Computing the Complexification of a Semi-Algebraic Set

Marie-Françoise Roy[*]
Nicolai Vorobjov [†]

Abstract

We describe an algorithm for producing the smallest complex algebraic variety containing a given semi-algebraic set S, and all the irreducible components of S. Let S be defined by s polynomials of degrees less than d with integer coefficients of bit lengths less than M. Then the complexity of the algorithm is bounded from above by a polynomial in M, s^n, d^{n^2}. The degree of the complexification is less than $s^n d^{O(n)}$, while the degrees of polynomials defining the complexification and irreducible components are less than $d^{O(n)}$.

1 Introduction

The *complexification* of a semi-algebraic set $S \subset \mathbf{R}^n$ of dimension p is the smallest (with respect to the set-theoretic inclusion) complex affine algebraic variety $C(S)$ containing S. The real and complex dimension of $C(S)$ is equal to p. The *degree* of S is the degree of the variety $C(S)$, defined as the sum of the degrees of the irreducible components of $C(S)$. The degree of an irreducible complex algebraic set of dimension p is the number of intersection points of this set with a generic $n-p$-plane. We are interested in computing the complexification and estimating the degree.

Upper bounds on the degree and on the number of real irreducible component as well as upper estimates on the degrees of polynomials defining the complexification and the irreducible components of a semi-algebraic set are of fundamental theoretical importance. For instance, the degree is one of the natural characteristics of the geometric complexity of a set, particularly valuable in situations when the topological characteristics are trivial. It is not immediately evident that its upper estimate should be roughly the same as in algebraically closed case: the degree of the input polynomial raised to the number of variables.

An upper estimate on the degree gives lower bounds on computational complexity for algebraic computation trees.

An upper bound for the degree of an algebraic variety in a projective space over algebraically closed field is provided by the classical Bézout's Theorem. Heintz [10] undertook a thorough examination of the degree concept for locally closed and constructive sets in affine spaces over algebraically closed fields. In particular he proved a "Bézout's Inequality" for locally closed sets. In Chistov [4] and Grigoriev [8] an algorithm with complexity singly exponential in the numer of variables was constructed for producing all irreducible components for projective and affine varieties over a wide class of algebraically closed fields.

An algorithm for finding the complexification and irreducible components of a semi-algebraic set was proposed in Galligo-Vorobjov [7]. It is based on effective quantifier elemination for real closed fields. The bounds for degree of the set and for complexity of the algorithm, being singly exponential in the number of variables, are still too rough, for instance the estimate for the degree is $d^{O(n^2)}$.

The emphasis of the algorithm described in the present paperis on the tightness of the bounds.

We would like to thank the referees and Thomas Lickteig for very useful suggestions.

2 The main theorems

Let S be a semi-algebraic set. A point x of S is a *point of S of local dimension* p if there is a real $r > 0$ such that for any $0 < r' \leq r$ the dimension of $S \cap B_x(r')$ is equal to p (where $B_x(r')$ is the ball of center x and radius r'). A point x of S of local dimension p is *smooth* if there exists a real $r > 0$ such that for any $0 < r' \leq r$ $S \cap B_x(r')$ is a smooth manifold of dimension p. There exists a real $r > 0$ such that for any $0 < r' \leq r$ the smallest complex affine algebraic variety containing $S \cap B_x(r')$ is the same. This set, denoted by $C_x(S)$, is the *local complexification* of S at x. The *local degree* of S at x $\deg_x(S)$ is the degree of $C_x(S)$.

We consider first the case of an irreducible algebraic set $V = Z(f)$ defined as the zero set of a polynomial $f \in \mathbf{Z}[X_1, \ldots, X_n]$ of degree less than d.'

Theorem 1 *Let $V = Z(f)$ be an irreducible algebraic set defined as the zero set of a polynomial $f \in \mathbf{Z}[X_1, \ldots, X_n]$ of degree less than d. If the dimension of V is p, then*

$$\deg(V) \leq (2(d+1))^{n-p} = (O(d))^{n-p}.$$

[*] IRMAR (URA CNRS 305), Université de Rennes, Campus de Beaulieu 35042 Rennes cedex FRANCE supported in part by the project ESPRIT- BRA 6846POSSO

[†] School of Mathematical Sciences, University of Bath, Bath, BA2 7AY, United Kingdom

Corollary 1 *Let V be an algebraic set defined as the zero set of polynomials of degree less than d. Let x be a smooth point of V of local dimension p. Then*

$$\deg_x(V) < (O(d))^{n-p}.$$

Consider now a semi-algebraic set $S \subset \mathbf{R}^n$ defined by an arbitrary Boolean combination of atomic inequalities of the kind $f > 0$ or $f = 0$, $f \in \mathbf{Z}[X_1, \ldots, X_n] = \mathbf{Z}[\mathbf{X}]$ of degrees $\deg_{\mathbf{X}}(f) < d$ and bit-lengths of integral coefficients $< M$. Let s be the number of different atomic polynomials. The semi-agebraic set $S \subset \mathbf{R}^n$ is *basic* if it is defined by a system of atomic inequalities of the kind $f > 0$ or $f = 0$, $f \in \mathbf{Z}[X_1, \ldots, X_n]$.

Theorem 2 *The degree of S is such that*

$$\deg(S) = s^n d^{O(n)}.$$

More precisely, let p_1 (resp. p_2) be the maximal (resp. minimal) dimension among all irreducible components of $C(S)$, then

$$\deg(S) \leq (60sd/n)^n \sum_{p_2 \leq p \leq p_1} ((n-p)p+1)(2(d+1))^{n-p}.$$

If S is basic

$$\deg(S) \leq d^{O(n)}.$$

More precisely, let p_1 (resp. p_2) be the maximal (resp. minimal) dimension among all irreducible components of $C(S)$. Then

$$\deg(S) \leq p_1 d^{O(n-p_2)} = d^{O(n)}.$$

We are proving these bounds through an algorithm which produces the complexification. In order to describe the output of the algorithm we explain the term "standard representation" [7].

Let $h \in \mathbf{C}_{alg}[Y_1, \ldots, Y_n] = \mathbf{C}_{alg}[\mathbf{Y}]$ be a polynomial with complex algebraic coefficients. We say that h is given in a *standard representation* with the *degrees* (d_1, d_2) and the *bit lengths* (N_1, N_2) for some positive integers d_1, d_2, N_1, N_2, if the following data is provided:

- a polynomial $\Phi \in \mathbf{Z}[Z]$, where Z is a new variable;
- a polynomial $\tilde{h} \in \mathbf{Z}[Z][Y_1, \ldots, Y_n]$, where each coefficient from $\mathbf{Z}[Z]$ is of the kind

$$\xi_\eta = \sum_{0 \leq \mu < \deg(\Phi)} \beta_{\eta\mu} Z^\mu, \qquad (1)$$

with $1 \leq \eta \leq (\deg_{\mathbf{Y}}(\tilde{h}))^s$.

