{Y_1,\ldots,Y_s}(\tilde{h}))^s$.

Here $\max\{\deg_{Y_1,\ldots,Y_s}(\tilde{h}), \deg(\Phi)\} = t$, and $\max\{\text{bit lengths of } \beta_{\eta\mu}, l(\Phi)\} = N$. The polynomial h is the result of substitution of a certain root of the equation $\Phi = 0$, instead of variable Z in each expression (2) for all η.

PROPOSITION 2 (Chistov, 1984; Grigoriev, 1984). *Consider a complex algebraic variety*

$$\mathcal{V} = \{h_1 = \cdots = h_r = 0\} \subset \mathbf{C}^s$$

with $h_i \in \mathbf{Z}[Y_1, \ldots, Y_s]$, $\deg_{Y_1,\ldots,Y_s}(h_i) < t$, $l(h_i) < N$, $1 \le i \le r$ *for some positive integers* r, s, t, N.

There is an algorithm which for a given $\mathcal{V}$ *outputs all its irreducible over* $\mathbf{C}_{\text{alg}}$ *in* $\mathbf{C}$ *components* $\mathcal{V}_1, \ldots, \mathcal{V}_q$. *The number of the components* $q \le t^s$ *(by Bézout's theorem). Each component* $\mathcal{V}_j$, $1 \le j \le q$, *is represented by its generic point (in particular the dimension value is assigned to* $\mathcal{V}_j$*), and by a system of equations*:

$$\tilde{h}_{j1} = \cdots = \tilde{h}_{jl_j} = 0,$$

with $l_j < (rt)^{s^{O(1)}}$, *and every* $\tilde{h}_{j\nu} \in \mathbf{C}_{\text{alg}}[Z_j][Y_1, \ldots, Y_s]$ *is given in a standard representation with the degree* $t^{O(s)}$ *and the bit length* $(rN)^{O(1)}t^{O(s^2)}$ *for* $1 \le l \le q$, $1 \le \nu \le l_j$.

The running time of the algorithm is less than $(rN)^{O(1)}t^{O(s^2)}$.

Remark. The procedures from Chistov (1984) and Grigoriev (1984) are actually valid for more general classes of the input systems.

PROPOSITION 3 (Chistov, 1984; Grigoriev, 1984; Rannou, 1993). *Let* $\mathcal{V}_1, \ldots, \mathcal{V}_q \subset \mathbf{C}^s$ *be complex algebraic varieties defined by systems of equations*:

$$\mathcal{V}_j = \{h_{j1} = \cdots = h_{jl_j} = 0\},$$

with $1 \le j \le q$, $h_{j\nu} \in \mathbf{R}_{\text{alg}}[Y_1, \ldots, Y_s]$, $1 \le \nu \le l_j$, *and each* $h_{j\nu}$ *is given in a standard representation with the degree* t *and the bit length* N. *Let* $\sum_{1 \le j \le q} l_j = L$. *There is an algorithm which for a given* $\mathcal{V}_1, \ldots, \mathcal{V}_q$ *outputs polynomials* $h_1, \ldots, h_r \in \mathbf{R}_{\text{alg}}[Y_1, \ldots, Y_s]$ *such that*

$$\bigcup_{1 \le j \le q} \mathcal{V}_j = \{h_1 = \cdots = h_r = 0\} \subset \mathbf{C}^s.$$

The number of equations $r \le t^s$, *each* h_j, $1 \le j \le r$, *is given in a standard representation with the degree* $t^{O(s)}$, *and the bit length* $(LN)^{O(1)}t^{O(s)}$. *The running time of the algorithm is less than* $(LN)^{O(1)}t^{O(s)}$.

Remark. This proposition is rather elementary; it appears in Chistov (1984) and Grigoriev (1984) implicitly and for more general classes of input systems.

PROPOSITION 4 (Krick and Logar, 1991). *Let $I = (h_1, \ldots, h_r)$ be a polynomial ideal of the dimension p, where each $h_i \in \mathbf{R}_{alg}[Y_1, \ldots, Y_s]$ is given in a standard representation with the degree t and the bit length N, $1 \le i \le r$. There is an algorithm which for a given $h_1, \ldots, h_r$ outputs the family $\tilde{h}_1, \ldots, \tilde{h}_l \in \mathbf{R}_{alg}[Y_1, \ldots, Y_s]$ of generators of the radical $\sqrt{I}$ of I (see the definition in Section 7). The number of generators $l < r^{O(1)}t^{s^{pO(1)}}$ and each $\tilde{h}_j$ is given in a standard representation with the degree $t^{s^{pO(1)}}$ and the bit length $(Nr)^{O(1)}t^{s^{pO(1)}}$. The running time of the algorithm is less than $(Nr)^{O(1)}t^{s^{pO(1)}}$.*

Remark. Note that the bounds for the output in Proposition 4 are doubly exponential in the dimension of the ideal, i.e., in the number of variables in the worst case, in contrast to singly exponential bounds in the previous propositions. This is, in a certain sense, related to a lower bound of Mayr and Meyer (1982).

2. COMPLEXIFICATIONS OF MAXIMAL IRREDUCIBLE COMPONENTS

Let, as before, $\dim_{\mathbf{R}}(W) = m$. This can be computed algorithmically by using Proposition 1. The algorithm starts by looking through all the m-dimensional coordinate subspaces of $\mathbf{R}^n$.

