Polynomial–Time Computation of the Degree of Algebraic Varieties in Zero–Characteristic and its Applications

Alexander L. Chistov*

St. Petersburg Institute for Informatics and Automation of the Academy of Sciences of Russia

and

Department of Computer Science
University of Bonn

Abstract

Let an algebraic variety over a zero–characteristic ground field be given as a set of common zeros of a family of polynomials of the degree less than d in n variables. In this paper the following algorithms with the working time polynomial in the size of input and d^n are constructed: an algorithm for the computation of the degrees of algebraic varieties, an algorithm for the computation of the dimension of the given algebraic variety in the neighborhood of a given point, an algorithm for the computation of the multiplicity of a given point of the algebraic variety, an algorithm for the computation smooth points with their tangent spaces on each component of a given algebraic variety.

*Research partially supported by the Volkswagen–Stiftung, Program on Computational Complexity, University of Bonn and by the International Science Foundation grant NT3000

Introduction

In the paper polynomial–time algorithms are suggested for the computation of such basic numerical characteristics of algebraic varieties as degrees, dimensions of components containing a given point, multiplicities of points. Besides that, smooth points with their tangent spaces on each component of the algebraic variety are constructed. The case of zero–characteristic ground field is considered.

This paper continues and uses the results and technics of [3], [4] and [5] where the problem of the computation of the dimension of algebraic varieties and their components was solved for the case of zero–characteristic, see Introductions of [3], [5]. The case of non–zero characteristic for all the problems considered here is open. The results of real algebraic geometry are essentially used in the present paper and in [3], [4] and [5]. We consider an algebraically closed field of zero characteristic as an extension of degree 2 of a real ordered field. The required property can be formulated over this real ordered field. After that we can apply the "transfer principle", see [1], and reduce everything to the case of the field of real numbers. For this field we have a developed theory. The result from [14] is crucial which in its turn is based on the result of [13].

It should be emphasized that this paper can not appear until two principle steps were made in [3] and [5]. In [3] the problem of the computation of dimension was solved for the case of projective varieties. The algorithm from [5] for the computation of dimensions of all components of an algebraic variety required additionally four embedded recursions. It is not clear whether one can avoid all this technique of [5] for more simple problems, e.g. to find a point of an algebraic variety which does not belong to a component of the highest dimension, or even to determine whether there are components of different dimensions. Note also that in other terms the construction from [5] is a polynomial–time algorithm for the choice of the projection in the Noether normalization theorem.

Now we give the precise statements. Let $k = \mathbb{Q}(t_1, \ldots, t_l, \theta)$ be the 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 $\mathrm{lc}_Z F$ of F is equal to 1. Let homogeneous polynomials $g_0, \ldots, g_m \in k[X_0, \ldots, X_n]$ be given. Consider the closed algebraic set or which is the same in this paper the algebraic variety

$$V = \{(x_0 : \ldots : x_n) \,:\, g_i(x_0, \ldots, x_n) = 0 \;\forall 0 \le i \le m\} \subset \mathbb{P}^n(\overline{k}) \,.$$

This is a set of all common zeros of polynomials $g_0, \ldots, g_m$ in the projective space $\mathbb{P}^n(\overline{k}$, where $\overline{k}$ is an algebraic closure of k. Below for brevity we shall use denotations like $V = \{g_0 = \ldots = g_m = 0\}$.

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

$$f = \frac{1}{a_0} \sum_{i_0, \ldots, i_n} \sum_{0 \le s < deg f} a_{i_1, \ldots, i_n, j} \theta^j X_0^{i_0} \cdots X_n^{i_n} \,,$$

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

$$\deg_{X_0,\ldots,X_n}(g_i) < d,\ \deg_{t_\alpha}(g_i) < d_2,\ l(g_i) < M,$$
$$\deg_Z(F) < d_1,\ \deg_{t_\alpha}(F) < d_1,\ l(F) < M_1\,.$$

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

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

Similarly $L(F) < d_1^{l+1} M_1$. Below if there is no special mention about it we set l to be fix.

Let V_s be the union of all the components of of V of the dimension $n-s$ where $0 \le s \le n$. The degree $\deg V_s$ of V_s is equal to $\max_H \#V_s \cap H$ where the maximum is taken over all the linear subspaces H of $\mathbb{P}^n(\overline{k})$ of the dimension s such that $\#V_s \cap H < +\infty$. The degree $\deg V$ of V is set to be $\sum_{0 \le s \le n} \deg V_s$.

THEOREM 1. Let a projective algebraic variety V over the ground field k be given as a set of common zeros in $\mathbb{P}^n(\overline{k})$ of a family of homogeneous polynomials $g_0,\ldots,g_m \in k[X_0,\ldots,X_n]$ of the degrees less than d. Then the degrees $\deg V_s$ for all $0 \le s \le n$ and $\deg V$ can be computed within the time polynomial in d^n, d_1, d_2, M, M_1, m.

Let $x \in \mathbb{P}^n(\overline{k})$. The dimension $\dim_x V$ of the variety V in the point x (or in the neighborhood of the point x) is set to be $\max_W \dim W$ where the maximum is taken over all the components W of V such that $x \in W$. Denote by $\mathcal{W}$ the set of all such components W.

THEOREM 2. Let $x \in \mathbb{P}^n(\overline{k})$. The dimensions of all the components containing the the point x, i.e. the set $\{\dim W : W \in \mathcal{W}\}$ can be computed within the time polynomial in d^n, d_1, d_2, M, M_1, m and the size of the point x. Therefore, the dimension $\dim_x V$ of the variety V in the point x can be computed within the same time.

Now let a point $x \in V_s$ and $0 \le s \le n-1$. Denote by $\mathcal{L}$ the set of linear subspaces L of $\mathbb{P}^n(\overline{k})$ such that $\dim L = s$, $x \in L$ and $\#V_s \cap L < +\infty$. The multiplicity $\mu(x, V_s)$ of the point x of the variety V_s is defined by the formula

$$\mu(x, V_s) = \min_{L \in \mathcal{L}}\{1 + \deg V_s - \#V_s \cap L\}.$$

This formula can be explained in the following way, c.f. [12]. By its initial meaning the multiplicity $\mu(x, V_s)$ is equal to to the number of points infinitely close to x of the intersection of a generic linear subspace $\tilde{L}$, $\dim \tilde{L} = s$, which is infinitely close to the point x. So $\# V_s \cap \tilde{L} = \deg V_s$. When one shifts this generic linear subspace to the generic subspace $\overline{L}$ containing the point x (by an infinitely small shift) all the points of the intersection which were in the infinitely small neighborhood of x goes to x, other points of the intersection go bijectively to $-1 + \# V_s \cap \overline{L} = \max_{L \in \mathcal{L}}\{-1 + \# V_s \cap L\}$ points. So one get this formula for $\mu(x, V_s)$.

If $x \in V_n$ then $\mu(x, V_n) = 1$. If $x \in V$ set $S(x) = \{s : x \in V_s\}$. The multiplicity $\mu(x, V)$ of the point x of the variety V is set to be

$$\mu(x, V) = \sum_{s \in S(x)} \mu(x, V_s).$$

THEOREM 3. The multiplicities $\mu(x, V_s)$ for all $0 \le s \le n$ and $\mu(x, V)$ can be computed within the time polynomial in d^n, d_1, d_2, M, M_1, m and the size of the point x.

THEOREM 4. Let a projective algebraic variety V over the ground field k be given as a set of common zeros in $\mathbb{P}^n(\overline{k})$ of a family of homogeneous polynomials $g_0, \ldots, g_m \in k[X_0, \ldots, X_n]$ of the degrees less than d. Let V_s as above be the union of all the components of V of the dimension j where $0 \le s \le n$. Then one can construct for every $0 \le s \le n$ a finite set A_s of smooth points of V_s and for every point $x \in A_s$ the tangent space T_x of the variety V_s in the point x. The tangent spaces are considered here as linear subspaces of $\mathbb{P}^n(\overline{k})$. Besides that, A_s satisfy to the property that for every component W of V_s there exists a point $x \in A_s \cap W$. The number of elements $\# A_s \le d^s$. The working time of the algorithm for constructing all A_s, $0 \le s \le n$ is polynomial in d^n, d_1, d_2, M, M_1, m.