Here $\deg_{\mathbf{Y}}(\tilde{h}) < d_1$, $\deg(\Phi) < d_2$, and bit length of $\beta_{\eta\mu} < N_1$, bit length $l(\Phi) < N_2$. The polynomial h is the result of substitution of a certain root of Φ, instead of variable Z in each expression (1) for all η.

If h has *real* algebraic coefficients, a standard representation includes the specification of the sequence of signs of the derivatives of all orders of Φ, which (by Thom's lemma, [3]) defines the unique real root of Φ.

Theorem 3 *Given a semi-algebraic set S as above, there is an algorithm which produces the complexification $C(S)$. The running time of the algorithm is linear in s^n and polynomial in M and d^{n^2}. The algorithm represents the complex affine variety $C(S)$ as a collection of its absolutely irreducible components:*

$$C(S) = \bigcup_\alpha V^{(\alpha)}.$$

For every component $V^{(\alpha)}$ of dimension p the algorithm constructs a system of polynomial equations

$$\Psi_1^{(\alpha)} = \ldots = \Psi_N^{(\alpha)} = 0$$

with $\Psi_j^{(\alpha)} \in \mathbf{R}_{alg}[X_1, \ldots, X_n]$. The number of equations N is bounded by $d^{O(n(n-p))}$, the degree of the component $\deg(V^{(\alpha)})$ is bounded by $(2(d+1))^{n-p}$. The polynomials $\Psi_j^{(\alpha)}$ are given in a standard representation with degrees

$$\left(d^{c(n-p)}, d^{c(n-p)}\right)$$

and bit lengths

$$\left((\log s) M d^{cp(n-p)}, (\log s) M d^{c(n-p)}\right)$$

for a certain integer $c > 0$.

The family of all real algebraic varieties defines a Zariski topology on $\mathbf{R}^n$ which induces a topology on any subset of $\mathbf{R}^n$, in particular, on any semi-algebraic subset.

A semi-algebraic set $S \subset \mathbf{R}^n$ is called (absolutely) irreducible *in* the space $\mathbf{R}^n$ if a representation $S = S_1 \cup S_2$, where S_1, S_2 are Zariski closed subsets *in* S (i.e., with respect to Zariski topology induced on S, these sets are semi-algebraic), implies either $S = S_1$ or $S = S_2$.

The set S is uniquely representable as a union $S = \bigcup_\alpha S^{(\alpha)}$ of its absolutely irreducible in $\mathbf{R}^n$ components, that is, semi-algebraic subsets $S^{(\alpha)}$ such that:

- every $S^{(\alpha)}$ is Zariski closed in S absolutely irreducible in $\mathbf{R}^n$;
- $S^{(\alpha)} \not\subset \bigcup_{\beta \neq \alpha} S^{(\beta)}$.

The systems of equations (with real coefficients) for the family of all absolutely irreducible components of the complexification $C(S)$ define the family of all absolutely irreducible in $\mathbf{R}^n$ components of semi-algebraic set S. Moreover every $V^{(\alpha)}$ is a complexification of the corresponding real component, and $C(S) \cap \mathbf{R}^n$ is the Zariski closure of S. The number of all real irreducible components of S is dominated by the degree of S, and, therefore, by $p_1 d^{O(n-p_2)}$.

The bound $p_1 d^{O(n-p_2)}$ on degree of a basic semi-algebraic set S is somewhat unnatural since it involves parameters of the complexification $C(S)$ rather than parameters depending only on S.

Denote by S_p the subset of S consisting of all points of S of a fixed dimension p. The complexification and the absolutely irreducible components can be produced for all the subsets S_p. The degrees of S_p is bounded similiary to the degree of S:

$$\deg(S_p) \leq ((n-p)p+1)(2(d+1))^{n-p},$$

a well as the estimates on the sizes of systems representing the complexification of S_p and its irreducible components. The running time of this procedure is also linear in s^n and polynomial in M but only polynomial in d^{n^3}.

Let us mention the following statements which are closely related to the previous results and can be proved within the same circle of ideas.

1) The complexification $C(S)$ can be represented by a single system of equations with real algebraic coefficients. An estimate on the size of this system is similiar to the bounds on systems for components.

2) The components $V^{(\alpha)}$ can be also represented by their generic points.

3) All the concepts and results of this paper can be formulated and proved in "relative version", with respect to a subfield of $\mathbf{F} \subset \mathbf{R}$, rather than the whole $\mathbf{R}$. In particular, we can definethe $\mathbf{F}$-complexification $V_{\mathbf{F}}$ of S as the smallest (with respect to set-theoretical inclusion) variety in $\mathbf{C}^n$ with coefficients from $\mathbf{F}$, containing S. Obviously, $V = V_{\mathbf{C}} \subset V_{\mathbf{F}}$.

Define the $\mathbf{F}$-degree of S, $\deg_{\mathbf{F}}(S)$, as $\deg(V_{\mathbf{F}})$. Clearly, $\deg_{\mathbf{F}}(S) \geq \deg(S)$, hence the largest possible degree of S is attained on the field of rationals.

In the "relative version" the role of the components of S absolutely irreducible in $\mathbf{R}^n$ is played by the components irreducible *over* $\mathbf{F}$ *in* $\mathbf{R}^n$ defined with respect to Zariski topology on $\mathbf{R}^n$ formed by all real varieties in $\mathbf{R}^n$ given by polynomials with coefficients in $\mathbf{F}$.

The theorems and statements above are true for the $\mathbf{F}$-complexification, $\mathbf{F}$- degree and irreducible over $\mathbf{F}$ components with the same upper bounds on the sizes of output objects and running time.

4) The dimension of S can be computed within the time bound linear in s^n and polynomial in M, d^{n^2}. This bound is, probably, not tight. The conjecture is that there exists an algorithm for computing the dimension of S in time linear in s^n and polynomial in M, d^n [6].

Note that the number of coefficients in the polynomials representing the complexification and irreducible components is, in the worst case, of the same order as the running time for producing these objects. This means that for the chosen method of representation of complexification and irreducible components the bound on complexity can't be improved [4].

We conclude this section with a short description of the technique.

First, the algorithm reduces the problem for a general semi- algebraic set S to the local case for a real algebraic variety $V = Z(f)$ defined by a polynomial f, at a point x where the dimension of V is p and x is a smooth point of V.

The algorithm writes out $n - p$ equations of degrees not exceeding $2(d + 1)$. The coefficients of these polynomials belong to a transcentental extension of $\mathbf{Q}$ by two infinitesimal elements, δ_0 and δ_1 and these polynomials define a p-dimensional variety $\mathcal{V}$ in the affine space $(\overline{\mathbf{C}(\delta_0, \delta_1)})^n$.

The variety "covers" V at the neighbourhood of x, that is for any x' of V close to x there exists $y \in \mathcal{V}$ such that $||x' - y||$ is infinitesimal.

Then we can say that the union of a certain subfamily of components of $\mathcal{V}$ "approximates" V at the neighbourhood of x. Passing to the limit is done roughly in the same way as in [4] and [8]. The rest of the paper describes the algorithm and proofs of the bounds in more detail. Full proofs will appear later.

