SPb. Math. Society Preprint 1999-10 06 Dec 1999

Strong Version of the Basic Deciding Algorithm for the Existential Theory of Real Fields

Alexander L. Chistov *

St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia
14th line 39, St. Petersburg 199178, Russia,
e-mail: labta@iias.spb.su or sliss@iias.spb.su

1999

Abstract

Let U be a real algebraic set in n–dimensional affine space which is given as a set of zeros of a family of polynomials of degrees less than d. Let U_i, $i \in I$ be the family of all irreducible components of U. Let $U_i^{(s)}$ be the closure in the classical topology of the set of all smooth points of dimension s of U_i. In the paper an algorithm is described for constructing a finite set S of points of U which has a non–empty intersection with every connected component of every $U_i^{(s)}$ for every $i \in I$, $0 \leq s \leq n$. The number of points of S is bounded from above by a polynomial in d^n. The similar result is valid for basic semi–algebraic sets. The working time of the algorithm (for the case of algebraic varieties) is polynomial in the size of input and d^n. More precise formulations are given below involving triangulations of U if U is bounded (respectively of the Alexandrov compactification of U if U is not bounded).

*Research partially supported by the Volkswagen–Stiftung, Program on Computational Complexity.

Introduction

Let U be a real algebraic set in n–dimensional affine space which is given as a set of zeros of a family of polynomials of degrees less than d. Let U_i, $i \in I$ be the family of all irreducible components of U. Let $U_i^{(s)}$ be the closure in the classical topology of the set of all smooth points of dimension s of U_i. In the paper an algorithm is described for constructing a finite set S of points of U which has a non–empty intersection with every connected component of every $U_i^{(s)}$ for every $i \in I$, $0 \leq s \leq n$. The number of points of S is bounded from above by a polynomial in d^n. The similar result is valid for basic semi–algebraic sets. The working time of the algorithm (for the case of algebraic varieties) is polynomial in the size of input and d^n. More precise formulations are given below involving triangulations of U if U is bounded (respectively of the Alexandrov compactification of U if U is not bounded).

Previously known algorithms with the same working time [14], [1] allow to construct only a finite set of points S' with the number of elements bounded from above by a polynomial in d^n which has a non–empty intersection only with every connected component of a real algebraic variety (or a real semi–algebraic set).

Now we give the precise statements. Let $k_0 = \mathbb{Q}(t_1, \ldots, t_l, \theta)$ be a real ordered field where $t_1, \ldots, t_l$ are algebraically independent over the field $\mathbb{Q}$ and θ is algebraic over $\mathbb{Q}(t_1, \ldots, t_l)$ with the minimal polynomial $F \in \mathbb{Q}[t_1, \ldots, t_l, Z]$ and leading coefficient $lc_Z F$ of F is equal to 1.

We shall assume in what follows that the field k_0 satisfies the following property.

(A) *Let a finite extension $k_1 \supset k_0$ of real ordered fields be given by its primitive element and minimal polynomial. Then for an element $a \in k_1$ one can decide whether $a > 0$ within the polynomial time.*

Note that if $k_0 = \mathbb{Q}$ then k_0 satisfies this property. If the field k_0 satisfies this property then any finite extension k_1 which is real ordered field extension of k_0 also satisfies this property. If $\varepsilon > 0$ is an infinitesimal relative to the field k_0 then the real ordered field $k_0(\varepsilon)$ satisfies the formulated property.

Let polynomials $f_1, \ldots, f_m \in k_0[X_1, \ldots, X_n]$ be given, $n \geq 1$, $m \geq 1$. Consider the closed algebraic set or algebraic variety (in this paper we do not distinguish these two concepts)

$$V = \{(x_1, \ldots, x_n) : f_i(x_1, \ldots, x_n) = 0,\ x_i \in \overline{k_0},\ \forall 1 \leq i \leq m\} \subset \mathbb{A}^n(\overline{k_0}) .$$

This is a set of all common zeros of polynomials $f_1, \ldots, f_m$ in $\mathbb{A}^n(\overline{k_0})$, where $\overline{k_0}$ is algebraic closure of k_0. In what follows we shall denote for brevity this set by $\mathcal{Z}(f_1, \ldots, f_m)$. The similar notation will be used also for the sets of all common zeros (in affine or projective spaces as it will be seen from the context) of other polynomials. So $V = \mathcal{Z}(f_1, \ldots, f_m)$.

Let R be a real closed field containing the real closure $\widetilde{k_0}$ of the field k_0 and $C = \overline{R}$ be the algebraic closure of R. Set

$$V(R) = \{(x_1, \ldots, x_n) : f_i(x_1, \ldots, x_n) = 0,\ x_i \in R,\ \forall 1 \leq i \leq m\} \subset \mathbb{A}^n(R) .$$

This is a set of all common zeros of polynomials $f_1, \ldots, f_m$ in $\mathbb{A}^n(R)$. In what follows we shall denote for brevity this set by $\mathcal{Z}_R(f_1, \ldots, f_m)$. The similar

notation will be used also for the sets of all common zeros (in affine or projective spaces as it will be seen from the context) of other polynomials. So $V(R) = \mathcal{Z}_R(f_1, \ldots, f_m)$ is a real algebraic set or (the set of points of) a real algebraic variety over R (the definition of real algebraic varieties see in [2]). The elements of $\mathcal{Z}_R(f_1, \ldots, f_m)$ are real roots of polynomials $f_1, \ldots, f_m$.

We shall represent each polynomial $f = f_i$ in the form

$$f = \frac{1}{a_0} \sum_{i_1, \ldots, i_n} \sum_{0 \le j < \deg_Z F} a_{i_1, \ldots, i_n, j} \theta^j X_1^{i_1} \cdots X_n^{i_n} ,$$

where $a_0, a_{i_1, \ldots, i_n, j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\gcd_{i_1, \ldots, i_n, j}(a_0, a_{i_1, \ldots, i_n, j}) = 1$. Define the length $l(a)$ of an integer a by the formula $l(a) = \min\{s \in \mathbb{Z} : |a| < 2^{s-1}\}$. The length of coefficients $l(f)$ of the polynomial f is defined to be the maximum of length of coefficients from $\mathbb{Z}$ of polynomials $a_0, a_{i_1, \ldots, i_n, j}$ and the degree

$$\deg_{t_\alpha}(f) = \max_{i_1, \ldots, i_n, j} \{\deg_{t_\alpha}(a_0), \deg_{t_\alpha}(a_{i_1, \ldots, i_n, j})\} ,$$

where $1 \le \alpha \le l$. In the similar way $\deg_{t_\alpha} F$ and $l(F)$ are defined.
We shall suppose that we have the following bounds

$$\deg_{X_1, \ldots, X_n}(f_i) < d,\ \deg_{t_\alpha}(f_i) < d_2,\ l(f_i) < M,$$
$$\deg_Z(F) < d_1,\ \deg_{t_\alpha}(F) < d_1,\ l(F) < M_1 .$$

The size $L(f)$ of the polynomial f is defined to be the product of $l(f)$ to the number of all the coefficients from $\mathbb{Z}$ of f in the dense representation. We have

$$L(f_i) < (\binom{d+n}{n} d_1 + 1) d_2^l M$$

Similarly $L(F) < d_1^{l+1} M_1$. Unless we state otherwise, in what follows we suppose l to be fix.

REMARK 1 *In what follows we shall assume without loss of generality that the polynomials $f_1, \ldots, f_m$ are linearly independent over k_0. Hence* $\dim V \le n - 1$.

Consider at first the case when $V(R)$ is bounded. Consider some triangulation of $V(R)$, see [2], i.e., a finite simplicial complex $K = \cup_{1 \le i \le p} \sigma_i$ defined over the field R (here it means a simplicial space, not an abstract simplicial scheme on finite sets, i.e., $K \subset R^N$ for some N and each simplex σ_i is the convex hull of its vertices). and a semi–algebraic homeomorphism $\phi : K \to V(R)$ in the topology of the real field. We shall call for brevity the simplex σ of K to be maximal if and only if it is not a face of any other simplex of K. Let $0 \le s \le n - 1$. Consider a non–zero s–dimensional cycle $e = \sum_{1 \le j \le q} \sigma_{p_j}$ with coefficients from $\mathbb{Z}/2\mathbb{Z}$ of the simplicial complex K such that σ_{p_j} is maximal for every j and $p_{j_1} \ne p_{j_2}$ if $j_1 \ne j_2$. So the dimension $\dim \sigma_{p_j} = s$ for every j. Denote $E = |e| = \cup_{1 \le j \le q} \phi(\sigma_{p_j})$.

REMARK 2 *Note that if there is an irreducible component W of $V(R)$ of dimension s over R then there is also a cycle e as described such that $|e|$ coincides with the set of all points of dimension s of W. This follows from the fact that for an arbitrary $(s-1)$–dimensional simplex t from the triangulation of W the number of all s–dimensional simplexes from the considered triangulation containing t as a face is even, see [2].*

Now let a non–zero vector $y = (y_1, \ldots, y_n) \in R^n$ be given. By the transfer principle, see [2], the function $\sum_{1 \le i \le n} y_i X_i$ has its maximum and minimum on E. Denote

$$m' = \max(\sum_{1 \le i \le n} y_i X_i)(E), \qquad E' = \{z \in E \, : \, (\sum_{1 \le i \le n} y_i X_i)(z) = m'\},$$
$$m'' = \min(\sum_{1 \le i \le n} y_i X_i)(E), \qquad E'' = \{z \in E \, : \, (\sum_{1 \le i \le n} y_i X_i)(z) = m''\}$$

(to avoid ambiguity of notation note that in next sections we shall also consider the cases when the coordinates of y are from a field extension of R).

THEOREM 1 *Let $V(R)$ be a bounded real affine algebraic variety given as a set of zeroes of polynomials $f_1, \ldots, f_m$. Then for a given non-zero vector $y \in k_0^n$ one can construct a finite set S_y of points of $V(R)$ such that for every $0 \le s \le n-1$ for any semi–algebraic triangulation $\phi : K \to V(R)$ and any non-zero s–dimensional cycle e with coefficients from $\mathbb{Z}/2\mathbb{Z}$ as described above the intersections $S_y \cap E'$ and $S_y \cap E''$ are non–empty. The number of points of S_y is bounded from above by a polynomial in d^n. The working time of the algorithm for constructing S_y is polynomial in d^n, d_1, d_2, M, M_1, m and the size of the vector y.*

Theorem 1 will be deduced from our existence theorem which will be formulated and proved in Section 2. Note that it may happen in some cases that $E = E' = E''$, e.g. when $s = 0$ and E consists of one point. Applying Theorem 1 to n linearly independent vectors $y^{(1)}, \ldots, y^{(n)}$ and defining $S = \cup_{1 \le i \le n} S_{y^{(i)}}$ we get the following result.

COROLLARY 1 *Let $1 \le s \le n-1$. One can construct a finite set S of points of $V(R)$ such that for any semi–algebraic triangulation $\phi : K \to V(R)$ and any s–dimensional cycle e as described above with coefficients from $\mathbb{Z}/2\mathbb{Z}$ the intersection $S \cap E$ consists of at least two different points. The number of points of S is bounded from above by a polynomial in d^n. The working time of the algorithm for constructing S is polynomial in d^n, d_1, d_2, M, M_1, m.*

In the general case, i.e. when $V(R)$ is not necessary bounded, one can verify that $V(R)$ is not bounded within the time polynomial in d^n, d_1, d_2, M, M_1, m. Recall, see [2], the construction of the algebraic variety V_1 such that $V_1(R)$ is the Alexandrov compactification of $V(R)$ if $V(R)$ is not bounded. Namely, one should construct a point $x^{(0)} \in \mathbb{A}^n(R)$ such that $x^{(0)} \notin V(R)$. We can suppose without loss of generality that $x^{(0)} = (0, \ldots, 0)$ effecting if it is necessary an appropriate linear transformation of coordinates in $\mathbb{A}^n(R)$. Set

$$g_i = (\sum_{1 \le i \le n} X_i^2)^{\deg f_i} f_i \left(\frac{X_1}{\sum_{1 \le i \le n} X_i^2}, \ldots, \frac{X_n}{\sum_{1 \le i \le n} X_i^2} \right), \; 0 \le i \le m.$$

Define $V_1 = \mathcal{Z}(g_1, \ldots, g_m)$. So V_1 is bounded. We have the isomorphism of real algebraic varieties $\iota : V(R) \to V_1(R) \setminus \{x^{(0)}\}$ induced by the inversion transformation

$$(X_1, \ldots, X_n) \mapsto \left(\frac{X_1}{\sum_{1 \le i \le n} X_i^2}, \ldots, \frac{X_n}{\sum_{1 \le i \le n} X_i^2} \right).$$

Let K, ϕ, s, e have the same meaning for $V_1(R)$ as previously for $V(R)$. Applying Corollary 1 to the real algebraic variety $V_1(R)$ we get the following result.

COROLLARY 2 *Let $V(R)$ be a not bounded real affine algebraic variety given as a set of zeroes of polynomials $f_1, \ldots, f_m$. One can construct a finite set S of points of $V(R)$ such that for any $0 \leq s \leq n-1$ for any semi–algebraic triangulation $\phi : K \to V_1(R)$ of $V_1(R)$ and any its s–dimensional cycle e with coefficients from $\mathbb{Z}/2\mathbb{Z}$ as described above the intersection $\iota(S) \cap E$ is non–empty. The number of points of S is bounded from above by a polynomial in d^n. The working time of the algorithm for constructing S is polynomial in d^n, d_1, d_2, M, M_1, m.*

Now let $g_1, \ldots g_s \in k_0[X_1, \ldots, X_n]$ be some polynomials which have the similar estimations for degrees and sizes of integer coefficients as $f_1, \ldots, f_m$. Consider a basic semi–algebraic set, see [14], [1],

$$U = \{x \in R^n : f_1(x) = \ldots = f_m(x) = 0 \,\&\, g_1(x) > 0 \,\&\, \ldots \,\&\, g_s(x) > 0\}. \quad (1)$$

Let $s \leq s'n < s+n$ and $s' \in \mathbb{Z}$. If $s < n$ set $g_j = 1$ for all $s+1 \leq j \leq n$. Set $s_j = s'j$ for $j = 0, \ldots, n-1$ and $s_n = \max\{s, n\}$. Let $Z_1, \ldots, Z_n$ and T be new variables. Consider the real algebraic variety $U_1 \subset \mathbb{A}^{n+2}$ which is the set of all common zeroes of polynomials $\prod_{s_{j-1}+1 \leq i \leq s_j} g_i - Z_j$, $1 \leq j \leq n$; $f_1, \ldots, f_m$ and $T \prod_{1 \leq j \leq n} Z_j - 1$ (so in the case when $s < n$ the polynomials $1 - Z_j$, $s+1 \leq j \leq n$, belong to the considered family). Denote by

$$\pi : R^{2n+1} \to R^n, \quad (X_1, \ldots, X_n, Z_1, \ldots, Z_n, T) \mapsto (X_1, \ldots, X_n)$$

the linear projection. Then the set U coincides with $\pi(U_2)$ where U_2 is a union of some connected components of U_1. Thus, applying Corollary 2 and Remark 2 to the real algebraic variety U_1 we get the following result.

