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

1999

Abstract

Consider an algebraic variety over a zero–characteristic ground field which is given as a set of all 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 a given algebraic variety in the neighbourhood of a given point, an algorithm for the computation of the multiplicity of a given point of an algebraic variety, an algorithm for the computation of a representative system of smooth points with their tangent spaces on each component of a given algebraic variety, an algorithm for deciding whether a given morphism of algebraic varieties is dominant.

1991 Math. Subject Class. 14Q15

*Research partially supported by the Volkswagen–Stiftung, Program on Computational Complexity, University of Bonn

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, a representative set of smooth points of a given algebraic variety V with their tangent spaces is constructed such that each irreducible component of V contains at least one point from this set. Given a point x of an algebraic variety and a family $\mathcal{Q}$ of rational functions an algorithm is suggested to decide whether there is an irreducible component W of this algebraic variety containing the point x and such that the family $\mathcal{Q}$ is a basis of transcendence of the field of rational function of W. This gives an algorithm for deciding whether a given morphism of algebraic varieties is dominant. The case of zero–characteristic ground field is considered.

This paper continues [2] and [3]. The methods of real algebraic geometry [1] are essentially used in the present paper as in [2], [3]. The results from [16] and [15] are important here. It should be emphasized that the present paper could not appear until two principle steps were made in [2] and [3]. In [2] the problem of the computation of dimension over zero–characteristic ground fields was solved for the case of projective varieties. The algorithm from [3] for the computation of dimensions of all components of an algebraic variety required additionally four embedded recursions. Note also that in other terms the construction from [2], [3] is a polynomial–time algorithm for the choice of the projection in the Noether normalization theorem.

The probabilistic algorithms for the problems considered in this paper (and many others in which it is required to find some element in "general position") can be easily obtained in any characteristic of the field of coefficients. The problem of the computation of the dimension of algebraic varieties is classical and it has been considered from the last century [11]. In [12] the problem of the computation of the dimension of algebraic varieties was formulated from the point of view which is close to theory of complexity. In [8] a well parallelizable arithmetical network is constructed for the computation of the dimension of an algebraic variety in non–uniform polynomial sequential time in the size of input and d^n. In the general case one can obtain from [8] only probabilistic algorithm for this problem with the complexity polynomial in d^n. In [8] also the problem was stated to find a deterministic algorithm for the computation of the dimension with a bitwise complexity $d^{O(n)}$. This problem is solved in [2], [3] for zero–characteristic. The situation in the theory of computation is reflected here that in many problems random objects (or objects in "general position") are difficult to construct deterministically.

In this paper we construct deterministic algorithms with a bitwise complexity polynomial in d^n and the size of input. The question is open whether there is such an algorithm for any of the problems considered in this paper and [2], [3] (i.e., for computing dimensions, degrees, multiplicities and so on) in the case of non–zero characteristic ground field. In [4] an algorithm is suggested for decomposing an algebraic variety into the irreducible components with the complexity polynomial in d^{n^2} and the size of input including the characteristic of the field. For an arbitrary characteristic using [4] the algorithms with the similar complexity bound (i.e., polynomial in d^{n^2} and the size of input) can be obtained for the problems considered in this paper and [2], [3]. This complexity bound is the best known for the case of an arbitrary characteristic. We would like to underline here again that we consider deterministic computations with a bitwise complexity. This model of computations is the most important from the theoretical point of view.

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. In what follows we shall denote for brevity this set by $\mathcal{Z}(g_0, \ldots, g_m)$. The similar notations 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 $V = \mathcal{Z}(g_0, \ldots, g_m)$.

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

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

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 $L(F) < d_1^{l+1} M_1$. In what follows if there is no special mention about it we set l to be fix. One can consider different dense representations of polynomials. For example, one can consider the class of polynomials f in $X_0, \ldots, X_n$ with $\deg_{X_i} f < d$ for all $0 \le i \le n$ as basic in a dence representation which is parametrized by d. Then the sizes of these polynomials are estimated by $(d^{n+1} d_1 + 1) d_2^l M$. In such a representation $L(f_i) < (d^{n+1} d_1 + 1) d_2^l M$ and, therefore, algorithms from the present paper have polynomial complexity, cf. [4].

Let V_s be the union of all the irreducible components of the dimension $n-s$ of of V where $0 \le s \le n$. The degree $\deg V_s$ of V_s is equal, see Lemma 1 below, 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 $\# V_s \cap H < +\infty$.

THEOREM 1 *Let a projective algebraic variety V defined 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 $0 \le s \le n$ 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 neighbourhood of the point x) is set to be $\max_W \dim W$ where the maximum is taken over all the irreducible 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 $0 \le s \le n$. 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 can be defined by the formula

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

see also Corollary 3 and Remark 5 in Section 5. This formula can be explained in the following way, c.f. [14]. 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 V_s with 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 infinitesimal shift) all the points of the intersection which were in the infinitesimal small neighbourhood of x go 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 $\mu(x, V_s)$.

THEOREM 3 *The multiplicities $\mu(x, V_s)$ for all $0 \leq s \leq n$ 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 $n - s$ where $0 \leq s \leq n$. Then one can construct for every $0 \leq s \leq n$ 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 the property that for every component W of V_s there exists a point $x \in A_s \cap W$. The points of A_s are also smooth points of V (i.e. they do not belong to any V_r with $r \neq s$). The number of elements $\# A_s \leq d^s$. The working time of the algorithm for constructing all A_s, $0 \leq s \leq n$ is polynomial in d^n, d_1, d_2, M, M_1, m.*

THEOREM 5 *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 a family $\mathcal{Q}$ of rational functions $q_{s+1}, \ldots, q_n \in k(X_1/X_0, \ldots, X_n/X_0)$, $0 \leq s \leq n$, be given. Let the degrees and the lengths of integer coefficients of numerators and denominators of rational functions $q_{s+1}, \ldots, q_n$ are bounded from above by the same values as ones for the polynomials $g_0, \ldots, g_m$. Let $x \in \mathbb{P}^n(\overline{k})$. An algorithm is suggested to decide whether there is an irreducible component W of the algebraic variety V containing the point x and such that the family $\mathcal{Q}$ is a basis of transcendence of the field of rational function $\overline{k}(W)$ of W. The working time of the algorithm is polynomial in d^n, d_1, d_2, M, M_1, m and the size of the point x.*

REMARK 1 *The working times of the algorithms from the theorems 1–5 are essentially the same as by solving systems of polynomial equations with a finite* *set of solutions in the projective space. So these theorems can be formulated also in the case when l is not fixed, see [4].*

REMARK 2 *In what follows we shall assume without loss of generality that the polynomials $g_0, \ldots, g_m$ are linearly independent over k. Hence* $\dim V \leq n-1$ *and* $V_0 = \emptyset$.

1 Preliminaries

We shall use in this paper the technique from [5], [2], [3], see Introductions of [2], [3]. Namely, we apply Newton–Puiseux expansions and the Newton–Puiseux algorithm for constructing roots of a polynomial in the field of fractional power series in one variable, see also [6], we apply infinitesimals, standard parts, constructing real structures.

The real structure on a field k is defined to be an embedding $k \to K[\sqrt{-1}]$ where K is a real ordered field. An algorithm of the polynomial complexity for constructing a real structure is suggested in [2] for a field k finitely generated over $\mathbb{Q}$. It is important here that for a given element $a \in K$ one can decide whether $a > 0$ within the polynomial time. Additionally $K \subset \overline{k}$ in this construction where $\overline{k}$ is algebraic closure of k. The absolute value $|a|$ of an element from $a \in \overline{k}$ can be defined in the natural way [2].

Consider inequalities of the type $A < 0$ or $A \leq 0$ where $A = \sum_{1 \leq i \leq r} a_i |A_i|^2$, $a_i \in K$, and A_i is a superposition of polynomials and functions $B \mapsto |B|^2$ for every i. The upper bound for the degree of A can be easily defined if we set $\deg |B|^2 = 2 \deg B$.

Each system of equations and inequalities over $\overline{k}$ is equivalent to the system of equations and inequalities over $\widetilde{K}$ with twice as much of variables. Applying the algorithm of [2] for constructing real structures, transfer principle and [16] in this situation we get, see [3], the following result.

PROPOSITION 1 *Consider a system of polynomial equations in n variables and a fixed number of inequalities with polynomials and squares of absolute values (of the described type $A < 0$ or $A \leq 0$) with coefficients from the field k finitely generated over $\mathbb{Q}$. Let the degrees of equations and inequalities be less than d. Then one can construct a real structure on k and decide within the time polynomial in d^n and the size of input whether this system has a solution in $\mathbb{A}^n(\overline{k})$ relative to the constructed real structure. If such a solution exists one can construct it within the same time. The coordinates of the solution belong to a finite extension of the field k. This finite extension is constructed and is given by a primitive element and its minimal polynomial.*

Since k is an arbitrary finitely generated field over $\mathbb{Q}$ this result is valid also in the case when one replaces the field of coefficients k by an extension of k by a fixed number of infinitesimals. In what follows we shall use many times Proposition 1 for solving systems of polynomial equations and inequalities with squares of absolute values and infinitesimals without references to this proposition.