3 Infinitesimals

The definitions below concerning infinitesimals follow [9]

Let $\mathbf{F}$ be an arbitrary real closed field (see, e.g., [11] and an element ε be infinitesimal relative to elements of $\mathbf{F}$. This means that for any positive element $a \in \mathbf{F}$ inequalities $0 < \varepsilon < a$ are valid in the ordered field $\mathbf{F}(\varepsilon)$. Obviously, the element ε is transcendental over $\mathbf{F}$. For an ordered field $\mathbf{F}'$ we denote by $\tilde{\mathbf{F}}'$ its (unique up to isomorphism) real closure, preserving the order on $\mathbf{F}'$ [11].

We recall some other well-known statements concerning real closed fields. A Puiseux (formal power-fractional) series over $\mathbf{F}$ is series of the kind

$$b = \sum_{i \geq 0} a_i \varepsilon^{\nu_i / \mu},$$

where $0 \neq a_i \in \mathbf{F}$ for all $i \geq 0$, integers $\nu_0 < \nu_1 < \ldots$ increase and the natural number $\mu \geq 1$. The field $\mathbf{F}\langle\varepsilon\rangle$ consisting of all Puiseux series (appended by zero) is real closed, hence $\mathbf{F}\langle\varepsilon\rangle \supset \widetilde{\mathbf{F}(\varepsilon)} \supset \mathbf{F}(\varepsilon)$. Besides the field $\mathbf{F}[\sqrt{-1}]\langle\varepsilon\rangle$ is algebraically closed.

If $\nu_0 < 0$, then the element $b \in \mathbf{F}\langle\varepsilon\rangle$ is infinitely large. If $\nu_0 > 0$, then b is infinitesimal relative to elements of the field $\mathbf{F}$. A vector $(b_1, \ldots, b_n) \in \mathbf{F}\langle\varepsilon\rangle^n$ is called $\mathbf{F}$-finite if each coordinate b_i, $1 \leq i \leq n$ is not infinitely large relative to elements of $\mathbf{F}$.

For any $\mathbf{F}$-finite element $b \in \mathbf{F}\langle\varepsilon\rangle$ its *standard part* $\mathrm{st}(b)$ is definable, namely $\mathrm{st}(b) = a_0$ in the case $\nu_0 = 0$ and $\mathrm{st}(b) = 0$ if $\nu_0 > 0$. For any $\mathbf{F}$-finite vector $(b_1, \ldots, b_n) \in \mathbf{F}\langle\varepsilon\rangle^n$ its standard part is defined by the equality

$$\mathrm{st}(b_1, \ldots, b_n) = (\mathrm{st}(b_1), \ldots, \mathrm{st}(b_n)).$$

For a set $\mathcal{W} \subset \mathbf{F}\langle\varepsilon\rangle^n$ we define

$$\mathrm{st}(\mathcal{W}) = \{\mathrm{st}(w) : \ w \in \mathcal{W} \text{ and } w \text{ is } \mathbf{F}\text{−finite}\}.$$

The following transfer principle is true (Tarski [15]). If $\mathbf{F}'$, $\mathbf{F}''$ are real closed fields with $\mathbf{F}' \subset \mathbf{F}''$ and $\mathcal{P}$ is a closed (without free variables) formula of the first order theory of the field $\mathbf{F}'$, then $\mathcal{P}$ is true over $\mathbf{F}'$ if and only if $\mathcal{P}$ is true over $\mathbf{F}''$.

If $S \subset \mathbf{F}^n$ is a semi-algebraic set the *extension* of S to $\mathbf{F}'$ is the semi-algebraic set of $\mathbf{F}'^n$ defined by the same boolean combination as S. The extension of S to $\mathbf{F}'$ will be denoted by $S(\mathbf{F}')$, or S when this does not lead to ambiguity .

4 Constructing approximating subvarieties of a given dimension

Consider an algebraic set V defined by $f = 0$, with f everywhere non negative (it is the case, for instance, if f is a sum of squares), and a smooth point x of V of local dimension p. According to the plan outlined at the end of Section 2, the algorithm will construct a variety $\mathcal{V}$ of real and complex dimension p covering V.. The coefficients of the systems of equations defining the varieties are polynomials in some infinitesimals. The variety $\mathcal{V}$ has two important properties. Firstly, $\mathcal{V}$ has the proper dimension p. Secondly, any point z from the neighbourhood is infinitely close to a point from $\mathcal{V}$.

The first property is purely algebraic and can be obtained by choosing a special structure for the system defining $\mathcal{V}$. This construction appears in [14].

Consider a real algebraic set V, defined without loss of generality as the zero set of a polynomial

$$f \in \mathbf{R}[X_1, \ldots, X_n] = \mathbf{R}[\mathbf{X}]$$

everywhere non negative with $\deg_{\mathbf{X}}(f) \leq 2d$ (if V was defined by several equations of degree d, take their sum of squares).

Let $a > 0$ be a real number. Let δ_1 be infinitesimal relative to $\mathbf{R}$. Denote by $\mathbf{R}_1$ (resp. $\mathbf{C}_1$) the real closure (resp. algebraic closure) of $\mathbf{R}(\delta_1)$.

Define

$$g = (1-\delta_1)f + \delta_1(X_{p+1}^{2(d+1)} + \cdots + X_n^{2(d+1)} - a)$$

$$\mathcal{H} = \left\{ g = 0 \right\} \subset \mathbf{R}_1^n$$

$$\mathcal{V} = \left\{ g = \frac{\partial g}{\partial X_{p+2}} = \cdots = \frac{\partial g}{\partial X_n} = 0 \right\} \subset \mathbf{R}_1^n$$

$$\mathcal{V}(\mathbf{C}_1) = \left\{ g = \frac{\partial g}{\partial X_{p+2}} = \cdots = \frac{\partial g}{\partial X_n} = 0 \right\} \subset \mathbf{C}_1^n.$$

Lemma 1 • *The dimension over the field $\mathbf{C}_1$ of $\mathcal{V}(\mathbf{C}_1)$ is equal to p.*

- *The dimension over the field $\mathbf{R}_1$ of $\mathcal{V}$ does not exceed p.*

Proof: For every choice of $(x_1, \ldots, x_p)$ in $\mathbf{C}_1^p$, the $n-p$-plane define by $X_1 = x_1, \ldots, X_p = x_p$ interesects the variety $\mathcal{V}(\mathbf{C}_1)$ in a finite number of points. Finally, the real dimension never exceeds the complex dimension. □

Let x be a smooth point of V of local dimension p and $B_0(r)$ a ball containing x. We denote by T_x the tangent p-plane to V at x and suppose, without loss of generality, that the projection of T_x on the $X_1, \ldots, X_p$- plane is a bijection. We choose $a = (n-p)r^{2(d+1)}$.

Proposition 1 *There exists $y \in \mathcal{V}$ such that* $\mathrm{st}(y) = x$.

Proof : The proof is based on the following lemma.

Lemma 2 *If x is an isolated point of V, then there exists $y \in \mathcal{V}$ such that* $\mathrm{st}(y) = x$.