Let the current subspace have coordinates $X_1, \ldots, X_m$ (in case $m = 0$ assume that this list is empty). The algorithm writes out a formula (with quantifiers) of first-order theory of reals defining the subset $W_{0,1,\ldots,m}$ of all points x of W such that under the projection map

$$\pi_0 : \mathbf{R}^n \to \mathbf{R}^m,$$

$$\pi_0(X_1, \ldots, X_n) = (X_1, \ldots, X_m)$$

the image of a neighborhood of x in W has the dimension m.

Let

$$\pi_i : \mathbf{R}^n \to \mathbf{R}^{m+1}$$

$$\pi_i(X_1, \ldots, X_n) = (X_1, \ldots, X_m, X_i)$$

for $m + 1 \le i \le n$. Note that $\dim_{\mathbf{R}}(\pi_i(W_{0,1,\ldots,m})) = m$ for each i.

The algorithm, using the quantifier elimination procedure from Proposition 1, produces all projections $\pi_i(W_{0,1,\ldots,m})$, $m + 1 \le i \le n$, as quantifier-free formulas in the disjunctive normal form with atomic subformulas of the kind $\tilde{f} > 0$ or $\tilde{f} = 0$ for some $\tilde{f} \in \mathbf{Z}[X_1, \ldots, X_m, X_i]$. Deleting all (strict) inequalities in the formula defining $\pi_i(W_{0,1,\ldots,m})$, taking the sum of the squares in the disjunction members and multiplying these sums, we

obtain in $\mathbf{R}^{m+1}$ the real algebraic hypersurface $\{g_i = 0\} \subset \mathbf{R}^{m+1}$, containing $\pi_i(W_{0,1,\ldots,m})$, with $g_i \in \mathbf{Z}[X_1, \ldots, X_m, X_i]$. Set

$$V^{(1)}_{0,1,\ldots,m} = \{g_{m+1} = \cdots = g_n = 0\} \subset \mathbf{R}^n.$$

Obviously, $W_{0,1,\ldots,m} \subset V^{(1)}_{0,1,\ldots,m}$.

For a semialgebraic set U a point $x \in U$ is called *smooth in* U if a neighborhood of x in U is a smooth manifold.

LEMMA 1. *On $W_{0,1,\ldots,m}$ the hypersurfaces $\{g_i = 0\} \subset \mathbf{R}^n$, $m + 1 \le i \le n$, intersect transversally (i.e., at every point of a Zariski open in $W_{0,1,\ldots,m}$ subset of $W_{0,1,\ldots,m}$ the $n - m$ normal vectors to hypersurfaces $\{g_i = 0\}$, respectively, are linearly independent).*

Proof. First we prove that the subset $S \subset W_{0,1,\ldots,m}$ of points $x \in W_{0,1,\ldots,m}$ such that for some $m + 1 \le i \le n$ the point x is nonsmooth in $\{g_i = 0\}$, has the dimension $\dim_{\mathbf{R}}(S) < \dim_{\mathbf{R}}(W_{0,1,\ldots,m}) = m$. Indeed, otherwise, for a certain i, a semialgebraic subset S_i of nonsmooth points of $\{g_i = 0\} \subset \mathbf{R}^n$, contained in $W_{0,1,\ldots,m}$, would have the dimension $\dim_{\mathbf{R}}(S_i) = \dim_{\mathbf{R}}(W_{0,1,\ldots,m}) = m$. It follows that there exists a (smooth in S_i) point $z \in S_i$ such that an m-dimensional neighborhood $\mathfrak{Z}$ of z in S_i coincides with a neighborhood of z in $W_{0,1,\ldots,m}$. According to the definition of $W_{0,1,\ldots,m}$, the dimension $\dim_{\mathbf{R}}(\pi_i(\mathfrak{Z})) = m$. On the other hand, the hypersurface $\{g_i = 0\}$ in the space $\mathbf{R}^n$ is the cylinder over

$$G = \{g_i = 0\} \cap \{X_{m+1} = \cdots = X_{i-1} = X_{i+1} = \cdots = X_n = 0\};$$

therefore S_i is the intersection of the cylinder over nonsmooth points of G with $W_{0,1,\ldots,m}$. In particular, $\pi_i(S_i)$ is contained in the set of all nonsmooth (in G) points of G. It follows that

$$\dim_{\mathbf{R}}(\pi_i(S_i)) < m;$$

i.e.,

$$\dim_{\mathbf{R}}(\pi_i(S_i)) < \dim_{\mathbf{R}}(\pi_i(\mathfrak{Z})).$$

This contradicts the inclusion $\mathfrak{Z} \subset S_i$.

Because $\{g_i = 0\} \subset \mathbf{R}^n$ is the cylinder over G, at each point $w \in W_{0,1,\ldots,m} \backslash S$, every normal vector $\alpha^{(i)}(w)$, $m + 1 \le i \le n$ to $\{g_i = 0\} \subset \mathbf{R}^n$ is collinear to the subspace of coordinates $X_1, \ldots, X_m, X_i$. By the definition of $W_{0,1,\ldots,m}$ and Sard's theorem, applied to the projections,

$$(X_1, \ldots, X_m, X_i) \mapsto (X_1, \ldots, X_m),$$

the subset $T \subset W_{0,1,\ldots,m} \backslash S$ of points $x \in W_{0,1,\ldots,m}$, such that for some $m + 1 \leq i \leq n$ the vector $\alpha^{(i)}(x)$ has a zero projection on the axis X_i, is of the dimension $\dim_{\mathbf{R}}(T) < \dim_{\mathbf{R}}(W_{0,1,\ldots,m}) = m$. It follows that for each point $w \in W_{0,1,\ldots,m} \backslash (S \cup T)$ and each $m + 1 \leq i \leq n$ the vector $\alpha^{(i)}(w)$ is of the kind

$$(\alpha_m^{(i)}(w), 0, \ldots, 0, a_i(w), 0, \ldots, 0),$$

where $\alpha_m^{(i)}(w)$ is an m-vector and $0 \neq a_i(w) \in \mathbf{R}$ is X_i-coordinate. Besides, $\dim_{\mathbf{R}}(\overline{S \cup T}) = \dim_{\mathbf{R}}(S \cup T) < m$. Therefore, the vectors $\alpha^{(i)}(w)$, $m + 1 \leq i \leq n$ are linearly independent for each w in a Zariski open in $W_{0,1,\ldots,m}$ subset of $W_{0,1,\ldots,m}$. ■