Let k_1 be an algebraic extension of the field $\mathbb{Q}(t_1, \ldots, t_l)$. Let $\varepsilon_i > 0$ be an infinitesimal, see [3], relative to the field $k_1(\varepsilon_1, \ldots, \varepsilon_{i-1})$, $1 \le i \le v$. Let $0 \le w \le v - 1$. Set $K' = k_1(\varepsilon_1, \ldots, \varepsilon_v)$ and $K'' = k_1(\varepsilon_1, \ldots, \varepsilon_w)$. Denote by

$$\mathrm{st} : \mathbb{P}^n(\overline{K'}) \to \mathbb{P}^n(\overline{K''})$$

the mapping of the standard part, see [3], (the standard part of an element $z \in \mathbb{P}^n(\overline{K'})$ is the element $z_1 \in \mathbb{P}^n(\overline{K''})$ which is infinitesimal close to z). We shall use many times the following result, see [3] Proposition 2.

PROPOSITION 2 *Let $W' \subset \mathbb{P}^n$ be a variety defined over the field $\overline{K''}$ and such that every component of W' has the dimension $n-s$. Let $D_i \in \overline{K''}[X_0, \ldots, X_n]$, $s+1 \le i \le n$, be linear forms in $X_0, \ldots, X_n$ and $\widetilde{D}_i \in \overline{K'}[X_0, \ldots, X_n]$, $s+1 \le i \le n$, linear forms all nonzero coefficients of which are infinitesimals relative to the field K''. Then the condition $\#W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) < +\infty$ in $\mathbb{P}^n(\overline{K''})$ implies that $\#W' \cap \mathcal{Z}(D_{s+1} - \widetilde{D}_{s+1}, \ldots, D_n - \widetilde{D}_n) < +\infty$ in $\mathbb{P}^n(\overline{K'})$ and*

$$\begin{aligned}&\mathrm{st}(W' \cap \mathcal{Z}(D_{s+1} - \widetilde{D}_{s+1}, \ldots, D_n - \widetilde{D}_n)) = \\ &W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n)\end{aligned}$$

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

2 Computation of the degree of an algebraic variety 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 $V_s \ne \emptyset$ and*

$$V_s \cap \mathcal{Z}(L_0, L_{s+1}, L_{s+2}, \ldots, L_n) = \emptyset$$

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

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

the linear projection which is a finite morphism [9]. Then

(i) *there exists a non–empty 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 Replacing k by $\overline{k}$ we can suppose without loss of generality that $V_s = W$ is irreducible over $\overline{k}$. Let $Y \in \overline{k}[X_0, \ldots, X_n]$ be a linear form. Consider the morphism

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

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

By the theorem about primitive element for fields there exists a linear form $Y \in \overline{k}[X_0, \ldots, X_n]$ such that the morphism p_1 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 by $R = \mathrm{Res}_Y(G, G'_Y)$ the discriminant of the polynomial G relative to Y. Then $0 \neq R$ is a homogeneous polynomial since G is a separable homogeneous polynomial. 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 $U = \mathbb{P}^{n-s}(\overline{k}) \setminus (\mathcal{Z}(R) \cup p_3(p_2(W) \setminus p_2(U_1)))$. Then for every $x \in U$

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

(b) 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

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

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.

Let us show that $\deg G = \deg W$. Let $\varepsilon > 0$ be an infinitesimal relative to the field k. So the map of the standard part

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

is defined for every $r \geq 0$, see [3]. 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 replace in the formulation of Lemma 1 the forms $L_0, L_{s+1}, L_{s+2}, \ldots, L_n$ by $H_0, H_{s+1}, H_{s+2}, \ldots, H_n$ then (i) 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], c.f. also Section 5, $\mathcal{H}_1$ 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 infinitesimal coefficients. Thus, by Proposition 2 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 an isomorphism. Therefore, by the implicit function theorem 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, $\deg G = \deg W$. Assertion (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 neighbourhood of each point $y \in p^{-1}(x)$. 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, $\# p_3^{-1}(x) = \deg W$ and so $R(x) \neq 0$, see 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 $0 \le i \le m$ replacing if it is necessary each polynomial g_i by the family of polynomials $\{g_i X_j^{-\deg(g_i)+d}\}_{0\le j\le n}$.

Recall that in [3] the algorithm of polynomial complexity is suggested which finds all s for which $V_s \ne \emptyset$. For every s at the step s the algorithm of [3] constructs polynomials $h_1, \dots, h_s$ and linear forms $L_{s+1}^{(s)}, \dots, L_n^{(s)}$ in $X_0, \dots, X_n$ with integer coefficients of the size $O(n \log d)$ such that

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

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

$$W_s = \mathcal{Z}(h_1, \dots, h_s) \subset \mathbb{P}^n(\overline{k})$$

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

$$W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \dots, L_n^{(s)})$$

is finite and

$$W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \dots, L_n^{(s)}) \cap W'' = \emptyset.$$

The form $L_0^{(s)}$ is not equal to zero in each point of $W' \cap \mathcal{Z}(L_{s+1}^{(s)}, \dots, L_n^{(s)})$. Besides that W'' consists of all components U of $\mathcal{Z}(g_0, \dots, g_m)$ with $\dim U > n - s$.

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

Set $L_{s,j} = L_j^{(s)}$, $s+1 \le j \le n$ or $j = 0$. Compute, see [3], all the points $\{x_u\}_{1\le u\le N}$ of the set $W' \cap \mathcal{Z}(L_{s,s+1}, \dots, L_{s,n})$. Let $x_u = (x_{u,0} : \dots : x_{u,n})$ where all $x_{u,i}$ are from a finite extension of k. Construct a real structure for the field $K = k(x_{u,0}, \dots, x_{u,n})$, see [2], [3], which induces the a structure on $\overline{k}$ (it is uniquely defined up to a conjugation).

Let $\varepsilon_1 > 0$ be an infinitesimal relative to the field K and $\varepsilon_2 > 0$ an infinitesimal relative 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 $1 \le u \le N$ consider the following system of equations and inequalities with coefficients in K_1

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

REMARK 3 *One can add also to this system the equation* $L_{s,0}(X_0 - x_{u,0}, \dots, X_n - x_{u,n}) = 0$ *but it is not necessary.*

LEMMA 2 *Let* $W' = W'_s$ *be as above. Then* $N = \deg W'$ *if and only if for every* $1 \le u \le N$ *there do not exist solutions of system (2) in* $\mathbb{A}^{2n+2}(\overline{K_1})$. *If for every* $1 \le u \le N$ *there do not exist solutions of system (2) 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*

$$p : W' \longrightarrow \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \dots : X_n) \mapsto (L_{s,0} : L_{s,s+1} : \dots : L_{s,n})$$

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

PROOF Follows directly from Lemma 1 if one replaces $g_0, \dots, g_m$ by $h_1, \dots, h_s$ and, therefore, V_s by W'_s, c.f. also the proof Lemma 17 below.

Return to the description of the algorithm. Our aim now is to compute $\deg W'$. Construct a solution of system (2) for some $1 \le u \le N$ or ascertain that for every $1 \le u \le N$ there do not exist solutions of system (2) 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

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

of system (2) with $u = u_0$. 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

$$L'_i = L_{s,i} - (L_{s,i}/L_{s,0})(x')L_{s,0},\ s+1 \le i \le n,\ L'_0 = L_{s,0}.$$

Compute, see [3], all the points from the set $W' \cap \mathcal{Z}(L'_{s+1}, \dots, L'_n)$ in $\mathbb{P}^n(\overline{K_1}$. Denote $N' = \#W' \cap \mathcal{Z}(L'_{s+1}, \dots, L'_n)$. By Proposition 2 for every $x^* \in W' \cap \mathcal{Z}(L'_{s+1}, \dots, L'_n)$ there exists $1 \le u \le n$ such that $\operatorname{st} x^* = x_u$. So $N' \ge N$. Further, $x', y' \in W' \cap \mathcal{Z}(L'_{s+1}, \dots, L'_n)$, $x' \ne y'$ and $\operatorname{st} x' = \operatorname{st} y'$. Therefore, $N' \ge N + 1 > N$.