Proof : The variety $\mathcal{H}$ is a smooth manifold of dimension $n-1$ and in a neighbourhood of x is semi-algebraically diffeomorphic to a sphere around x. □

Define P as the $n-p$-plane defined by $X_1 = x_1, \ldots, X_p = x_p$. Since the tangent plane to V at x, T_x is transversal to P, the point x is an isolated point of the variety $V \cap P \subset \mathbf{R}^{n-p}$ and we can apply lemma 2 to $V \cap P$ and $\mathcal{V} \cap P$. Note that $\mathcal{H} \cap P$ is a smooth hypersurface in R^{n-p}. □

Let the element $\delta_0 > 0$ be infinitesimal relative to $\mathbf{R}$, the element $\delta_1 > 0$ be infinitesimal relative to $\mathbf{R}(\delta_0)$. Denote by $\mathbf{R}_0$ (resp. $\mathbf{C}_0$) the real closure (resp. algebraic closure) of $\mathbf{R}(\delta_0)$ and by $\mathbf{R}_1$ (resp. $\mathbf{C}_1$) the real closure (resp. algebraic closure) of $\mathbf{R}(\delta_0, \delta_1)$. Denote by st_0 the map from $\mathbf{R}_1$ to $\mathbf{R}_0$ associating to a Puiseux series in δ_1 finite over $\mathrm{R}(\delta_0)$ its initial term.

For a polynomial $f \in \mathbf{R}[X_1, \ldots, X_n]$ of degree less than $2d$ and a multi-index $I = (i_{p+1}, \ldots, i_n)$ we introduce the polynomial f_I. We use the following notations:

$$D = B_0(\delta_0^{-1})$$

$$a = (n-p)\delta_0^{-2(d+1)}$$

$$f_I = (1-\delta_1)f - \delta_1(X_{i_{p+1}}^{2(d+1)} + \cdots + X_{i_n}^{2(d+1)} - a)$$

$$\mathcal{V}_I = \left\{ f_I = \frac{\partial f_I}{\partial X_{i_{p+2}}} = \cdots = \frac{\partial f_I}{\partial X_{i_n}} = 0 \right\} \subset \mathbf{R}_1^n$$

$$V' = \{f = 0\} \cap D \subset \mathbf{R}_1^n$$

$$\mathcal{W} = \bigcup \{\mathcal{V}_I : I \in \{1, \ldots, n\}^{n-p}\} \subset \mathbf{R}_1^n$$

$$\mathcal{V}_I(\mathbf{C}_1) = \left\{ f_I = \frac{\partial f_I}{\partial X_{i_{p+2}}} = \cdots = \frac{\partial f_I}{\partial X_{i_n}} = 0 \right\} \subset \mathbf{C}_1^n$$

Proposition 2 *Let V_p be the subset of points of local dimension p of V'. There exists $y \in \mathcal{W}$ such that* $\mathrm{st}_0(y) = x$.

Proof : Denote by V_I the points of V' having a tangent p-plane which projects bijectively on the $X_{i_1} \ldots, X_{i_p}$-plane with $\{i_1, \ldots, i_p\} = \{1 \ldots, n\} \setminus I$. Then the union of the V_I for all choice of I is a semi-algebraic subset of V' whose euclidean closure is V'. By proposition 1, the image under st_0 of $\mathcal{W}$ contains $\cup V_I$. Moreover the image under st_0 of a semi-algebraic set is closed [14]. □

Introduce a new variable Y, and denote by $\mathcal{V}_{Y,I}(\mathbf{C}_0) \subset \mathbf{C}_0^{n+1}$ the variety defined by the equations obtained by substituting Y to δ_1 in the equations defining $\mathcal{V}_I(\mathbf{C}_1)$.

Set

$$\mathcal{W}_Y(\mathbf{C}_0) = \bigcup \{\mathcal{V}_{Y,I}(\mathbf{C}_0) : I \in \{1, \ldots, n\}^{n-p}\} \subset \mathbf{C}_0^{n+1}.$$

Denote by $\mathcal{W}'_Y(\mathbf{C}_0)$ the union of all the absolutely irreducible in $\mathbf{C}_0^{n+1}$ components of $\mathcal{V}_Y(\mathbf{C}_1)$ whose extention to $\mathbf{C}_1$ have non-empty intersections with $\{Y = \delta_1\} \subset \mathbf{C}_1^{n+1}$.

Lemma 3 • *The affine dimension over $\mathbf{C}_0$ of $\mathcal{W}'_Y(\mathbf{C}_0)$, is equal to $p+1$;*

- *$V_p \subset (\mathcal{W}'_Y(\mathbf{C}_0) \cap \{Y = 0\} \cap \mathbf{R}_0^{n+1})$;*
- *The affine dimension over $\mathbf{C}_0$ of $\mathcal{W}'_Y(\mathbf{C}_0) \cap \{Y = 0\}$ is equal to p.*

5 Construction of the complexification

The algorithm we are going to describe relies on two main subroutines

- an algorithm for computing all the irreducible components of an algebraic set over algebraically closed field, and selecting those intersecting another algebraic set [4] and [8]. These results are summarized in the appendix;
- an algorithm for testing the emptyness of a semi-algebraic set (using [1] which has the most precise bounds, see also [7], [13]).

Let us now describe the algorithm for constructing the complexification and the absolutely irreducibe components of the semi-algebraic set S.

Let $f_1, \ldots, f_s$ be all atomic polynomials in the Boolean formula defining S. A *$(f_1, \ldots, f_s)$-semi-algebraic set* is any non-empty set of the kind $\{f_1 *_1 0 \& \cdots \& f_s *_r 0\}$ where $*_j$ is either $>$ or $<$ or $=$. Then S is a union of certain $(f_1, \ldots, f_s)$-semi-algebraic sets.

Let the degrees $\deg_{\mathbf{X}}(f_j) < d$. ¿From Warren [16] and Pollack-Roy [12] we know that the number of all $(f_1, \ldots, f_s)$-semi-algebrac sets (even the total number of connected components in all these sets) does not exceed

$$(4ed(4s+1)/n)^n \leq (60ds/n)^n.$$

Moreover there is an algorithm producing the list of all the non empty $(f_1, \dots, f_s)$-semi- algebraic sets in time $s^{n+1}d^{O(n)}$ [1].

It is easy to show that for two semi-algebraic sets S_1, $S_2 \subset \mathbf{R}^n$ we have:

$$C(S_1 \cup S_2) = C(S_1) \cup C(S_2).$$

Therefore, it is sufficient to construct the complexifications of elements of the decomposition of S into basic $(f_1, \dots, f_s)$-semi-algebraic sets.

Let us now describe the algorithm for constructing the complexification and absolutely irreducibe components of the basic semi-algebraic set

$$S' = \{f_1 = \dots = f_{k_1} = 0 \,\& f_{k_1+1} > 0 \,\& \cdots \& f_s > 0\} \subset \mathbf{R}^n.$$

If there are no equalities, the complexification is the whole space.