REMARK 1. The working time of the algorithm from the theorems 1, 2, 3 and 4 is essentially the same as by solving system of polynomial equations with a finite set of solutions in the projective space. So it can be formulated also in the case when l is not fixed, see [6]

1 Computation of the degree of algebraic varieties and its smooth points

We need the following lemma.

LEMMA 1. Let V_s, $0 \le s \le n$ be the variety from the statement of Theorem 1 and $L_0, L_{s+1}, L_{s+2}, \ldots, L_n$ be $n - s + 1$ linear forms from $\overline{k}[X_0, \ldots, X_n]$ such that

$$V_s \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. Denote by

$$p : V_s \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+1} : \ldots : L_n)$$

which is a finite morphism [9]. Then

(i) there exists an open in the Zariski topology subset U of $\mathbb{P}^{n-s}(\overline{k})$ such that for every $x \in U$ the cardinality $\#p^{-1}(x) = \deg V_s$,

(ii) if for some point $x \in \mathbb{P}^{n-s}(\overline{k})$ the cardinality $\#p^{-1}(x) = \deg V_s$ then for every $y \in p^{-1}(x)$ the point y is a smooth point of the variety V_s and the differential of p in the point y

$$d_y p \,:\, T_{y,V_s} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

is the isomorphism of tangent spaces T_{y,V_s} and $T_{x,\mathbb{P}^{n-s}}$ of the varieties V_s and $\mathbb{P}^{n-s}(\overline{k})$ in the points y and x respectively.

PROOF. We can suppose without loss of generality that $V_s = W$ is irreducible over $\overline{k}$. Let $Y \in \overline{k}[X_0, \dots, X_n]$ be a linear form. Consider the morphism

$$p_1 \,:\, W \longrightarrow \mathbb{P}^{n-s+1}(\overline{k}),\ (X_0 \,:\, \dots \,:\, X_n) \mapsto (Y \,:\, L_0 \,:\, L_{s+1} \,:\, L_n).$$

Since p is finite morphism $p_1(W)$ is a closed subset in $\mathbb{P}^{n-s+1}(\overline{k})$ and $p_1(W) = \{G = 0\}$ where $G \in k[Y, L_0, L_{s+1}, \dots, L_n]$ is a separable homogeneous polynomial with leading coefficient $\mathrm{lc}_Y G = 1$.

By the theorem about the primitive element for fields there exists a linear form $Y \in \overline{k}[X_0, \dots, X_n]$ such that that the morphism

$$p_1 \,:\, W \longrightarrow \mathbb{P}^{n-s+1}(\overline{k}),\ (X_0 \,:\, \dots \,:\, X_n) \mapsto (Y \,:\, L_0 \,:\, L_{s+1} \,:\, L_n)$$

induces the birational isomorphism $W \longrightarrow p_1(W)$ which we shall denote p_2. So there exists an open subset $U_1 \subset W$ such that $p_2(U_1)$ is open in $p_1(W)$ and p_2 induces the isomorphism $U_1 \longrightarrow p_2(U_1)$.

There exists a projection $p_3 \,:\, p_1(W) \longrightarrow \mathbb{P}^{n-s}(\overline{k})$ such that $p = p_3 \circ p_2$. Denote $R = \mathrm{Res}_Y(G, G'_Y)$ the discriminant of the polynomial G relatively to Y. Then $0 \neq R$ is a homogeneous polynomial since G is a separable homogeneous polynomial with leading coefficient $\mathrm{lc}_Y G = 1$. If $R(x) \neq 0$ then the cardinality $\#p_3^{-1}(x) = \deg_Y G$, for every $y \in p_3^{-1}(x)$ the point y is a smooth point of the variety $p_1(W)$ and the differential of p_3 in the point y

$$d_y p_3 \,:\, T_{y,p_1(W)} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

is the isomorphism of tangent spaces $T_{y,p_1(W)}$ and $T_{x,\mathbb{P}^{n-s}}$ of the varieties $p_1(W)$ and $\mathbb{P}^{n-s}(\overline{k})$ in the points y and x respectively. The last statement follows here just from the fact that $G'_Y(y) \neq 0$ since $R(x) \neq 0$.

Set $U = \{R \neq 0\} \setminus p_3(p_2(W) \setminus p_2(U_1))$. Then for every $x \in U$

(i) the cardinality $\#p^{-1}(x) = \deg G$,

(ii) for every $y \in p^{-1}(x)$ the point y is a smooth point of the variety W and the differential of p in the point y

$$d_y \,:\, T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

is the isomorphism of tangent spaces $T_{y,W}$ and $T_{x,\mathbb{P}^{n-s}}$ of the varieties W and $\mathbb{P}^{n-s}(\overline{k})$ in the points y and x respectively.

Show that $\deg G = \deg W$. Let $\varepsilon > 0$ be an infinitely small value relatively to the field k. So the map of the standard part

$$\mathrm{st} \,:\, \mathbb{P}^r(\overline{k(\varepsilon)}) \longrightarrow \mathbb{P}^r(\overline{k})$$

for every $r \geq 0$ is defined, see [5]. Denote by $\mathcal{H}_1$ the set of families H of $n-s+1$ linear forms $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ in $X_0, \ldots, X_n$ such that if one change in the formulation of Lemma 1 the forms $L_0, L_{s+1}, L_{s+2}, \ldots, L_n$ for $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ then (i) and (ii) will be satisfied for $U(H)$ and $p(H)$ corresponding to U and p. Consider $\mathcal{H}_1$ as a subset of $\mathbb{A}^{(n-s+1)(n+1)}$. Then [9] $\mathcal{H}_1$ is an open subset of $\mathbb{A}^{(n-s+1)(n+1)}$ in the Zariski topology.

Therefore, there exists a family $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ in $\mathcal{H}_1(\overline{k(\varepsilon)})$ such that all the forms $H_j - L_j$ have infinitely small coefficients. Thus, by Lemma 8 from [4] for every $x \in U \cap U(H)$ for every $y^* \in p(H)^{-1}(x)$ the element $y = \mathrm{st}\, y^* \in p^{-1}(x)$. The differential of p in the point y is the isomorphism. Therefore, by the theorem about the implicit function there exists a unique $y' \in p(H)^{-1}(x)$ such that $\mathrm{st} y' = y$. Hence, $y' = y^*$. Thus,

$$\deg W = \#p(H)^{-1}(x) = \#p^{-1}(x) = \deg_Y G$$

and, therefore, $\deg G = \deg W$ and (i) is proved.

To prove (ii) note that if $R(x) \neq 0$ and $y \in p^{-1}(x)$ then the point $p_1(y)$ is smooth, the local ring $\mathcal{O}_{p_1(y),p_1(W)}$ of the variety $p_1(W)$ in the point $p_1(y)$ is integrally closed. Therefore, the local rings

$$\mathcal{O}_{y,W} \simeq \mathcal{O}_{p_1(y),p_1(W)}$$

since $\mathcal{O}_{y,W}$ is integral over $\mathcal{O}_{p_1(y),p_1(W)}$ and has the same fraction field. Thus, p_1 is an isomorphism in the neighborhood of each point $y \in p^{-1}(x)$. So we can suppose that $p^{-1}(x) \subset U_1$ and, therefore, $x \in U$. Now (ii) follows from the fact that for each point x for which $\#p^{-1}(x) = \deg W$ there exists a linear form Y such that the corresponding p_1 is birational, $\#p_2^{-1}(x) = \deg W$ and so $R(x) \neq 0$ by the proved above. The Lemma is proved.

We shall suppose without loss of generality that

$$\deg(g_i) = \deg_{X_0,\ldots,X_n}(g_i) = d$$

for all $0 \leq i \leq m$ changing if it is necessary each polynomial g_i for the family of polynomials $\{g_i X_j^{-\deg(g_i)+d}\}_{0 \leq j \leq n}$.