Let $D_{s+1}, \dots, D_n \in \overline{K_1}[X_0, \dots, X_n]$ be linear forms (in what follows we shall consider also other ground fields different from K_1). Similarly to definition 1 from [3] the property $\mathcal{A}$ of linear forms $D_{s+1}, \dots, D_n$ is called good if and only if the it satisfies the following condition. Consider $\mathcal{A}$ as a function of $D_{s+1}, \dots, D_n$. Let $D_i = \sum_{0\le j\le n} l_{i,j} L_j$ where $l_{i,j} \in \overline{K_1}$ for all i, j. Replace one arbitrary coefficient $l_{i,j}$ in the forms $D_{s+1}, \dots, D_n$ by the coefficient ε' where ε' is an infinitesimal relative to the field K_1. We get the new linear form D'_i with coefficients in $\overline{K_1(\varepsilon')}$. Suppose for the convenience of the notations that we have replaced $l_{s+1,0}$ and got D'_{s+1}. The condition for the property $\mathcal{A}$ is as follows. There exists a polynomial P such that if the property $\mathcal{A}$ holds for the forms $D_{s+1}, \dots, D_n$ then

(i) it is not satisfied for at most $P(d^n)$ arbitrary values ε^* of ε' (considered as a variable) for the forms $D'_{s+1}|_{\varepsilon'=\varepsilon^*}, D_{s+2}, \ldots, D_n$,

(ii) for a given value ε^* of ε' one can check the property $\mathcal{A}$ for the forms $D'_{s+1}|_{\varepsilon'=\varepsilon^*}, D_{s+2}, \ldots, D_n$ within the time polynomial in d^n, d_1, d_2, M_1, M_2 (provided that the size of ε^* is bounded by the same values).

For a good property $\mathcal{A}$ one can construct replacing subsequently coefficients of linear forms $D_{s+1}, \ldots, D_n$ by integer coefficients (c.f. the algorithm from [3] Section 3 step (24); it is called in [3] second auxiliary algorithm) linear forms $M_{s+2}, \ldots, M_n$ in $X_0, \ldots, X_n$ with integer coefficients with the lengths $O(n \log d)$ satisfying the property $\mathcal{A}$ within the time polynomial in d^n, d_1, d_2, M_1, M_2. In what follows we shall use few times this construction (not formulating explicitly the property $\mathcal{A}$ except of the first time) referring to it as to the analog of the second auxiliary algorithm from [3].

Now note that according to [3] the property that

$$\#W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) \geq N' \quad \text{and}$$
$$W' \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) \cap W'' = \emptyset \quad \text{and} \quad D_0 = L'_0$$

is good.

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

$$\#W' \cap \mathcal{Z}(M_{s+1}, \ldots, M_n) \geq N',$$
$$W' \cap \mathcal{Z}(M_{s+1}, \ldots, M_n) \cap W'' = \emptyset \text{ and } M_0 = L'_0.$$

After that, return recursively to the beginning of the algorithm described replacing the forms $L_{s,0}, L_{s,s+1}, \ldots, L_{s,n}$ by $M_0, M_{s+1}, \ldots, M_n$. Since $N' > N$ there are at most d^s such returns in the algorithm.

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

Let us show how to choose among the points x_u, $1 \leq u \leq N$ the points from V_s. Let $1 \leq u \leq N$. Consider the following system of equations and inequalities in $X_0, \ldots, X_n$, Z with coefficients from $\overline{k(\varepsilon_1)}$

$$h_1 = \ldots = h_s = h_{s+1}Z - 1 = 0, \sum_{0 \leq i \leq n} |X_i - x_{u,i}|^2 < \varepsilon_1. \tag{3}$$

LEMMA 3 *The point* $x_u = (x_{u,0} : \ldots : x_{u,n}) \in V_s$ *if and only if system (3) 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 [3]). The lemma is proved.

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

By Lemma 1, Lemma 2 and Lemma 3 we have $\#A = \deg V_s$, the set $V_s \cap \mathcal{Z}(L_{s,s+1}, \ldots, L_{s,n}) = \{x_u : u \in A\}$ 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. Each point x_u, $u \in A$, does not belong to W''. Hence the points x_u, $u \in A$ are smooth points of V Theorem 1 is proved.

To prove 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 is given by the rational functions* $\phi_1, \ldots, \phi_r \in \overline{k}(V')$, *let the point* $y \in V'$ *be smooth, the rational functions* $\phi_1, \ldots, \phi_r$ *are defined in the point* y *and the differential*

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

of ϕ *in the point* y *be an isomorphism of the tangent spaces* $T_{y,V'}$ *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 neighbourhood 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 if one replaces $\overline{k}$ by $\mathbb{C}$ the statements of the lemma follow directly from the implicit function theorem. Now it is sufficient to apply the transfer principle for the field supplied with a real structure, c.f. [2], see [1]. The lemma is proved.

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

$$D_j = \mathcal{Z}(h_1, \ldots, h_s) \cap \mathcal{Z}(L_{s,m} - (L_{s,m}/L_{s,0})(x_u)L_{s,0},\ s+1 \le m \le n,\ m \ne s+j)$$

for $1 \le j \le n-s$ in some neighbourhood of x_u.

Thus, construct using the algorithm from [4] generic points of curves D_j (more precisely irreducible components of D_j containing the point x_u) and Newton–Puiseux expansions of coordinate functions of generic points of D_j in uniformizing elements in some neighbourhood of x_u, c.f. [2] section 3, steps (11), (12), (13) and also [3], section 1, step (16). 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.

REMARK 4 *Actually one can see that the algorithm from [4] (or it minor modifcation) gives a system of local parameters of D_j in the neighborhood of the smooth point x_u. So it is not necessary even to consider Newton–Puiseux expansions.*

3 Dimensions of components containing a point and dominantness of a morphism of algebraic varieties

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

LEMMA 5 *Let $x \in V$, see the Introduction. 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 Let us construct the set $\{x_u : u \in A\}$ of smooth points of V and linear forms $L_{s,s+1}, \ldots, L_{s,n}$ such that

$$\{x_u : u \in A\} = V_s \cap \mathcal{Z}(L_{s,s+1}, \ldots, L_{s,n}),$$

see Section 2. Construct linear forms L_i, $s+1 \le i \le n$, vanishing in the point x and such that L_i, $s+2 \le i \le n$, are linear forms in $L_{s,s+1}, \ldots, L_{s,n}$. Denote $\mathcal{L} = \mathcal{Z}(L_{s+2}, \ldots, L_n)$.

The intersection $\mathcal{L} \cap V_s$ is a curve. Denote it by C_s. Each irreducible component of C_s is an irreducible component of the variety of solutions of the system

$$h_1 = \ldots = h_s = L_{s+2} = \ldots = L_n = 0. \tag{4}$$

There is a linear form L' (coinciding with one of the linear forms $L_{s,s+1}, \ldots, L_{s,n}$) such that

$$C_s \cap \mathcal{Z}(L') = V_s \cap \mathcal{Z}(L_{s,s+1}, \ldots, L_{s,n}).$$

Hence, each irreducible component of C_s being a projective algebraic variety has a non–empty intersection with $\mathcal{Z}(L')$ and, therefore, contains some point x_u, $u \in A$. The points $\{x_u : u \in A\}$ are smooth on the variety of solutions of (4) by the construction of Section 2 and $C_s \supset \{x_u : u \in A\}$. So applying the algorithm from [4], c.f. also [2], [3], construct in the required time the systems of equations which gives one–dimensional irreducible components of the variety of solutions of (4). 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.

COROLLARY 1 *Let $\varepsilon > 0$ be an infinitesimal relative to the field k. Under conditions of Lemma 3 for every $0 \le s \le n$ one can construct the family of points $x_\beta \in \mathbb{P}^n(\overline{k(\varepsilon)})$, $\beta \in B_s$, such that*

- *every point x_β is infinitesimal close to x,*
- *every point $x_\beta \in V_s$ and x_β is a smooth point of the algebraic variety V,*
- *for every irreducible component W_1 of V_s containing the point x there is $\beta \in B_s$ such that $x_\beta \in W_1$.*

PROOF Choose $s+1 \le i_0 \le n$ such that the linear forms $L_{s,i_0}, L_{s+1}, \ldots, L_n$ are linearly independent. We shall suppose without loss of generality and for convenience of notations that $i_0 = s+1$. Construct the isolated solutions of the system

$$h_1 = \ldots = h_s = L_{s+1} - \varepsilon L_{s,s+1} = L_{s+2} = \ldots = L_n = 0. \tag{5}$$

Choose among these solutions those which are infinitesimal close to the point x. We claim that the obtained family of solutions gives the required family x_β, $\beta \in B_s$. Indeed, by Proposition 2 it is sufficient to check only that x_β is a smooth point of the algebraic variety V. To ascertain this fact note that every irreducible component of the curve C_s contains some smooth point x_u, $u \in A$ of V and $x_u \in V_s$. Hence, the curve C_s contains only a finite set of singular points of V. Therefore, the point x_β is a smooth point of V since it is infinitesimal close to x. The corollary is proved.