Otherwise, set $f \equiv \sum_{1 \le i \le k_1} (f_i)^2$. For each number p from 0 to $n-1$ and for each multi-index $I = (i_{p+1}, \dots, i_n)$ the algorithm produces the variety $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ constructed previously (i.e., writes down the corresponding system of equations). The algorithm computes the family of all irreducible over $\mathbf{C}_{alg}(\delta_0)$ components of $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ using [4], [8] (see Proposition 3 in Appendix). Observe that every component is of dimension $p+1$. By the transfer principle, the family of systems of equations defining these components also defines the family of all absolutely irreducible components of $\mathcal{V}_{Y,I}(\mathbf{C}_1)$.

The algorithm selects (using [4], [8], see Proposition 3) all the components of $\mathcal{V}_{Y,I}(\mathbf{C}_1)$ having non-empty intersections with $\{Y = \delta_1\}$. Using [4], [8] (see Proposition 4), the algorithm gets the family of all irreducible components $\mathcal{W}_\beta^{(p)}$ for all $\mathcal{U}_\alpha^{(p)} \cap \{Y = 0\}$. Observe that every $\mathcal{W}_\beta^{(p)}$ has dimension p. Let $\mathcal{W}^{(p)} \subset \mathbf{C}_0^n$ be the union of all these components $\mathcal{W}_\beta^{(p)}$.

Each component $\mathcal{W}_\beta^{(p)}$ is described by a system of polynomial equations with coefficients in $\mathbf{C}_{alg}(\delta_0)$. The algorithm rewrites the system so that it would have coefficients from the field of real algebraic numbers $\mathbf{R}_{alg}$. We denote by $\mathcal{W}^{(p)}(\mathbf{R}_0^n)$ the intersection of $\mathcal{W}^{(p)}$ with $\mathbf{R}_0^n$.

After that, the algorithm decides whether $\mathcal{W}^{(p)}$ "covers" $S'(\mathbf{R}_0) \subset \{f = 0\}(\mathbf{R}_0)$, by checking the emptyness of the difference $S'(\mathbf{R}_0) \setminus \mathcal{W}^{(p)}(\mathbf{R}_0)$. In other words, the algorithm checks the emptyness of the intersection of all differences $S'(\mathbf{R}_0) \setminus \mathcal{W}_\beta^{(p)}(\mathbf{R}_0)$ for all components $\mathcal{W}_\beta^{(p)}$, using [1]. Since the real variety $\mathcal{W}_\beta^{(p)}(\mathbf{R}_0)$ can be defined by a single equation, say, $g = 0$, the difference $S'(\mathbf{R}_0) \setminus \mathcal{W}_\beta^{(p)}(\mathbf{R}_0)$ can be defined by a system $f = 0, f_{k_1+1} > 0, \cdots, f_k > 0, g^2 > 0$. Hence, the algorithm has to check the consistency of the system containing $f = 0, f_{k_1+1} > 0, \cdots, f_s > 0$ and strict inequalities corresponding bijectively to all components $\mathcal{W}_\beta^{(p)}$.

Suppose that $\mathcal{W}^{(p)}$ covers $S'(\mathbf{R}_0)$, then

$$\dim_{\mathbf{R}_0}(S'(\mathbf{R}_0)) = p$$

because the system $f_{k_1+1} > 0 \,\& \cdots \& f_s > 0$ defines an open set in $\mathbf{R}_0^n$. Moreover, the union $\hat{\mathcal{W}}^{(p)}$ of all components $\mathcal{W}_\beta^{(p)}$ such that

$$\dim_{\mathbf{R}_1}(\mathcal{W}_\beta^{(p)}(\mathbf{R}_0)) = p$$

forms a complexification of the union of all irreducible components of $S'(\mathbf{R}_0)$ of maximal dimension. The algorithm selects all the components $\mathcal{W}_\beta^{(p)}$ such that

$$\dim_{\mathbf{R}_0}(\mathcal{W}_\beta^{(p)}(\mathbf{R}_0)) = p$$

by deciding whether $\mathcal{W}^{(p-1)}$ (i.e., the corresponding variety for the previous value of the dimension) covers $\mathcal{W}_\beta^{(p)}$. Then the algorithm repeats the just described procedure replacing p by $p-1$ and $S'(\mathbf{R}_0)'$ by $T(\mathbf{R}_0) \setminus (\hat{\mathcal{W}}^{(p)}(\mathbf{R}_0))$. Thus, the complexification of all irreducible components of $S'(\mathbf{R}_0)$ of the "second maximal" dimension will be found.

If $\mathcal{W}^{(p)}$ does not cover $S'(\mathbf{R}_0)$ then the algorithm passes to consideration of the next value of p (in increasing order). For $p = \dim_{\mathbf{R}_0}(S)$ the variety $\mathcal{W}^{(p)}$ covers $S'(\mathbf{R}_0)$.

Iterating the procedure, the algorithm gets the complexifications for unions of components of $S'(\mathbf{R}_0)$ of all dimensions.

6 The complexity analysis and estimates

Let, as in the Introduction, a semi-algebraic set $S \subset \mathbf{R}^n$ be defined by a Boolean combination of atomicequations and inequalities of the kind $f > 0$ or $f = 0$, $f \in \mathbf{Z}[X_1, \dots, X_n] = \mathbf{Z}[\mathbf{X}]$ of degrees $\deg_{\mathbf{X}}(f) < d$ and bit-lengths of integral coefficients $\ell(f) < M$. Let s be the number of different atomic polynomials.

We described above a procedure for reducing the complexification problem and irreducible components problem for S to the same problems for all $(f_1, \dots, f_s)$-semi-algebraic sets. The number of these sets does not exceed $(60sd/n)^n$ and the complexity of the procedure for finding them is $M^{O(1)}s^{n+1}d^{O(n)}$. Thus, the degree (resp. complexity bounds) for the input set S can be obtained from the degree (resp. complexity bbounds) for a $(f_1, \dots, f_s)$-semi-algebraic sets by multiplying by $(60sd/n)^n$ (resp. $M^{O(1)}s^{n+1}d^{O(n)}$).

The procedure for the $(f_1, \dots, f_s)$-semi-algebraic set

$$S' = \{f_1 = \dots = f_{k_1} = 0 \,\& f_{k_1+1} > 0 \,\& \cdots \& f_s > 0\}$$

was described at the end of the previous section.

First the polynomial $f \equiv \sum_{1 \le i \le k_1} (f_i)^2$ was introduced; evidently $\deg_{\mathbf{X}}(g') < 2d$. Then the algorithm proceeds recursively on p starting from $p = 0$. For a current value of p the algorithm produces the varieties $\mathcal{V}_{Y,I}(\mathbf{C}_1)$ for all possible multi-indices I of length $n-p$. The number of all multi-indices is $\binom{n}{p} \le 2^n$, the degrees of the equations defining $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ are less than $2(d+1)$, the bit- lengths of coefficients are less than $\log(s) + M$.