Denote by $V_{\mathbf{C}}^{(1)}$ a complex variety defined in $\mathbf{C}^n$ by the same system

$$g_{m+1} = \cdots = g_n = 0$$

as $V_{0,1,\ldots,m}^{(1)}$. It contains $W_{0,1,\ldots,m}$.

LEMMA 2. *For every irreducible over* $\mathbf{C}_{\text{alg}}$ *in* $\mathbf{C}^n$ *component* $U_{\mathbf{C}}$ *of* $V_{\mathbf{C}}^{(1)}$ *such that* $\dim_{\mathbf{R}}(U_{\mathbf{C}} \cap W_{0,1,\ldots,m}) = m$, *the dimension* $\dim_{\mathbf{C}}(U_{\mathbf{C}}) = m$. *Each component* U *of the Zariski closure* $\overline{W}_{0,1,\ldots,m}$ *lies in an* m*-dimensional component* $U_{\mathbf{C}}$ *of* $V_{\mathbf{C}}^{(1)}$.

Proof. Because it can happen that $\operatorname{grad}(g_i) \equiv 0$ on $\{g_i = 0\}$ for some $m \leq i \leq n$, replace, in the system for $V_{\mathbf{C}}^{(1)}$, every polynomial g_i, $m + 1 \leq i \leq n$, by its square-free part $\tilde{g}_i$. Then, according to Lemma 1, at every point of a Zariski open in $W_{0,1,\ldots,m}$ subset of $W_{0,1,\ldots,m}$ the rank of the Jacobian matrix

$$\left(\frac{\partial \tilde{g}_i}{\partial X_j}\right)_{m+1 \leq i \leq n; 1 \leq j \leq n}$$

is maximal. Hence, there exists a point $x \in U_{\mathbf{C}}$ such that at x the matrix has rank $n - m$. It follows (see, e.g., Shafarevich, 1974) that $\dim_{\mathbf{C}}(U_{\mathbf{C}}) = m$.

Denote by $\mathfrak{U}$ the family of all components $U_{\mathbf{C}}$ such that $\dim_{\mathbf{R}}(U_{\mathbf{C}} \cap W_{0,1,\ldots,m}) = m$. Obviously,

$$\overline{W}_{0,1,\ldots,m} \subset \bigcup_{U_{\mathbf{C}} \in \mathfrak{U}} U_{\mathbf{C}}.$$

Now let U be a component of $\overline{W}_{0,1,\ldots,m}$ (then $\dim_{\mathbf{R}}(U) = m$). Observe that the intersection of a complex algebraic variety (defined by a system of equations with complex coefficients) with the space $\mathbf{R}^n$ is a real alge-

braic variety definable by a system of equations with real coefficients. This can be shown by passing to real and imaginary parts of the complex system. It follows that there exists a component $U_{\mathbf{C}} \in \mathcal{U}$ such that $U \subset U_{\mathbf{C}}$. ■

Now we shall prove that for U and $U_{\mathbf{C}}$ from Lemma 2, U is actually the only component of $\overline{W}_{0,1,\ldots,m}$ contained in $U_{\mathbf{C}}$.

LEMMA 3. $U = U_{\mathbf{C}} \cap \mathbf{R}^n$; *i.e.*, $U_{\mathbf{C}}$ *is the complexification of* U.

Proof. Suppose that there is another irreducible in $\mathbf{R}^n$ component $U' \neq U$ of $\overline{W}_{0,1,\ldots,m}$ such that $U' \subset U_{\mathbf{C}} \cap \mathbf{R}^n$. Let $U = \{g = 0\} \subset \mathbf{R}^n$ for a polynomial $g \in \mathbf{R}_{\text{alg}}[X_1, \ldots, X_n]$. The equation $g = 0$ defines a hypersurface in $\mathbf{C}^n$ and by the dimension of intersection theorem (see, e.g., Shafarevich, 1974) either $U_{\mathbf{C}} \cap \{g = 0\} \subset \mathbf{C}^n$ or $\dim_{\mathbf{C}}(U_{\mathbf{C}} \cap \{g = 0\}) < m$. The first alternative contradicts the existence of U', the second contradicts the dimension of U. ■

LEMMA 4 (cf. Whitney, 1957, Lemma 6). $U_{\mathbf{C}}$ *from Lemma* 3 *can be defined by a system of equations with coefficients in* $\mathbf{R}_{\text{alg}}$.

Proof. Let $U_{\mathbf{C}}$ be defined in $\mathbf{C}^n$ by a system of equations,

$$g_1 = \cdots = g_t = 0,$$

where $g_i \in \mathbf{C}_{\text{alg}}[X_1, \ldots, X_n]$. Consider the variety

$$\hat{U}_{\mathbf{C}} = \{\hat{g}_1 = \cdots = \hat{g}_t = 0\} \subset \mathbf{C}^n,$$

where $\hat{g}_i \in \mathbf{C}_{\text{alg}}[X_1, \ldots, X_n]$, $1 \leq i \leq t$, is obtained from g_i by replacing each coefficient by the complex conjugate. Then $U = U_{\mathbf{C}} \cap \mathbf{R}^n = \hat{U}_{\mathbf{C}} \cap \mathbf{R}^n$, since a polynomial with real coefficients has pairwise conjugate complex roots.