Our aim now is to prove Theorem 5. We can suppose without loss of generality that V is an affine algebraic variety which is a set of zeroes of polynomials $g_0, \dots, g_m \in k[X_1, \dots, X_n]$, rational functions $q_{s+1}, \dots, q_n \in k(X_1, \dots, X_n)$, the degrees (respectively the lengths of integer coefficients) of (non–homogeneous) polynomials $g_0, \dots, g_m$, of numerators and denominators of rational functions from the family $q_{s+1}, \dots, q_n$ are bounded from above by d (respectively M). At fist we decide whether $V_s \neq \emptyset$ using the algorithm from [3]. If $V_s = \emptyset$ then there are no irreducible components of V_s.

Let $V_s \neq \emptyset$. Extending the field k by an infinitesimal $\varepsilon > 0$ (and replacing k by $k(\varepsilon)$), applying Corollary 1 and considering separately every point x_β, $\beta \in B_s$ we can suppose without loss of generality that x is a smooth point of the algebraic variety V and $x \in V_s$ where $0 \leq s \leq n$ is known. Therefore, there is only one irreducible component W_1 of the algebraic variety V containing the point x and $W_1 \subset V_s$.

Let $q_i = q_i^{(1)}/q_i^{(2)}$ where $q_i = q_i^{(1)}, q_i^{(2)} \in k[X_1, \dots, X_n]$ and $\mathrm{GCD}(q_i^{(1)}, q_i^{(2)}) = 1$ in the ring $k[X_1, \dots, X_n]$ for every $s+1 \leq i \leq n$. Introduce new variables $Y_{s+1}, \dots, Y_n$, $Z_{s+1}, \dots, Z_n$. Consider the algebraic variety

$$V' = \mathcal{Z}(g_0, \dots, g_m, q_i^{(2)} Y_i - 1, q_i^{(2)} Z_i - q_i^{(1)}, s+1 \leq i \leq n) \subset \mathbb{A}^{n+2(n-s)}(\overline{k}).$$

Denote by

$$\begin{gathered} \pi : \mathbb{A}^{n+2(n-s)}(\overline{k}) \to \mathbb{A}^n(\overline{k}), \\ (X_1, \dots, X_n, Y_{s+1}, \dots, Y_n, Z_{s+1}, \dots, Z_n) \mapsto (X_1, \dots, X_n) \end{gathered}$$

the linear projection. Let $\varepsilon_1 > 0$ be an infinitesimal relative to the field k. Consider the following system of algebraic equations and inequalities in $X_1, \dots, X_n$, $Y_{s+1}, \dots, Y_n$, $Z_{s+1}, \dots, Z_n$

$$\left\{ \begin{array}{ll} g_i = 0, & 0 \leq i \leq m, \\ q_i^{(2)} Y_i - 1 = 0, & s+1 \leq i \leq n, \\ q_i^{(2)} Z_i - q_i^{(1)} = 0, & s+1 \leq i \leq n, \\ \sum_{1 \leq i \leq n} |X_i - X_i(x)|^2 = \varepsilon_1. & \end{array} \right. \tag{6}$$

Let us show that if the family $\mathcal{Q}$ is algebraically independent over $\overline{k}$ in the field $\overline{k}(W_1)$ then there is a solution $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ of system (6). Indeed, in this case there is an irreducible component W_1' of the algebraic variety V' such that W_1' is birationally isomorphic to W_1 and this birational isomorphism is induced by the projection π. Hence, there is a solution $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ of system (6). Note that if there is a solution $x' \in \mathbb{A}^{n+2(n-s)}(\overline{k(\varepsilon_1)})$ of system

(6) then $x' \in V'$, $q_i^{(2)}(x') \neq 0$ and there is an irreducible component W_1' of the algebraic variety V' such that W_1' is birationally isomorphic to W_1. The rational functions q_i coincide with the coordinates functions Z_i on the algebraic variety V', $s+1 \leq i \leq n$.

Thus, replacing k by $k(\varepsilon_1)$, n by $n+2(n-s)$, the algebraic variety V by V' and the point x by x' we can suppose additionally without loss of generality that the rational functions q_i are the coordinates functions Z_i, $s+1 \leq i \leq n$. Finally, effecting a linear transformation of $\mathbb{A}^n$ we can assume without loss of generality that q_i are the coordinates functions X_i, $s+1 \leq i \leq n$, $x = (0, \ldots, 0) \in \mathbb{A}^n(\overline{k})$ is a smooth point of the algebraic variety V and $x \in V_s$ where $0 \leq s \leq n$ is known.

Let $\varepsilon_i > 0$ be an infinitesimal relative to the field $k(\varepsilon_2, \ldots, \varepsilon_{i-1})$, $2 \leq i \leq 4$. Let $\xi = (\xi_1, \ldots, \xi_n) \in V_s$. Let $s \leq r \leq n-1$. Let $L_{r+1}, \ldots, L_n \in \mathbb{Z}[X_0, \ldots, X_n]$ be linear forms with integer coefficients. Consider the following system of algebraic equations and inequalities in $X_1, \ldots, X_n$, $Y_1, \ldots, Y_n$.

$$\begin{cases} g_i = 0, & 0 \leq i \leq m, \\ g_i(Y_1, \ldots, Y_n) = 0, & 0 \leq i \leq m, \\ \sum_{1 \leq i \leq n} |X_i - \xi_i|^2 = \varepsilon_2, & \\ \sum_{1 \leq i \leq n} |X_i - Y_i|^2 = \varepsilon_4^2, & \\ X_i - Y_i = 0, & s+1 \leq i \leq r, \\ |X_{r+1} - Y_{r+1}|^2 > \varepsilon_4^2 \varepsilon_3. & \end{cases} \tag{7}$$

In what follows we shall identify for convenience of notations the tangent space $\mathcal{Z}(\sum_{1 \leq i \leq n} a_{\gamma,i} dX_i, \gamma \in \Gamma)$ (where $a_{\gamma,i}$ belongs to the coefficients field) in a point of an arbitrary affine algebraic variety with the subspace $\mathcal{Z}(\sum_{1 \leq i \leq n} a_{\gamma,i} X_i, \gamma \in \Gamma) \subset \mathbb{A}^n$, herewith $\mathbb{A}^n$ has the coordinates functions $X_1, \ldots, X_n$.

LEMMA 6 *Let $\xi \in V_s$ be a smooth point of V. Let W_1 be the unique irreducible component of the algebraic variety V such that $\xi \in W_1$. Let $s \leq r \leq n-1$. Let the intersection of the tangent space in the point ξ of the algebraic variety W_1*

$$T_{\xi, W_1} \cap \mathcal{Z}(X_{s+1}, \ldots, X_r, L_{r+1}, \ldots, L_n) = \{0\} \tag{8}$$

(and, hence, the linear forms $X_{s+1}, \ldots, X_r$, $L_{r+1}, \ldots, L_n$ are algebraically independent in the field of rational functions $\overline{k}(W_1)$ of the irreducible component W_1). Then system (7) has a solution in $\mathbb{A}^{2n}(\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)})$ if and only if the coordinates functions $X_{s+1}, \ldots, X_r, X_{r+1}$ are algebraically independent over $\overline{k}$ in the field of rational functions $\overline{k}(W_1)$ of the algebraic variety W_1.

PROOF Let system (7) has a solution

$$(x'_1, \ldots, x'_n, y'_1, \ldots, y'_n) \in \mathbb{A}^{2n}(\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}). \tag{9}$$

Set $x' = (x'_1, \ldots, x'_n)$ and $y' = (y'_1, \ldots, y'_n)$. Then by (8) and since x' is infinitesimal close to ξ equality (8) holds if one replaces the point ξ by x'. Hence, the coordinate functions X_j, $1 \le j \le n$, on the tangent space T_{x',W_1} of the algebraic variety W_1 in the point x' satisfy equalities

$$X_j = \sum_{s+1 \le i \le r} \alpha_{j,i} X_i + \sum_{r+1 \le u \le n} \beta_{j,u} L_u, \quad 1 \le j \le n,$$

for some elements $\alpha_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $s+1 \le i \le r$, $1 \le j \le n$, and $\beta_{j,u} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $r+1 \le u \le n$, $1 \le j \le n$.