Fixing a multi-index $I = (i_{p+1}, \dots, i_n)$, the algorithm of Proposition 3 decomposes the variety $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ into absolutely irreducible $(p+1)$-dimensional components, describing each component $\mathcal{V}_\alpha$ by a system of equations $\Psi_1^{(\alpha)} = \cdots = \Psi_{\ell_\alpha}^{(\alpha)} = 0$. The degrees with respect to $X_1, \dots, X_n$ of the polynomials defining $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ are less than $2(d+1)$, the degrees of these polynomials with respect to δ_0 are less than 1, and the bit-lengthsof coefficients of these polynomials are $O((\log s)M)$. Then, due to the Bézout's theorem, the number of all components is less than $2(d+1)^{n-p}$. According to Proposition 3 the number of equations ℓ_α is bounded by $(3(2d+3)^{n-p})^{n+1}$, the degrees $\deg_{\delta_0,\mathbf{X}}(\Psi_i^{(\alpha)})$ are bounded by $d^{c(n-p)}$. Every polynomial

$\Psi_i^{(\alpha)}$ is given in a *standard representation* (see Introduction) with degrees

$$\left(d^{c(n-p)}, d^{c(n-p)}\right)$$

and bit lengths

$$\left((\log s)Md^{cp(n-p)}, (\log s)Md^{c(n-p)}\right)$$

for a certain integer $c > 0$. On the decomposition of $\mathcal{V}_{Y,I}(\mathbf{C}_0)$ the algorithm spends time not exceeding

$$((\log s)M)^{O(1)}d^{O((n-p)n)}.$$

After that the algorithm selects with the help of Proposition 4 all the components of $\mathcal{V}_{Y,I}(\mathbf{C}_1)$ having non-empty intersections with $\{Y = \delta_1\}$. The running time of the algorithm up to this point does not exceed

$$((\log s)M)^{O(1)}d^{O((n-p)n)}.$$

For each selected component $\mathcal{U}_\alpha$ of dimension p the algorithm applies Proposition 4 to the intersection $\mathcal{U}_\alpha \cap \{Y = 0\}$ and gets a family of all absolutely irreducible components $\mathcal{W}_\beta$ of all such intersections. Let, as before, $\mathcal{W}^{(p)}$ denote the union of all the components $\mathcal{W}_\beta$.

Each $\mathcal{W}_\beta$ has dimension p and is represented by a system of equations:

$$\Psi_1^{(\alpha,\beta)} = \cdots = \Psi_{\ell_{\alpha,\beta}}^{(\alpha,\beta)} = 0.$$

According to Proposition 4, the number of equations in the latter system $\ell_{\alpha,\beta}$ is bounded by $(3(2d+3))^{n-p})^{n+1}$, and the following holds

$$\deg(\mathcal{W}_\beta) < (2(d+1))^{n-p}$$
$$\deg_{\delta_0,\mathbf{X}}(\Psi_i^{(\alpha,\beta)}) < d^{c(n-p)}$$

Every polynomial $\Psi_i^{(\alpha,\beta)}$ is given in a standard representation with degrees

$$\left(d^{c(n-p)}, d^{c(n-p)}\right)$$

and bit lengths

$$\left((\log s)Md^{cp(n-p)}, (\log s)Md^{cp}\right)$$

for a certain integer $c > 0$.

Then the algorithm rewrites the system of equations for $\mathcal{W}_\beta$ so that it has coefficients from $\mathbf{R}_{alg}$. The polynomials in these equations are given in a standard representation with the same degrees and bit lengths as $\Psi_i^{(\alpha,\beta)}$.

Up to this point the algorithm spends time not exceeding

$$((\log s)M)^{O(1)}d^{O((n-p)n)}.$$

After that the algorithm decides whether $\mathcal{W}^{(p)}$ "covers" the set $S'(\mathbf{R}_0)$, by checking the emptyness of the intersection of all differences $S'(\mathbf{R}_0) \setminus \mathcal{W}_\beta(\mathbf{R}_0)$ for all components $\mathcal{W}_\beta$. This reduces to checking the consistency of a system of polynomal inequalities

$$f = 0 \;\&\; f_{k_1+1} > 0 \;\&\cdots\&\; f_k > 0 \;\&\; g_1 > 0 \;\&\ldots\&\; g_q > 0,$$

where the inequalities $g_1 > 0, \ldots, g_q > 0$ correspond bijectively to the components $\mathcal{W}_\beta$. The polynomial g_i corresponding to the component $\mathcal{W}_\beta$ is a sum of squares of polynomials defining $\mathcal{W}_\beta$; thus its degree $\deg_{\delta_0,\mathbf{X}} < d^{c(n-p)}$. The standard representation of g_i has degrees

$$\left(d^{c(n-p)}, d^{c(n-p)}\right)$$

and bit lengths

$$\left((\log s)Md^{cp(n-p)}, (\log s)Md^{cp}\right)$$

for a certain integer $c > 0$. The number q of all polynomials g_i is equal to the number of the components $\mathcal{W}_\beta$, i.e., is less than $(2(d+1))^{n-p}$. So the total number of inequalities in the system is less than $s + (2(d+1))^{n-p}$. The deciding of consistency is done with the help of the procedure of [13] or [1], therefore the working time of the algorithm up to this point is

$$M^{O(1)}s^n d^{O((n-p)n)}.$$

In the case when $\mathcal{W}^{(p)}$ covers $S'(\mathbf{R}_0)$, the algorithm selects all the components $\mathcal{W}_\beta$ such that

$$\dim_{\mathbf{R}_0}(\mathcal{W}_\beta(\mathbf{R}_0)) = p$$

by deciding whether $\mathcal{W}^{(p-1)}$ covers $\mathcal{W}_\beta$. That is done by applying the procedure from [1] similary to checking whether $\mathcal{W}^{(p)}$ covers $S'(\mathbf{R}_0)$. For each component the checking requires less than $((\log s)M)^{O(1)}d^{O((n-p)n)}$ time. The union all the selected components is the complexification of of the union of all irreducible components of R of maximal dimension. Then the algorithm repeats the just described procedure recursively to find the "second maximal" dimension, etc.

In the case when $\mathcal{W}^{(p)}$ does not cover S' the algorithm passes to the next value of p.

Thus, the total running time of the algorithm is

$$M^{O(1)}s^{O(n)}d^{O(n^2)}.$$

Now we look at estimates on the degree. Since in the irreducible we have only to consider the dimension p,

$$\deg_x(V) \le O(d)^{n-p}.$$

Let, as in the formulation of our theorems, p_1 denote the maximal dimension among all irreducible components of the complexification $C(S)$, and p_2 be the minimal dimension among the components of $C(S)$. The algorithm implies the following upper bound for the *real degree* of S:

$$\deg(S) \le (60sd/n)^n \sum_{p_2 \le p \le p_1} \binom{n}{p} (2(d+1))^{n-p} \le$$
$$\le (60sd/n)^n (p_1 - p_2 + 1)2^n(2(d+1))^{n-p_2} =$$
$$= \left(O(sd/n)\right)^n d^{O(n-p_2)} = s^n d^{O(n)}.$$

Observe that if S is basic, then the factor $(60sd/n)^n$ does not occur in the bound for the degree:

$$\deg(S) \le \sum_{p_2 \le p \le p_1} \binom{n}{p} (2(d+1))^{n-p} \le$$
$$\le (p_1 - p_2 + 1)2^n(2(d+1))^{n-p_2} = 2^n d^{O(n-p_2)} = d^{O(n)}.$$

Modifying slightly our arguments, we obtain a better bound for $\deg(S)$ (and hence for the number of absolutely irreducible components). The idea is to use a smaller family of $p(n-p)+1$ $(n-p)$-subspaces instead of all $\binom{n}{p}$ coordinate $(n-p)$-planes in the construction of $\mathcal{V}$ based on the following lemma due to Chistov [5].