Suppose that $U_{\mathbf{C}} \neq \hat{U}_{\mathbf{C}}^{(1)}$ for every irreducible over $\mathbf{C}_{\text{alg}}$ in $\mathbf{C}^n$ component $\hat{U}_{\mathbf{C}}^{(1)}$ of $\hat{U}_{\mathbf{C}}$. Then, by the dimension of intersection theorem (see, e.g., Shafarevich, 1974),

$$\dim_{\mathbf{C}}(U_{\mathbf{C}} \cap \hat{U}_{\mathbf{C}}^{(1)}) < m,$$

this contradicts the assumption that $\dim_{\mathbf{R}}(U) = m$. Thus, $U_{\mathbf{C}}$ coincides with some component $\hat{U}_{\mathbf{C}}^{(1)}$ of $\hat{U}_{\mathbf{C}}$.

Denote by $\text{Re}(g_i)$ (respectively by $\text{Im}(g_i)$), $1 \leq i \leq t$, the polynomial obtained from g_i by replacing each coefficient by its real (respectively imaginary) part. Let us prove that

$$U_{\mathbf{C}} = \{\text{Re}(g_1) = \cdots = \text{Re}(g_t) = \text{Im}(g_1) = \cdots = \text{Im}(g_t) = 0\}.$$

The inclusion $\supset$ is obvious. Now let $x \in U_{\mathbf{C}} = \hat{U}_{\mathbf{C}}^{(1)}$. Then $g_i(x) = \hat{g}_i(x) = 0$ for all $1 \leq i \leq t$; hence

$$1/2(g_i(x) + \hat{g}_i(x)) = \mathrm{Re}(g_i(x)) = 0$$

and

$$1/2(g_i(x) - \hat{g}_i(x)) = \mathrm{Im}(g_i(x)) = 0.$$

Since $\mathrm{Re}(g_i)$, $\mathrm{Im}(g_i) \in \mathbf{R}_{\mathrm{alg}}[X_1, \ldots, X_n]$, the lemma is proved. ∎

3. Finding m-Dimensional Components

Lemmas of the previous section imply that in order to produce all irreducible over $\mathbf{R}_{\mathrm{alg}}$ in $\mathbf{R}^n$ components of $\overline{W}_{0,1,\ldots,m}$ (which are all m-dimensional) it is sufficient to perform the following steps:

(1) decompose $V_{\mathbf{C}}^{(1)}$ into its irreducible over $\mathbf{C}_{\mathrm{alg}}$ in $\mathbf{C}^n$ components;

(2) passing to real and imaginary parts in coefficients, replace them by the varieties defined by systems with *real* algebraic coefficients;

(3) choose the varieties which have m-dimensional intersections with $\mathbf{R}^n$;

(4) among the latter select these which are components of

$$\overline{W}_{0,1,\ldots,m},$$

i.e., have m-dimensional intersections with $W_{0,1,\ldots,m}$.

Now in order to find all the m-dimensional components of the Zariski closure $\overline{W}$ we first produce for all m-subsets $\mathbf{i} = \{i_1, \ldots, i_m\} \cap \{1, \ldots, n\}$ the corresponding decompositions for $\overline{W}_{0,i_1,\ldots,i_m}$:

$$\overline{W}_{0,i_1,\ldots,i_m} = \bigcup_{1 \leq j \leq s_{\mathbf{i}}} U_{\mathbf{i}}^{(j)}.$$

Here $W_{0,1,\ldots,m} = W_{\mathbf{i}}$ is the subset of all points $x \in W$ such that under the projection map

$$(X_1, \ldots, X_n) \mapsto (X_{i_1}, \ldots, X_{i_m})$$

the image of the neighborhood of x in W is m-dimensional.

LEMMA 5. *Each m-dimensional component U of $\overline{W}$ is among the irreducible varieties $U_{\mathbf{i}}^{(j)}$, $\mathbf{i} \cap \{1, \ldots, n\}$, $1 \leq j \leq s_{\mathbf{i}}$.*

Proof. Since the set of all points $x \in W$ having m-dimensional neighborhoods in W coincides with the union

$$\bigcup_i W_i,$$

the union of Zariski closures

$$\bigcup_i \overline{W}_i = \overline{\bigcup_i W_i} \subset \overline{W},$$

and, moreover, $\dim_{\mathbf{R}}(W \setminus \bigcup_i W_i) < m$; thus (Bochnak *et al.*, 1987), $\dim_r (\overline{W \setminus \bigcup_i W_i}) < m$. It follows that $\overline{W}$ is a union of m-dimensional variety $\bigcup_i W_i$ and a variety of a smaller dimension, so the sets of all m-dimensional components of $\overline{W}$ and $\overline{\bigcup_i W_i}$ coincide. ■

The decomposition of $\overline{W}$ into its irreducible components can be found by scanning the varieties $U_i^{(j)}$ one by one and deleting the duplicates.