THEOREM 2 *Consider a basic semi–algebraic set (1). Let U_i, $i \in I$ be the family of all irreducible components of U (see e.g. [15]). Let $U_i^{(s)}$ be the closure in the classical topology of the set of all smooth points of dimension s of U_i. Then one can construct a finite set S of points of U which has a non–empty intersection with every connected component of every $U_i^{(s)}$ for every $i \in I$, $0 \leq s \leq n-1$. The number of points of S is bounded from above by a polynomial in $((1+s/n)d)^n$. The working time of the algorithm for constructing S is polynomial in $((1+s/n)d)^n$, d_1, d_2, M, M_1, m*

REMARK 3 *The working time of the algorithms from theorems of this paper and their corollaries is essentially the same as for solving system of polynomial equations with a finite set of solutions in the projective space over an algebraically closed field. So they can be formulated also in the case when l is not fixed, see [5].*

1 One algorithm of reduction to general position

Let $V(R)$ be a real algebraic variety such as in the Introduction. So

$$V(R) = \mathcal{Z}_R(f_1, \ldots, f_m),$$

see the Introduction. We shall suppose in this section $V(R)$ to be non-empty and bounded, i.e. there is $a \in R$, $a > 0$ such that

$$\emptyset \neq V(R) \subset \{(x_1, \ldots, x_n) \in R^n \ : \ \sum_{1 \leq i \leq n} x_i^2 \leq a\} = B_a.$$

We shall suppose also in what follows that the intersection with the bound of the ball B_a

$$V(R) \cap \partial B_a = V(R) \cap \mathcal{Z}_R(\sum_{1 \leq i \leq n} x_i^2 - a) = \emptyset. \tag{2}$$

Denote $f = \sum_{1 \leq i \leq m} f_i^2$. Let $g = 1 + X_1^{2d+2} + \ldots + X_n^{2d+2}$.

Let $\varepsilon > 0$ be an infinitesimal relative to the field R. Denote $f_\varepsilon = f - \varepsilon g$. Let $\varepsilon^{(0)}$ and $\varepsilon^{(1)}$ be new variables.

Set $\overline{f} = X_0^{2d+2} f(X_1/X_0, \ldots, X_n/X_0)$, $\overline{g} = \sum_{0 \leq i \leq n} X_i^{2d+2}$ and

$$h = \varepsilon^{(0)} \overline{f} - \varepsilon^{(1)} \overline{g} \in R[\varepsilon^{(0)}, \varepsilon^{(1)}, X_0, \ldots, X_n,]$$

i.e., h is the $\mathbb{P}^1 \times \mathbb{P}^n$–homogenization of f_ε, herewith the coordinates of $\mathbb{P}^1$ are $(\varepsilon^{(0)} : \varepsilon^{(1)})$, $\varepsilon = \varepsilon^{(0)}/\varepsilon^{(1)}$, and the coordinates of $\mathbb{P}^n$ are $(X_0 : \ldots : X_n)$. Let $y_2, \ldots, y_n$ be elements from a field extension of R. Denote $y = (y_2, \ldots, y_n)$, and set the fields

$$\begin{array}{ll} K_1 = R(y_2, \ldots, y_n), & C_1 = C(y_2, \ldots, y_n), \\ K_2 = R(\varepsilon, y_2, \ldots, y_n), & C_2 = C(\varepsilon, y_2, \ldots, y_n) \end{array}$$

In the case when $y_2, \ldots, y_n$ are elements from a real ordered field extension of R we shall denote also $R_1 = K_1$ and $R_2 = K_2$. In this case R_i are real ordered fields and C_i have real structures, see [3], [4], in the natural way. In the general case we shall suppose without loss of generality that the field K_1 is supplied with a real structure. Then it induces the real structures on C_1, K_2, C_2.

Consider the following system of polynomial equations in $X_0, \ldots, X_n$ and $\varepsilon^{(0)}, \varepsilon^{(1)}$

$$\left\{ \begin{array}{l} h = 0, \\ \frac{\partial h}{\partial X_i} - y_i \frac{\partial h}{\partial X_1} = 0, \quad 2 \leq i \leq n. \end{array} \right. \tag{3}$$

LEMMA 1 *Let $\varepsilon = \varepsilon^{(1)}/\varepsilon^{(0)}$. Consider (3) as a system in $X_0, \ldots, X_n$. Then system (3) has a finite number of solutions in $\mathbb{P}^n(\overline{C_2})$.*

PROOF Consider the system

$$\left\{ \begin{array}{ll} X_0^{2d+2} + X_1^{2d+2} + \ldots + X_n^{2d+2} = 0, & \\ X_i^{2d+1} - y_i X_1^{2d+1} = 0, & 2 \leq i \leq n. \end{array} \right. \tag{4}$$

which is obtained by replacing h by $\overline{g}$ in (3). System (4) has a finite number of solutions in $\mathbb{P}^n(\overline{C_1})$. So, cf. [5] or [3], Corollary 4.1, system (3) has a finite number of solutions in $\mathbb{P}^n(\overline{C_2})$. The lemma is proved.

COROLLARY 3 *Let system (3) have a solution $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_2})$ with $\eta_0 = 0$. Then $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_1})$ is a solution of system (4). Such a solution $(\eta_0 : \ldots : \eta_n)$ exists if and only if there are integers $j_2, \ldots, j_n$ for which*

$$1 + \sum_{2 \leq i \leq n} \zeta_{2d+1}^{j_i} y_i^{(2d+2)/(2d+1)} = 0,$$

where ζ_{2d+1} is a primitive root of the unit of degree $2d+1$.

PROOF It follows from the fact that $\deg f < 2d+2$. The corollary is proved.

Let $\varepsilon^{(1)}/\varepsilon^{(0)} = \varepsilon$. Then the solutions $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_2})$ of system (3) can be of the following types

(i) with $\eta_0 = 0$, then $(\eta_0 : \ldots : \eta_n) \in \mathbb{P}^n(\overline{C_1})$ by Corollary 3,

(ii) with $\eta_0 = 1$ and such that $\sum_{1 \le i \le n} |\eta_i|^2$ is an infinitely large relative to C_1,

(iii) with $\eta_0 = 1$ and such that every η_i, $1 \le i \le n$, is not infinitely large relative to the field C_1.

Using the algorithms from [5], [3], [4] when $y_2, \ldots, y_n \in k_0$ one can compute all the solutions of system (3) of type (i) (respectively (ii), (iii)) within the time polynomial in d^n, d_1, d_2, M, M_1, m and the size of the vector y.

Denote by $\mu_2(y) = \mu_2(y_2, \ldots, y_n)$ (respectively $\mu_0(y) = \mu_0(y_2, \ldots, y_n)$) the number of all roots counting with multiplicities of type (iii) (respectively of type (ii) or (iii)) of system (3). So we have by the Bézout theorem $\mu_0(y) \le (2d+2)(2d+1)^{n-1}$.

LEMMA 2 *Let $y_2, \ldots, y_n$ be elements from a real ordered field extension of R. Then system (3) has at least two different roots η' and η'' of type (iii) with coordinates in the real closure $\widetilde{R_2}$ of the field R_2. All the coordinates of the roots η' and η'' are not infinitely large relative to the field R.*

PROOF (Cf. [15], [14].) Replace R by $\mathbb{R}$, the infinitesimal ε by a positive number $\varepsilon \in \mathbb{R}$, and let $y_2, \ldots, y_n \in \mathbb{R}$. Then $\mathcal{Z}_{\mathbb{R}}(f_\varepsilon)$ for all sufficiently small $\varepsilon > 0$ has a connected component W' which is contained in B_a, see (2), and does not have any connected component W'' which has a non–empty intersection with the sphere ∂B_a. Denote by W_1 the union of all connected components W' of $\mathcal{Z}_{\mathbb{R}}(f_\varepsilon)$ such that W' is contained in B_a. The set

$$\mathcal{Z}_{\mathbb{R}}(f) = \mathcal{Z}_{\mathbb{R}}(f/g) \subset \mathcal{Z}_{\mathbb{R}}(\partial(f/g)/\partial X_1, \ldots, \partial(f/g)/\partial X_n) = W_2.$$

The function f/g is constant on every piecewise smooth connected curve contained in W_2. Hence the function f/g is constant on every connected component of W_2. Hence $\mathcal{Z}_{\mathbb{R}}(f)$ is a union of some compact connected components of W_2. Therefore, there is an open in the classic topology neighborhood U_1 of $\mathcal{Z}_{\mathbb{R}}(f)$ such that $U_1 \cap W_2 = \mathcal{Z}_{\mathbb{R}}(f)$. The function f/g is positive in every point of the compact set $B_a \setminus U_1$. Hence for all sufficiently small $\varepsilon > 0$ the set $W_1 \subset U_1$. Therefore, W_1 is a smooth bounded hypersurface in $\mathbb{A}^n(\mathbb{R})$ for all sufficiently small $\varepsilon > 0$.

Since W_1 is a bounded hypersurface there are at least two different points η', η'' of W_1 in which the hyperplanes of support have the normal vector parallel to $(1, y_2, \ldots, y_n)$. These hyperplanes of support are tangent spaces of $\mathcal{Z}_{\mathbb{R}}(f_\varepsilon)$ in the points η' and η''. So η' and η'' are solutions of (3) in $\mathbb{A}^n(\mathbb{R})$. Now the required assertion follows from the transfer principle, see [2]. The last statement of the lemma follows from the fact that the absolute values of the coordinates of all points from $V(R_2)$ are bounded from above by the same constant from R as the absolute values of the coordinates of all points from $V(R)$. The lemma is proved.

COROLLARY 4 *Let $y_2, \ldots, y_n$ be elements from a real ordered field extension of R. Then the inequality $\mu_2(y) \geq 2$ holds.*

Denote by

$$D(y) \in K_1[\varepsilon^{(0)}, \varepsilon^{(1)}, U_0, \ldots, U_n]$$

the U–resultant, see e.g. [9], [11], of (3) considered as a system in $X_0, \ldots, X_n$. The polynomial $D(y)$ is equal (up to a factor from $R(\varepsilon^{(0)}, \varepsilon^{(1)}, y_2, \ldots, y_n)$) to the product $\prod_{j \in J}(\sum_{0 \leq i \leq n} U_i \eta_i^{(j)})$ where $\eta^{(j)} = (\eta_0^{(j)} : \ldots : \eta_n^{(j)})$, $j \in J$ is a family of all roots (counting them with multiplicities) of system (3) in $\mathbb{P}^n(\overline{C_2})$. Denote by J' (respectively J'', J''') the subset of indices of J such that $j \in J'$ (respectively $j \in J''$, $j \in J'''$) if and only if the root $\eta^{(j)}$ of system (3) is of type (i) (respectively (ii), (iii)).

Let q be a coefficient in a monomial in $U_0, \ldots, U_n$ of the U–resultant of n homogeneous polynomials $F_1, \ldots, F_n$ in $X_0, \ldots, X_n$. Then it is known that q is a homogeneous polynomial in the coefficients of F_i of the degree $(\prod_{1 \leq j \leq n} \deg F_j)/\deg F_i$ for every $1 \leq i \leq n$. Hence, the degree

$$\deg_{\varepsilon^{(1)}, \varepsilon^{(0)}} D(y) = (2dn + 2n - 1)(2d + 1)^{n-2}.$$

Let $L = l_0 X_0 + \ldots + l_n X_n \in \mathbb{Z}[X_0, \ldots, X_n]$ be a linear form with integer coefficients l_i, $0 \leq i \leq n$, such that L is not vanishing in any point of type (i) of the variety $\mathcal{W}' \subset \mathbb{P}^n(\overline{C_2})$ of solutions of system (3) and $L \neq l_0 X_0$. According to [11], see also [5], one can verify this condition within the time polynomial in d^n and the size of input including L.

Define the set of linear forms

$$\mathcal{L}_N = \{ \sum_{0 \leq i \leq n} c^i X_i \ : \ 1 \leq c \leq N, c \in \mathbb{Z}\}.$$

The form L satisfying the considered condition can be chosen from the set $\mathcal{L}_N$ with $N \leq \mathcal{P}(d^n)$ for a polynomial $\mathcal{P}$.

The linear form L is not vanishing in any point of type (i) of the variety $\mathcal{W}'$ if and only if the polynomial

$$D(y)(1, \varepsilon, L - l_0 X_0, -l_1 X_0, \ldots, -l_n X_0) \in K_1[L, X_0, \varepsilon]$$

is non–zero. This polynomial is vanishing on the variety $\mathcal{W}'$. Set $\iota_0(y)$ (respectively $\iota_1(L, y)$) to be the maximal integer a such that X_0^a (respectively ε^a) divides the polynomial $D(y)(1, \varepsilon, L - l_0 X_0, -l_1 X_0, \ldots, -l_n X_0)$. Then $\iota_0(y)$ is the number of roots of system (3) of type (i) and, hence, does not depend on the choice of L. Set

$$G(y) = D(y)(1, \varepsilon, L - l_0, -l_1, \ldots, -l_n) \in K_1[\varepsilon, L].$$

Denote by $H(y) \in K_1[\varepsilon, L]$ the separable polynomial which is equal to the product of all different irreducible factors of $G(y)$ which do not belong to $K_1[\varepsilon]$. According to [11], see also [5], one can compute the polynomial $G(y)$ within the time polynomial in d^n and the size of input including L.

We have $\mu_0(y) = \deg_L G(y) = \deg_{U_0, \ldots, U_n} D(y) - \iota_0(y)$. Represent

$$G(y) = \varepsilon^{\iota_1(L,y)} \sum_{0 \leq i \leq \mu_0(y)} a_i L^i,$$

where $a_i \in K_1[\varepsilon]$ for all i. Note that a_i depends on the coefficients $l_0, \ldots, l_n$ of the linear form L. So we shall denote also $a_i = a_i(l_0, \ldots, l_n)$.

LEMMA 3 *Let L be an arbitrary linear form which is not vanishing in any point of type (i) of the variety of solutions of system (3). Let $\mathrm{lc}_\varepsilon(a_{\mu_0(y)}(l_0, \ldots, l_n))$ be leading coefficient of the polynomial $a_{\mu_0(y)}(l_0, \ldots, l_n)$ in ε. Then the polynomial*

$$\varepsilon^{\iota_1(L,y)} a_{\mu_0(y)}(l_0, \ldots, l_n) / \mathrm{lc}_\varepsilon(a_{\mu_0(y)}(l_0, \ldots, l_n))$$

does not depend on the choice of L. Besides that,

$$\iota_1(L, y) + \deg_\varepsilon a_{\mu_0(y)}(l_0, \ldots, l_n) = (2dn + 2n - 1)(2d + 1)^{n-2}.$$

PROOF Represent the polynomial $D(y) = D_1 D_2$ where the polynomial D_1 (respectively D_2) is equal to $\prod_{j \in J'} \sum_{1 \le i \le n} U_i \eta_i^{(j)}$ (respectively $\prod_{j \in J'' \cup J'''} \sum_{0 \le i \le n} U_i \eta_i^{(j)}$) up to a factor from $K_1[\varepsilon]$. Hence, by Corollary 3 we can choose these factors such that $D_1 \in K_1[U_0, \ldots, U_n]$ and $D_2 \in K_1[\varepsilon^{(0)}, \varepsilon^{(1)}, U_0, \ldots, U_n]$. Represent

$$D_2 = \sum_{0 \le i \le \mu_0(y)} A_i U_0^i,$$

where all $A_i \in K_1[\varepsilon^{(0)}, \varepsilon^{(1)}, U_1, \ldots, U_n]$ are homogeneous polynomials in $U_1, \ldots, U_n$ with $\deg_{U_1, \ldots, U_n} A_i = \mu_0(y) - i$. In particular $A_{\mu_0(y)} \in K_1[\varepsilon^{(0)}, \varepsilon^{(1)}]$. Now we get immediately that

$$\varepsilon^{\iota_1(L,y)} a_{\mu_0(y)}(l_0, \ldots, l_n) = D_1(-l_1, \ldots, -l_n) A_{\mu_0(y)}(1, \varepsilon).$$

The first assertion of the lemma follows from this equality. The second assertion follows from the fact that $D(y)(0, 1, U_0, \ldots, U_n)$ is the $U-$resultant of system (4). Hence,

$$0 \ne A_{\mu_0(y)}(0, \varepsilon^{(1)}) = (\varepsilon^{(1)})^{(2dn+2n-1)(2d+1)^{n-2}} \alpha$$

where $\alpha \in K_1$. The lemma is proved.