Lemma 4 *For each p with $1 \leq p \leq n$ there exists a family $\mathcal{A}_p$ with $p(n-p)+1$ elements of $n-p$-planes in $\mathbf{R}^n$ such that for any p- plane $P \subset \mathbf{R}^n$ there is a $n-p$-plane $Q \in \mathcal{A}_p$ which is transversal to P.*

We get

$$\deg(S) \leq (60sd/n)^n \sum_{p_2 \leq p \leq p_1} ((n-p)p+1)(2(d+1))^{n-p}$$
$$\leq (60sd/n)^n (p_1 - p_2 + 1)(p_1(n-p_2)+1)(2(d+1))^{n-p_2}$$
$$= (O(sd/n))^n d^{O(n-p_2)} = s^n d^{O(n)}$$

in the case of a general semi-algebraic set S; and

$$\deg(S) \leq \sum_{p_1 \leq p \leq p_2} ((n-p)p+1)(2(d+1))^{n-p}$$
$$\leq (p_1 - p_2 + 1)(p_1(n-p_2)+1)(2(d+1))^{n-p_2}$$
$$= p_1 d^{O(n-p_2)} = d^{O(n)}$$

in the case of a basic semi-algebraic S.

Observe that for a basic S the bound $p_1 d^{O(n-p_2)}$ is better than the original bound $2^n d^{O(n-p_2)}$.

The theorems announced in the Introduction are proved.

Remark that unfortunately, we do not know how to construct the linear spaces of the preceeding Lemma 4 within polynomial time.

7 Application to complexity theory

Let us mention an application of the degree estimate to complexity theory. One of the central problems there is to obtain *lower* complexity bounds for deciding membership to a semi-algebraic set with respect to algebraic computation tree model. The lower bound is expected to be of the kind $\Omega(\nu(S))$ where $\nu(S)$ is a nonnegative characteristic of (i.e., nonnegative function on) the semi-algebraic set S. Examples of ν are: number of all connected components, Euler characteristic, sum of all Betti numbers of S.

The general methodology (see Yao, [17] says that if ν satisfies certain three axioms, then the complexity k of testing membership (i.e., the height k of algebraic computation tree) can be bounded from below:

$$k \geq \Omega(\log(\nu(S))).$$

The axioms are:

- $\nu(S_1 \cup S_2) \leq \nu(S_1) + \nu(S_2)$;
- $\nu(\text{isomorphic} \quad \text{projection}(S)) \leq \nu(S)$;
- if S is defined by system of equations and s inequalities of degrees at most d, then $\nu(S) \leq (sd)^{O(n)}$.

The degree of S verifies theese axioms (the proof of (2) is straightforward for the degree). Hence, any algebraic computation tree testing membership to S must have the height not less than $\Omega(\log(\deg(S)))$. This bound appears to be a useful complement to topological lower bounds, because it can be nontrivial for sets S having simple topology (for example for a neighbourhood of a smooth point of a real variety of high degree).

To get a better lower bound, take as $\nu(S)$ the sum of degrees of subsets of points of s of a fixed local dimension.

8 Appendix

Here we formulate some propositions describing the fundamental procedures used as subroutines in our algorithm, coming from [4] and [8].

Consider the ring $\mathbf{F} = \mathbf{Z}[T_1, \ldots, T_\ell] = \mathbf{Z}[\mathbf{T}] =$ where elements $T_1, \ldots, T_\ell$ are algebraically independent over $\mathbf{Q}$ and denote by $\mathbf{C}'$ the algebraic closure of $\mathbf{F}$.

Let $\mathcal{V} \subset \mathbf{C}'^n$ by a variety irreducible over

$$\mathbf{F}' = \mathbf{C}_{alg}(T_1, \ldots, T_\ell)$$

of affine dimension $\dim'_{\mathbf{C}}(\mathcal{V}) = p$Let $t_1, \ldots, t_p$ be algebraically independent over $\mathbf{F}$. A generic point can be described by the following isomorphism of fields:

$$\mathbf{F}'(t_1, \ldots, t_p)[\theta] \simeq \mathbf{F}'(\chi_{j_1}, \ldots, \chi_{j_p}, \chi_1, \ldots, \chi_n) \subset \mathbf{F}'(\mathcal{V}),$$

where θ is an algebraic element over the field $\mathbf{F}'(t_1, \ldots, t_p)$. Let $\Phi \in \mathbf{F}'(t_1, \ldots, t_p)[Z]$ with be the monic minimal polynomial of θ. The elements χ_j are considered as regular functions on $\mathcal{V}$; under the above isomorphism, $t_i \longrightarrow \chi_{j_i}$ where $1 \leq i \leq p$. Formally we shall describe a generic point by a list: Φ, $\chi_1, \ldots, \chi_n$, where these polynomials a given in a *standard representation*

Proposition 3 *([4],[8]). Consider a complex algebraic variety*

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

where $h_i \in \mathbf{F}[Y_1, \ldots, Y_n] = F[\mathbf{Y}]$; the degrees $\deg_{\mathbf{Y}}(h_i) < d$, $\deg_{\mathbf{T}}(h_i) < d_1$; the bit-lengths of integral coefficients of h_i are less than M.

There is an algorithm which given $\mathcal{V}$ and m, $1 \leq m \leq n$ outputs all its absolutely irreducible over $\mathbf{F}'$ in $\mathbf{C}'$ components $\mathcal{V}_1, \ldots, \mathcal{V}_q$ of codimension m. The number of the components q is less than d^m and the degree $\deg(\mathcal{V})$ is less than d^n (by Bézout's theorem). Each component $\mathcal{V}_\alpha$, $1 \leq \alpha \leq q$ is represented by its generic point

$$\Phi^{(\alpha)},\ \chi_1^{(\alpha)}, \ldots, \chi_n^{(\alpha)}$$

and by a system of equations:

$$h_1^{(\alpha)} = \cdots = h_{\ell_\alpha}^{(\alpha)} = 0,$$

with $\ell_\alpha < (3(d+d_1)^m)^{n+\ell}$, and every $h_i^{(\alpha)} \in \mathbf{F}'[Y_1, \ldots Y_n]$ is given in a standard representation with degrees

$$\left((d+d_1)^{cm}, (d^m d_1)^c\right)$$

and bit lengths

$$\left(M(d+d_1)^{cm(n-m+\ell)}, M(d^m d_1)^{c\ell}\right)$$

for a certain integer $c > 0$.