In the remaining part of this section we shall describe the details of steps (1)–(4). The algorithm applies to the complex variety $V_{\mathbf{C}}^{(1)}$ the procedure from Proposition 2 for finding all absolutely irreducible components. This procedure for each component U_α of $V_{\mathbf{C}}^{(1)}$ outputs an irreducible over $\mathbf{Q}$ polynomial $\Psi_\alpha \in \mathbf{Z}[Z]$ and coefficients $a_l^{(\alpha,\beta)} \in \mathbf{Q}$ of the expressions

$$\xi_{\alpha,\beta}(\theta_\alpha) = \sum_{1 \le l < \deg(\Psi_\alpha)} a_l^{(\alpha,\beta)} \theta_\alpha^l,$$

where θ_α is a root of Ψ_α, and $\xi_{\alpha,\beta}$, for different β, runs over all the coefficients of all the equations, defining U_α. Thus, θ_α is a primitive element of the minimal field of definition of U_α; Ψ_α is a minimal polynomial for θ_α. Besides, the procedure from Proposition 2 can construct the generic point of U_α and, in particular, computes $\dim_{\mathbf{C}}(U_\alpha)$.

The algorithm represents the variable Z in the form $Z = Z_1 + \sqrt{-1}Z_2$, where Z_1, Z_2 are new variables, and it replaces the coefficients of the system, defining U_α by the expressions $\xi_{\alpha,\beta}(Z_1 + \sqrt{-1}Z_2)$. Let the resulting system be $g_1 = \cdots = g_t = 0$; here $g_i \in \mathbf{Q}[Z_1, \sqrt{-1}Z_2][X_1, \ldots, X_n]$, $1 \le i \le t$.

Write each coefficient of g_i in the form $p + \sqrt{-1}q$, with $p, q \in \mathbf{Q}[Z_1, Z_2]$ and denote by $\mathrm{Re}(g_i) \in \mathbf{Q}[Z_1, Z_2][X_1, \ldots, X_n]$ (respectively by $\mathrm{Im}(g_i) \in \mathbf{Q}[Z_1, Z_2][X_1, \ldots, X_n]$) the result of the replacement of each coefficient of g_i by the corresponding p (respectively by q). According to Lemma 3, for a certain fixed real root $(z_1^{(\alpha)}, z_2^{(\alpha)})$ of the equation $\Psi_\alpha(Z_1 + \sqrt{-1}Z_2) = 0$, the following holds:

$$U_\alpha = \{\mathrm{Re}(g_1) = \cdots = \mathrm{Re}(g_t) = \mathrm{Im}(g_1) = \cdots = \mathrm{Im}(g_t) = 0\}.$$

Write

$$\Psi_\alpha(Z_1 + \sqrt{-1}Z_2) = \Psi_1(Z_1, Z_2) + \sqrt{-1}\Psi_2(Z_1, Z_2).$$

Using, e.g., Grigoriev and Vorobjov (1988), the algorithm finds all the real roots of the system of equations $\Psi_1 = \Psi_2 = 0$ in two (real) variables Z_1, Z_2. Note that there are only a finite number of roots. They will be represented in the following form.

For every root (z_1, z_2) the algorithm produces an irreducible over $\mathbf{Q}$ polynomial $\Phi \in \mathbf{Z}[Y]$, together with the sequence of signs of its derivatives of all orders, which defines the unique real root θ of Φ. Also there are constructed the expressions

$$z_j = \sum_{1 \le l < \deg(\phi)} c_l^{(j)} \theta^l, \qquad c_l^{(j)} \in \mathbf{Q}, j = 1, 2.$$

Let $\tilde{g}_i$ for $1 \le i \le t$ (respectively for $t + 1 \le i \le 2t$) be the result of the substitution

$$Z_1 = \sum_{1 \le l < \deg(\phi)} c_l^{(1)} Z^l, \qquad Z_2 = \sum_{1 \le l < \deg(\phi)} c_l^{(2)} Z^l$$

into $\mathrm{Re}(g_i)$ (respectively into $\mathrm{Im}(g_i) \in \mathbf{Q}[Z_1, Z_2][X_1, \ldots, X_n]$).

Let $\theta^{(\alpha)}$ be the root of Φ corresponding to $(z_1^{(\alpha)}, z_2^{(\alpha)})$. Then, for the specification $\theta^{(\alpha)}$ of the variable Z, the system $\tilde{g}_1 = \cdots = \tilde{g}_{2t} = 0$ defines the component $U_\alpha \subset \mathbf{C}^n$. Thus, steps (1) and (2) are done.

Observe that the property of the component U_α to have an m-dimensional intersection with $\mathbf{R}^n$ can be expressed by a formula (with quantifiers) of the first-order theory of reals. The algorithm selects the components having m-dimensional intersections with $\mathbf{R}^n$ by using the decision procedure in this theory from Proposition 1. The same procedure is applied to perform step (4) (in fact, both steps (3) and (4) can be done simultaneously by a single application of quantifier elimination).

4. Constructing Component Graph

The algorithm constructs the component graph using a recursion on decreasing p. The base of the recursion, for $p = m$, is done in Section 3, where all the m-dimensional components of $W^{(m)}$ are produced.

Assume that the algorithm has produced all the l-dimensional irreducible components of $W^{(l)}$ for all l, $p < l \le m$, and also established the adjacency relations between these components.

The algorithm writes out a formula of the first-order theory of reals (with a constant number of quantifiers) defining $W^{(p)}$. Using the quantifier elimination process from Proposition 1, the algorithm finds a quantifier-free formula for $W^{(p)}$ and checks whether $W^{(p)}$ is empty. If $W^{(p)} = \varnothing$, then the algorithm passes to the next recursion step, else it produces (as in Section 3) all the p-dimensional components of $W^{(p)}$.