Set $\mu_1(L, y) = \deg_\varepsilon a_{\mu_0(y)}$.

Set $\mu_2(L, y)$ to be maximal i such that ε does not divide a_i. Note that $\mu_2(L, y)$ is the number of roots η counting them with multiplicities of type (ii) or (iii) of system (3) such that $|(L/X_0)(\eta)|$ is not infinitely large relative to the field C_1. So $\mu_2(L, y) \ge \mu_2(y)$.

Set $\mu_1(y) = \mu_1(y_2, \ldots, y_n) = \max_L \mu_1(L, y)$ where the maximum is taken over all linear forms L for which $\mu_1(L, y)$ is defined.

Let L be a linear form which is not vanishing in any point of type (i) of the variety of solutions of system (3). Consider $G(y)$ as a polynomial in ε, L. Let (u_0, v_0), $(u_1, v_1), \ldots, (u_r, v_r)$ be subsequent vertices of the Newton polygon of $G(y)$, cf. [6], in the coordinates (ε, L) such that

- $(u_0, v_0) = ((2dn + 2n + 1)(2d + 1)^{n-2}, \mu_0(y))$,
- $u_{i+1} < u_i$ for $0 \le i \le r - 1$,
- $u_r = \iota_1(L, y)$.

Such a sequence exists by Lemma 3 and by the definition of $\iota_1(L, y)$. So $r \ge 0$. Besides that, our definitions imply

- $v_1 \leq v_0$ and $v_{i+1} < v_i$ for $1 \leq i \leq r-1$,
- $u_0 - u_r = \mu_1(L, y)$,
- $v_r = \mu_2(L, y)$, hence if $y_2, \ldots, y_n$ are elements from a real ordered field extension of R then $v_r \geq 2$.

Define $(u_{r+1}, v_{r+1}) = (\iota_1(L, y), 0)$. We shall denote also $u_i = u_i(L, y)$, $v_i = v_i(L, y)$ and $r = r(L, y)$ when the dependence on L and y will be important.

For a linear form L as above and y define $w_i = w_i(L, y) \in \mathbb{Q}, 0 \leq i \leq \mu_0(y)$ by the following conditions

- $w_{\mu_0(y)} = u_0$ if $v_1 < v_0$,
- $w_{\mu_0(y)} = u_1$ if $v_1 = v_0$,
- $w_i = u_{j+1} + (u_j - u_{j+1})(i - v_{j+1})/(v_j - v_{j+1})$ if $v_{j+1} \leq i \leq v_j$ and $1 \leq j \leq r$ (and $v_r \neq v_{r+1}$ if $j = r$).

Hence, the points with the coordinates (w_i, i), $\mu_2(L, y) \leq i \leq \mu_0(y)$ belong to the Newton broken line of the polynomial $G(y)$. Set

$$w = w(L, y) = (w_0(L, y), \ldots, w_{\mu_0(y)}(L, y)) \in \mathbb{Q}^{\mu_0(y)+1}.$$

Define a partial order on $\mathbb{Q}^{\mu_0(y)+1}$ in the following way. Let $z = (z_0, \ldots, z_{\mu_0(y)})$ and $z' = (z'_0, \ldots, z'_{\mu_0(y)})$ be two elements of $\mathbb{Q}^{\mu_0(y)+1}$. Then $z \geq z'$ if and only if $z_i \geq z'_i$ for all $0 \leq i \leq \mu_0(y)$.

Note that $\mu_0(y)$, $\mu_1(L, y)$, $\mu_2(L, y)$, $r(L, y)$, all $u_i(L, y)$, $v_i(L, y)$, $w(L, y)$ can be computed within the time polynomial in d^n and the size of input including L and y.

LEMMA 4 *Set $N_1 = (2d+2)(2d+1)^{n-1}n + 1$. Then there is a linear form $L_1 \in \mathcal{L}_{N_1}$ such that L_1 is not vanishing in any point of type (i) of the variety of solutions of system (3) and*

$$w(L_1, y) \leq w(L, y)$$

for every linear form L as above. Further, there is a family of at most $(2d+2)(2d+1)^{n-1}$ hyperplanes in $(n+1)$-dimensional space such that if coefficients of an arbitrary linear form L does not belong to the union of hyperplanes from this family then L is not vanishing in any point of type (i) of the variety of solutions of system (3) and

$$w(L, y) = w(L_1, y).$$

PROOF We shall use the notation from the proof of Lemma 3. The form L is not vanishing in any point of type (i) of the variety of solutions of system (3) if and only if $\sum_{1 \leq i \leq n} l_i \eta_i^{(j)} \neq 0$ for all $j \in J'$. In what follows in the proof of the lemma we shall suppose that $L = \sum_{0 \leq i \leq n} l_i X_i$ is not vanishing in any point of type (i) of the variety of solutions of system (3).

Let $\mathrm{ord}_\varepsilon : \overline{C_2} \to \mathbb{Q} \cup \{+\infty\}$ be the order function. Recall that $\mathrm{ord}_\varepsilon(a)$ is the exponent of the term of the least degree in the expansion of a in fractional power series in ε with coefficients from $\overline{C_1}$.

We have $G(y) = \varepsilon^{\iota_1(L,y)} a_{\mu_0(y)}(l_0, \ldots, l_n) \prod_{j \in J'' \cup J'''} (L - (L/X_0)(\eta^{(j)}))$ where $\eta^{(j)} = (\eta_0^{(j)} : \ldots : \eta_n^{(j)})$ is the family of all roots (counting them with multiplicities) of types (ii) or (iii) of system (3) in $\mathbb{P}^n(\overline{C_2})$. By Lemma 3 the Newton broken line (u_i, v_i), $0 \le i \le r$ of the polynomial $G(y)$ is completely defined by the orders of its roots $(L/X_0)(\eta^{(j)})$, $j \in J''$ and $w(L, y)$ is the least possible if and only if the equality

$$\operatorname{ord}_\varepsilon (L/X_0)(\eta^{(j)}) = \min_{0 \le i \le n} \operatorname{ord}_\varepsilon (\eta_i^{(j)}/\eta_0^{(j)}), \tag{5}$$

holds for every $j \in J''$. Now note that (5) holds for every $j \in J''$ if and only if the coefficients of L do not belong to the union of at most $\#J''$ hyperplanes in $(n+1)$–dimensional space. Hence the required linear form L_1 can be chosen from $\mathcal{L}_{N_1}$. The lemma is proved.

Define $r(y) = r(L_1, y)$, $u_i(y) = w(L_1, y)$, $v_i(y) = w(L_1, y)$ for $1 \le i \le r(y)+1$ and $w(y) = w(L_1, y)$ where L_1 is a linear form from the formulation of Lemma 4. So $\mu_1(y) = u_0(y) - u_{r(y)}(y)$ by our definitions.

Define $\mu(y) = (\mu_0(y), w(y)) \in \mathbb{Z} \times \mathbb{Q}^{\mu_0(y)+1}$.

Consider (3) as a system in $\varepsilon^{(0)}, \varepsilon^{(1)}$ and $X_0, \ldots, X_n$ with coefficients from the field K_1. Then it has solutions in the product of projective spaces $(\mathbb{P}^1 \times \mathbb{P}^n)(\overline{C_1})$ with the coordinates $((\varepsilon^{(0)} : \varepsilon^{(1)}), (X_0 : \ldots : X_n))$. Denote by $\mathcal{W}$ the union of all irreducible over $\overline{C_1}$ components W of the variety of solutions of (3) in $(\mathbb{P}^1 \times \mathbb{P}^n)(\overline{C_1})$ such that W is not contained in a hyperplane $\mathcal{Z}(c_0\varepsilon^{(0)} + c_1\varepsilon^{(1)})$ for any $c_0, c_1 \in \overline{C_1}$. On the other hand, consider system (3) over the field C_2 and recall that $\mathcal{W}'$ is the variety of solutions of system (3) in $\mathbb{P}^n(\overline{C_2})$. Then, see [5] or [3], Corollary 4.1, every irreducible components W of $\mathcal{W}$ corresponds bijectively by localization to the irreducible component W' defined over the field $\overline{C_1}(\varepsilon)$ of the variety $\mathcal{W}'$. Thus, every irreducible components W of $\mathcal{W}$ corresponds to the subset of solutions of (3) contained in W'. Note that if W' is fixed then one of the following conditions hold

- for every $\eta \in W'$ the solution η is of type (i),
- for every $\eta \in W'$ the solution η is of type (ii) or (iii).

Besides that, all considered components W are curves, i.e., $\dim W = 1$.

Denote by $\mathcal{V} = \mathcal{V}(y)$ the union of all irreducible components W of $\mathcal{W}$ which corresponds to the solution of (3) of type (ii) or (iii). Then the intersection $\mathcal{V} \cap \mathcal{Z}(X_0)$ is not infinite by Corollary 3 and since $\dim \mathcal{V} = 1$.

Consider a linear form $L \in \mathbb{Z}[X_0, \ldots, X_n]$ such that

(a) L is not vanishing in any point of $\mathcal{W}'$ of type (i),

(b) L is not vanishing in any point of $\mathcal{V} \cap \mathcal{Z}(X_0)$.

LEMMA 5 *Let L be a linear form satisfying condition (a), hence, $w(L, y)$ is defined. Then $w(L, y) = w(y)$ if and only if L satisfies condition (b).*

PROOF We shall use one fact from the proof of Lemma 4. Let $\zeta_0^{(j)}, \ldots, \zeta_n^{(j)} \in \overline{K_2}$ be such that

$$\zeta^{(j)} = (\zeta_0^{(j)} : \ldots : \zeta_n^{(j)}) = (\eta_0^{(j)} : \ldots : \eta_n^{(j)}) \in \mathbb{P}^n(\overline{K_2}),$$

$\mathrm{ord}_\varepsilon(\zeta_i^{(j)}) \geq 0$ for every $0 \leq i \leq n$ and there exists $1 \leq i_0 \leq n$ (it depends on j) such that $\mathrm{ord}_\varepsilon(\zeta_{i_0}^{(j)}) = 0$. Now let a linear form $L = \sum_{0 \leq i \leq n} l_i X_i$ satisfies conditions (a) and (b). We have $\mathcal{V} \cap \mathcal{Z}(X_0) \subset \mathcal{Z}(\varepsilon^{(1)})$. Hence

$$\mathcal{V} \cap \mathcal{Z}(X_0) = \{\mathrm{st}_\varepsilon(\zeta^{(j)}) \ : \ j \in J''\}$$

where $\mathrm{st}_\varepsilon \ : \ \mathbb{P}^n(\overline{C_2}) \to \mathbb{P}^n(\overline{C_1})$ is the mapping of the standard part, see [3], [4] (the standard part of an element $z \in \mathbb{P}^n(\overline{C_2})$ is the element $z' \in \mathbb{P}^n(\overline{C_1})$ which is infinitely close to z). Hence, $0 \notin L(\mathcal{V} \cap \mathcal{Z}(X_0))$ if and only if for every $j \in J''$ the equality $\mathrm{ord}_\varepsilon(\sum_{0 \leq i \leq n} l_i \zeta_i^{(j)}) = 0$ holds, i.e. if and only if

$$\mathrm{ord}_\varepsilon(\sum_{0 \leq i \leq n} l_i \zeta_i^{(j)}) = \min_{0 \leq i \leq n} \mathrm{ord}_\varepsilon(\zeta_i^{(j)})$$

for every $j \in J''$. This is equivalent to the condition that for every $j \in J''$ the equality

$$\mathrm{ord}_\varepsilon((L/X_0)(\eta^{(j)})) = \min_{0 \leq i \leq n} \mathrm{ord}_\varepsilon((X_i/X_0)(\eta^{(j)}))$$

holds. It was ascertained in the proof of Lemma 4 that this is equivalent to the equality $w(L, y) = w(y)$. The lemma is proved.

By [3], [4] one can compute the standard part of an element from $\mathbb{P}^n(\overline{C_2})$ within the time polynomial in d^n and the size of input. Hence one can verify whether a linear form L satisfies (a) and (b) within the time polynomial in d^n and the size of input including L. Besides that for every y, such a linear form L can be chosen from a set $\mathcal{L}_{N_2}$ with N_2 bounded from above by a polynomial in d^n.

LEMMA 6 *Let L be a linear form satisfying conditions (a) and (b). Denote by $\Lambda_1 = K_1[\mathcal{V} \setminus \mathcal{Z}(X_0)]$ the ring of regular functions of the algebraic variety $\mathcal{V} \setminus \mathcal{Z}(X_0)$ and by $\Lambda_2 = K_1[\varepsilon, (L/X_0)|_{\mathcal{V} \setminus \mathcal{Z}(X_0)}]$ the subalgebra of Λ_1 generated by the regular functions ε and L/X_0. Then $\Lambda_2 \subset \Lambda_1$ is a finite extension of algebras. Besides that, the isomorphism*

$$\Lambda_2 \longrightarrow K_1[Z_1, Z_2]/(H(y)(Z_1, Z_2))$$

holds where Z_1, Z_2 are new variables, $H(y) \in K_1[\varepsilon, L]$ is the polynomial introduced previously and $\varepsilon \mapsto Z_1 \bmod H(y)(Z_1, Z_2)$, $L \mapsto Z_2 \bmod H(y)(Z_1, Z_2)$ under this isomorphism.

PROOF There is an integer λ such that $\varepsilon^{(0)} + \lambda\varepsilon^{(1)}$ is not vanishing in any point of $\mathcal{V} \cap \mathcal{Z}(X_0)$. Consider the rational morphism $\pi : \mathbb{P}^1 \times \mathbb{P}^n \to \mathbb{P}^2$ defined by the formula

$$((\varepsilon^{(0)} : \varepsilon^{(1)}), (X_0 : \ldots : X_n)) \mapsto ((\varepsilon^{(0)} + \lambda\varepsilon^{(1)})L : \varepsilon^{(1)}X_0 : \varepsilon^{(0)}X_0).$$

By the choice of L and λ the morphism π is defined everywhere on $\mathcal{V}$. The inverse image $(\pi|_{\mathcal{V}})^{-1}(z)$ is finite for every point $z \in \pi(\mathcal{V})$. Thus, $\pi(\mathcal{V})$ is closed in the Zariski topology and the morphism

$$\pi|_{\mathcal{V}} \ : \ \mathcal{V} \to \pi(\mathcal{V})$$

is finite. So the coordinates functions $(X_i/X_0)|_{\mathcal{V} \setminus \mathcal{Z}(X_0)}$ of the algebraic variety $\mathcal{V} \setminus \mathcal{Z}(X_0)$ (they are regular functions on this variety) are integral over the algebra

$K_1[\varepsilon, ((1+\lambda\varepsilon)L/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}]$ for all i. Hence, these coordinates functions are also integral over the algebra $K_1[\varepsilon, (L/X_0)|_{\mathcal{V}\setminus\mathcal{Z}(X_0)}]$. The last statement of the lemma follows directly from the definitions of the algebraic variety $\mathcal{V}$ and the polynomial $H(y)$. The lemma is proved.