Remind that in [5] for each s the algorithm of polynomial complexity is suggested which finds all the s for which $V_s \neq \emptyset$. For every s at the step s the algorithm of [5] constructs polynomials $h_1, \ldots, h_s$ and linear forms $L_{s+1}^{(s)}, \ldots, L_n^{(s)}$ in $X_0, \ldots, X_n$ with integer coefficients of the size $O(n \log d)$ such that

$$h_i = \sum_{0 \leq j \leq m} \lambda_{i,j} g_j, \ \lambda_{i,j} \in \mathbb{Z}$$

for all i, j. Besides that, the following property is fulfilled. Let

$$W_s = \{h_1 = \ldots = h_s = 0\} \subset \mathbb{P}^n(\overline{k})$$

be the variety of all common zeros of polynomials $h_1, \ldots, h_s$ in $\mathbb{P}^n(\overline{k})$, the variety W' be the union of all the components U_1 of W such that $\dim U_1 = n - s$, and W'' be the union of all the components U_1 of W such that $\dim U_1 > n - s$. Then the subset of $\mathbb{P}^n(\overline{k})$

$$W' \cap \{L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\}$$

is finite and

$$W' \cap \{L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\} \cap W'' = \emptyset .$$

The form $L_0^{(s)}$ is such that it is not equal to zero in each point of $W' \cap \{L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\}$.

We shall denote also $W' = W'_s, W'' = W''_s$ when the dependence on s will be essential.

Compute, see [3], [5], all the points $\{x_u\}_{1 \le u \le N}$ of the set $W' \cap \{L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\}$. Let $x_u = (x_{u,0} : \ldots : x_{u,n})$ where all $x_{u,i}$ are from a finite extension of k. Construct a real structure for the field $K = k(x_{u,0}, \ldots, x_{u,n})$, see [3], [5], which induces the real structure on $\overline{k}$.

Let $\varepsilon_1 > 0$ be an infinitely small value relatively to the field K and $\varepsilon_2 > 0$ an infinitely small value relatively to the field $K(\varepsilon_1)$, the field $K_1 = K(\varepsilon_1, \varepsilon_2)$.

Let $Y_0, \ldots, Y_n$ be new variables. For every $0 \le u \le N$ consider the following system of equations and inequalities with coefficients in K_1

$$\begin{cases} h_i = 0, & 1 \le i \le s \\ h_i(Y_0, \ldots, Y_n) = 0, & 1 \le i \le s \\ L_j^{(s)}(X_0 - Y_0, \ldots, X_n - Y_n) = 0, & j \in \{0, s+1, \ldots, n\} \\ \sum_{0 \le i \le n} |X_i - x_{u,i}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Y_i - x_{u,i}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Y_i - X_i|^2 \ge \varepsilon_2, & \end{cases} \qquad (1, u)$$

LEMMA 2. Let $W' = W'_s$ as above. Then $N = \deg W'$ if and only if for every $1 \le u \le N$ there exist no solutions of system $(1, u)$ in $\mathbb{A}^{2n+2}(\overline{K_1})$. If for every $1 \le u \le N$ there exist no solutions of system $(1, u)$ in $\mathbb{A}^{2n+2}(\overline{K_1})$ then all the points $\{x_u\}_{1 \le u \le N}$ of the variety W' are smooth and the differentials of the projection

$$p : W' \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0^{(s)} : L_{s+1}^{(s)} : \ldots : L_n^{(s)})$$

in points $\{x_u\}_{1 \le u \le N}$ are isomorphisms.

PROOF. Follows directly from Lemma 1 when one changes $g_0, \ldots, g_m$ for $h_1, \ldots, h_s$ and therefore V_s for W'_s, c.f. also the proof of lemmas 14, 15 of [5].

Return to the description of the algorithm. Our aim now is to compute $\deg W'$. Construct a solution of some system $(1, u)$ or ascertain that for every $1 \le u \le N$

there exists no solutions of system $(1, u)$ in $\mathbb{A}^{2n+2}(\overline{K_1})$. In the last case by Lemma 2 the degree $\deg W' = N$ is already computed. Suppose that there exists a solution

$$(x'_0, \ldots, x'_n, y'_0, \ldots, y'_n) \in \mathbb{A}^{2n+2}(\overline{K_1})$$

of some system $(1, u_0)$. Denote $x' = (x'_0 : \ldots : x'_n)$ and $y' = (y'_0 : \ldots : y'_n)$, so $x', y' \in \mathbb{P}^n(\overline{K_1})$. Set

$$L'_i = L_i^{(s)} - (L_i^{(s)}/L_0^{(s)})(x')L_0^{(s)},\ s+1 \le i \le n,\ L'_0 = L_0^{(s)}.$$

Compute all the points from the set $W' \cap \{L'_{s+1} = \ldots = L'_n = 0\}$ in $\mathbb{P}^n(\overline{K_1}$. Denote $N' = \#W' \cap \{L'_{s+1} = \ldots = L'_n = 0\}$. By Lemma 8 from [4] for every $x^* \in W' \cap \{L'_{s+1} = \ldots = L'_n = 0\}$ there exists $1 \le u \le n$ such that $\mathrm{st}\, x^* = x_u$. So $N' \ge N$. Further, $x', y' \in W' \cap \{L'_{s+1} = \ldots = L'_n = 0\}$, $x' \ne y'$ and $\mathrm{st}\, x' = \mathrm{st}\, y'$. Therefore, $N' \ge N + 1 > N$.

Now apply the second auxiliary algorithm from [5] to $L'_0, L'_{s+1}, \ldots, L'_n$ and construct linear forms $M_0, M_{s+1}, \ldots, M_n$ with coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$ such that

$$\#W' \cap \{M_{s+1} = \ldots = M_n = 0\} \ge N',$$

$$W' \cap \{M_{s+1} = \ldots = M_n = 0\} \cap W'' = \emptyset \text{ and } M_0 = L'_0.$$

After that, return recursively to the beginning of the algorithm described changing the forms $L_0^{(s)}, L_{s+1}^{(s)}, \ldots, L_n^{(s)}$ for $M_0, M_{s+1}, \ldots, M_n$. Since $N' > N$ there are at most d^s such returns in the algorithm.

Thus, we shall compute in the required time $\deg W'$ and we can suppose without loss of generality by Lemma 2 that $N = \deg W'$, all the points x_u, $1 \le u \le N$ are smooth on the variety W' and the differentials of the projection p, see Lemma 2, in the points x_u, $1 \le u \le N$ are isomorphisms.

Show how to choose among the points x_u, $1 \le u \le N$ the points from V_s. Let $1 \le u \le N$. Consider the following system of equations and an inequality with coefficients from $\overline{k(\varepsilon_1)}$

$$h_1 = \ldots = h_s = 0,\ h_{s+1} \ne 0,\ \sum_{0 \le i \le n} |X_i - x_{u,i}|^2 < \varepsilon_1. \qquad (2, u)$$

LEMMA 3. The point $x_u = (x_{u,0} : \ldots : x_{u,n}) \in V_s$ if and only if system $(2, u)$ has no solutions in $\mathbb{A}^{n+1}(\overline{k(\varepsilon_1)})$.

PROOF. It follows directly from the fact that the point x_u is smooth and from the definition of polynomials $h_1, \ldots, h_{s+1}$, see above (and also [5]). The lemma is proved.

Now construct, c.f. [3], [5], solving systems $(2, u)$ the subset $A \subset \{1, \ldots, n\}$ of all indices u such that system $(2, u)$ has no solutions in $\mathbb{A}^{n+1}(\overline{k(\varepsilon_1)})$.

By Lemmas 1, 2 and 3 we have $\#A = \deg V_s$, the set $V_s \cap \{L_{s+1}^{(s)} = \ldots = L_n^{(s)} = 0\} = \{x_u : u \in A\}$ and the differentials of the projection p, see Lemma 2, in the points x_u, $u \in A$ are isomorphisms.

Thus, the degree $\deg V_s$ and the set of smooth points $\{x_u : u \in A\} \subset V_s$ can be computed for every s. Theorem 1 is proved.

To proves Theorem 4 it is sufficient now to construct the tangent spaces of V_s in the points from $\{x_u : u \in A\}$.