Let $W_i^{(p)}$ be such a component. Because the algorithm has already constructed all the irreducible components of $W^{(t)}$ (for all $t > p$), a decision procedure of Proposition 1 allows us to decide whether there exists a component $W_j^{(l)}$ $p < l$ of $W^{(l)}$ such that $W_i^{(p)} \subset W_j^{(l)}$ and there is no intermediate component $W_{i'}^{(p')}$ of $W^{(p')}$, $j < p' < l$, with $W_i^{(p)} \subset W_{i'}^{(p')} \subset W_j^{(l)}$. If not, the set $W_i^{(p)}$ is a p-dimensional component of W and is not adjacent to any vertex of the component graph. If yes, $W_i^{(p)}$ is adjacent to $W_j^{(l)}$.

In the process of constructing $W_i^{(p)}$ the algorithm also produces the complexification and the Zariski closure of $W_i^{(p)}$ (see Section 2). Using Proposition 3, it can also produce the complexifaction and the Zariski closure of $W^{(t)}$ (each defined by a single system of equations) for all t, $0 \leq t \leq n$.

5. The Complexity Analysis

The estimations of the running time of the algorithm and of the parameters of the output are straightforward. The algorithm essentially involves two auxiliary procedures: for decomposing a complex algebraic variety into its absolutely irreducible components from Proposition 2 and for quantifier elimination in the first-order theory of reals from Proposition 1. The latter procedure is the first in each step of the recursion. Let us examine an arbitrary step.

For each of less than 2^n tuples of the kind $(i_1, \ldots, i_m)$ the bounds for quantifier elimination imply that the complex algebraic variety of the kind $V_{\mathbf{C}}^{(l)}$, which has to be decomposed into its irreducible components on a step of the recursion, is defined by a system of n or less equations of the kind $g = 0$, where $g \in \mathbf{Z}[X_1, \ldots, X_n]$, $\deg_{X_1,\ldots,X_n}(g) < (kd)^{n^{O(1)}}$, $l(g) < M^{n^{O(1)}}(kd)^{n^{O(1)}}$.

Applying the procedure from Proposition 2 to $V_{\mathbf{C}}^{(l)}$, the algorithm constructs the components of this set in time $M^{O(1)}(kd)^{n^{O(1)}}$. The form in which the components are presented was described in Section 2. Every component of $V_{\mathbf{C}}^{(l)}$ will be given by a system of $(kd)^{n^{O(1)}}$ equations of the kind $\tilde{g}_{j\eta} = 0$, $\tilde{g}_{j\eta} \in \mathbf{Z}[Z_j][X_1, \ldots, X_n]$ and by a system of one-variable inequalities $\Phi_j = 0$ and $\mathcal{S}_j$, where Z_j, $1 \leq j < (kd)^{n^{O(1)}}$, are new variables and $\mathcal{S}_j$ is the sequence of certain sign assignments for derivatives of all orders of Φ_j.

Here $\deg_{X_1,\ldots,X_n,Z_j}(\tilde{g}_{j\eta}), \deg_{Z_j}(\Phi_j) < (kd)^{n^{O(1)}}$, $l(\tilde{g}_{j\eta}), l(\Phi_j) < M^{O(1)}(kd)^{n^{O(1)}}$. Note that the procedure from Grigoriev and Vorobjov (1988), used in between in order to solve a polynomial system in two variables for defining a component by polynomials with *real* coefficients, has, in this particular case, polynomial time complexity.

The selection among the produced components of $V_{\mathbf{C}}^{(1)}$ which have intersections of the proper dimension with $\mathbf{R}^n$ of the Zariski closure (see steps (3) and (4) at the beginning of Section 3) is made, by the algorithm, with the help of the quantifier elimination procedure. Hence, the time bounds for the recursion step will remain of the same kind.

The process of establishing the adjacency relations in the component graph requires us to check whether one of the already produced vertices is contained (as a semialgebraic set) in another. This is done by an application of quantifier elimination and preserves the time bound

$$M^{O(1)}(kd)^{n^{O(1)}}.$$

This finishes the complexity analysis of the algorithm.

6. Application of the Main Construction: The Whitney System

Let, as before, $W \subset \mathbf{R}^n$ be an m-dimensional semialgebraic set satisfying the bounds from the Introduction. The family of systems of polynomial equations

$$h_{1,j}^{(p)} = \cdots = h_{n-p,j}^{(p)} = 0, \qquad 0 \le p \le m,\ 1 \le j \le t_p,$$

for some integers $t_p \ge 1$, where $h_{i,j}^{(p)} \in \mathbf{Z}[X_1, \ldots, X_n]$ is called a *Whitney system* for W (cf. Whitney, 1957) if for every x from a Zariski open in $W^{(p)}$ subset of $W^{(p)}$ with $\dim_{\mathbf{R}}(x, W) = p$, there exists j, $1 \le j \le t_p$, such that for all sufficiently small $r > 0$ the intersection $W \cap B_x(r)$ coincides with

$$\{h_{1,j}^{(p)} = \cdots = h_{n-p,j}^{(p)} = 0\} \cap B_x(r),$$

and the rank of the Jacobian matrix of the system

$$h_{1,j}^{(p)} = \cdots = h_{n-p,j}^{(p)} = 0$$

is maximal at x.

Using the main construction of our algorithm we can, *for a given W, produce a Whitney system for W. In this system for each $0 \le p \le m$ the*

number of subsystems $t_p \leq \binom{n}{p}$. *For each* $0 \leq p \leq m$, $1 \leq j \leq t_p$, $1 \leq i \leq n - p$, *the degree* $\deg_{X_1,\ldots,X_n}(h_{i,j}^{(p)}) < (kd)^{n^{O(1)}}$, $l(h_{1,j}^{(1)}) < M^{O(1)}(kd)^{n^{O(1)}}$. *The running time of the procedure of constructing the Whitney system is less than* $M^{O(1)}(kd)^{n^{O(1)}}$.