COROLLARY 5 *Let L be a linear form satisfying conditions (a) and (b). Then $\mu_2(L,y) = \mu_2(y)$.*

PROOF The number of solutions η of (3) of types (ii) or (iii) for which $(L/X_0)(\eta)$ is not infinitely large relative to the field C_1 is equal to $\mu_2(L,y)$. Further, by the proved assertion about integral dependence of coordinates functions if $(L/X_0)(\eta)$ is not infinitely large (respectively is infinitely large) relative to field the C_1 then $(X_i/X_0)(\eta)$ is not infinitely large for every $1 \le i \le n$ (respectively is infinitely large for at least one $1 \le i \le n$). Thus, we have $\mu_2(y) = \mu_2(L,y)$. The corollary is proved. One can deduce also this corollary from Lemma 5.

LEMMA 7 *Let L be a linear form satisfying conditions (a) and (b). Then η is a root of type (iii) (respectively (ii)) of system (3) if and only if $|(L/X_0)(\eta)|$ is not infinitely large (respectively is infinitely large) relative to the field C_1. Besides that, the family of roots counting with multiplicities of the polynomial $G(y)$ coincides with the family $\{(L/X_0)(\eta^{(j)})\}_{j\in J''\cup J'''}$ where $\{\eta^{(j)}\}_{j\in J''\cup J'''}$ is a family of all roots of types (ii) or (iii) of system (3).*

PROOF The first assertion follow directly from definitions. The second one was ascertained in the proof of Lemma 4. The lemma is proved.

Let $Y_2, \dots, Y_n$ be new variables. Denote $Y = (Y_2, \dots, Y_n)$. Thus, we have $\mu_0(Y) \ge \mu_0(y)$ and if $\mu_0(Y) = \mu_0(y)$ then $w(Y) \le w(y)$ for every y.

The U–resultant

$$D(Y) \in R[Y_2, \dots, Y_n, \varepsilon^{(0)}, \varepsilon^{(1)}, U_0, \dots, U_n]$$

is a polynomial in $Y_2, \dots, Y_n$. Note that the degree of $D(Y)$ in $Y_2, \dots, Y_n$ is bounded from above by a polynomial in d^n.

LEMMA 8 *For an arbitrary y there is a polynomial $\Phi_2(y) \in R[Y_2, \dots, Y_n]$ with the degree bounded from above by a polynomial in d^n such that $\Phi_2(y)(y_2, \dots, y_n) \ne 0$ and if $y' = (y'_2, \dots, y'_n) \in \mathbb{A}^{(n-1)}(K_3)$, $\Phi_2(y)(y'_2, \dots, y'_n) \ne 0$ (where K_3 is an arbitrary extension of C_2) then $\mu_0(y') \ge \mu_0(y)$ and if $\mu_0(y') = \mu_0(y)$ then $w(y') \le w(y)$.*

PROOF Let L be a linear form satisfying the condition (a) and (b) for y. Then $w(L,y) = w(y)$ by Lemma 5. Let us consider the polynomials $G(y)$ and $G(Y)$ corresponding to L. Let

$$G(Y) = \sum_{i,j\ge 0} g_{i,j}\varepsilon^i L^j,$$

where all $g_{i,j} \in R[Y_2, \dots, Y_n]$. Then $G(y) = \sum_{i,j} g_{i,j}(y_2, \dots, y_n)\varepsilon^i L^j$. Let $r = r(y)$, $u_i = u_i(L,y)$, $v_i = v_i(L,y)$, $1 \le i \le r$, By definition, put

$$\Phi_2(y) = \prod_{0\le i\le r} g_{u_i,v_i}.$$

The polynomial $\Phi_2(y)$ is required by Lemma 4 and Lemma 5. The lemma is proved.

COROLLARY 6 *For an arbitrary y and a linear form L satisfying (a), (b) for y there is a polynomial $\Phi_3(y) \in R[Y_2, \ldots, Y_n]$ with the degree bounded from above by a polynomial in d^n such that $\Phi_3(y)(y_2, \ldots, y_n) \neq 0$ and if $y' = (y'_2, \ldots, y'_n) \in \mathbb{A}^{(n-1)}(K_3)$, $\Phi_3(y)(y'_2, \ldots, y'_n) \neq 0$ (where K_3 is an arbitrary extension of C_2) then the linear form L satisfies (a) for y' and one of the conditions is fulfilled*

- $\mu_0(y') > \mu_0(y)$,
- $\mu_0(y') = \mu_0(y)$ *and* $w(L, y') \leq w(L, y)$.

PROOF This statement was ascertained in the proof of lemma.

LEMMA 9 *There are non–empty open in the Zariski topology subsets U_0, U_1 in $\mathbb{A}^{(n-1)}(C_1)$ such that $U_1 \subset U_0$ and*

- $y \in U_0$ *if and only if* $\mu_0(y) = \mu_0(Y)$,
- $y \in U_1$ *if and only if* $\mu_0(y) = \mu_0(Y)$ *and* $w(y) = w(Y)$.

Besides that, $\mu_0(Y) = (2d+2)(2d+1)^{n-1}$.

PROOF We have $\mu_0(Y) = (2d+2)(2d+1)^{n-1}$ by our definitions and Corollary 3. Set $Y_i - y_i$, $2 \leq i \leq n$, to be algebraically independent infinitesimals relative to the field K_1. Then all the required assertions follows from Lemma 8. The lemma is proved.

COROLLARY 7 *For any y if $\mu_0(y) = \mu_0(Y)$ then $\iota_0(y) = 0$.*

PROOF This follows from Corollary 3 and the definition of $\mu_0(Y)$.

Let $\varepsilon > 0$ be an infinitesimal relative to the field R_1, the element $\varepsilon_1 > 0$ be an infinitesimal relative to the field $R_1(\varepsilon)$ (recall that $R_2 = R_1(\varepsilon)$) and $\varepsilon_2 > 0$ be an infinitesimal relative to the field $R_1(\varepsilon, \varepsilon_1)$. The algebraic closure $\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)}$ is supplied with the real structure. So we can consider systems of polynomial equations and inequalities with squares of absolute values, see [3], [4]. Namely, consider the system of polynomial equations in $X_0, X_1, \ldots, X_n, Y_2, \ldots, Y_n$

$$\begin{cases} h = 0, \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \leq i \leq n, \\ \sum_{2 \leq i \leq n} |Y_i - y_i|^2 = \varepsilon_2, \\ \sum_{0 \leq i \leq n} |X_i|^2 > \varepsilon_1^{-1}, \\ X_0 = 1. \end{cases} \tag{6}$$

LEMMA 10 *(i) If $\mu_0(Y) > \mu_0(y)$ then system (6) has a solution in the affine space $\mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$.*

(ii) Let $(1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$ be an arbitrary solution of (6). Then $\mu_0(y') > \mu_0(y)$.

PROOF Choose the elements $y'_i \in \overline{R_1(\varepsilon_2)}$, $2 \leq i \leq n$, such that

- $\sum_{2 \leq i \leq n} (y'_i - y_i)^2 = \varepsilon_2$,
- $(y'_2, \ldots, y'_n) \in U_0$,

and set $y' = (y'_2, \dots, y'_n)$. Let L be a linear form satisfying (a) and (b) simultaneously for y, y' and the variables Y.

Let $\mu_0(Y) > \mu_0(y)$. Then the degree $\deg_L G(y') > \deg_L G(y)$. The coefficients of both polynomials $D(y')$ and $D(y)$ are obtained from coefficients of $D(Y)$ by substituting the values $Y_i = y_i$ and $Y_i = y'_i$ respectively. The coefficient of $G(Y)$ in L^i can be represented as a polynomial $\psi_i(Z_2, \dots, Z_n)$ in $Z_j = Y_j - y_j$, $2 \le j \le n$. So by our definitions if $i > \deg_L G(y)$ then the free term of the polynomial ψ_i is equal to zero. Hence there is a root $L = \lambda' \in \overline{R_1(\varepsilon, \varepsilon_2)}$ of the polynomial $G(y')$ such that $|\lambda'|$ is infinitely large relative to the field $\overline{R_1(\varepsilon, \varepsilon_1)}$. By Lemma 6 there are $\eta_1, \dots, \eta_n \in \overline{R_1(\varepsilon, \varepsilon_2)}$ such that $L(1, \eta_1, \dots, \eta_n) = \lambda'$ and $(1, \eta_1, \dots, \eta_n, y'_2, \dots, y'_n)$ is the required solution of (6). The assertion (i) is proved.

Suppose that there is a solution

$$(1, \eta_1, \dots, \eta_n, y'_2, \dots, y'_n) \in \mathbb{A}^{2n}(\overline{R_1(\varepsilon, \varepsilon_1, \varepsilon_2)})$$

of (6). We shall assume without loss of generality that the linear form L as previously satisfies (a), (b) simultaneously for Y, y and y'. Since $y'_i - y_i$ are infinitesimals we have by Lemma 8 $\mu_0(y') \ge \mu_0(y)$. Suppose that $\mu_0(y') = \mu_0(y)$. Then there is a polynomial $\Psi \in R_1(\varepsilon)[L, Z_2, \dots, Z_n]$ of the degree $\deg_L \Psi \le \mu_0(y)$ such that $\Psi(L, 0, \dots, 0) = 0$ and

$$G(y') = G(y) + \Psi(L, y'_2 - y_2, \dots, y'_n - y_n). \tag{7}$$

All the roots of the polynomial $G(y) \in R_2[L]$ (considered as a polynomial in L) are not infinitely large relative to the field $R_1(\varepsilon)$. Hence (7) implies that all the roots of the polynomial $G(y')$ are also not infinitely large relative to the field $R_1(\varepsilon)$. Now by Lemma 6 we get that $\sum_{0 \le i \le n} |\eta'_i|^2$ is not infinitely large relative to field $R_1(\varepsilon)$. It is a contradiction. The assertion (ii) and the lemma are proved.

Let $\varepsilon_0 > 0$ be an infinitesimal relative to the field R_1, the element $\varepsilon_1 > 0$ be an infinitesimal relative to the field $R_1(\varepsilon_0)$, the element $\varepsilon_2 > 0$ be an infinitesimal relative to the field $R_1(\varepsilon_0, \varepsilon_1)$ and $\varepsilon_3 > 0$ be an infinitesimal relative to the field $R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2)$. The algebraic closure $\overline{R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)}$ is supplied with the real structure.

Let L be a linear form satisfying conditions (a) and (b) for y. Denote $r = r(L, y)$, $0 \le j \le r-1$, $u_j = u_j(L, y)$, $u_{j+1} = u_{j+1}(L, y)$, $v_j = v_j(L, y)$, $v_{j+1} = v_{j+1}(L, y)$. Consider the system of polynomial equations and inequalities in $\varepsilon, X_0, X_1, \dots, X_n, Y_2, \dots, Y_n$

$$\begin{cases} h = 0, \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \le i \le n, \\ \sum_{2 \le i \le n} |Y_i - y_i|^2 = \varepsilon_1, \\ L\varepsilon_3 = 1, \\ \varepsilon_2 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})} < |\varepsilon|^2 < \varepsilon_0 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}, \\ X_0 = 1. \end{cases} \tag{8}$$

LEMMA 11 *Let $\mu_0(y) = \mu_0(Y)$. Let $0 \le j \le r-1$, $j \in \mathbb{Z}$. Let $u_i = u_i(L, Y)$, $v_i = v_i(L, Y)$ for all $0 \le i \le j$.*

(i) Let

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} = \frac{v_j(L, Y) - v_{j+1}(L, Y)}{u_j(L, Y) - u_{j+1}(L, Y)}$$

and $u_{j+1} \neq u_{j+1}(L, Y)$. *Then system (8) has a solution in* $\mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_3)})$.

(ii) Let

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)}) \tag{9}$$

be an arbitrary solution of (8). Then $\mu_0(y') = \mu_0(Y)$, $u_{j+1}(L, y') < u_{j+1}$ *and* $w(L, y') < w(L, y)$.

PROOF We shall use the facts ascertained in the proof of Lemma 6. To prove (i) choose the elements $y'_i \in \overline{R_1(\varepsilon_1)}$, $2 \leq i \leq n$, such that

- $\sum_{2 \leq i \leq n} (y'_i - y_i)^2 = \varepsilon_1$,
- $w(L, y'_2, \ldots, y'_n) = w(L, Y)$

(such elements exist by Corollary 6) and set $y' = (y'_2, \ldots, y'_n)$. Let $G(y) = \sum_{i_1, i_2 \geq 0} g_{i_1, i_2} \varepsilon^{i_1} L^{i_2}$ where all $g_{i_1, i_2} \in R_1$. Set

$$B_j = \{(i_1, i_2) \in \mathbb{Z}^2 : (v_{j+1} - v_j) i_1 - (u_{j+1} - u_j) i_2 = v_{j+1} u_j - u_{j+1} v_j\},$$
$$A_j = \{(i_1, i_2) \in B_j : u_{j+1} \leq i_1 \leq u_j\},$$
$$G^*(y) = \sum_{(i_1, i_2) \in A_j} g_{i_1, i_2} \varepsilon^{i_1}.$$

So A_j is the set of all points with integer coordinates which are contained in the edge with the vertices (u_{j+1}, v_{j+1}), (u_j, v_j) of Newton broken line of the polynomial $G(y)$. Similarly the polynomial $G^*(y')$ is defined. By the conditions of the lemma and since $w(L, y') = w(L, Y)$ there is a root $\varepsilon'_0 \in \overline{R_1(\varepsilon_1)}$ of $G^*(y')$ considered as a polynomial in ε such that ε'_0 is infinitesimal relative to the field $\overline{R_1}$. Hence, $2\varepsilon_2 < |\varepsilon'_0|^2 < \varepsilon_0/2$.

Considering the Newton polygon of the polynomial $G(y')$ relative to ε and L we get that there is a root of this polynomial in the field of fractional power series in ε_3 with coefficients from $\overline{R_1(\varepsilon_1)}$ such that

$$L = \varepsilon_3^{-1}, \quad \varepsilon = \varepsilon' = \varepsilon'_0 \varepsilon_3^{(v_j - v_{j+1})/(u_j - u_{j+1})} + \sum_{1 \leq i \in \mathbb{Z}, i/\nu > (v_j - v_{j+1})/(u_j - u_{j+1})} \varepsilon'_i \varepsilon_3^{i/\nu}, \tag{10}$$

where $0 < \nu \in \mathbb{Z}$ and $\varepsilon'_i \in \overline{R_1(\varepsilon_1)}$ for all i. Hence, $\varepsilon_2 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})} < |\varepsilon'|^2 < \varepsilon_0 \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}$.

The polynomial $G(y')(L/X_0, \varepsilon)$ considered as a polynomial in $X_1/X_0, \ldots, X_n/X_0, \varepsilon$ with coefficients from $\overline{R_1(\varepsilon_1)}$ is vanishing on the affine algebraic variety $\mathcal{V}(y') \setminus \mathcal{Z}(X_0)$. More than that, by Lemma 6 there is a root (9) of system (8) such that the element ε' from (9) and (10) is the same. The assertion (i) is proved.

Conversely under conditions of (ii) $\mu_0(y') = \mu_0(y)$ and $w(L, y') \leq w(L, y)$ since y' belongs to the infinitesimal neighborhood of y. Further, by the similar arguments as in the proof of (i) we deduce that $u_{j+1}(L, y') < u_{j+1}$. Hence $w(L, y') < w(L, y)$. The lemma is proved.