LEMMA 4. Let $\phi = (\phi_1, \ldots, \phi_r) : V' \longrightarrow \overline{k}^r$, $r \geq 0$, be a morphism of algebraic varieties which $\phi_1, \ldots, \phi_r$ is given by the coordinate its functions $\phi_1, \ldots, \phi_r$ in $\overline{k}^r$, let the point $y \in V'$ be smooth and the differential

$$d_y\phi : T_{y,V'} \longrightarrow T_{\phi(y),\overline{k}^r}$$

of ϕ in the point y be the isomorphism of the tangent space $T_{y,V'}$ of V' in the point y and $T_{\phi(y),\overline{k}^r}$ of $\overline{k}^r$ in $\phi(y)$. Denote

$$C_j = \{(z_1, \ldots, z_r) \in \overline{k}^r : z_m - \phi_m(y) = 0,\ 1 \leq m \leq r,\ m \neq j\}$$

for every $1 \leq j \leq r$. Then $D_j = \phi^{-1}(C_j) = \{x \in V' : \phi_m(x) - \phi_m(y) = 0,\ 0 \leq m \leq r,\ m \neq j\}$ is a curve in some neighborhood of y, the point y is smooth on D_j, so the tangent space T_{y,D_j} of D_j in the point y is the subset $T_{y,D_j} \subset T_{y,V'}$. Finally, we have $\sum_{1 \leq j \leq r} T_{y,D_j} = T_{y,V'}$.

PROOF. In the case when one changes $\overline{k}$ for $\mathbb{C}$ the statements of the lemma follow directly from the theorem about the implicit function. In the considered case it is sufficient to apply the transfer principle for the field supplied with a real structure, c.f. [3], see [1]. The lemma is proved.

Now set $V' = p^{-1}(\{L_0^{(s)} \neq 0\}) \subset W'$ where p is the projection from Lemma 2 and $y = x_u$ for some $u \in A$. So $\{L_0 \neq 0\} \simeq \overline{k}^{n-s}$. Set $\phi = p|_{V'}$. Apply Lemma 4. We have

$$D_j = \{h_1 = \ldots = h_s = 0 \;\&\; L_{s+m}^{(s)} - (L_{s+m}^{(s)}/L_0^{(s)})(x_u)L_0^{(s)} = 0,\ 1 \leq m \leq n-s,\ m \neq j\}$$

for $1 \leq j \leq n-s$ in some neighborhood of x_u.

Thus, construct general points of curves D_j and Newton–Puiseux expansions of coordinate functions of general points of D_j in uniformizing elements in some neighborhood of x_u, c.f. [3] section 3, paragraphs (<u>11</u>), (<u>12</u>), (<u>13</u>) and also [5], section 1, paragraph (<u>16</u>). Now one can easily construct the tangent space T_{x_u,D_j} of D_j in the point x_u. Hence, by Lemma 4 all the tangent spaces $T_{x_u V_s}$, $u \in A$, can be constructed in the required time. Theorem 4 is proved.

2 Computation of dimensions of components containing the point and the multiplicity of a point

Now we are going to prove Theorem 2. This theorem follows immediately from the following lemma.

LEMMA 5. Let $x \in W' = W'_s$, see Section 1. Then one can decide whether $x \in V_s$ within the time polynomial in d^n, d_1, d_2, M, M_1, m and the size of the point x.

PROOF. Construct the set $\{x_u : u \in A\}$ of smooth points of V_s such that

$$\{x_u : u \in A\} = V_s \cap \{L^{(s)}_{s+1} = \ldots = L^{(s)}_n = 0\}$$

, see Section 1. Construct a linear subspace L of $\mathbb{P}^n(\overline{k})$ of dimension $s+1$ containing the point x and the linear subspace $\{L^{(s)}_{s+1} = \ldots = L^{(s)}_n = 0\}$ of dimension s. So the linear subspace $L = \{L_{s+2} = \ldots = L_n = 0\}$ where the linear forms L_i, $s+2 \le i \le n$, in $L^{(s)}_{s+1}, \ldots, L^{(s)}_n$ are constructed.

The intersection $L \cap V_s$ is a curve C_s. Each irreducible component of C_s is an irreducible component of the variety of solutions of the system

$$h_1 = \ldots = h_s = L_{s+2} = \ldots = L_n = 0. \tag{3}$$

The points $\{x_u : u \in A\}$ are smooth on the variety of solutions of (3) by the construction of Section 1 and $C_s \supset \{x_u : u \in A\}$. So applying the algorithm from [6], c.f. also [3],[5], construct in the required time the systems of equations which gives one–dimensional irreducible components of the variety of solutions of (3), then substituting in them the coordinates of the points from $\{x_u : u \in A\}$ choose among these irreducible components those which are components of C_s. Finally, substituting in the systems of equations which gives irreducible components of C_s the coordinates of the point x decide whether $x \in C_s$, i.e. whether $x \in V_s$. The lemma is proved.

Theorem 2 is proved. Now we are going to prove Theorem 3.

Denote by $\mathrm{con}(x, V_s)$ the tangent cone of the variety V_s in the point x. It consists by definition of the lines containing x which are limits of secants of V_s containing x when another point of the intersection of the secant with V_s tends to x. Strictly speaking this definition is valid for the case when the ground field is $\mathbb{C}$. Another definition of $\mathrm{con}(x, V_s)$ is valid for arbitrary fields. The cone is defined as the variety of zeros of the ideal generated by the forms of the lowest degree of the elements of the ideal of the initial variety in the case when it is affine and the point x has coordinates equal to zero, see just below. Factually, if one use the second definition in many cases one can give the sense to the first one.

We can effect a linear automorphism of $\mathbb{P}^n(\overline{k})$ and suppose without loss of generality (may be changing the ground field k) that $x = (1 : 0 : \ldots : 0)$. We have the following definition of the cone $\mathrm{con}(x, V)$. Identify $\mathbb{A}^n(\overline{k})$ with $\{X_0 \neq 0\} \subset \mathbb{P}^n(\overline{k})$. Let $X_1, \ldots, X_n$ be the coordinate functions in $\mathbb{A}^n(\overline{k})$ corresponding to $X_1/X_0, \ldots, X_n/X_0$ in $\mathbb{P}^n(\overline{k})$. Denote $U_s = V_s \cap \{X_0 \neq 0\} \subset \mathbb{A}^n(\overline{k})$. Let $I(U_s) \subset k[X_1, \ldots, X_n]$ be the ideal of the affine variety U_s. Each element of $F \in k[X_1, \ldots, X_n]$ is represented as a sum $F = F_r + F_{r+1} + \ldots + F_m$ of homogeneous polynomials F_j in $X_1, \ldots, X_n$. So for each element of $F \in k[X_1, \ldots, X_n]$ the form of the lowest degree F_r is defined. Denote by $I'(U_s)$ (respectively $I'(V_s)$)

the ideal generated by the forms of the lowest degree of the elements of $I(U_s)$. Then $\mathrm{con}(x, V) \cap \{X_0 \neq 0\}$ (respectively $\mathrm{con}(x, V)$) is set of zeros of the ideal $I'(U_s)$ (respectively $I'(V_s)$). About the equivalence of the definition with secants, this one and other definitions of the tangent cone see [10], [15].

Note that in the case of a field of zero–characteristic with a real structure the equivalence of the definition with secants and the second given here can be proved by applying the transfer principal [1] if this equivalence is known in the classical case. It is essential here that the fact that the point y belongs to the variety of zeros of the ideal $I'(V_s)$ can be expressed in the language of the first order theory of real fields, since one can bound the degrees of generators of $I'(V_s)$ by a function in d and n.