We can apply the implicit function theorem in the point x' when all coordinates functions on W_1 are considered as formal power series with coefficients in $\overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$ in the linear polynomials $X_{s+1} - X_{s+1}(x')$, $\ldots, X_r - X_r(x')$, $L_{r+1} - L_{r+1}(x'), \ldots, L_n - L_n(x')$. By (8) and since the point x' is infinitesimal close to ξ all the coefficients of these formal power series are not infinitely large relative to the field k. By (7) $x'_i = y'_i$ for $s+1 \le i \le r$ and $|x'_{r+1} - y'_{r+1}|^2 > \varepsilon_4^2 \varepsilon_3$. Hence, the implicit function theorem implies that there is $r+1 \le i_0 \le n$ such that $\beta_{r+1,i_0} \ne 0$. We shall suppose without loss of generality for convenience of notations that $i_0 = r+1$. Therefore, the coordinate functions X_j, $1 \le j \le n$, on the tangent space T_{x',W_1} of the algebraic variety W_1 in the point x' satisfy equalities

$$X_j = \sum_{s+1 \le i \le r+1} \alpha'_{j,i} X_i + \sum_{r+2 \le i \le n} \beta'_{j,i} L_i, \quad 1 \le j \le n,$$

for some elements $\alpha'_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $s+1 \le i \le r+1$, $1 \le j \le n$, and $\beta'_{j,i} \in \overline{k(\varepsilon_2, \varepsilon_3, \varepsilon_4)}$, $r+2 \le i \le n$, $1 \le j \le n$. Hence,

$$T_{x',W_1} \cap \mathcal{Z}(X_{s+1}, \ldots, X_{r+1}, L_{r+2}, \ldots, L_n) = \{0\}. \tag{10}$$

Therefore, by the implicit function theorem the coordinates functions $X_{s+1}, \ldots, X_r, X_{r+1}$ are algebraically independent in the field of rational functions $\overline{k}(W_1)$ of the algebraic variety W_1.

Conversely, let the coordinates functions $X_{s+1}, \ldots, X_r, X_{r+1}$ be algebraically independent in the field of rational functions $\overline{k}(W_1)$ of the algebraic variety W_1. Then there is $r+1 \le i_0 \le n$ such that the linear forms

$$X_{s+1}, \ldots, X_r, X_{r+1}, L_{r+1}, \ldots, L_{i_0-1}, L_{i_0+1}, \ldots, L_n$$

are algebraically independent in the field $\overline{k}(W_1)$. We shall suppose without loss of generality for convenience of notations that $i_0 = r+1$.

The set of points $x' \in W_1(\overline{k(\varepsilon_2)})$ such that (10) holds contains a non–empty open in the Zariski topology subset of $W_1(\overline{k(\varepsilon_2)})$. Hence, c.f. the proof of Lemma 8 below and Lemma 9 from [3], there is a smooth point $x' = (x'_1, \ldots, x'_n) \in W_1(\overline{k(\varepsilon_2)})$ such that (10) holds and $\sum_{1\leq i\leq n} |x'_i - \xi_i|^2 = \varepsilon_2$.

We can apply the implicit function theorem in the point x' when all coordinates functions on W_1 are considered as formal power series with coefficients in $\overline{k(\varepsilon_2)}$ in the linear polynomials $X_{s+1} - X_{s+1}(x')$, $\ldots, X_r - X_r(x')$, $L_{r+1} - L_{r+1}(x'), \ldots, L_n - L_n(x')$. Hence, c.f. the proof of Lemma 8 below and Lemma 9 from [3], system (7) with the additional equations

$$L_i(X_1 - Y_1, \ldots, X_n - Y_n) = 0, \quad r+2 \leq i \leq n,$$

has a solution (9). The lemma is proved.

COROLLARY 2 *Under conditions of Lemma 6 if system (7) has a solution one can construct solution (9) of this system and compute i_0 within the polynomial time in d^n and the size of input. So we shall suppose as previously without loss of generality that $i_0 = r+1$. Then equality (10) holds.*

PROOF It is sufficient to check that one can compute i_0. Applying Lemma 4 to the point x' and the morphism ϕ given by the linear forms $X_1, \ldots, X_r$, $L_{r+1}, \ldots, L_n$ construct the tangent space T_{x',W_1} and then i_0 can be computed immediately. The corollary is proved.

Now we can describe the algorithm which is required to construct in Theorem 5. Denote by W_1 the unique irreducible component of V_s such that $x \in W_1$. Set $z_s = x = (0, \ldots, 0)$. Applying Lemma 4 construct the tangent space T_{z_s,W_1}. Then construct linear forms $D_i^{(s)}$, $s+1 \leq i \leq n$, with lengths of integer coefficients $O(n \log d)$ such that

$$T_{z_s,W_1} \cap \mathcal{Z}(D_{s+1}^{(s)}, \ldots, D_n^{(s)}) = \{0\}.$$

Set $a_i^{(s)} = 0$, $s+1 \leq i \leq n$.

Let $s \leq r \leq n-1$ and we have already constructed recursively $z_r \in W_1$ which is a smooth point of V, linear forms $D_i^{(r)}$, $s+1 \leq i \leq n$, with lengths of integer coefficients $O(n \log d)$ and integers $a_i^{(r)}$, $s+1 \leq i \leq n$, with lengths $O(n \log d)$ such that $D_i^{(r)} = X_i$ for all $s+1 \leq i \leq r$, the point z_r is isolated in the algebraic variety

$$\mathcal{Z}(g_0, \ldots, g_m, D_{s+1}^{(r)} - a_{s+1}^{(r)}, \ldots, D_n^{(r)} - a_n^{(r)}) \subset \mathbb{A}^n(\overline{k})$$

and the intersection

$$T_{z_r,W_1} \cap \mathcal{Z}(D_{s+1}^{(r)}, \ldots, D_n^{(r)}) = \{0\}.$$

The base of the recursion is $r = s$. We shall refer to this recursion as to the first one. Now we shall describe the next step of this recursion, i.e. our aim is to construct the point z_{r+1}, linear forms $D_i^{(r+1)}$ and integers $a_i^{(r+1)}$, $s+1 \le i \le n$.

Using Lemma 6 for $\xi = z_r$ we decide whether $X_{s+1}, \dots, X_{r+1}$ are algebraically independent in the field of rational functions $\overline{k}(W_1)$ of the algebraic variety W_1.

In the case when $X_{s+1}, \dots, X_{r+1}$ are algebraically dependent over $\overline{k}$ in the field of rational functions $\overline{k}(W_1)$ the coordinates functions $X_{s+1}, \dots, X_n$ are also algebraically dependent in this field and the described algorithm finishes its work.

In the case when $X_{s+1}, \dots, X_{r+1}$ are algebraically independent we apply Corollary 2, construct the point (x', y') (it depends on r) which is solution (9) of system (7) with $\xi = z_r$ and compute i_0. Set the family $D_i^{(r+1)}$, $r+2 \le i \le n$, to be $D_i^{(r)}$, $r+1 \le i \le n$, $i \ne i_0$. We shall suppose without loss of generality that $i_0 = r+1$. Then set $D_i^{(r+1)} = D_i^{(r)}$, $r+2 \le i \le n$, and $D_i^{(r+1)} = X_i$ for all $s+1 \le i \le r+1$.

Let us show how to construct the required integers $a_i^{(r+1)}$, $s+1 \le i \le n$ and the point z_{r+1}. Set $b_i = D_i^{(r+1)}(x')$, $s+1 \le i \le n$. Set $z'_s = x'$. Suppose that $s \le j \le n-1$ and we have already constructed recursively integers $a_i^{(r+1)}$, $s+1 \le i \le j$ with lengths $O(n \log d)$ and $z'_j \in W_1$ which is a smooth point of V and such that

$$z'_j \in V^{(j)} = \mathcal{Z}(g_0, \dots, g_m, D_{s+1}^{(r+1)} - a_{s+1}^{(r+1)}, \dots, D_j^{(r+1)} - a_j^{(r+1)},$$
$$D_{j+1}^{(r+1)} - b_{j+1}, \dots, D_n^{(r+1)} - b_n) \subset \mathbb{A}^n(\overline{k})$$

and the intersection

$$T_{z'_j, W_1} \cap \mathcal{Z}(D_{s+1}^{(r+1)}, \dots, D_n^{(r+1)}) = \{0\}. \tag{11}$$

Note that (11) implies that z'_j is an isolated point of the algebraic variety $V^{(j)}$.

The base of the recursion is $j = s$. We shall refer to this recursion as to the second one. Now we shall describe the next step of this recursion, i.e. our aim is to construct the point z'_{j+1} and the integer $a_{j+1}^{(r+1)}$.