Herewith, the following estimates hold:

$$\deg(\mathcal{V}_\alpha) < d^m \deg_{\mathbf{T},\mathbf{Y}}(h_i^{(\alpha)}) < (d+d_1)^{cm}$$
$$\deg_Z(\Phi^{(\alpha)}) < d^m$$
$$\deg_{\mathbf{T},\mathbf{t}}(\Phi^{(\alpha)}),\ \deg_{\mathbf{T},\mathbf{t}}(\chi_i^{(\alpha)}) < (d^m d_1)^c$$

for a certain integer $c > 0$.

Every $\Phi^{(\alpha)}$, $\chi_i^{(\alpha)}$ is given in a standard representation with degrees

$$\left(d^m, (d^m d_1)^c\right),$$

and bit lengths

$$\big((M+n+\ell)(d^m d_1)^c, (M+n+\ell)(d^m d_1)^c\big)$$

for a certain integer $c > 0$.

The running time of the algorithm does not exceed

$$M^{O(1)}(d+d_1)^{O(m(n+\ell))}.$$

Proposition 4 *([4],[8]). Let*

$$\mathcal{V}_\alpha = \{h_1^{(\alpha)} = \cdots = h_{\ell_\alpha}^{(\alpha)} = 0\} \subset \mathbf{C}'^n$$

be an absolutely irreducible variety of codimension m and degree $\deg(\mathcal{V}_\alpha) \le d^m$. Here the polynomials

$$h_i^{(\alpha)} \in \mathbf{F}'[Y_1, \dots, Y_n]$$

are given in a standard representation with degrees

$$\big((d+d_1)^{cm}, (d^m d_1)^c\big)$$

and bit lengths

$$\big(M(d+d_1)^{cm(n-m+\ell)}, N(d^m d_1)^{c\ell}\big)$$

for a certain integer $c > 0$.

Let also a representation of $\mathcal{V}_\alpha$ in the form of the generic point be given, described by a list $\Phi^{(\alpha)}$, $\chi_1^{(\alpha)}, \dots, \chi_n^{(\alpha)}$. Each $\Phi^{(\alpha)}$, $\chi_i^{(\alpha)}$ is given in a standard representation with degrees

$$\big(d^m, (d^m d_1)^c\big),$$

and bit lengths

$$\big((M+n+\ell)(d^m d_1)^c, (M+n+\ell)(d^m d_1)^c\big)$$

for a certain integer $c > 0$.

Suppose that the same bounds as in the conclusion of Proposition 3 are true for

$$\ell_\alpha, \quad \deg_{\mathbf{T},\mathbf{X}}(h_i^{(\alpha)}),$$
$$\deg_Z(\Phi^{(\alpha)}), \quad \deg_{\mathbf{T},\mathbf{t}}(\Phi^{(\alpha)}), \quad \deg_{\mathbf{T},\mathbf{t}}(\chi_i^{(\alpha)}).$$

Then there is an algorithm which outputs all irreducible over $\mathbf{F}'$ components $\mathcal{V}_{\alpha,\beta}$ of the variety $\mathcal{V}_\alpha \cap \{Y_1 = 0\} \subset \mathbf{C}'^n$. The number of the components is less than d^m (by Bézout's theorem). Each component $\mathcal{V}_{\alpha,\beta}$ of the codimension $m+1$ is represented by its generic point

$$\Phi^{(\alpha,\beta)}, \chi_1^{(\alpha,\beta)}, \dots, \chi_n^{(\alpha,\beta)}$$

and by a system of equations:

$$h_1^{(\alpha,\beta)} = \cdots = h_{\ell_{\alpha,\beta}}^{(\alpha,\beta)} = 0,$$

with $\ell_{\alpha,\beta} < (3(d+d_1)^m)^{n+\ell}$, and every $h_i^{(\alpha,\beta)} \in \mathbf{F}'[\mathbf{Y}]$ is given in a standard representation with the same bounds as for polynomials $h_i^{(\alpha)}$ in Proposition 3. Estimates for polynomials $\Phi^{(\alpha,\beta)}, \chi_i^{(\alpha,\beta)}$ are the same as for $\Phi^{(\alpha)}, \chi_i^{(\alpha)}$ in Proposition 3. The running time of the algorithm does not exceed

$$M^{O(1)}(d+d_1)^{O(m(n+\ell))}$$

References

[1] S. Basu, R. Pollack, M.-F. Roy, *A New Algorithm to Find a Point in Every Cell Defined by a Family of Polynomials.* "Quantifier Elimination and Cylindrical Algebraic Decomposition", B. Caviness and J. Johnson Eds., Springer-Verlag, to appear.

[2] S. Basu, R. Pollack, M.-F. Roy, *On the Combinatorial and Algebraic Complexity of Quantifier Elimination.* Journal of the ACM , to apperar.

[3] J. Bochnak, M. Coste, and M.-F. Roy, *Géométrie Algébrique Réelle.* Springer-Verlag, Berlin, 1987.

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

[5] A. Chistov, *Fast parallel calculation of the rank of matrices over a field of arbitrary characteristic.* Lecture Notes Computer Sci. **199** (1985), 63–69.

[6] A. Chistov, *Polynomial time computation of the dimension of components of algebraic varieties in zero-characteristic.* Preprint 95-06, Université Paris 12 (1995).

[7] A. Galligo, N. Vorobjov, *Complexity of finding irreducible components of a semialgebraic set.* J. Complexity **11** (1995), 174–193.

[8] D. Grigoriev, *Factorization of polynomials over finite field and the solution of systems of algebraic equations.* In Zapiski Nauchnykh Seminarov LOMI**137** (1984), 20–79. English translation in J. Soviet Math. **34** (1986), 1762–1803.

[9] D. Grigoriev, N. Vorobjov , *Solving systems of polynomial inequalities in subexponential time.* J. Symbolic Comput. **5** (1988), 37–64.

[10] J. Heintz, , *Definability and fast quantifier elimination in algebraically closed fields.* Theoret. Comput. Sci. **24** (1983), 239–278.

[11] S. Lang, *Algebra.* New York: Addison-Wesley (1965).

[12] R. Pollack, M.-F. Roy, *On the number of cells defined by a set of polynomials.* C. R. Acad. Sci. Paris **316** (1993), 573–577.

[13] J. Renegar, *A faster PSPACE algorithm for existential theory of reals.* Proc. 29th IEEE Symp. on Foundations of Comput. Sci. (1988), 291–295.

[14] M.-F. Roy, N. Vorobjov, *Finding irreducible components of some real transcendental varieties.* Comput. Complexity **4** (1994), 107–132.

[15] A. Tarski, *A Decision Method for Elementary Algebra and Geometry.* Univerity of California Press, Berkeley (1951).

[16] H. E. Warren, (*Lower bounds for approximation of nonlinear manifolds.* Trans. Amer. Math. Soc. **133** (1968), 167–178.

[17] A. YAO, *Decision tree complexity and Betti numbers*. Proc. of ACM Symposium on Theory of Computing (1994), 615–624.

MARIE-FRANÇOISE ROY is Professor of Mathematics at the University of Rennes I (France). She is a specialist in real algebraic geometry, more particularly (and recently), in the algorithmic aspects of this theory.

NICOLAI VOROBJOV is a Lecturer in Computing at the University of Bath, U.K. His research interests are in complexity theory and computational algebraic geometry.