Let L be a linear form satisfying conditions (a) and (b) for y. Denote $r = r(L, y)$, $0 \leq j \leq r$, $u_i = u_i(L, y)$, $v_i = v_i(L, y)$ for all $0 \leq i \leq r + 1$. Set

$u_{-1} = u_0 + 1$, $v_{-1} = v_0 - 1$. Consider the system of polynomial equations and inequalities in $\varepsilon, X_0, X_1, \ldots, X_n, Y_2, \ldots, Y_n$

$$\begin{cases} h = 0, \\ \frac{\partial h}{\partial X_i} - Y_i \frac{\partial h}{\partial X_1} = 0, & 2 \le i \le n, \\ \sum_{2 \le i \le n} |Y_i - y_i|^2 = \varepsilon_1, \\ L\varepsilon_3 = 1, \\ \varepsilon_2 |\varepsilon|^2 > \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})} & \text{if } j \le r-1, \\ |\varepsilon|^2 < \varepsilon_2 \varepsilon_3^{2(v_{j-1} - v_j)/(u_{j-1} - u_j)}, \\ X_0 = 1. \end{cases} \tag{11}$$

LEMMA 12 *Let $\mu_0(y) = \mu_0(Y)$. Let $0 \le j \le r$, $j \in \mathbb{Z}$. Let $r(L,Y) \ge j+1$ and $u_i = u_i(L,Y)$, $v_i = v_i(L,Y)$ for all $0 \le i \le j$. Let $v_0 \ne v_1$ if $j = 0$.*

(i) Let

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} > \frac{v_j(L,Y) - v_{j+1}(L,Y)}{u_j(L,Y) - u_{j+1}(L,Y)}$$

if $j \le r-1$. Then system (11) has a solution in $\mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_3)})$.

(ii) Let

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}(\overline{R_1(\varepsilon_1, \varepsilon_2, \varepsilon_3)}) \tag{12}$$

be an arbitrary solution of (11). Then $r(L,y') \ge j+1$,

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} > \frac{v_j(L,y') - v_{j+1}(L,y')}{u_j(L,y') - u_{j+1}(L,y')}$$

if $j \le r-1$,

$$\frac{v_j(L,y') - v_{j+1}(L,y')}{u_j(L,y') - u_{j+1}(L,y')} > \frac{v_{j-1} - v_j}{u_{j-1} - u_j}.$$

Hence $\mu_0(y') = \mu_0(Y)$ and $w(L,y') < w(L,y)$.

PROOF To prove (i) define y' as in the proof of Lemma 11. Since $u_j = u_j(L,Y)$, $v_j = v_j(L,Y)$ the inequality

$$\frac{v_j(L,Y) - v_{j+1}(L,Y)}{u_j(L,Y) - u_{j+1}(L,Y)} > \frac{v_{j-1} - v_j}{u_{j-1} - u_j}$$

holds. Considering the Newton polygon of the polynomial $G(y')$ relative to ε and L we get that there is a root of this polynomial in the field of fractional power series in ε_2 with coefficients from $\overline{R_1(\varepsilon_1)}$ such that

$$L = \varepsilon_3^{-1}, \quad \varepsilon = \varepsilon' = \sum_{i_0 \le i \in \mathbb{Z}} \varepsilon'_i \varepsilon_3^{i/\nu}, \tag{13}$$

where $0 < \nu \in \mathbb{Z}$,

$$\begin{aligned} &i_0/\nu < (v_j - v_{j+1})/(u_j - u_{j+1}) \quad \text{if} \quad j \le r-1, \\ &i_0/\nu > (v_{j-1} - v_j)/(u_{j-1} - u_j), \end{aligned}$$

$\varepsilon'_i \in \overline{R_1(\varepsilon_1)}$ for all i and $0 \ne \varepsilon'_{i_0}$ is an infinitesimal relative to the field R_1. Hence, $\varepsilon_2 |\varepsilon'|^2 > \varepsilon_3^{2(v_j - v_{j+1})/(u_j - u_{j+1})}$ if $j \le r-1$ and $|\varepsilon'|^2 < \varepsilon_2 \varepsilon_3^{2(v_{j-1} - v_j)/(u_{j-1} - u_j)}$. The remaining part of the proof of assertion (i) is similar to the one of Lemma 11.

To prove (ii) consider the polynomial $G(y')$, its Newton broken line, and the root (13) of $G(y')$. We have $\mu_0(y') = \mu_0(Y)$, $w(L,y') \le w(L,y)$ and $u_i(L,y') = u_i(L,Y)$, $v_i(L,y') = v_i(L,Y)$ for all $0 \le i \le j$ since y' belongs to the infinitesimal neighborhood of y.

Denote $p_j = (v_j - v_{j+1})/(u_j - u_{j+1})$ if $j \le r-1$ and $q_j = (v_{j-1} - v_j)/(u_{j-1} - u_j)$. We have $i_0/\nu \le p_j$ if $j \le r-1$ and $i_0/\nu \ge q_j$. Further, $i_0/\nu > q_j$ since, otherwise, ε'_{i_0} is infinitesimal relative to the field R_1 which contradicts to the equalities $u_j(L,y') = u_j(L,y)$, $v_j(L,y') = v_j(L,y)$.

If $j = r$ or $j \le r-1$ and $i_0/\nu < p_j$ all the assertions of the Lemma are proved.

Let $j \le r-1$ and $i_0/\nu = p_j$. Then ε'_{i_0} is infinitely large relative to the field R_1. This is possible only in the case when the Newton broken line of $G(y')$ contains an edge e' which is parallel to the edge e with the vertices (u_j, v_j), (u_{j+1}, v_{j+1}) of the Newton broken line of $G(y)$ (so e' and e lie on different parallel lines). Hence if $(u_\alpha(L,y'), v_\alpha(L,y'))$, $(u_{\alpha+1}(L,y'), v_{\alpha+1}(L,y'))$ are vertices of e then $\alpha > j$. This implies all the assertions of the lemma in this case. The lemma is proved.

Set $N_3 = 2(2d+2)(2d+1)^{n-1}n + 1$. Then by Lemma 4 and Lemma 5 there is a linear form $L \in \mathcal{L}_{N_3}$ satisfying simultaneously the conditions (a) and (b) for y and Y.

Now we shall describe an algorithm for constructing integers $z_2, \dots, z_n$ with lengths $O(n \log d)$ such that $\mu_0(Y) = \mu_0(z_2, \dots, z_n)$ and $w(Y) = w(z_2, \dots, z_n)$. Choose integers $y_2, \dots, y_n$ with lengths $O(n \log d)$, say, $y_i = 0$, $2 \le i \le n$. So now $R_1 = R$. Construct a solution of system (6) or ascertain that it has no solutions, see [3], [4] (here one should use condition (A) from the Introduction). In the case when system (6) has no solutions we have $\mu_0(Y) = \mu_0(y)$ by Lemma 10.

Let system (6) have a solution $(1, \eta_1, \dots, \eta_n, y'_2, \dots, y'_n) \in \mathbb{A}^{2n}(\overline{R(\varepsilon, \varepsilon_1, \varepsilon_2)})$. Then $\mu_0(y'_2, \dots, y'_n) > \mu_0(y)$ by Lemma 10. Let us show that we can construct subsequently $y''_2, \dots, y''_n \in \mathbb{Z}$ such that $\mu_0(y''_2, \dots, y''_i, y'_{i+1}, \dots, y'_n) \ge \mu_0(y'_2, \dots, y'_n)$ for every $2 \le i \le n$, cf. the auxiliary algorithms from [3], [4]. Enumerating integer values $y''_2 = 0, \dots, N$ where N is bounded from above by a polynomial in d^n and computing each time $\mu_0(y''_2, y'_3, \dots, y'_n)$ we shall find the required y''_2. The last fact follows from Lemma 8. In the similar way construct $y''_3, \dots, y''_n$. Now replace $y_2, \dots, y_n$ by $y''_2, \dots, y''_n$ and return to the beginning of the algorithm under description.

Note that $\mu_0(Y)$ is bounded from above by a polynomial in d^n. Hence there might be at most polynomial in d^n such returns to the beginning of the algorithm. So finally we shall come to the case when system (6) has no solutions and $\mu_0(Y) = \mu_0(y)$.

Now let $\mu_0(Y) = \mu_0(y)$. Enumerate all the linear forms $L \in \mathcal{L}_{N_3}$. Construct the subset $\mathcal{L}'$ of $\mathcal{L}$ consisting of all linear forms L satisfying conditions (a) and (b). So by the choice of N_3 we have $w(L,y) = w(y)$ for every $L \in \mathcal{L}'$ and there is $L \in \mathcal{L}'$ such that $w(L,Y) = w(Y)$. Enumerate all the linear forms $L \in \mathcal{L}'$.

For the considered linear form L construct the polynomial $G(y)$ and $w(L,y)$. Set $r = r(L,y)$ and $u_i = u_i(L,y)$, $v_i = v_i(L,y)$ for all $0 \le i \le r+1$. Set $u_{-1} = u_0 + 1$, $v_{-1} = v_0 - 1$. Suppose $0 \le j \le r$, $j \in \mathbb{Z}$ (the base of the recursion $j = 0$) and we have already ascertained that $u_i = u_i(L,Y)$, $v_i = v_i(L,Y)$ for all

$0 \le i \le j$. So if $j \le r-1$ then

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} \ge \frac{v_j(L,Y) - v_{j+1}(L,Y)}{u_j(L,Y) - u_{j+1}(L,Y)}$$

for every $L \in \mathcal{L}'$.

Let $v_0 \ne v_1$ if $j = 0$. Then for each $L \in \mathcal{L}'$ construct a solution of system (11) or ascertain that it has no solutions, see [3], [4] (here one should use condition (A) from the Introduction).

Let system (11) have a solution

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}\,(\overline{R(\varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

for some $L \in \mathcal{L}'$. Then $\mu_0(y') = \mu_0(Y)$ and $w(L, y') < w(L, y) = w(y)$ by Lemma 12 (ii).

If $j = r$ and system (11) has no solutions for all $L \in \mathcal{L}'$ then $w(y) = w(Y)$ by Lemma 12 (i) and by the choice of N_3. Set in this case $z_i = y_i$ for $2 \le i \le n$.

Let $j = 0$ and $v_0 = v_1$ or $0 \le j \le r-1$ and system (11) has no solutions for all $L \in \mathcal{L}'$. Then

$$\frac{v_j - v_{j+1}}{u_j - u_{j+1}} = \frac{v_j(Y) - v_{j+1}(Y)}{u_j(Y) - u_{j+1}(Y)} \tag{14}$$

by Lemma 12 (i) and by the choice of N_3. In this case again enumerate $L \in \mathcal{L}'$. For every $L \in \mathcal{L}'$ construct a solution of system (8) or ascertain that it has no solutions, see [3], [4] (here one should use condition (A) from the Introduction).

Let system (8) have a solution

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}\,(\overline{R(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

for some $L \in \mathcal{L}'$. Then $\mu_0(y') = \mu_0(Y)$ and $w(L, y') < w(L, y) = w(y)$ by Lemma 11 (ii).

When system (8) has no solutions for all $L \in \mathcal{L}'$ and $j \le r-1$ we have $u_{j+1} = u_{j+1}(Y)$ and $v_{j+1} = v_{j+1}(Y)$ by Lemma 11 (i) and by the choice of N_3. In this case we replace j by $j+1$ and return to the beginning of the algorithm under description. Now j is greater than it was previously.

Thus, it remains to consider the cases when system (11) or system (8) has a solution

$$(\varepsilon', 1, \eta_1, \ldots, \eta_n, y'_2, \ldots, y'_n) \in \mathbb{A}^{2n+1}\,(\overline{R(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)})$$

(for system (11) this solution does not depend on ε_0). Hence $\mu_0(y') = \mu_0(Y)$ and $w(L, y') < w(L, y) = w(y)$, see above. Let us show that we can construct subsequently $y''_2, \ldots, y''_n \in \mathbb{Z}$ such that $\mu_0(y''_2, \ldots, y''_i, y'_{i+1}, \ldots, y'_n) = \mu_0(Y)$ and

$$w(y''_2, \ldots, y''_i, y'_{i+1}, \ldots, y'_n) \le w(y'_2, \ldots, y'_n)$$

for all $2 \le i \le n$, cf. the auxiliary algorithms from [3], [4]. Enumerating integer values $y''_2 = 0, \ldots, N$ where N is bounded from above by a polynomial in d^n and computing each time $\mu_0(y''_2, y'_3, \ldots, y'_n)$ and $w(y''_2, y'_3, \ldots, y'_n)$ we shall find the required y''_2. The last fact follows from Lemma 8. In the similar way construct $y''_3, \ldots, y''_n$. Now replace $y_2, \ldots, y_n$ by $y''_2, \ldots, y''_n$ and return to the beginning of the algorithm under description. This completes the description of the algorithm for constructing $z_2, \ldots, z_n$.

Note that in the recursion of the described algorithm the quotient $(v_j - v_{j+1})/(u_j - u_{j+1})$ can take at most polynomial in d^n values and when (14) holds the integer u_{j+1} also can take at most polynomial in d^n values. Hence, in the described algorithm there might be at most polynomial in d^n returns to the beginning when the value of j is the same. Since there are at most polynomial in d^n different values j the total number of such returns is bounded from above by a polynomial in d^n.

Note that the degrees of all equations and inequalities from systems (6), (11), (8) relative to all their variables are $O(d)$. The constant field in system (8), (respectively (11)) is an extension of $R(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ (respectively $R(\varepsilon_1, \varepsilon_2, \varepsilon_3)$) of the degree polynomial in d^n. According to [14], [7], see also [3], [4], the working time of the algorithm for deciding whether systems (6), (11), (8) have solutions and constructing these solutions is polynomial d^n, d_1, d_2, M, M_1, m. Thus, the working time of the algorithm described in this section is polynomial in d^n, d_1, d_2, M, M_1, m.

2 Existence theorem

We shall suppose that $R = \mathbb{R}$ in this section. Let $V = \mathcal{Z}(f_1, \ldots, f_m)$ be an algebraic variety from the Introduction and $V(\mathbb{R})$ the corresponding real algebraic variety. We shall suppose in this section as in the previous one $V(\mathbb{R})$ to be non–empty and bounded.

We need the following lemmas

LEMMA 13 *Let a compact set $C' \subset \mathbb{C}^{m_1+1}$, $m_1 \geq 0$, be given. Let for an arbitrary point $(b_0, \ldots, b_{m_1}) \in C'$ the coordinate $b_0 \neq 0$. Let*

$$C = \{ \sum_{0 \leq i \leq m_1} b_i Z^{m_1 - i} \, : \, (b_0, \ldots, b_{m_1}) \in C' \}$$

be the set of polynomials $\psi = \sum_{0 \leq i \leq m_1} b_i Z^{m_1 - i} \in \mathbb{C}[Z]$ of degree $\deg \psi = m_1$ with coefficients from C'. Let m_2 be an integer such that $m_2 \geq m_1$ and $0 < \delta \in \mathbb{R}$. Let $\widetilde{\psi} \in \mathbb{C}[Z]$ be a polynomial of degree $\deg \widetilde{\psi} \leq m_2$ such that the absolute values of all coefficients of the polynomial $\widetilde{\psi} - \psi$ are less than δ. Denote by $z_i \in \mathbb{C}$, $1 \leq i \leq m_1$, (respectively $\widetilde{z}_i \in \mathbb{C}$, $1 \leq i \leq \deg \widetilde{\psi}$) the family of roots taking into account their multiplicities of the polynomial ψ (respectively $\widetilde{\psi}$). Then for every $\delta_0 > 0$ there is $\delta > 0$ such that for every $\psi \in C$ for every $\widetilde{\psi}$ as described there is a permutation σ of the set $1, \ldots, \deg \widetilde{\psi}$ such that

- $|\widetilde{z}_{\sigma(i)} - z_i| < \delta_0$ *for* $1 \leq i \leq m_1$,
- $|\widetilde{z}_{\sigma(i)}| > \delta_0^{-1}$ *for* $m_1 + 1 \leq i \leq \deg \widetilde{\psi}$.