Since z'_j is a smooth point of V the algebraic variety

$$\mathcal{Z}(g_0, \dots, g_m, D_{s+1}^{(r+1)} - a_{s+1}^{(r+1)}, \dots, D_j^{(r+1)} - a_j^{(r+1)},$$
$$D_{j+2}^{(r+1)} - b_{j+2}, \dots, D_n^{(r+1)} - b_n) \subset \mathbb{A}^n(\overline{k})$$

contains a unique irreducible component C'_j such that the point $z'_j \in C'_j$. The component C'_j is a curve and $\deg C'_j$ is bounded from above by a polynomial in

d^s by the Bézout inequality. Construct the generic point of C'_j and a system of polynomial equations giving the curve C'_j using the algorithm from [4]. There is, see e.g. [7], a family $\psi_1, \dots, \psi_s$ of local parameters of the algebraic variety W_1 in the point z'_j with degrees polynomial in d^s. Hence by (11) the curve C'_j contains only a polynomial in d^n number of points z'' of V such that the equality

$$T_{z'',V} \cap \mathcal{Z}(D^{(r+1)}_{s+1}, \dots, D^{(r+1)}_n) = \{0\}. \tag{12}$$

does not hold. In particular the curve C'_j contains only a polynomial in d^n number of singular points of V. For a given point $z'' \in C'_j$ one can compute applying the algorithm of Theorem 3 from Section 4 and Section 6 all the multiplicities $\mu(z'', V_i)$, $0 \le i \le n$, within the time polynomial in d^n and the size of input including the size of the point z'' (the algorithm of Section 4 and Section 6 does not use the algorithm under description). Now z'' is a smooth point of V if and only if $\mu(z'', V_s) = 1$ and $\mu(z'', V_u) = 0$ for all $u \ne s$.

The algorithm from Section 4 and Section 6 also allows to construct for $z'' \in W_1$ which is a smooth point of V the family of linear forms $\phi_{s+1}, \dots, \phi_n$ in $X_1, \dots, X_n$ with lengths of integer coefficients $O(n \log d)$ such that

$$T_{z'',W_1} \cap \mathcal{Z}(\phi_{s+1}, \dots, \phi_n) = \{0\}$$

(the tangent space of a smooth point coincides with the tangent cone in this point). Hence, we can apply Lemma 4 and construct the tangent space T_{z'',W_1}. So one can decide for a given point $z'' \in C'_j$ whether (12) holds within the time polynomial in d^n and the size of input including the size of the point z''.

Now enumerate integers $a = 0, 1, \dots$. Construct, c.f. [3] step (16), the intersection

$$B_j = C'_j \cap \mathcal{Z}(D^{(r+1)}_{j+1} - a) \subset \mathbb{A}^n(\overline{k}).$$

If B_j is infinite proceed to the next value of a.

If B_j is finite enumerate points $z'' \in B_j$. For a considered point z'' decide whether (12) holds. If equality (12) does not hold proceed to the next element $z'' \in B_j$. If all the elements from B_j are enumerated proceed to the next value of a. If equality (12) holds set $a^{(r+1)}_{j+1} = a$ and $z'_{j+1} = z''$.

Thus, by the previous considerations we shall construct the required z'_{j+1} and the integer $a^{(r+1)}_{j+1}$ with the length $O(n \log d)$.

If $j < n-1$ then replace j by $j+1$ and proceed to the next step of the second recursion. If $j = n-1$ then set $z_{r+1} = z'_{j+1}$ and if $r < n-1$ replace r by $r+1$ and proceed to the next step of the first recursion. If $j = n-1$ and $r = n-1$ then the algorithm finishes its work.

Thus, we shall decide finally whether the family $X_{s+1}, \ldots, X_n$ is algebraically independent in the field $\overline{k}(W_1)$. The estimation for the working time of the described algorithm follows immediately from the estimations for the working time of the algorithms applied. Theorem 5 is proved.

4 Computation of the multiplicity of a point

The aim of this and next sections is to proof Theorem 3. Consider an algebraic variety V such as in the Introduction and a point x. Denote by $\mathrm{con}(x, V)$ the tangent cone of the variety V in the point x. If x is not an isolated point of V then $\mathrm{con}(x, V)$ consists by definition of the lines containing x which are limits of secants of V containing x when another point of the intersection of the secant with V tends to x (the degenerated case when the line l is such that $x \in l \subset V$ is not excluded: in this case this line $l \subset \mathrm{con}(x, V)$). Strictly speaking this definition is valid for the case when the ground field is $\mathbb{C}$. Another definition of $\mathrm{con}(x, V)$ is valid for arbitrary fields (and in the case when x is an arbitrary not necessary isolated point of V or even when $x \notin V$). The cone is defined as the variety of zeros of the ideal generated by the forms of the least degree of the elements of the ideal of the initial variety in the case when it is affine and the point x has zero coordinates, see just below. Factually, if one uses 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 shall suppose without loss of generality (may be replacing the ground field k) that $x = (1 : 0 : \ldots : 0)$. We shall use the following definition of the cone $\mathrm{con}(x, V)$. Identify $\mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. 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 $U = V \setminus \mathcal{Z}(X_0) \subset \mathbb{A}^n(\overline{k})$. Let $I(U) \subset k[X_1, \ldots, X_n]$ be the ideal of the affine variety U. Each non–zero element $F \in k[X_1, \ldots, X_n]$ is represented as a sum $F = F_r + F_{r+1} + \ldots + F_m$ of homogeneous in $X_1, \ldots, X_n$ polynomials F_j such that $\deg F_j = j$ and $F_r \neq 0$. So for each non–zero element of $F \in k[X_1, \ldots, X_n]$ the form of the least degree $F_r \neq 0$ is defined. Set also the form of the least degree of the zero polynomial to be zero. Denote by $I'(U)$ (respectively $I'(V)$) the ideal of the ring $k[X_1, \ldots, X_n]$ (respectively $k[X_0, \ldots, X_n]$) generated by the forms of the least degree of the elements of $I(U)$. Then $\mathrm{con}(x, U)$ (respectively $\mathrm{con}(x, V)$) is set of zeros of the ideal $I'(U)$ in $\mathbb{A}^n(\overline{k})$ (respectively $I'(V)$ in $\mathbb{P}^n(\overline{k})$). Other definitions of the tangent cone, the proof of the equivalence of the definition with secants and the one which we use see in [10], [17] and Lemma 7 below.

Now let $x = (0, \ldots, 0) = (1 : 0 : \ldots : 0)$ and Z be a new variable. Introduce the variety of secants $\sec(x, U) \subset (\mathbb{A}^n \times \mathbb{A}^1)(\overline{k})$ of the variety U in the following way. Let I_1 be the ideal of $k[X_1 \ldots, X_n, Z]$ generated by all the polynomials $p(ZX_1, \ldots, ZX_n)$ for all $p \in I(U)$. Then $\mathrm{sec}(x, U)$ is a union of all components U_1 of the variety of zeros of the ideal I_1 in $(\mathbb{A}^n \times \mathbb{A}^1)(\overline{k})$ such that $U_1 \not\subset \mathcal{Z}(Z)$.

LEMMA 7 *The equality* $\mathrm{con}(x, U) = \mathrm{sec}(x, U) \cap \mathcal{Z}(Z)$ *holds. If* $x \in U$ *then the dimension in the point* $\dim_x U = \dim \mathrm{con}(x, U)$.

PROOF If x is an isolated point of U or $x \notin U$ the proof is straightforward. So we shall assume that x is not an isolated point of U. We have the isomorphism of algebraic varieties

$$\begin{aligned} &U \times (\mathbb{A}^1 \setminus \{0\}) \simeq \mathrm{sec}(x, U) \setminus \mathcal{Z}(Z), \\ &((X_1, \ldots, X_n), Z) \mapsto ((X_1/Z, \ldots, X_n/Z), Z) \end{aligned} \tag{13}$$

which induces the isomorphism of rings of regular functions

$$\overline{k}[X_1, \ldots, X_n]/I(U) \otimes_{\overline{k}} \overline{k}[Z, Z^{-1}] \simeq \overline{k}[Z, Z^{-1}] \otimes_{\overline{k}[Z]} \overline{k}[X_1, \ldots, X_n, Z]/I_1.$$