Let $\varepsilon > 0$ be an infinitely small value relatively to the field k. So the map of the standard part

$$\mathrm{st} : \mathbb{P}^r(\overline{k(\varepsilon)}) \longrightarrow \mathbb{P}^r(\overline{k})$$

for every $r \geq 0$ is defined, see [5]. Let $h_1, \ldots, h_n$ be as in Section 1. Consider the following system of equations and an inequality with coefficients from $\overline{k(\varepsilon)}$

$$h_1 - \varepsilon X_1^d = \ldots = h_n - \varepsilon X_n^d = 0. \tag{4}$$

Denote by V'_ε the variety of solutions of system (4) in $\mathbb{P}^n(\overline{k(\varepsilon)})$. Each irreducible component of V'_ε has the dimension $n - s$. Set $V' = \mathrm{st}(V'_\varepsilon)$. Then, c.f. [6], V' is an algebraic variety in $\mathbb{P}^n(\overline{k})$ and each irreducible component of V' has the dimension $n - s$. Besides that each component of V_s is a component of V', see [6]. Set $U'_\varepsilon = V'_\varepsilon \cap \{X_0 \neq 0\}$ and $U' = V' \cap \{X_0 \neq 0\}$. These are affine varieties.

Construct using the algorithm from [3] the family $L_0, L_{s+1}, L_{s+2}, \ldots, L_n$ of linear forms with integer coefficients of the size $O(n \log d)$ such that

$$V'_\varepsilon \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\} = \emptyset \tag{5}$$

in $\mathbb{P}^n(\overline{k(\varepsilon)})$ and L_0 is not vanishing in each point of $V'_\varepsilon \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\}$. Condition (5) is equivalent, c.f. [6], to $V' \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{k})$. We shall suppose without loss of generality that $L_{s+1}(x) = L_{s+2}(x) = \ldots = L_n(x) = 0$ changing if it is necessary each L_i for $L_i - (L_i/L_0)(x)L_0$, $s + 1 \leq i \leq n$. So $L_{s+1}, L_{s+2}, \ldots, L_n$ are linear forms in $X_1, \ldots, X_n$.

Our aim now is to construct a family of linear forms $M_0, M_{s+1}, M_{s+2}, \ldots, M_n$ such that $M_0 = L_0$, the forms $M_{s+1}, M_{s+2}, \ldots, M_n \in k[X_1, \ldots, X_n]$ have the coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$,

$$V' \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$ and

$$\mathrm{con}(x, V') \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$.

We need the following definition. Let an algebraic curve $C \subset \mathbb{A}^n(\overline{k})$ and its branch C^* in the point $(0,\dots,0)$ with a uniformizing element τ be given. So we have the decompositions of coordinate functions of the branch C^* in formal power series

$$x_i = \gamma_{i,m}\tau^m + \sum_{m<j\in\mathbb{Z}} \gamma_{i,j}\tau^j,\ 1 \le i \le n,$$

where $\gamma_{i,j} \in \overline{k}$ for all $1 \le i \le n, m \le j \in \mathbb{Z}$ and $(\gamma_{1,m},\dots,\gamma_{n,m}) \ne (0,\dots,0)$. Then the tangent line l to this branch is defined by the formula

$$l = \{(\gamma_{1,m},\dots,\gamma_{n,m})t\ :\ t \in \overline{k}\}.$$

As in Section 1 construct a real structure for the field k, see [3], [5], which induces the real structure on $\overline{k}$. Let

$\varepsilon_0 > 0$ be an infinitely small value relatively to the field k,

$\varepsilon_1 > 0$ an infinitely small value relatively to the field $k(\varepsilon_0)$,

$\varepsilon_2 > 0$ an infinitely small value relatively to the field $k(\varepsilon_0, \varepsilon_1)$,

the field $K_2 = k(\varepsilon_0, \varepsilon_1, \varepsilon_2)$.

Denote $L = \{L_{s+1} = L_{s+2} = \dots = L_n = 0\} \subset \mathbb{A}^n(\overline{k})$ where $\mathbb{A}^n$ has the coordinate functions $X_1,\dots,X_n$. Consider the following system of equations and inequalities with coefficients from the field K_2 in $X_1\dots,X_n,Y_1\dots,Y_n$

$$\begin{cases} h_i(1,X_1\dots,X_n) - \varepsilon_2 X_i^d = 0, & 1 \le i \le s \\ \sum_{1\le i\le n} |X_i|^2 = \varepsilon_1^2, & \\ L_j(Y_1,\dots,Y_n) = 0, & s+1 \le j \le n, \\ \sum_{1\le i\le n} |X_i - Y_i|^2 < \varepsilon_0\varepsilon_1^2. & \end{cases} \qquad (6)$$

LEMMA 6. Let the family $L_0, L_{s+1}, L_{s+2}, \dots, L_n$ of linear forms be as above. The following conditions are equivalent

(i) $\mathrm{con}(x, V') \cap \{L_0 = L_{s+1} = L_{s+2} = \dots = L_n = 0\} = \emptyset$ in $\mathbb{P}^n(\overline{k})$

(ii) $\mathrm{con}(x, U') \cap \{L_{s+1} = L_{s+2} = \dots = L_n = 0\} = \{x\}$ in $\mathbb{A}^n(\overline{k})$

(iii) system (6) has no solutions in $\mathbb{A}^{2n}(\overline{K_2})$.

PROOF. The equivalence of (i) and (ii) is straightforward.

Let $0 \le i \le 2$. If $z \in \overline{k(\varepsilon_0,\dots,\varepsilon_i)}$ is not infinitely great relatively to the field $\overline{k(\varepsilon_0,\dots,\varepsilon_{i-1})}$ the the standard part $\mathrm{st}_{\varepsilon_i}(z) \in \overline{k(\varepsilon_0,\dots,\varepsilon_{i-1})}$ is defined, see [5], If $z = (z_1,\dots z_n) \in \mathbb{A}^n(\overline{k(\varepsilon_0,\dots,\varepsilon_i)})$ and all the standard parts $\mathrm{st}_{\varepsilon_i}(z_j)$, $1 \le j \le n$ are defined then set

$$\mathrm{st}_{\varepsilon_i}(z) = (\mathrm{st}_{\varepsilon_i}(z_1),\dots,\mathrm{st}_{\varepsilon_i}(z_n)) \in \mathbb{A}^n(\overline{k(\varepsilon_0,\dots,\varepsilon_{i-1})}).$$

Besides that, the maps of the standard part

$$\mathrm{st}_{\varepsilon_i} : \mathbb{P}^n(\overline{k(\varepsilon_0, \ldots, \varepsilon_i)}) \longrightarrow \mathbb{P}^n(\overline{k(\varepsilon_0, \ldots, \varepsilon_{i-1})})$$

are defined, see [5], for $i = 0, 1, 2$. The restrictions of these maps to $\mathbb{A}^n = \{X_0 \neq 0\}$ coincide with the standard part of the elements of $\mathbb{A}^n$ as above when the latter is defined.

Suppose that there exists a solution $(x_1^*, \ldots, x_n^*, y_1^*, \ldots, y_n^*) \in \mathbb{A}^{2n}(\overline{K_2})$ of system (6). Denote $x^* = (x_1^*, \ldots, x_n^*)$ and $y^* = (y_1^*, \ldots, y_n^*)$. Then one can see immediately that the line (the standard parts here are considered in $\mathbb{A}^n$)

$$l = \{\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1}(\mathrm{st}_{\varepsilon_2} y^*/\varepsilon_1)t \, : \, t \in \overline{k}\} \subset \mathrm{con}(x, U') \cap \{L_{s+1} = \ldots, L_n = 0\},$$

since l is in the set of zeros of the corresponding ideal of the forms of the lowest degree.

Conversely, suppose that there exists a line $l \subset \mathrm{con}(x, U') \cap \{L_{s+1} = L_{s+2} = \ldots = L_n = 0\}$, $x \in l$. Let $l = \{L_2 = \ldots = L_n = 0\}$ where $L_2, \ldots, L_s$ are linear forms in $X_1, \ldots, X_n$. Hence,

$$l \subset \mathrm{con}(x, U' \cap \{L_2 = \ldots = L_s = 0\})$$

by the definition of the cone as the ideal of forms of the lowest degree. But $U' \cap \{L_2 = \ldots = L_s = 0\}$ is a curve. One can see that l is a tangent to some branch of this curve. If one takes τ as a uniformizing element of this branch in the point x one can easily get the existence of a solution of (6) considering the coordinate functions of this branch as functions in τ. The lemma is proved. Factually, one can also prove this lemma applying the transfer principle.