PROOF Since C' is compact it is sufficient to prove this lemma for a small neighborhood W of an arbitrary polynomial ψ_0 in place of the compact set C'. Consider a finite family of non–intersecting circumferences c_α, $\alpha \in A$, with the radiuses less than $\delta_0/2$ such that inside each circumference c_α there is only one but may be multiple root of the polynomial ψ_0. Consider also a circumference c with the center in zero containing inside all the roots of the polynomial ψ_0 with the radius more than δ_0^{-1}. Let ψ be a polynomial from a sufficiently small

neighborhood W of ψ_0. Let c' be c_α for some α or c. Then we can choose δ and W so small that ψ and $\widetilde{\psi}$ do not have any zero on c' and the absolute value of every integral $(2\pi\sqrt{-1})^{-1}\int_{c'}(\psi'(z)/\psi(z) - \widetilde{\psi}'(z)/\widetilde{\psi}(z))dz$ is less than $1/2$. The lemma is proved.

Now let integers $y_2, \ldots, y_n$ have lengths $O(n \log d)$. Recall that in Section 1 $\mu_0(y)$, $\mu_1(y)$, $\mu_2(y)$, $w(y)$ and $\mu(y)$ were defined. Let $\mu(y_2, \ldots, y_n) = \mu(Y)$ where $Y = (Y_2, \ldots, Y_n)$, see Section 1. Recall that the polynomial $h \in R[\varepsilon^{(0)}, \varepsilon^{(1)}, X_0, \ldots, X_n]$, the polynomial $G(y) \in \mathbb{R}[\varepsilon, L]$. Let $v_2, \ldots, v_n \in \mathbb{R}$ and $0 \neq \delta \in \mathbb{R}$. Denote for brevity $v = (v_2, \ldots, v_n)$ and $|v|^2 = \sum_{2 \leq i \leq n} |v_i|^2$. Also denote $\mu_i = \mu_i(Y)$, $i = 1, 2, 3$, $\mu = \mu(Y)$ and $w = w(Y)$. Define $F(y) = G(y)/\varepsilon^{\iota_1(L,y)} \in \mathbb{R}[\varepsilon, L]$.

Consider the following system of polynomial equations in $X_0, \ldots, X_n$.

$$\begin{cases} h(1, \delta, X_0, \ldots, X_n) = 0, \\ \frac{\partial h}{\partial X_i}(1, \delta, X_0, \ldots, X_n) - y_i \frac{\partial h}{\partial X_1}(1, \delta, X_0, \ldots, X_n) = 0, \quad 2 \leq i \leq n. \end{cases} \tag{15}$$

LEMMA 14 *Let $\mu(y) = \mu$. There is $\nu > 0$ such that for every $v_2, \ldots, v_n \in \mathbb{R}$ for every $0 \neq \delta \in \mathbb{R}$ if $|v|^2 \leq \nu$ and $|\delta| \leq \nu$ then $\mu(y + v) = \mu(y)$ and system (15) has a finite number of solutions in $\mathbb{P}^n(\mathbb{C})$.*

PROOF Choose a linear form L with integer coefficients satisfying (a) and (b) for y, see Section 1. Let v be a vector with sufficiently small $|v|^2$. Then by Lemma 8 we have $\mu_0(y + v) = \mu_0(y)$ and $w(L, y + v) = w(L, y)$. Hence $\iota_1(L, y + v) = \iota_1(L, y)$, $\mu_2(L, y + v) = \mu_2(L, y) = \mu_2$. Therefore,

$$D(y + v)(1, \delta, L - l_0, -l_1, \ldots, -l_n) = \delta^{\iota_1(L,y)} F(y + v)(\delta, L).$$

The similar equality holds if one replace $y + v$ by y. Since $D(Y)$ is a polynomial in $Y_2, \ldots, Y_n$ and by the definition of $\mu_2(L, y)$ the coefficient in $L^{\mu_2(L,y)}$ of the polynomial $F(y + v)(\delta, L)$ is non–zero for all $\delta \neq 0$ and v with sufficiently small $|\delta|$ and $|v|^2$. Hence under these conditions $D(y + v)$ is non–zero and therefore, system (15) has a finite number of solutions. The lemma is proved.

Let $v_2, \ldots, v_n \in \mathbb{R}$ be such that $|v|^2 \leq \nu$. Replace in system (3) y by $y + v$. Denote by

$$\xi^{(j)}(\varepsilon, v) = (1 : \xi_1^{(j)}(\varepsilon, v) : \ldots : \xi_n^{(j)}(\varepsilon, v)) \in \mathbb{P}^n(\overline{\mathbb{C}(\varepsilon)}),\ 1 \leq j \leq \mu_2,$$

the family of all roots of type (iii) of the considered system. Set

$$\xi^{(j)}(v) = (1 : \mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon, v)) : \ldots : \mathrm{st}_\varepsilon(\xi_n^{(j)}(\varepsilon, v))) \in \mathbb{P}^n(\mathbb{C}), \quad 1 \leq j \leq \mu_2,$$

where st_ε is the standard part defined for the elements of the field $\overline{\mathbb{C}(\varepsilon)}$ which are not infinitely large relative to the field $\mathbb{C}$, see [3], [4].

Let v and δ be such that system (15) has a finite number of solutions in $\mathbb{P}^n(\mathbb{C})$. Denote by $\xi^{(j)}(\delta, v) \in \mathbb{P}^n(\mathbb{C})$, $1 \leq j \leq \mu_0$ (recall that $\mu_0 = (2d+2)(2d+1)^{n-1}$) the family of roots of (15) counting with multiplicities. Denote

$$\xi^{(j)}(\delta, v) = (\xi_0^{(j)}(\delta, v) : \xi_1^{(j)}(\delta, v) : \ldots : \xi_n^{(j)}(\delta, v))$$

where $\xi_i^{(j)}(\delta, v) \in \mathbb{C}$. We shall suppose without loss of generality that for every j if $\xi_0^{(j)}(\delta, v) \neq 0$ then $\xi_0^{(j)}(\delta, v) = 1$.

REMARK 4 *Let some $\xi^{(j)}(\varepsilon, v)$ (respectively $\xi^{(j)}(v)$, $\xi^{(j)}(\delta, v)$) does not belong to the hyperplane $\mathcal{Z}(X_0)$ in $\mathbb{P}^n$. Then we shall use the same notation for this element considered as a point from $\mathbb{A}^n$. This will not lead to an ambiguity.*

LEMMA 15 *Let $\mu(y) = \mu$. Let $\nu > 0$ be from the statement of Lemma 14. There is $0 < \nu_1 \leq \nu$ such that for every $\delta_1 > 0$ there is $0 < \delta_2 \leq \nu$ such that for every $v_2, \ldots, v_n \in \mathbb{R}$ satisfying the inequality $|v|^2 \leq \nu_1$ if $|\delta| < \delta_2$ then there is a permutation σ of the set $1, \ldots, \mu_0$ such that*

- *for every $1 \leq j \leq \mu_2$ the element $\xi_0^{(\sigma(j))}(\delta, v) = 1$ and the inequality $\sum_{0 \leq i \leq n} |\xi_i^{(\sigma(j))}(\delta, v) - \xi_i^{(j)}(v)|^2 < \delta_1$ holds,*
- *for every $\mu_2 + 1 \leq j \leq \mu_0$ if $\xi_0^{(\sigma(j))}(\delta, v) = 1$ then $\sum_{0 \leq i \leq n} |\xi_i^{(\sigma(j))}(\delta, v)|^2 > \delta_1^{-1}$.*

PROOF There is a family of different linear forms L_u, $1 \leq u \leq (n-1)\mu_0! + 1$ such that

$$L_u = \sum_{0 \leq i \leq n} c_u^i X_i, \quad c_u \in \mathbb{Z}$$

and for every u the form L_u satisfies conditions (a) and (b) for y. Denote the polynomials $F(y)$ and $F(y+v)$ corresponding to the linear form L_u by $F_u(y)$ and $F_u(y+v)$ respectively. Denote by $J_u(\delta, v) \subset \{1, \ldots, \mu_0\}$ the subset of indices such that $\xi_0^{(j)}(\delta, v) \neq 0$ if and only if $j \in J_u(\delta, v)$. Note that the number of elements $\#J_u(\delta, v) = \deg_{L_u} F_u(y+v)$. Since $D(Y)$ is a polynomial in $Y_2, \ldots, Y_n$ we can represent

$$F_u(y+v) = \varepsilon \Psi_3(\varepsilon, L_u, v_2, \ldots, v_n) + \Psi_4(L_u, v_2, \ldots, v_n)$$

where the polynomials $\Psi_3 \in \mathbb{R}[\varepsilon, Z, Z_2, \ldots, Z_n]$, $\Psi_4 \in \mathbb{R}[Z, Z_2, \ldots, Z_n]$. By the choice of y and L_u we have $\deg_Z \Psi_4(Z, 0, \ldots, 0) = \mu_2$. Besides that,

$$\deg_Z \Psi_4(Z, v_2, \ldots, v_n) = \deg_Z F_u(y+v)(0, Z) = \mu_2(L, y+v) = \mu_2$$

by Corollary 6 for all v with sufficiently small $|v|^2$.

By our definitions the family of roots the polynomial $F_u(y+v)$ coincides with $(L_u/X_0)(\xi^{(j)}(\delta, v))$, $j \in J_u(\delta, v)$. The family of roots of the polynomial $\Psi_4(Z, v_2, \ldots, v_n)$ coincides with $(L_u/X_0)(\xi^{(j)}(v))$, $1 \leq j \leq \mu_2$.

Now Lemma 13 implies that there is $\nu_1 > 0$ such that for every $\delta_3 > 0$ there is $\delta_2 > 0$ such that for every u for all $v_2, \ldots, v_n \in \mathbb{R}$ with $|v|^2 \leq \nu_1$ if $|\delta| < \delta_2$ then there is a permutation $\rho = \rho_u$ (it depends on u) of the set $\{1, \ldots, \mu_0\}$ such that $\rho(j) \in J_u(\delta, v)$ for every $1 \leq j \leq \deg_{L_u} F_u(y+v)$ and

- $|(L_u/X_0)(\xi^{(\rho(j))}(\delta, v)) - (L_u/X_0)(\xi^{(j)}(v))| < \delta_3$ for $1 \leq j \leq \mu_2$,
- $|(L_u/X_0)(\xi^{(\rho(j))}(\delta, v))| > \delta_3^{-1}$ for $\mu_2 + 1 \leq j \leq \deg_Z F_u(y+v)(\delta, Z)$.

For every u consider the projections

$$p_u : \mathbb{A}^n(\mathbb{C}) \to \mathbb{A}^1(\mathbb{C}), \ (X_1, \ldots, X_n) \mapsto L_u(1, X_1, \ldots, X_n).$$

Set for every $\delta_1 > 0$, $\delta_3 > 0$, u and $1 \leq j \leq \mu_2$

$$W_{u,j}(\delta_3) = \{z \in \mathbb{C} : |z - (L_u/X_0)(\xi^{(j)}(v))| < \delta_3\},$$
$$W_j(\delta_1) = \{(z_1, \ldots, z_n) \in \mathbb{A}^n(\mathbb{C}) : \sum_{1 \leq i \leq n} |z_i - \xi_i^{(j)}(v))|^2 < \delta_1\}.$$

Choose δ_3 so small that for all v with $|v|^2 \leq \nu_1$ for all $1 \leq j \leq \mu_2$ for all $1 \leq u_1 < \ldots < u_n \leq (n-1)\mu_0! + 1$ the intersection

$$\bigcap_{1 \leq i \leq n} p_{u_i}^{-1}(W_{u_i,j}(\delta_3)) \subset W_j(\delta_1) \tag{16}$$

(it is possible since the linear forms $L_{u_1} - X_0, \ldots, L_{u_n} - X_0$ are linearly independent). Note that actually δ_3 does not depend on v since it is sufficient to satisfy (16) for only one point. Besides that, we shall require, may be choosing smaller δ_3, that for every u the inequality $|(L_u/X_0)(1, z_1, \ldots, z_n)| > \delta_3^{-1}$ implies $\sum_{1 \leq i \leq n} |z_i|^2 > \delta_1^{-1}$.

Now note that there is a permutation σ of the set $\{1, \ldots, \mu_0\}$ and indices $1 \leq u_1 < \ldots < u_n \leq (n-1)\mu_0! + 1$ such that $\sigma = \rho_{u_i}$ for every $1 \leq i \leq n$. The permutation σ is required. The lemma is proved.

Recall that for every $v_2, \ldots, v_n \in \mathbb{R}$ satisfying the inequality $\sum_{2 \leq i \leq n} |v|^2 \leq \nu$ the equalities $\mu_2(y + v) = \mu_2(y) = \mu_2$ hold.

LEMMA 16 *Let $\mu(y) = \mu$. Let $\nu > 0$ be from the statement of Lemma 14. For every $\delta > 0$ there is $0 < \nu_2 < \nu$ such that for every $v_2, \ldots, v_n \in \mathbb{R}$ satisfying the inequality $|v|^2 \leq \nu_2$ there is a permutation σ of the set $1, \ldots, \mu_2$ such that $\sum_{0 \leq i \leq n} |\xi_i^{(\tau(j))}(v) - \xi_i^{(j)}(0)|^2 < \delta$ for every $1 \leq j \leq \mu_2$.*

PROOF The proof of this lemma is similar to one of Lemma 15 but easier. It follows from Lemma 13 and the fact that $\deg_Z \Psi_4(Z, 0, \ldots, 0) = \mu_2$, see the proof of Lemma 15. The lemma is proved.

REMARK 5 *In what follows for convenience of notation applying Lemma 15 or Lemma 16 we shall suppose without loss of generality that σ and τ are the identity permutations. We shall say in this situation that the families $\xi^{(j)}(\delta, v)$, $1 \leq j \leq \mu_0$, and $\xi^{(j)}(v)$, $1 \leq j \leq \mu_2$, (respectively $\xi^{(j)}(v)$, $1 \leq j \leq \mu_2$, and $\xi^{(j)}(0)$, $1 \leq j \leq \mu_2$), are coordinated by Lemma 15 (respectively Lemma 16).*

Recall that the family of roots of type (iii) of system (3) in $\mathbb{A}^n(\overline{\mathbb{C}(\varepsilon)})$ is $\xi^{(j)}(\varepsilon, 0)$, $1 \leq j \leq \mu_2$. Denote for brevity for every $1 \leq j \leq \mu_2$

$$\xi^{(j)} = (\xi_1^{(j)}, \ldots, \xi_n^{(j)}) = \xi^{(j)}(0) =$$
$$\mathrm{st}_\varepsilon(\xi^{(j)}(\varepsilon, 0)) = (\mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon, 0)), \ldots, \mathrm{st}_\varepsilon(\xi_1^{(j)}(\varepsilon, 0))) \in \mathbb{A}^n(\mathbb{C}).$$

For any vector $z = (z_1, \ldots, z_n) \in \mathbb{C}^n$ denote $|z| = (\sum_{1 \leq i \leq n} |z_i|^2)^{1/2}$. Define also $\mathrm{Re}(z) \in \mathbb{R}^n$ and $\mathrm{Im}(z) \in \mathbb{R}^n$ by the equality $z = \mathrm{Re}(z) + \sqrt{-1}\,\mathrm{Im}(z)$. So $|\xi^{(j)}|^2 = \sum_{1 \leq i \leq n} |\xi_i^{(j)}|^2$ for $1 \leq j \leq \mu_2$.