Let a polynomial F is vanishing on $\mathrm{con}(x, U)$. Then F^a is the form of the least degree of a polynomial $F_1 \in I(U)$ for some integer $a \geq 1$. Therefore, $F^a = F_1(ZX_1, \ldots, ZX_n)/Z^{a \deg F} + ZF_2$ for a polynomial F_2. Hence F is vaishing on $\mathrm{sec}(x, U) \cap \mathcal{Z}(Z)$. Conversely, let a polynomial $F \in \overline{k}[X_1, \ldots, X_n, Z]$. Let us show that F can be uniquely represented in the in the form

$$F = \sum_{i \in J} Z^i F_i(ZX_1, \ldots, ZX_n) \tag{14}$$

where $F_i \in \overline{k}[X_1, \ldots, X_n]$, $Z^i F_i(ZX_1, \ldots, ZX_n) \in \overline{k}[X_1, \ldots, X_n, Z]$ and $J \subset \mathbb{Z}$ is a finite set. Indeed, it is sufficient to check (14) for monomials and in this case it is straightforward. Note that (14) induces the graduation of the algebra $\overline{k}[X_1, \ldots, X_n, Z]$ such that $Z^i F_i(ZX_1, \ldots, ZX_n)$ is the graded component of F of degree i. Since I_1 has a system of homogeneous generators of degree 0 relative to this graduation the ideal I_1 is a graded ideal relative to the considered graduation. If F is vanishing on $\mathrm{sec}(x, U)$ then $Z^b F \in I_1$ for some integer $b \geq 1$. Hence $Z^{b+i} F_i(ZX_1, \ldots, ZX_n) \in I_1$ since homogeneous components of an element of a graded ideal belong to this ideal. Since Z is not vanishing on every component of $\mathrm{sec}(x, U)$ the polynomials $F_i(ZX_1, \ldots, ZX_n)$ are vanishing on $\mathrm{sec}(x, U)$ for all $i \in J$. Hence $F_i \in I(U)$, $i \in J$ since we have the surjective projection

$$\mathrm{sec}(x, U) \setminus \mathcal{Z}(Z) \to U \setminus \{x\},\ (X_1, \ldots, X_n, Z) \mapsto (ZX_1, \ldots, ZX_n)$$

and $U \setminus \{x\}$ is a dense subset of U in the Zariski topology due to the fact that x is not isolated point of U. Set $J_1 = \{i \in J : Z^i F_i(ZX_1, \ldots, ZX_n)|_{Z=0} \neq 0\}$. Then $\sum_{i \in J_1} Z^i F_i(ZX_1, \ldots, ZX_n)|_{Z=0}$ belongs to the ideal generated by the forms of the least degree of the ideal $I(U)$. Now suppose that a polynomial G is vanishing on $\sec(x,U)\cap\mathcal{Z}(Z)$. Then there exists a polynomial G_1 and an integer $a\geq 1$ such that $F=G^a+ZG_1$ is vanishing on $\sec(x,U)$. Therefore, $G^a=\sum_{i\in I_1}Z^iF_i(ZX_1,\ldots,ZX_n)|_{Z=0}$ is vanishing on $\mathrm{con}(x,U)$. Hence G is also vanishing on $\mathrm{con}(x,U)$. The first assertion of the lemma is proved.

Note that (13) implies that $\dim\sec(x,U)=1+\dim U$. By (13) for any algebraic varieties U_1 and U_2 the equality $\sec(x,U_1\cup U_2)=\sec(x,U_1)\cup\sec(x,U_2)$ holds. Hence, to prove the last assertion we can suppose without loss of generality that U is irreducible and $x\in U$. Then (13) implies that $(x,0)\in\sec(x,U)$. Thus, $\sec(x,U)$ has a non–empty intersection with $\mathcal{Z}(Z)$. Therefore, $\dim\mathrm{con}(x,U)=\dim_x U$. The lemma is proved.

Factually the equivalence of the definition of the tangent cone with secants and the second one with the ideal of forms of the least degree follows from the proved lemma.

Consider in details the case when V is a curve. We need the following definition. Let an algebraic curve $V\subset\mathbb{P}^n(\overline{k})$ and its branch V^* in the point $x=(1:0:\ldots:0)$ with a uniformizing element τ be given, i.e. we have the representations of the coordinate functions of V as formal power series

$$(X_i/X_0)|_V=\gamma_{i,m}\tau^m+\sum_{m<j\in\mathbb{Z}}\gamma_{i,j}\tau^j,\ 1\leq i\leq n,$$

where $\gamma_{i,j}\in\overline{k}$ for all $1\leq i\leq n, 0<m\in\mathbb{Z}$ and $(\gamma_{1,m},\ldots,\gamma_{n,m})\neq(0,\ldots,0)$. Then the tangent line l to this branch is the closure in $\mathbb{P}^n$ of the affine line l' defined by the formula

$$l'=\{(\gamma_{1,m}t,\ldots,\gamma_{n,m}t)\ :\ t\in\overline{k}\}.$$

Note that l does not depend on the choice of the uniformizing element τ. It turns out that $\mathrm{con}(x,V)=\cup_{i\in I}l_i$ is a union of all tangent lines l_i to all branches of V containing the point $x=(1:0:\ldots:0)$.

Now we can go to the description of the algorithm for the computation of the multiplicity of a point of an algebraic variety. We shall use the construction from [3] and the notations W_s, W_s', W_s'', $h_1,\ldots h_s$, $L_{s+1}^{(s)},\ldots,L_n^{(s)}$ for $1\leq s\leq n-1$, and $W^{(1)}$, see Section 2. Recall that $W^{(1)}$ is a union of all components U_1 of W_s' such that $U_1\cap\mathcal{Z}(h_{s+1})\neq U_1$. So V_{s+1} is a union of some components of $W^{(1)}\cap\mathcal{Z}(h_{s+1})$.

If $s=0$ set $W_s'=W^{(1)}=\mathbb{P}^n(\overline{k})$, $W_s''=\emptyset$ and $L_n^{(s)}=X_j$ for $1\leq j\leq n$. So we shall suppose further that $0\leq s\leq n-1$. Our aim is to compute the multiplicity $\mu(x,V_{s+1})$ for $0\leq s\leq n-2$. The case $s=n-1$ is trivial since in this case V_{s+1} consists of points. Further, decide using the algorithm from

Section 3 whether $x \in V_{s+1}$. If $x \notin V_{s+1}$ then $\mu(x, V_{s+1}) = 0$. So in what follows we shall suppose without loss of generality that $x \in V_{s+1}$.

Let us show that if linear forms $D_{s+2}, \dots, D_n$ in $X_0, \dots, X_n$ with coefficients from an extension k_1 of k are given such that $W^{(4)} = W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(D_{s+2}, \dots, D_n)$ is a finite set in $\mathbb{P}^n(\overline{k_1})$ then one can construct within the polynomial time in the size of input and d^{s+1} all the points from this finite set. Indeed, if $W^{(4)}$ is finite then one see immediately from the construction of [3] that $W^{(1)} \cap \mathcal{Z}(D_{s+2}, \dots, D_n)$ is a union of all irreducible components C of dimension one of $\mathcal{Z}(h_1, \dots, h_s, D_{s+2}, \dots, D_n)$ such that h_{s+1} is not identically zero on C. Using the algorithm from [4] construct generic points and systems of equations defining all such curves C and may be some additional curves C' which are contained in the components of the dimension more than one of the algebraic variety $\mathcal{Z}(h_1, \dots, h_s, D_{s+2}, \dots, D_n)$. The working time of the algorithm for constructing all these curves is polynomial in d^n and the size of input. Note that h_{s+1} is identically zero on each C'. So we can choose all the required curves C among constructed

Now the union of all intersections $C \cap \mathcal{Z}(h_{s+1})$ is the required set $W^{(4)}$. Hence, it is sufficient to construct all the intersections $C \cap \mathcal{Z}(h_{s+1})$. The algorithm for this using the Newton–Puiseux expansions in the case when h_{s+1} is a linear form is described in [3], [2]. The general case can be reduced to this one in the following way. Let ξ be a constructed generic point of C and $k_1(\xi)$ be the field generated by coordinates of ξ. So according to [4] ξ is algebraic over a field $k_1(t)$ where $t = D'/D''$ is a rational function on C which is equal to the quotient of two linear forms D' and D'' with coefficients from k and the degree $[k_1(\xi) : k_1(t)]$ is bounded by a polynomial in d^{s+1}. There are at most $\mathcal{P}(d^{s+1})$ (for a polynomial $\mathcal{P}$) values of t from $\overline{k_1}$ in which the specializations of ξ are not defined. The set of these values is included in the set of roots of a polynomial $F_1 \in k_1[t]$ which is known when the generic point is constructed. Herewith $\deg_t F_1 \le \mathcal{P}(d^{s+1})$. Let $N_{k_1(\xi)/k_1(t)}$ denotes the norm from the field $k_1(\xi)$ to the field $k_1(t)$. Compute $N_{k_1(\xi)/k_1(t)}(h_{s+1}(\xi)) = F_2/F_3$ where $F_2, F_3 \in k_1[t]$ and $\deg_t F_2 \le \mathcal{P}(d^{s+1})$, $\deg_t F_1 \le \mathcal{P}(d^{s+1})$. Then the set of values from k_1 which can take t on $C \cap \mathcal{Z}(h_{s+1})$ is included in the set of roots of the polynomial $F = F_1F_2F_3$. Construct all the roots y of this polynomial and the set T_1 of all the points from all the intersection $C \cap \mathcal{Z}(D' - D''y)$ and also $C \cap \mathcal{Z}(D'')$. Then construct the set T_2 of all the points $z \in T_1$ such that $h_{s+1}(z) = 0$. Thus, we get the required set $C \cap \mathcal{Z}(h_{s+1}) = T_2$.