Suppose that system (6) has a solution x^*. Construct such a solution, see [3], [5], Let the line

$$l = \{\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1}(\mathrm{st}_{\varepsilon_2} x^*/\varepsilon_1)t \, : \, t \in \overline{k}\} \subset \mathrm{con}(x, U')$$

and $l = \{L_2 = \ldots = L_n = 0\}$ in the denotations of the proof of Lemma 6. Construct linear forms $L_2, \ldots, L_s$ and also L_1 in $X_1, \ldots, X_n$ such that $L_1, \ldots, L_n$ are linearly independent over $\overline{k}$, see [3], [5],. Denote $L' = \{L_1 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\}$. This is a linear subspace such that $L' + l = L$.

Let the line

$$l' = \{x^* t \, : \, t \in \overline{K_2}\} \subset \mathrm{con}(x, U').$$

Construct the linear subspace $L' + l'$. Then the subspace $L' + l'$ is infinitely close to $L' + l$ since x^* is a solution of (6). Construct linear forms $L'_{s+1}, \ldots, L'_n \in \overline{K_2}[X_1, \ldots, X_n]$ such that $L' + l' = \{L'_{s+1} = \ldots = L'_n = 0\}$ in $\mathbb{A}^n(\overline{K_2})$. Set also $L'_0 = L_0$.

Since $L' + l'$ is infinitely close to $L' + l$ we can suppose without loss of generality (may be changing equations of $L' + l'$ and $L' + l$) that the linear forms $L'_i - L_i$,

$s+1 \le i \le n$ have infinitely small coefficients relatively to the field $\overline{k}$. So by Lemma 8 from [4] we have

$$\#V' \cap \{L_{s+1} = L_{s+2} = \ldots = L_n = 0\} \le \#V' \cap \{L'_{s+1} = L'_{s+2} = \ldots = L'_n = 0\}.$$

Further, there exist two points $x, x^* \in V' \cap \{L'_{s+1} = L'_{s+2} = \ldots = L'_n = 0\}$ such that their standard parts in $\mathbb{P}^n(\overline{k})$ are equal to x. Therefore, $N =$ $\#V' \cap \{L_{s+1} = L_{s+2} = \ldots = L_n = 0\} < \#V' \cap \{L'_{s+1} = L'_{s+2} = \ldots = L'_n = 0\} =$ N'.

Set $M_0 = L_0$. Now apply the analog of the second auxiliary algorithm from [5] to the linear forms $L'_0, L'_{s+1}, \ldots, L'_n$ and construct linear forms $M_{s+1}, \ldots, M_n$ in $X_1, \ldots, X_n$ with coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$ such that $\#V' \cap \{M_{s+1} = \ldots = M_n = 0\} \ge N'$ and $V' \cap \{M_0 = M_{s+1} = \ldots = M_n = 0\} = \emptyset$. After that, return recursively to the beginning of the algorithm described changing the forms $L_0, L_{s+1}, \ldots, L_n$ for $M_0, M_{s+1}, \ldots, M_n$. Since $N' > N$ there are at most d^s such returns in the algorithm.

So we shall obtain finally by Lemma 6 a family of linear forms M_0, M_{s+1}, $M_{s+2}, \ldots, M_n$ such that $M_0 = L_0$, the forms $M_{s+1}, M_{s+2}, \ldots, M_n \in k[X_1, \ldots, X_n]$ with coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$,

$$V' \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$ and

$$\mathrm{con}(x, V') \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. We shall suppose changing as described above the forms $L_0, L_{s+1}, \ldots, L_n$ for $M_0, M_{s+1}, \ldots, M_n$ that these properties are satisfied for $L_0, L_{s+1}, \ldots, L_n$, i.e. the forms $L_{s+1}, L_{s+2}, \ldots, L_n \in k[X_1, \ldots, X_n]$ have the coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$,

$$V' \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$ and

$$\mathrm{con}(x, V') \cap \{L_0 = L_{s+1} = L_{s+2} = \ldots = L_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$.

Our aim now is to construct a family of linear forms $M_0, M_{s+1}, M_{s+2}, \ldots, M_n$ such that $M_0 = L_0$, the forms $M_{s+1}, M_{s+2}, \ldots, M_n \in k[X_1, \ldots, X_n]$ have the coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$,

$$V' \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$,

$$\mathrm{con}(x, V') \cap \{M_0 = M_{s+1} = M_{s+2} = \ldots = M_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$ and all the points from $V' \cap \{M_{s+1} = M_{s+2} = \ldots = M_n = 0\} \setminus \{x\}$ are smooth points of the variety V'.

Construct, c.f. [5], all the points of the set $V'_\varepsilon \cap \{L_{s+1} = L_{s+2} = \ldots = L_n = 0\}$ and then taking their standard parts all points x_u, $1 \le u \le N$ from the set $V' \cap \{L_{s+1} = L_{s+2} = \ldots = L_n = 0\}$ in $\mathbb{P}^n(\overline{k})$. We can suppose without loss of generality that $x_1 = x$. Construct a linear form L'_0 in $X_1, \ldots, X_n$ with coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$ such that $L'_0(x_u) \neq 0$ for all $2 \le j \le N$.

Consider the projection

$$p\,:\,V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L'_0 : L_{s+1} : \ldots : L_n).$$

Show that for every irreducible component W of V' such that there exists $u \ge 2$ for which $x_u \in W$ the morphism $p_1 = p|_{W \setminus \{x\}}$ is dominant.

Indeed, we should show that for every such component W of V' the closure F in the Zariski topology of the image $p(W \setminus \{x\})$ coincides with $\mathbb{P}^{n-s}(\overline{k})$. For every $\lambda_{s+1}, \ldots, \lambda_n \in \overline{k(\varepsilon)}$ which are infinitely small relatively to the field k by Lemma 8 from [4] the set $W \cap \{L_{s+1} - \lambda_{s+1} L'_0 = \ldots = L_n - \lambda_n L'_0 = 0\} \setminus \{x\} \neq \emptyset$ in $\mathbb{P}^{n-s}(\overline{k(\varepsilon)})$. Therefore, $p^{-1}(1 : \lambda_{s+1} : \ldots : \lambda_n)$ is not empty in $\mathbb{P}^{n-s}(\overline{k(\varepsilon)})$. Therefore,

$$F(\overline{k(\varepsilon)}) = \mathbb{P}^{n-s}(\overline{k(\varepsilon)}),$$

and hence, $F = \mathbb{P}^{n-s}(\overline{k})$.

We have the following analog of Lemma 1.

LEMMA 7. Let the variety V', its component W, $x_u \in W$, $u \ge 2$, the linear forms $L'_0, L_{s+1}, L_{s+2}, \ldots, L_n$ and the projection $p_1\,:\,W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k})$ be as above.

(i) there exists an open in the Zariski topology subset U of $\mathbb{P}^{n-s}(\overline{k})$ such that for every $x^* \in U$ the cardinality $\# p_1^{-1}(x^*) = \delta > 0$

(ii) if for some point $x^* \in \mathbb{P}^{n-s}(\overline{k})$ the cardinality $\# p_1^{-1}(x^*) = \delta$ then for every $y \in p_1^{-1}(x^*)$ the point y is a smooth point of the variety W and the differential of p in the point y

$$d_y p\,:\,T_{y,W} \longrightarrow T_{x,\mathbb{P}^{n-s}}$$

is the isomorphism of tangent spaces $T_{y,W}$ and $T_{x^*,\mathbb{P}^{n-s}}$ of the varieties W and $\mathbb{P}^{n-s}(\overline{k})$ in the points y and x^* respectively.

PROOF. The proof is similar to the proof of Lemma 1. The lemma is proved.

Let $x_u = (x_{u,0} : \ldots : x_{u,n})$ where all $x_{u,i}$ are from a finite extension of k. Construct a real structure for the field $K = k(x_{u,0}, \ldots, x_{u,n})$, see [3], [5], which induces the real structure on $\overline{k}$.

Let $\varepsilon_1 > 0$ be an infinitely small value relatively to the field K and $\varepsilon_2 > 0$ an infinitely small value relatively to the field $K(\varepsilon_1)$, the field $K_1 = K(\varepsilon_1, \varepsilon_2)$.