Consider some semi–algebraic triangulation of $V(\mathbb{R})$, see the Introduction, i.e., a finite simplicial complex $K = \cup_{1 \leq i \leq p} \sigma_i$ (here it means a simplicial space, not an abstract simplicial scheme on finite sets, i.e., $K \subset \mathbb{R}^N$ for some N and each simplex σ_i is the convex hull of its vertices) and a semi–algebraic homeomorphism $\phi : K \to V(\mathbb{R})$.

THEOREM 3 *Let $n \geq 3$ and $V(\mathbb{R})$ be a bounded non–empty real affine algebraic variety given as a set of all common zeroes of polynomials $f_1, \ldots, f_m \in \mathbb{R}[X_1, \ldots, X_n]$, see Introduction. Let $\dim V(\mathbb{R}) \leq n-2$. Let $y_1 = 1$, $y_2, \ldots, y_n \in \mathbb{R}$. Let*

$$\mu = \mu(Y_2, \ldots, Y_n) = \mu(y_2, \ldots, y_n),$$

see Section 1. Let $e = \sum_{1 \le j \le q} \sigma_{p_j}$ *be a non–zero* s*–dimensional cycle with coefficients from* $\mathbb{Z}/2\mathbb{Z}$ *of the simplicial complex* K*, herewith all the simplexes* σ_{p_j} *are maximal. Hence, see the Introduction,* $E = \cup_{1 \le j \le q} \phi(\sigma_{p_j}) \subset V(\mathbb{R})$*,* m'*,* E'*,* m''*,* E'' *are defined for the vector* $(1, y_2, \ldots, y_n)$*. Suppose that the image of every simplex* $\phi(\sigma_{p_j})$*,* $1 \le j \le q$*, is not contained in any hyperplane* $\mathcal{Z}_{\mathbb{R}}(\sum_{1 \le i \le n} y_i X_i - a)$*,* $a \in \mathbb{R}$ *(hence* $s \ge 1$*). Then there are at least two different points* $\xi^{(j)}$*,* $1 \le j \le \mu_2$ *which belong to* E*. More precisely,* $E' \cup E'' \subset \{\xi^{(j)} : 1 \le j \le \mu_2\}$*. In particular under the conditions of this theorem the sets* E' *and* E'' *are finite.*

PROOF Effecting the linear transformation of coordinates $X_1 \mapsto X_1 + \sum_{2 \le j \le n} y_j X_j$, $X_i \mapsto X_i$, $i = 0, 2, 3, \ldots, n$ we shall suppose in what follows that $(y_2, \ldots, y_n) = (0, \ldots, 0)$ and $\mu(0, \ldots, 0) = \mu$. Thus, (3) with $X_0 = 1$ is equivalent to the system of polynomial equations in $X_1, \ldots, X_n$ with coefficients from the field $\mathbb{R}(\varepsilon)$

$$\begin{cases} f_\varepsilon = 0, \\ \frac{\partial f_\varepsilon}{\partial X_i} = 0, \quad 2 \le i \le n. \end{cases} \tag{17}$$

Recall that $m' = \max X_1(E)$ and $E' = \{z \in E : X_1(z) = m'\}$. We shall suppose without loss of generality that $m' = 0$ effecting if necessary the linear transformation $X_1 \mapsto X_1 + m'$. Denote by W' the algebraic variety which is the closure in the Zariski topology of E'. Then $\dim W' < s$ since every simplex $\phi(\sigma_{p_j})$, $1 \le j \le q$, is not contained in any hyperplane $\mathcal{Z}_{\mathbb{R}}(X_1 - a)$, $a \in \mathbb{R}$. Suppose that there is a point $\xi^{(0)} \in E'$ and $\xi^{(0)} \ne \xi^{(j)}$ for every $1 \le j \le \mu_2$.

Denote by $J_1 \subset \{1, \ldots, \mu_2\}$ the subset of indices such that $j \in J_1$ if and only if $X_1(\xi^{(j)}) = 0$ and $\xi^{(j)} \in \mathbb{R}^n$.

Denote by $J_2 \subset \{1, \ldots, \mu_2\}$ the subset of indices such that $j \in J_2$ if and only if $X_1(\xi^{(j)}) \ne 0$ and $\xi^{(j)} \in \mathbb{R}^n$.

Denote by $J_3 \subset \{1, \ldots, \mu_2\}$ the subset of indices such that $j \in J_3$ if and only if $\xi^{(j)} \notin \mathbb{R}^n$.

So $\{1, \ldots, \mu_2\} = J_1 \cup J_2 \cup J_3$ and $J_i \cap J_j = \emptyset$ for all $1 \le i \ne j \le 3$.

Consider the projection

$$p_1 : \mathbb{R}^n \to \mathbb{R}^{n-1} \quad (X_1, \ldots, X_n) \mapsto (X_2, \ldots, X_n).$$

Note that the point $p_1(\xi^{(0)})$ is different from each point $p_1(\xi^{(j)})$, $j \in J_1$. Therefore, since $n - 1 \ge 2$ there is a C^∞–function $\beta : \mathbb{R}^{n-1} \to \mathbb{R}$ such that $\beta(p_1(\xi^{(j)})) < 0$ for all $j \in J_1$ and $\beta(p_1(\xi^{(0)})) > 0$. Define the function $\gamma = \beta \circ p_1$. Then $\gamma(\xi^{(j)}) < 0$ for all $j \in J_1$ and $\gamma(\xi^{(0)}) > 0$.

Definition of ϵ_1. Choose $\epsilon_1 > 0$ so small that

(1a) for every $j \in J_1$ the inequality $\gamma(\xi^{(j)}) < -2\epsilon_1$ holds,

(1b) for every $j \in J_2$ the inequality $|X_1(\xi^{(j)})| > 2\epsilon_1$ holds,

(1c) for every $j \in J_3$ the inequality $|\operatorname{Im}(\xi^{(j)})| > 2\epsilon_1$ holds,

(1d) $\gamma(\xi^{(0)}) > 2\epsilon_1$ holds.

Definition of ϵ_2. Choose $\epsilon_2 > 0$ so small that

(2a) $\epsilon_2 \le \nu_1$ where ν_1 is from Lemma 15

Now note that there is $w > 0$ so small that (1a), (1b) and (1c) take place also if one replaces $2\epsilon_1$ by $2\epsilon_1 + w$. Hence there is $\delta' > 0$ such that if $z \in \mathbb{C}^n$ and $|z - \xi^{(j)}|^2 \leq \delta'$ then for every $j \in J_1$ (respectively $j \in J_2$, $j \in J_3$) the inequality $\gamma(\mathrm{Re}(z)) < -2\epsilon_1$ (respectively $|X_1(z)| > 2\epsilon_1$, $|\,\mathrm{Im}(z)| > 2\epsilon_1$) holds.

Recall that $\nu_1 < \nu$. So set $\delta = \delta'$, apply Lemma 16 and Remark 5. We shall suppose in what follows that the corresponding families $\xi^{(j)}(v)$, $1 \leq j \leq \mu_2$, and $\xi^{(j)}$, $1 \leq j \leq \mu_2$, are coordinated by Lemma 16. We shall require that

(2b) $\epsilon_2 \leq \nu_2$ where ν_2 corresponds to $\delta = \delta'$ by Lemma 16.

Note that (2b) implies

(2i) for every $j \in J_1$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $\gamma(\mathrm{Re}(\xi^{(j)}(v))) < -2\epsilon_1$ holds,

(2ii) for every $j \in J_2$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|X_1(\xi^{(j)}(v))| > 2\epsilon_1$ holds,

(2iii) for every $j \in J_3$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|\,\mathrm{Im}(\xi^{(j)}(v))| > 2\epsilon_1$ holds,

(2iv) there is $m_0 > 0$ such that for every $1 \leq j \leq \mu_2$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|\xi^{(j)}(v)|^2 < m_0$ holds.

Definition of ϵ_3. Let $r : \mathbb{R} \to \mathbb{R}$ be a C^∞–function such that $r(x) = 1$ if $x \leq -\epsilon_1$, $r(x) = 0$ if $x \geq \epsilon_1$ and r is a monotone decreasing function in the open interval $-\epsilon_1 < x < \epsilon_1$.

Choose an open n-dimensional ball $B \subset \mathbb{R}^n$ with the center in the point $(0, \ldots, 0)$ containing $V(\mathbb{R})$. Denote by $\overline{B}$ the closure in the classic topology of B. Denote $r' = dr/dx$. Set

$$\begin{aligned} m_1 &= \max\{r'(x) \,:\, x \in \mathbb{R}\} \\ m_2 &= \max_{2 \leq i \leq n} \max\{|\frac{\partial \gamma}{\partial X_i}(z)| \,:\, z \in \overline{B}\,\&\,|\gamma(z)| \leq \epsilon_1\}. \end{aligned}$$

We shall require that

(3a) $\epsilon_3 < \min\{\sqrt{\epsilon_2/(n-1)}/(m_1 m_2), \epsilon_1/2\}$.

This implies $(\epsilon_3 m_1 m_2)^2 (n-1) < \epsilon_2$.

Definition of ϵ_4. Note that for every sufficiently small neighborhood U in the classic topology of the point $\xi^{(0)}$ there is a smooth point $z_0 \in U$ such that

(4i) the point $z_0 \in E$,

(4ii) the point z_0 is smooth of dimension s on $V(\mathbb{R})$,

(4iii) the tangent space $T_{z_0, V(\mathbb{R})}$ is not contained in the hyperplane $\mathcal{Z}_{\mathbb{R}}(X_1)$, i.e. the vector $(1, 0, \ldots, 0)$ is not orthogonal to $T_{z_0, V(\mathbb{R})}$,

(4iv) $\gamma(z_0) > 2\epsilon_1$.

These requirements can be satisfied due to the fact that every simplex $\phi(\sigma_{p_j})$, $1 \leq j \leq q$, is not contained in any hyperplane $\mathcal{Z}_{\mathbb{R}}(X_1 - a)$, $a \in \mathbb{R}$.

Choose $\epsilon_4 > 0$ such that

(4a) $\epsilon_4 < \epsilon_3/2$,

(4b) the intersection $E \cap \mathcal{Z}_{\mathbb{R}}(X_1 + \epsilon_4)$ contains a point z_0 which satisfies conditions (4i)–(4iv).

Definition of ϵ_5. Consider the n-dimensional ball $B \subset \mathbb{R}^n$ introduced previously. Set

$$m_4 \quad = \quad \min\{(f/g)(z) \ : \ z \in \overline{B} \cap (\mathbb{R}^n \setminus B)\},$$

Then $m_4 > 0$. Denote by m_5 radius of B. Set $m_6 = \max\{m_0 + 2, m_5 + 1\}$.

Denote $V_\epsilon = \mathcal{Z}_{\mathbb{R}}(f - \epsilon g) \cap B$ for $0 < \epsilon \in \mathbb{R}$. We shall require

(5a) $0 < \epsilon_5 < m_4$,

(5b) for every ϵ, $0 < \epsilon < \epsilon_5$ V_ϵ is a smooth manifold, cf. the proof of Lemma 2,

(5c) $\epsilon_5 \leq \nu_1$ where ν_1 is from the formulation of Lemma 15.

By (2i)–(2iv) there is $\delta'' > 0$ such that for every $v \in \mathbb{R}^{n-1}$ for every $z \in \mathbb{C}^n$ if $|v|^2 \leq \epsilon_2$ and $|z - \xi^{(j)}(v)|^2 \leq \delta''$ then

- for every $j \in J_1$ the inequalities $\gamma(\mathrm{Re}(z)) < -\epsilon_1$ and $|X_1(z) - X_1(\xi^{(j)}(v)))| < \epsilon_3/2$ hold,
- for every $j \in J_2$ the inequality $|X_1(z)| > \epsilon_1$ holds,
- for every $j \in J_3$ the inequality $|\,\mathrm{Im}(z)| > \epsilon_1$ holds.

So set $\delta_1 = \min\{\delta'', m_6^{-2}\}$, apply Lemma 15 and Remark 5. We shall suppose in what follows that the corresponding families $\xi^{(j)}(\epsilon, v)$, $1 \leq j \leq \mu_0$, and $\xi^{(j)}(v)$, $1 \leq j \leq \mu_2$, are coordinated by Lemma 15 if $0 < \epsilon < \epsilon_5$, $|v|^2 \leq \epsilon_2$. We shall require that

(5d) $\epsilon_5 \leq \delta_2$ where δ_2 corresponds to $\delta_1 = \min\{\delta'', m_6^{-2}\}$ by Lemma 15.

Then (5d) implies

(5i) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $j \in J_1$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $\gamma(\mathrm{Re}(\xi^{(j)}(\epsilon, v))) < -\epsilon_1$ holds,

(5ii) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $j \in J_1$ the inequality $|X_1(\xi^{(j)}(\epsilon, 0))| < \epsilon_3/2$ holds,

(5iii) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $j \in J_2$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|X_1(\xi^{(j)}(\epsilon, v))| > \epsilon_1$ holds,

(5iv) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $j \in J_3$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|\,\mathrm{Im}(\xi^{(j)}(\epsilon, v))| > \epsilon_1$ holds,

(5v) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $1 \leq j \leq \mu_2$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ the inequality $|\xi^{(j)}(\epsilon, v)|^2 < m_0 + 1$ holds,

(5vi) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $\mu_2 + 1 \leq j \leq \mu_0$ for every $v \in \mathbb{R}^{n-1}$ such that $|v|^2 \leq \epsilon_2$ if $\xi_0^{(j)}(\epsilon, v) = 1$ then the inequality $|\xi^{(j)}(\epsilon, v)|^2 > m_6^2 - 1 > (\max\{m_0 + 1, m_5\})^2$ holds.

Note that (5i)–(5iv) and (3a) imply

(5vii) for every ϵ, $0 < \epsilon < \epsilon_5$, if $j \in J_1 \cup J_2$ and $\gamma(\mathrm{Re}(\xi^{(j)}(\epsilon, 0))) < -\epsilon_1$ then $|X_1(\xi^{(j)}(\epsilon, 0)) - \epsilon_3| > \epsilon_3/2$,

(5viii) for every ϵ, $0 < \epsilon < \epsilon_5$, if $j \in J_2$ then $|X_1(\xi^{(j)}(\epsilon, 0))| > \epsilon_3/2$,

(5ix) for every ϵ, $0 < \epsilon < \epsilon_5$, if $j \in J_3$ then $|\,\mathrm{Im}(\xi^{(j)}(\epsilon, 0))| > \epsilon_3/2$.