To prove this observe first that

$$W = \bigcup_{0 \leq p \leq m} \bigcup_{\{i_1,\ldots,i_p\} \subset \{1,\ldots,n\}} W_{0,i_1,\ldots,i_p},$$

where (cf. above) $W_{0,i_1,\ldots,i_p}$ is the subset of all points $x \in W$ such that $\dim_{\mathbf{R}}(x, W) = p$ and, under the projection map

$$(X_1, \ldots, X_n) \mapsto (X_{i_1}, \ldots, X_{i_p}),$$

the image of a neighborhood of x in W has the dimension p. It is sufficient to construct a Whitney system for each $W_{0,i_1,\ldots,i_p}$ separately. Let us consider, as in Section 2, for definiteness, the case of $W_{0,1,\ldots,m}$ (utilizing also other notations from that section).

The set $W_{0,1,\ldots,m}$ is contained in

$$V_{0,1,\ldots,m}^{(1)} = \{g_{m+1} = \cdots = g_n = 0\} \subset \mathbf{R}^n,$$

where $g_i \in \mathbf{Z}[X_1, \ldots X_m, X_i]$, and, according to Lemma 1, the hypersurfaces $\{g_i = 0\} \subset \mathbf{R}^n$, $m + 1 \leq i \leq n$, intersect transversally on $W_{0,1,\ldots,m}$.

Replace in the system, defining $V_{0,1,\ldots,m}^{(1)}$ each g_i by its *square-free part*,

$$\tilde{g}_i = g_i \Big/ \mathrm{GCD}\left(g_i, \frac{\partial g_i}{\partial X_1}, \ldots, \frac{\partial g_i}{\partial X_n}\right),$$

where the denominator is computed by a standard polynomial time procedure (see, e.g., Buchberger *et al.*, Eds., 1983). Then $\{g_i = 0\} = \{\tilde{g}_i = 0\}$ and at every point x of a Zariski open in $\{\tilde{g}_i = 0\}$ subset of $\{\tilde{g}_i = 0\}$ the gradient

$$\left(\frac{\partial \tilde{g}_i}{\partial X_1}, \ldots, \frac{\partial \tilde{g}_i}{\partial X_n}\right)(x) \neq 0.$$

LEMMA 6. *The family, consisting of a single system of equations* $\tilde{g}_{m+1} = \cdots = \tilde{g}_n = 0$ *is a Whitney system for* $W_{0,1,\ldots,m}$.

Proof. Verbatim repetition of the proof of Lemma 1 shows that at every point of a Zariski open in $W_{0,1,\ldots,n}$ subset of $W_{0,1,\ldots,m}$, the gradients of all polynomials $\tilde{g}_i$ are nonzero and linearly independent in common.

Besides,

$$\{\tilde{g}_{m+1} = \cdots = \tilde{g}_n = 0\} \supset W_{0,1,\ldots,m},$$

so the requirements on a Whitney system are fulfilled. ∎

The proofs of the bounds on the degrees and coefficients of the resulting Whitney system and on the running time are straightforward and analogous to the analysis in Section 5.

7. Application of the Main Construction: The Real Radical

Let $I = (f_1, \ldots, f_k)$ be a polynomial ideal generated by polynomials $f_i \in \mathbf{Z}[X_1, \ldots, X_n]$. The ideal

$$\sqrt{I} = \{f \in \mathbf{C}[X_1, \ldots, X_n] : \exists l \in \mathbf{Z},\ l > 0\ (f^l \in I)\}$$

is called the *radical* of the ideal I.

According to Hilbert's Nullstellensatz, $\sqrt{I}$ coincides with the ideal of all polynomials vanishing identically on the complex variety $\{f_1 = \cdots = f_k = 0\} \subset \mathbf{C}^n$. Following this analogy, call the *real radical* of I the ideal $\sqrt[\mathbf{R}]{I}$ of all polynomials vanishing identically on the real variety $\{f_1 = \cdots = f_k = 0\} \subset \mathbf{R}^n$. It turns out that

$$\sqrt[\mathbf{R}]{I} = \{f \in \mathbf{R}[X_1, \ldots, X_n] : \exists l \in \mathbf{Z},\ l > 0,$$
$$\exists g_1 \cdots \exists g_r \in \mathbf{R}[X_1, \ldots, X_n](f^{2l} + g_1^2 + \cdots + g_r^2 \in I)\},$$

see Bochnak *et al.* (1987). In this section we describe an algorithm for computing the set of generators of $\sqrt[\mathbf{R}]{I}$, more precisely, for reducing this problem to a case of "ordinary" radicals.

In a more general setting the problem of finding the real radical was considered in Becker and Neuhaus (1993); however, no complexity bounds are explicitly stated there.

Let the polynomials $f_1, \ldots, f_k$ satisfy the bounds described at the beginning of the Introduction and $\dim_{\mathbf{R}}(\{f_1 = \cdots = f_k = 0\}) = m$. The main algorithm outputs (see the Introduction) the systems of equations defining in $\mathbf{C}^n$ complexifications of all irreducible over $\mathbf{R}_{\text{alg}}$ in $\mathbf{R}^n$ components of the real variety $U_{\mathbf{R}} = \{f_1 = \cdots = f_k = 0\} \subset \mathbf{R}^n$ which are the varieties irreducible over $\mathbf{C}_{\text{alg}}$ in $\mathbf{C}^n$. Using the procedure from Proposition 3, we can produce a single system of equations $g_1 = \cdots = g_t = 0$ defining in $\mathbf{C}^n$ the complexification $U_{\mathbf{C}}$ of the real variety $U_{\mathbf{R}}$, with $g_i \in \mathbf{R}_{\text{alg}}[X_1, \ldots, X_n]$, $1 \le i \le t$. Let $J = (g_1, \ldots, g_t)$ be the ideal generated by $g_1, \ldots, g_t$.