Let $Y_0, \dots, Y_n$ be new variables. For every $0 \le u \le N$ consider the following system of equations and inequalities with coefficients in K_1

$$\begin{cases} h_i = 0, & 1 \le i \le s \\ h_i(Y_0, \dots, Y_n) = 0, & 1 \le i \le s \\ L_j(X_0 - Y_0, \dots, X_n - Y_n) = 0, & s+1 \le j \le n \\ L'_0(X_0 - Y_0, \dots, X_n - Y_n) = 0, & \\ \sum_{0 \le i \le n} |X_i - x_{u,i}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Y_i - x_{u,i}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Y_i - X_i|^2 \ge \varepsilon_2, & \end{cases} \qquad (7, u)$$

We have the following analog of Lemma 2

LEMMA 8. Let V' and the projection $p : V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k})$ be as above. If for every $2 \le u \le N$ there exist no solutions of system $(7, u)$ in $\mathbb{A}^{2n+2}(\overline{K_1})$ then all the points $\{x_u\}_{2 \le u \le N}$ of the variety V' are smooth and the differentials of the projection p in points $\{x_u\}_{1 \le u \le N}$ are isomorphisms.

PROOF. Follows directly from Lemma 7 and Lemma 8 from [4], c.f. also the proof of lemmas 14, 15 of [5].

Return to the description of the algorithm. Construct a solution of some system $(7, u)$ or ascertain that for every $2 \le u \le N$ there exists no solutions of system $(7, u)$ in $\mathbb{A}^{2n+2}(\overline{K_1})$. In the last case by Lemma 8 all the points $\{x_u\}_{2 \le u \le N}$ of the variety V' are smooth and the differentials of the projection p in points $\{x_u\}_{1 \le u \le N}$ are isomorphisms.

Suppose that there exists a solution

$$(x'_0, \dots, x'_n, y'_0, \dots, y'_n) \in \mathbb{A}^{2n+2}(\overline{K_1})$$

of some system $(1, u_0)$. Denote $x' = (x'_0 : \dots : x'_n)$ and $y' = (y'_0 : \dots : y'_n)$, so $x', y' \in \mathbb{P}^n(\overline{K_1})$. Set

$$L'_i = L_i - (L_i/L'_0)(x')L'_0, \; s+1 \le i \le n.$$

Compute all the points from the set $V' \cap \{L'_{s+1} = \dots = L'_n = 0\}$ in $\mathbb{P}^n(\overline{K_1})$. Denote $N' = \#V' \cap \{L'_{s+1} = \dots = L'_n = 0\}$. By Lemma 8 from [4] for every $x^* \in V' \cap \{L'_{s+1} = \dots = L'_n = 0\}$ there exists $1 \le u \le N$ such that $\operatorname{st} x^* = x_u$. So $N' \ge N$. Further, $x', y' \in V' \cap \{L'_{s+1} = \dots = L'_n = 0\}$, $x' \ne y'$ and $\operatorname{st} x' = \operatorname{st} y'$. Therefore, $N' \ge N + 1 > N$.

Apply the second auxiliary algorithm from [5] to the linear forms $L'_{s+1}, \dots, L'_n$ and construct linear forms $M_{s+1}, \dots, M_n$ in $X_1, \dots, X_n$ with coefficients from $\mathbb{Z}$ of the length $\mathcal{O}(n \log d)$ such that

$\#V' \cap \{M_{s+1} = \dots = M_n = 0\} \ge N' > N$,

$V' \cap \{L_0 = M_{s+1} = \dots = M_n = 0\} = \emptyset$ and set also $M_0 = L_0$

in $\mathbb{P}^n(\overline{k})$.

After that, return recursively to the beginning of the algorithm described changing the forms $L_0, L_{s+1}, \dots, L_n$ for $L_0, M_{s+1}, \dots, M_n$. Since $N' > N$ there are at most d^s such returns in the algorithm.

Thus, effecting this recursive construction till the end we can suppose without loss of generality by Lemma 8 that all the points x_u, $2 \le u \le N$ are smooth on the variety V' and the differentials of the projection p, see Lemma 8, in the points x_u, $2 \le u \le N$ are isomorphisms. That is we can construct the required $M_j = L_j$, $j = 0, s+1, s+2, \dots, n$.

Now construct applying Lemma 5 the subset of indices $A \subset \{2, \dots, N\}$ such that

$$\{x_u \,:\, u \in A\} = V_s \cap \{L_{s+1} = \ldots = L_n = 0\} \tag{8}$$

in $\mathbb{P}^n(\overline{k})$.

LEMMA 9. Let W be an irreducible component of V' and linear forms $L_0, L^{(i)}_{s+1}, \dots, L^{(i)}_n$, $i = 0, 1$ be such that for $i = 0, 1$ it is hold $L^{(i)}_{s+1}, \dots, L^{(i)}_n \in \overline{k}[X_1, \dots, X_n]$,

$$W \cap \{L_0 = L^{(i)}_{s+1} = \ldots = L^{(i)}_n = 0\} = \emptyset,$$

$$\mathrm{con}(x, W) \cap \{L_0 = L^{(i)}_{s+1} = \ldots = L^{(i)}_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. Further, let for $i = 0, 1$ all the points of $W \cap \{L^{(i)}_{s+1} = \ldots = L^{(i)}_n = 0\} \setminus \{x\}$ be smooth and the differentials of the projection

$$p^{(i)} \,:\, W \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : L^{(i)}_{s+1} : \ldots : L^{(i)}_n).$$

are isomorphisms in all the point from $W \cap \{L^{(i)}_{s+1} = \ldots = L^{(i)}_n = 0\} \setminus \{x\}$. Then

$$\# W \cap \{L^{(0)}_{s+1} = \ldots = L^{(0)}_n = 0\} = \# W \cap \{L^{(1)}_{s+1} = \ldots = L^{(1)}_n = 0\}.$$

PROOF. Suppose contrary, that

$$\# W \cap \{L^{(0)}_{s+1} = \ldots = L^{(0)}_n = 0\} < \# W \cap \{L^{(1)}_{s+1} = \ldots = L^{(1)}_n = 0\}.$$

Let $L^{(i)}_j = \sum_{1 \le r \le n} l^{(i)}_{j,r} X_r$ where $l^{(i)}_{j,r} \in \overline{k}$ for all i, j, r.

Consider the product of projective spaces $\mathbb{P}^n \times \mathbb{P}^1$ with the coordinates $((X_0 : \ldots : X_n), (Z'_0 : Z'_1))$. Let

$$\tilde{L} = \{Z'_0 L^{(0)}_j + Z'_1 L^{(1)}_j = 0,\ s+1 \le j \le n\}$$

be the variety in $(\mathbb{P}^n \times \mathbb{P}^1)(\overline{k})$. Define $\tilde{C}$ as the union of components of $\tilde{L} \cap (W \times \mathbb{P}^1(\overline{k}))$ which are not equal to $\{X_1 = \ldots = X_n = 0\}$ and not contained in a union of a finite number of hyperplanes $\{c_1 Z'_0 - c_0 Z'_1 = 0\}$ where $c_0, c_1 \in \overline{k}$. Then $\tilde{C}$ is a curve in $(\mathbb{P}^n \times \mathbb{P}^1)(\overline{k})$ since, c.f. [6], $\# \tilde{L} \cap (W \times \mathbb{P}^1(\overline{k})) \cap \{c_1 Z'_0 - c_0 Z'_1 = 0\} < +\infty$ for all points $(c_0 : c_1) \in \mathbb{P}^1(\overline{k})$ excepting a finite number of them.

Let $\varepsilon > 0$ be an infinitely small value relatively the field k as above. So the map of the standard part

$$\mathrm{st} \,:\, (\mathbb{P}^n \times \mathbb{P}^1)(\overline{k(\varepsilon)}) \longrightarrow (\mathbb{P}^n \times \mathbb{P}^1)(\overline{k})$$

is defined, c.f. [5].