Now consider the point z_0 defined in (4i)–(4iv) and (4b). Choose linear forms $L_1, \ldots, L_s \in \mathbb{R}[X_1, \ldots, X_n]$ such that $L_1 = X_1$ and the intersection

$$T_{z_0, V(\mathbb{R})} \cap \mathcal{Z}_{\mathbb{R}}(L_1, \ldots, L_s) = \{0\}.$$

Then by the implicit function theorem z_0 is an isolated point of the intersection $V(\mathbb{R}) \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \ldots, L_s - L_s(z_0))$. The connected component B_1 of the intersection

$$\{z \,:\, f(z) - \epsilon g(z) \leq 0\} \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \ldots, L_s - L_s(z_0)) \tag{18}$$

containing the point z_0 tends to the point z_0 when ϵ tends to zero. For all sufficiently small $\epsilon > 0$ the bound $S_1 = \partial B_1$ is a smooth compact $(n - s - 1)$–dimensional manifold, cf. the proof of Lemma 2. Since $n - s - 1 > 0$ this manifold is a connected component of the real algebraic variety

$$\mathcal{Z}_{\mathbb{R}}(f - \epsilon g) \cap \mathcal{Z}_{\mathbb{R}}(L_1 - L_1(z_0), \ldots, L_s - L_s(z_0)). \tag{19}$$

In what follows we shall suppose that the semi–algebraic set B_1 is triangulated, see [2]. Then this triangulation induces the triangulation of S_1. The set B_1 defines the $(n-s)$–dimensional chain b_1 and S_1 defines the $(n-s-1)$–dimensional cycle s_1 which is the bound of b_1, i.e. $s_1 = \partial b_1$.

Finally, we put forth the following requirements.

(5e) for every ϵ, $0 < \epsilon < \epsilon_5$, the bound $S_1 = \partial B_1$ is a smooth manifold which is a connected component of a real algebraic variety,

(5f) for every ϵ, $0 < \epsilon < \epsilon_5$, for every $z' \in B_1$ the inequality $\gamma(z') \geq \epsilon_1$ holds.

Define the C^∞–function $\omega : \mathbb{R}^n \to \mathbb{R}$ by the formula

$$\omega(X_1, \ldots, X_n) = X_1 - \epsilon_3 r(\gamma(X_1, \ldots, X_n)).$$

Note also that $\omega(X_1, \ldots, X_n) = X_1 - \epsilon_3 r(\beta(X_2, \ldots, X_n))$. We claim that for every ϵ, $0 < \epsilon < \epsilon_5$ for every $z \in V_\epsilon$ such that $|\omega(z)| \leq \epsilon_4$ the point z is not a critical point, see [13], of the function ω on the compact smooth manifold V_ϵ, see (5a), (5b).

Indeed, suppose contrary that z is a critical point of the function ω. If $|\gamma(z)| > \epsilon_1$ then the gradients of the functions $f - \epsilon g$ and ω in the point z are parallel to the vector $(1, 0, \ldots, 0)$. Hence, $z = \xi^{(j)}(\epsilon, 0)$ for some $1 \leq j \leq \mu_0$. Conditions (5v) and (5vi) imply that $1 \leq j \leq \mu_2$. Condition (5iv) (or (5ix)) implies that $j \in J_1 \cup J_2$. Now from the definition of the function ω conditions (4a), (5vii) and (5viii) we get a contradiction.

If $|\gamma(z)| \le \epsilon_1$ then the gradients of the functions $f - \epsilon g$ and ω in the point z are parallel to the vector

$$\left(1,\, -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_2}(z),\, \ldots,\, -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_n}(z)\right).$$

Set

$$v_i = -\epsilon_3\, r'(\gamma(z))\, \frac{\partial \gamma}{\partial X_i}(z), \qquad 2 \le i \le n.$$

Recall that $V_\epsilon \subset \overline{B}$. Hence (3a) implies $|v|^2 \le \epsilon_2$. In this case $z = \xi^{(j)}(\epsilon, v)$ for some $1 \le j \le \mu_0$. Conditions (5v) and (5vi) imply that $1 \le j \le \mu_2$. We obtain a contradiction from the definition of the function ω and conditions (4a), (5i), (3a), (5iii) and (5iv). The required assertion is proved.

Now, see [13], we get that there is a diffeomorphism

$$\alpha : [-\epsilon_4, \epsilon_4] \times (V_\epsilon \cap \{z : \omega(z) = -\epsilon_4\}) \longrightarrow V_\epsilon \cap \{z : |\omega(z)| \le \epsilon_4\} \qquad (20)$$

such that $\omega(\alpha(a, w)) = a$ for every $-\epsilon_4 \le a \le \epsilon_4$ and $w \in V_\epsilon \cap \{z : \omega(z) = -\epsilon_4\}$. Denote $V_{\epsilon,a} = V_\epsilon \cap \{z : \omega(z) = a\}$ for $-\epsilon_4 \le a \le \epsilon_4$. Denote by $i_a : V_{\epsilon,a} \to V_\epsilon \cap \{z : |\omega(z)| \le \epsilon_4\}$ the mappings of the inclusions. Then (20) implies that the homomorphisms of the groups of singular homologies induced by i_a

$$i_{a\,*} : H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) \to H_{n-s-1}(V_\epsilon \cap \{z : |\omega(z)| \le \epsilon_4\}, \mathbb{Z}/2\mathbb{Z})$$

have the same image for all $-\epsilon_4 \le a \le \epsilon_4$. Hence the same is true for the through homomorphisms

$$\begin{array}{ccccc} H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}(V_\epsilon \cap \{z : |\omega(z)| \le \epsilon_4\}, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow \\ H_{n-s-1}(V_\epsilon, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z}). & \end{array}$$

Denote by $j(a) : H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) \to H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z})$ this through homomorphism. Denote $j_- = j(-\epsilon_4)$ and $j_+ = j(\epsilon_4)$.

We have the commutative diagram of the homology groups induced by the inclusions of topological spaces

$$\begin{array}{ccc} H_{n-s-1}(V_{\epsilon,a}, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}((\mathbb{R}^n \setminus E) \cap \{z : \omega(z) = a\}, \mathbb{Z}/2\mathbb{Z}) \\ \downarrow & & \downarrow \\ H_{n-s-1}(V_\epsilon, \mathbb{Z}/2\mathbb{Z}) & \longrightarrow & H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z}). \end{array}$$

The topological space $(\mathbb{R}^n \setminus E) \cap \{z : \omega(z) = \epsilon_4\}$ is homeomorphic to $\mathbb{R}^{n-1}$ since $E \cap \{z : \omega(z) = \epsilon_4\} = \emptyset$. Hence the homology group $H_{n-s-1}((\mathbb{R}^n \setminus E) \cap \{z : \omega(z) = \epsilon_4\}, \mathbb{Z}/2\mathbb{Z}) = 0$ since $n - s - 1 > 0$. Therefore, the image $\mathrm{Im}(j_+) = 0$.

On the other hand, by (5f) and (5e) the image $\mathrm{Im}(j_-)$ contains the homological class of the cycle $s_1 \in Z_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z})$ defined above. Let us show that s_1 is not homological to zero in $H_{n-s-1}(\mathbb{R}^n \setminus E, \mathbb{Z}/2\mathbb{Z})$. Indeed, the intersection of $B_1 \cap E$ consists of one point z_0 and is transversal in this point. So by the general topological duality theory, see [16], the linking coefficient in $\mathbb{Z}/2\mathbb{Z}$ of cycles e and s_1 is not zero. From here our assertion follows immediately.

Thus, we have $0 \ne \mathrm{Im}(j_-) = \mathrm{Im}(j_+) = 0$. Hence, the initial assumption that $E' \not\subset \{\xi^{(j)} : 1 \le j \le \mu_2\}$ leads to a contradiction. Therefore, $E' \subset \{\xi^{(j)} : 1 \le j \le \mu_2\}$. In the similar way $E'' \subset \{\xi^{(j)} : 1 \le j \le \mu_2\}$. The theorem is proved.

REMARK 6 *Slightly modifying the proof of Theorem 3 one can consider also the case when* $\dim V(\mathbb{R}) = n-1$.

REMARK 7 *The condition that the image of every simplex* $\phi(\sigma_{p_j})$, $1 \le j \le q$, *is not contained in any hyperplane* $\mathcal{Z}_{\mathbb{R}}(\sum_{1\le i\le n} y_i X_i - a)$, $a \in \mathbb{R}$ *implies that* $\dim E', \dim E'' < s$ *and this condition is used only with the aim to prove these inequalities.*

REMARK 8 *In the general case under the conditions of Theorem 3 the points from* E' *and* E'' *may belong to many different components of* $V(\mathbb{R})$ *even in the case when* E *is contained in one irreducible component of* $V(\mathbb{R})$.

3 Proof of Theorem 1

Note that the case $s = 0$ is known, see [14]. Similarly, by [14] one can decide whether $V(R) = \emptyset$. So we shall assume in what follows that $s \ge 1$ and $\dim V(R) \ge 1$. We can suppose without loss of generality that $n \ge 3$ and $\dim V(R) \le n-2$ considering if it is necessary the embedding $\mathbb{A}^n \to \mathbb{A}^{n+2}$.

At first consider the case when $R = \mathbb{R}$. Construct using the algorithm from Section 1 the vector $z = (1, z_2, \ldots, z_n)$ with integer coordinates with the lengths $O(n \log d)$ such that $\mu(z_2, \ldots, z_n) = \mu$. Effecting if necessary a linear transformation of $\mathbb{A}^n$ we can suppose without loss of generality that $z = (1, 0, \ldots, 0)$ and $y_1 = 1$. In this section we suppose that $y_2, \ldots, y_n \in k_0$.

Let V_s be the closure in the Zariski topology of the set of all smooth points of the real algebraic variety $V(R)$. The number of irreducible components of V_s is bounded from above by $\mathcal{P}(d^n)$ for a polynomial $\mathcal{P}$, see [15].

By Lemma 8 there is an integer $a \ne 0$ bounded from above by a polynomial in d^n such that

$$\mu(ac, ac^2, \ldots, ac^{n-1}) = \mu$$

for all integers $1 \le c \le n\mathcal{P}(d^n)+1$. Construct such an integer a within the time polynomial in d^n and the size of input according to Section 1. Note that any n vectors of the set

$$\mathcal{C} = \{(1, ac, ac^2 \ldots, ac^{n-1}) \,:\, 1 \le c \le n\mathcal{P}(d^n)+1\}$$

are linearly independent. For every simplex σ_{p_j} of the considered cycle e the image $\phi(\sigma_{p_j})$ is contained in some irreducible component of V_s, see [2]. Hence there is $c_0 \in \mathcal{C}$ such that every $\phi(\sigma_{p_j})$ is not contained in any hyperplane

$$\mathcal{Z}(X_1 + ac_0 X_2 + ac_0^2 X_3 + \ldots + ac_0^{n-1} X_n - b), \quad b \in R.$$

Denote $v_c = (1, ac, ac^2 \ldots, ac^{n-1})$ for all c and $v_0 = v_{c_0}$.

By Lemma 8 the equality $\mu(y+\delta v_0) = \mu$ holds for all sufficiently small $\delta > 0$. Besides that, every $\phi(\sigma_{p_j})$ is not contained in any hyperplane

$$\mathcal{Z}((1+\delta)X_1 + (y_2+\delta ac_0)X_2 + (y_3+\delta ac_0^2)X_3 + \ldots + (y_n+\delta ac_0^{n-1})X_n - b), \quad b \in R$$

for all sufficiently small $\delta > 0$.

Consider the system of polynomial equations

$$\begin{cases} f_\varepsilon = 0, \\ (1+\delta)\frac{\partial f_\varepsilon}{\partial X_i} - (y_i + \delta a c^{i-1})\frac{\partial f_\varepsilon}{\partial X_1} = 0, \quad 2 \le i \le n. \end{cases} \tag{21}$$

Let the sets E'_δ and E''_δ correspond to the vector $y + \delta v_0$ in the similarly way as E', E'' correspond to y. Theorem 3 implies that for all sufficiently small $\delta > 0$ there are points $z'_\delta \in E'_\delta$ and $z''_\delta \in E''_\delta$ which are standard parts of some solutions of the system (21) with $c = c_0$.

The compactness of E implies now that there is a sequence $\delta_i > 0, i = 1, 2, \ldots$ which tends to zero such that the points z'_{δ_i} and z''_{δ_i} tend to points $z' \in E'$ and $z'' \in E''$.

Now let δ be a variable. Consider the set W of all the points which are standard parts relative to ε of solutions of system (21) in $(\mathbb{A}^n \times \mathbb{A}^1)(\overline{C(\varepsilon)})$ where $\mathbb{A}^n$ has coordinates $X_1, \ldots, X_n$ and $\mathbb{A}^1$ has the coordinate δ. Then W is an algebraic variety and the union of all components of W which are not contained in $\mathcal{Z}(1+\delta)$ is a curve W_c since for every $\delta \neq -1$ system (21) has a finite number of solutions by Section 1. Further, $z', z'' \in W_{c_0} \cap \mathcal{Z}(\delta)$. So we define

$$S_y = \bigcup_{c \in \mathcal{C}} (W_c(R) \cap \mathcal{Z}(\delta)).$$

Note that every curve W_c can be constructed within the required time considering standard parts relative to ε of solutions of system (21) in $\mathbb{A}^n(\overline{(C(\delta, \varepsilon)})$ by [5] and using Newton–Puiseux expansions, cf. [3], [4], [6], [7]. Further in a similar way one can construct the set S_y. The theorem is now proved for the case $R = \mathbb{R}$.

In the general case we use the transfer principle, [2]. It is sufficient to note that the fact that the real algebraic variety is semi–algebraically triangulated can be expressed in the language of the first order theory of real fields. The theorem is proved.

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.* in: "Quantifier Elimination and Cylindrical Algebraic Decomposition", B. Caviness and J. Johnson Eds., Springer-Verlag.

[2] J. Bochnak, M. Coste, M.–F. Roy, *Géométrie algébrique réelle*, (Springer–Verlag, Berlin, Heidelberg, New York, 1987).

[3] A. L. Chistov, Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic, *Journal of Symbolic Computation* **22** # 1 (1996) 1–25.

[4] A. L. Chistov, Polynomial–time computation of the dimensions of components of algebraic varieties in zero–characteristic,*Journal of Pure and Applied Algebra*. **117 & 118** (1997) 145–175.

[5] A. L. Chistov, Polynomial complexity algorithm for factoring polynomials and constructing components of a variety in subexponential time, *Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* **137** (1984) 124–188 (Russian) [English transl.: *J. Sov. Math.* **34** # 4 (1986)].

[6] A. L. Chistov, Polynomial complexity of the Newton–Puiseux algorithm, in: *Lecture Notes in Computer Science* **233** (Springer, New York, Berlin, Heidelberg, 1986) 247–255.

[7] A. L. Chistov, Polynomial complexity algorithms for computational problems in the theory of algebraic curves, *Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* **176** (1989) 124–188 (Russian) [English transl. in: *J. Sov. Math. or J. Math. Sciences.*].

[8] R. Hartshorne, *Algebraic geometry*, (Springer–Verlag, New York, Heidelberg, Berlin, 1977).

[9] W. V. D. Hodge, D. Pedoe, *Methods of algebraic geometry*, v. 1, (Cambridge, 1947).

[10] D. Lazard, Algèbre linéaire sur $k[x_1, \ldots, x_n]$ et élimination, *Bull. Soc. Math. France.* **105** (1977) 165–190.

[11] D. Lazard, Résolution des systèmes d'équations algébrique, *Theoretical Computer Science.* **15** (1981) 77–110.

[12] J. Milnor, On Betti numbers of real varieties, *Proceedings of the American Math. Soc.* **15** # 2 (1964) 275–280.

[13] J. Milnor, *Morse theory* , (Princeton University Press, Princeton, New Jersey, 1963).

[14] J. Renegar, A faster PSPACE algorithm for deciding the existential theory of reals, *Proc. 29th Annual Symp. on Foundations of Computer Sci., October 24–26* (1988) 291–295.

[15] M.–F. Roy, N. Vorobjov, Computing the Complexification of a Semi-algebraic Set, in: *Proc. of ISSAC'96 conference.*

[16] E. H. Spanier, *Algebraic topology*, (McGrow–Hill, New York, 1966).