LEMMA 7. $\sqrt[\mathbf{R}]{I} = \sqrt{J} \cap \mathbf{R}[X_1, \ldots, X_n]$.

Proof. Obviously, $\sqrt{J} \subset \sqrt[\mathbf{R}]{I}$. Let $h \in \mathbf{R}[X_1, \ldots, X_n]$ be identically zero on $U_{\mathbf{R}}$, and suppose that h is not identically zero on an irreducible over $\mathbf{C}_{\text{alg}}$ in $\mathbf{C}^n$ component $U_{\mathbf{C}}^{(1)}$ of $U_{\mathbf{C}}$. By the theorem on the dimension of intersection,

$$\dim_{\mathbf{C}}(U_{\mathbf{C}}^{(1)} \cap \{h = 0\}) < \dim_{\mathbf{C}}(U_{\mathbf{C}}^{(1)}).$$

Let $U_{\mathbf{R}}^{(1)}$ be the component of $U_{\mathbf{R}}$ having the complexification $U_{\mathbf{C}}^{(1)}$. Observe that

$$\dim_{\mathbf{R}}(U_{\mathbf{R}}^{(1)}) = \dim_{\mathbf{C}}(U_{\mathbf{C}}^{(1)})$$

(Lemmas 1 and 3). Then

$$\dim_{\mathbf{R}}(U_{\mathbf{R}}^{(1)} \cap \{h = 0\}) < \dim_{\mathbf{C}}(U_{\mathbf{C}}^{(1)} \cap \{h = 0\}) < \dim_{\mathbf{C}}(U_{\mathbf{C}}) = \dim_{\mathbf{R}}(U_{\mathbf{R}}^{(1)}),$$

and we get a contradiction. ∎

The algorithm computes the finite set of generators $h_1, \ldots, h_s$ of the radical $\sqrt{J}$ (and, hence, of $\sqrt[\mathbf{R}]{I}$), using the procedure from Proposition 4. Here $h_i \in \mathbf{R}_{\text{alg}}[X_1, \ldots, X_n]$, $1 \le i \le s$, $s < (kd)^{n^{m^{O(1)}}}$, and each h_i is given in a standard representation. Combining the bounds from Propositions 3 and 4, we conclude that the degree of this representation is $(kd)^{n^{m^{O(1)}}}$, its bit length is $M^{O(1)}(kd)^{n^{m^{O(1)}}}$. The running time of the algorithm does not exceed $M^{O(1)}(kd)^{n^{m^{O(1)}}}$.

REFERENCES

BECKER, E., AND NEUHAUS, R. (1993), Computation of real radicals of polynomial ideals, *in* "Computational Algebraic Geometry," pp. 1–20, Birkhüser, Boston.

BOCHNAK, J., COSTE, M., AND ROY, M.-F. (1987), "Géométrie Algébrique Réelle," Springer-Verlag, Berlin.

BUCHBERGER, B., COLLINS, G., AND LOOS, R. (Eds.) (1983), "Computer Algebra: Symbolic and Algebraic Computation," Springer-Verlag, New York.

CHISTOV, A. L. (1984), Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time, *Zapiski Nauchnykh Seminarov LOMI* **137**, 124–188; *J. Soviet Math.* **34** (1986), 1838–1882. [Eng. transl.]

GRIGORIEV, D. (1984), Factorization of polynomials over finite field and the solution of systems of algebraic equations, *Zapiski Nauchnykh Seminarov LOMI* **137**, 20–79; *J. Soviet Math.* **34** (1986), 1762–1803. [Engl. transl.]

GRIGORIEV, D. (1988), The complexity of deciding Tarski algebra, *J. Symbolic Comput.* **5**, 65–108.

GRIGORIEV, D., AND VOROBJOV, N. (1988), Solving systems of polynomial inequalities in subexponential time, *J. Symbolic Comput.* **5**, 37–64.

HARTSHORN, R. (1977), "Algebraic Geometry," Springer-Verlag, Berlin.

HEINTZ, J., ROY, M.-F., AND SOLERNÓ, P. (1990), Sur la complexité du principe de Tarski–Seidenberg, *Bull. Soc. Math. France* **118,** 101–126.

KALTOFEN, E. (1990), Computing the irreducible real factors and components of an algebraic curve, *Appl. Alg. Eng. Comm. Comp.* **1,** 135–148.

KRICK, T., AND LOGAR, A. (1991), An algorithm for the computation of the radical of an ideal in the ring of polynomials, Lecture Notes in Computer Sci., Vol. 539, pp. 195–205, Springer-Verlag, Berlin.

MAYR, E., AND MEYER, A. (1982), The complexity of the word problems for commutative semigroups and polynomial ideals, *Adv. in Math.* **46,** 305–329.

RANNOU, E. (1993), "Complexité d'algorithmes de stratifications," These, Université de Rennes I, Rennes.

RENEGAR, J. (1992), On the computational complexity and geometry of the first-order theory of reals, *J. Symbolic Comput.* **13** (1992), 329–352.

SHAFAREVICH, I. R. (1974). "Basic Algebraic Geometry," Springer-Verlag, Berlin.

WHITNEY, H. (1957), Elementary structure of real algebraic varieties, *Ann. Math.* **66,** 456–467.