Show that the point $(x, (1:0)) \in \tilde{C}$. Indeed, c.f. [6], $\#\tilde{C} \cap \{Z'_0\varepsilon - Z'_1 = 0\} = \#W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+1 \le j \le n\} \ge \#W \cap \{L_{s+1}^{(1)} = \ldots = L_n^{(1)} = 0\}$. Let $x_i^*, 1 \le i \le N_1$ be all the points of $\tilde{C} \cap \{Z'_0\varepsilon - Z'_1 = 0\}$. Then $\mathrm{st}(x_j^*) \in \tilde{C} \cap \{Z'_1 = 0\}$, i.e. $\mathrm{st}(x_j^*)$ has the form $((x', (1:0))$ where $x' \in W \cap \{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\}$. The differentials of the projection $p^{(0)}$ are isomorphisms in all the point from $W \cap \{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\} \setminus \{x\}$. Thus, by the theorem about the implicit function for every $x' \in W \cap \{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\} \setminus \{x\}$ there exists a unique $1 \le j \le N_1$ such that $st(x_j^*) = x'$. So there exists at least one $1 \le j_0 \le N_1$ such that $st(x_{j_0}^*) = x$. Thus, $(x, (1:0)) \in \tilde{C}$ and our assertion is proved.

Denote by $\pi \,:\, \mathbb{P}^n \times \mathbb{P}^1 \longrightarrow \mathbb{P}^n$ the projection to the first factor $\mathbb{P}^n$ and set $\tilde{C}_1 = \pi(\tilde{C})$, $\tilde{C}_2 = \tilde{C}_1 \cap \{X_0 \ne 0\} \subset \{X_0 \ne 0\} = \mathbb{A}^n(\overline{k}) \subset \mathbb{P}^n(\overline{k})$. Then by the proved $x \in \tilde{C}_2$. Denote $x^* = \pi(x_{j_0}^*) \in \tilde{C}_2$ and by the y^* the projection (which is defined when a real structure is defined) of the point x^* to the linear subspace $\{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\} \cap \{X_0 \ne 0\} \subset \mathbb{A}^n(\overline{k})$. Denote $x^* = (x_1^*, \ldots, x_n^*)$ and $y^* = (y_1^*, \ldots, y_n^*)$. Then $\sum_{1 \le i \le n} |x_i^* - y_i^*|^2 / \sum_{1 \le i \le n} |x_i^*|^2$ is an infinitely small value relatively to the field $\overline{k}$ since the linear subspace, see above, $\{L_j^{(0)} + \varepsilon L_j^{(1)} = 0,\ s+1 \le j \le n\}$ is infinitely close to $\{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\}$. Therefore, c.f. the proof of Lemma 6, the line

$$l = \{\mathrm{st}_\varepsilon(y^*/(\sum_{1 \le i \le n} |y_i^*|^2)^{1/2})\, t \,:\, t \in \overline{k}\} \subset \mathrm{con}(x, W) \cap \{L_{s+1}^{(0)} = \ldots = L_n^{(0)} = 0\}.$$

We get a contradiction. The lemma is proved.

Return to the consideration of the algorithm. Note that the condition that the differentials of the projection

$$p(W) \,:\, W \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+1} : \ldots : L_n).$$

are isomorphisms in all the point from $W \cap \{L_{s+1} = \ldots = L_n = 0\} \setminus \{x\}$ follows from the condition that the differentials of the projection

$$p_1 \,:\, W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+1} : \ldots : L_n).$$

are isomorphisms in all the point from $W \cap \{L_{s+1} = \ldots = L_n = 0\} \setminus \{x\}$. This fact follows directly from the theorem about the implicit function.

LEMMA 10. Let $\mu(x, V_s)$ be the multiplicity of the point x on the variety V_s as above. Then

$$\mu(x, V_s) = \deg V_s - \#A. \tag{9}$$

PROOF. Let W be an arbitrary irreducible component of V' and $A(W) \subset \{1, \dots, N\}$ be the subset of indices such that

$$\{x_u \,:\, u \in A(W)\} = W \cap \{L_{s+1} = \, \dots \, = L_n = 0\}$$

in $\mathbb{P}^n(\overline{k})$. It is sufficient to prove that $\mu(x, W) = \deg W - \#A(W)$ since all the terms in this formula are additive relatively to the union of components of varieties.

Consider the set of families H of $n - s$ linear forms $H_{s+1}, \dots, H_n$ in $X_1, \dots, X_n$ with coefficients from $\overline{k}$ as the affine space $\mathbb{A}^{(n-s)n}(\overline{k})$.

Denote by U_3 the subset of $\mathbb{A}^{(n-s)n}(\overline{k})$ of such families $H_{s+1}, \dots, H_n$ for which

$$W \cap \{L_0 = H_{s+1} = \, \dots \, = H_n = 0\} = \emptyset,$$

$$\mathrm{con}(x, W) \cap \{H_0 = H_{s+1} = \, \dots \, = H_n = 0\} = \emptyset$$

in $\mathbb{P}^n(\overline{k})$, all the points of $W \cap \{H_{s+1} = \, \dots \, = H_n = 0\} \setminus \{x\}$ are smooth and the differentials of the projection

$$p(H) \,:\, W \longrightarrow \mathbb{P}^{n-s}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : H_{s+1} : \ldots : H_n).$$

are isomorphisms in all the point from $W \cap \{H_{s+1} = \, \dots \, = H_n = 0\} \setminus \{x\}$. Then U_3 is open in the Zariski topology. So by the definition of the multiplicity there exists such a family $H = \{H_j\}_{s+1 \le j \le n}$ for which $\mu(x, W) = \deg W - \#(W \cap \{H_{s+1} = \dots = H_n = 0\} \setminus \{x\})$

By the remark just after the proof of Lemma 9 the conditions of Lemma 9 are satisfied for $L_j^{(0)} = L_j$ and $L_j^{(1)} = H_j$, $0 \le j \le n$. Now applying Lemma 9 we get the required formula $\mu(x, W) = \deg W - \#A(W)$. The lemma is proved.

Thus, by Lemma 10 we can compute the multiplicity $\mu(x, V_s)$ and, therefore, $\mu(x, V)$. The algorithm for the computation of the multiplicity of a point is completely described. Theorem 3 is proved.

References

[1] **Bochnak J., Coste M., Roy M.–F.:** *"Géométrie algébrique réelle"*, Springer–Verlag, Berlin, Heidelberg, New York, 1987.

[2] **Bourbaki N.:** *"Algèbre commutative"*, Chap. 1–7, Actualités Sci. Indust., nos. 1290, 1293, 1308, 1314, Paris 1961, 1964, 1965.

[3] **Chistov A. L.:** *"Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic"*, Research Report No. 8597-CS, Institut fuer Informatik der Universitaet Bonn, May 1993, 23 p.

[4] **Chistov A. L.:** *"Polynomial–Time Computation of the Dimension of Affine Algebraic Varieties in Zero–Characteristic"*, Research Report No. 8597-CS, Institut fuer Informatik der Universitaet Bonn, March 1994, 24 p.

[5] **Chistov A. L.:** *"Polynomial-time computation of the dimension of components of algebraic varieties in zero-characteristic"*, Preprint Université Paris XII-Val de Marne, Faculté des Sciences et Technologies, Informatique. No. 95–06, 1995, 23 p.

[6] **Chistov A. L.:** *"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), pp. 124–188 (Russian) [English transl.: J. Sov. Math. 34 (4) (1986)].

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

[8] **Chistov A. L.:** *"Polynomial complexity algorithms for computational problems in the theory of algebraic curves"*, Zap. Nauchn. Semin. Leningrad. Otdel. Mat. Inst. Steklov (LOMI) 176 (1989) pp. 127–150 (Russian).

[9] **Hartshorne R.:** *"Algebraic geometry"*, Springer–Verlag, New York, Heidelberg, Berlin, 1977.

[10] **Igusa J.:** Mem. Coll. Sci. Univ. Kyoto 27 (1951), 189–201.

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

[12] **Mumford D.:** *"Algebraic geometry 1. Complex projective varieties"*,Springer–Verlag, Berlin, Heidelberg, New York, 1976.

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

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

[15] **Samuel P.:** *"Métodes d'algebre abstracte en géométrie algébrique"*, B. 1967.