In [3] linear forms $L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)}$ are constructed with integer coefficients of the size $O(n \log d)$. It follows from [3] that for every irreducible component U_1 of W'_s with $U_1 \cap \mathcal{Z}(h_{s+1}) \neq U_1$ the set

$$U_1 \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)})$$

is a finite subset of $\mathbb{P}^n(\overline{k})$. Construct all the points from the set

$$W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)}).$$

Construct a linear form L_0'' with integer coefficients of the size $O(n \log d)$ which is not vanishing in any point of the set $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)})$ and in the point x. So $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_0'', L_{s+2}^{(s+1)}, \dots, L_n^{(s+1)}) = \emptyset$.

Set $L_j = L_j^{(s+1)} - (L_j^{(s+1)}/L_0'')(x)L_0''$ for all $s+2 \le j \le n$ and $L_0 = L_0''$. Then $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_{s+2}, \dots, L_n)$ is a finite set containing x and $W^{(1)} \cap \mathcal{Z}(h_{s+1}) \cap \mathcal{Z}(L_0, L_{s+2}, \dots, L_n) = \emptyset$. Besides that, $L_{s+2}, \dots, L_n$ are linear forms in $X_1, \dots, X_n$ since $x = (1 : 0 : \ldots : 0)$.

Set $V' = W^{(1)} \cap \mathcal{Z}(h_{s+1})$ and $U' = V' \setminus \mathcal{Z}(X_0) \subset \mathbb{A}^n(\overline{k})$. Hence, the dimension of every irreducible component of V' is $n-s-1$ and $x \in V'$.

Our aim now is to construct a family of linear forms $M_0, M_{s+2}, M_{s+3}, \dots, M_n$ with coefficients from $\mathbb{Z}$ of the length $O(n \log d)$ such that $M_0 = L_0$, the forms $M_{s+2}, \dots, M_n \in k[X_1, \dots, X_n]$ and

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset,$$
$$\mathrm{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$$

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

As in Section 2 construct a real structure for the field k, see [2], [3], which induces a real structure on $\overline{k}$. Let $\varepsilon_i > 0$ be an infinitesimal relative to the field $k(\varepsilon_0, \dots, \varepsilon_{i-1})$, $0 \le i \le 2$, and the field $K_2 = k(\varepsilon_0, \varepsilon_1, \varepsilon_2)$.

If $z \in \overline{k(\varepsilon_0, \dots, \varepsilon_i)}$, $0 \le i \le 2$, is not infinitely great relative 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 [3], 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

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

are defined, see [3], for $i = 0, 1, 2$.

Denote $L = \mathcal{Z}(L_{s+2}, \dots, L_n) \subset \mathbb{A}^n(\overline{k})$ 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 $X_1 \ldots, X_n, Y_1 \ldots, Y_n, Z_1, \ldots, Z_n, Z$

$$\begin{cases} h_i(1, Z_1, \ldots, Z_n) = 0, & 1 \leq i \leq s, \\ h_{s+1}(1, Z_1, \ldots, Z_n)Z - 1 = 0, & \\ h_i(1, X_1, \ldots, X_n) = 0, & 1 \leq i \leq s+1, \\ \sum_{1 \leq i \leq n} |X_i - Z_i|^2 \leq \varepsilon_2, & \\ \sum_{1 \leq i \leq n} |X_i|^2 = \varepsilon_1^2, & \\ L_j(Y_1, \ldots, Y_n) = 0, & s+2 \leq j \leq n, \\ \sum_{1 \leq i \leq n} |X_i - Y_i|^2 < \varepsilon_0 \varepsilon_1^2. & \end{cases} \tag{15}$$

LEMMA 8 *Let the family $L_0, L_{s+2}, L_{s+3}, \ldots, L_n$ of linear forms be as above. The following conditions are equivalent*

(i) $\mathrm{con}(x, V') \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \ldots, L_n) = \emptyset$ *in* $\mathbb{P}^n(\overline{k})$

(ii) $\mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n) = \{x\}$ *in* $\mathbb{A}^n(\overline{k})$

(iii) system (15) has no solutions in $\mathbb{A}^{3n+1}(\overline{K_2})$.

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

Suppose that there exists a solution

$$(x_1^*, \ldots, x_n^*, y_1^*, \ldots, y_n^*, z_1^*, \ldots, z_n^*, z') \in \mathbb{A}^{3n+1}(\overline{K_2})$$

of system (15). Denote $x^* = (x_1^*, \ldots, x_n^*)$ and $y^* = (y_1^*, \ldots, y_n^*)$. We have

$$\begin{array}{ll} h_i(1, z_1^* \ldots, z_n^*) = 0, & 1 \leq i \leq s, \\ h_{s+1}(1, z_1^* \ldots, z_n^*) \neq 0, & \\ h_i(1, x_1^* \ldots, x_n^*) = 0, & 1 \leq i \leq s+1, \\ \sum_{1 \leq i \leq n} |x_i^* - z_i^*|^2 \leq \varepsilon_2, & \end{array}$$

Therefore, $\sum_{1 \leq i \leq n} |\mathrm{st}_{\varepsilon_2} x_i^* - z_i^*|^2$ is infinitesimal relative to the field $k(\varepsilon_0, \varepsilon_1)$. The point $\mathrm{st}_{\varepsilon_2} x^*$ is defined over the field $\overline{k(\varepsilon_0, \varepsilon_1)}$. Hence, the polynomials $h_1, \ldots, h_s$ are vanishing in the point $\mathrm{st}_{\varepsilon_2} x^*$. The polynomial h_{s+1} is not vanishing in the point x^* which is infinitesimal close to $\mathrm{st}_{\varepsilon_2} x^*$. Thus, $\mathrm{st}_{\varepsilon_2} x^* \in U'$, c.f. also [3] the proof of Lemma 13. Therefore, the line (the standard parts here are considered in $\mathbb{A}^n$)

$$l = \{(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(\mathrm{st}_{\varepsilon_2} y^* / \varepsilon_1)t \; : \; t \in \overline{k}\} \subset \mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, \ldots, L_n),$$

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

Conversely, suppose that there exists a line $l \subset \mathrm{con}(x, U') \cap \mathcal{Z}(L_{s+2}, \ldots, L_n)$, $x \in l$. Choose a point $x \neq (l_1, \ldots, l_n) \in l \subset \mathbb{A}^n(\overline{k})$. Then there exists an algebraic curve $C \subset \sec(x, U')$ such that $\{(l_1, \ldots, l_n)\}$ is a component of $C \cap \mathcal{Z}(Z)$.

So there exists a branch C^* of C in the point $(l_1, \dots, l_n)$ with a uniformizing element τ such that the corresponding representations of the coordinate functions of C as formal power series has the form

$$Z|_C = z_m \tau^m + \sum_{m<j\in\mathbb{Z}} z_j \tau^j,$$
$$X_i|_C = l_i + \sum_{0<j\in\mathbb{Z}} x_{i,j}\tau^j, \quad 1 \le i \le n$$

where $0 < m \in \mathbb{Z}$, $z_j, x_{i,j} \in \overline{k}$ for all j, $z_m \neq 0$. Consider the irreducible algebraic curve C_1 which has the branch C_1^* in the point x with a uniformizing element τ such that

$$X_i|_{C_1} = (z_m\tau^m + \sum_{m<j\in\mathbb{Z}} z_j\tau^j)(l_i + \sum_{0<j\in\mathbb{Z}} x_{i,j}\tau^j), \quad 1 \le i \le n.$$

Then C_1 is contained in U' and has the tangent line l. Choose a new uniformizing element τ_1 of the branch C_1^* such that $\tau_1 \in \overline{k}(C_1)$ where $\overline{k}(C_1)$ is the field of rational functions on C_1. So we have

$$X_i|_{C_1} = w_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} w_{i,j}\tau_1^j, \quad 1 \le i \le n$$

where $w_{i,j} \in \overline{k}$ for all j and $x \neq (w_{1,m}, \dots, w_{n,m}) \in l$. Denote $X_i|_{C_1} = w_i$ for $1 \le i \le n$. So $(w_1, \dots, w_n) \in C_1$ in $\mathbb{A}^n(\overline{k((\tau_1))})$ where $k((\tau_1))$ is a field of formal power series in τ_1 and $(w_1, \dots, w_n)$ corresponds to the embedding $\overline{k}[C_1] \hookrightarrow \overline{k}[[\tau_1]]$ where $\overline{k}[C_1]$ is the ring of regular functions on C_1 and $\overline{k}[[\tau_1]]$ is the ring of formal power series in τ_1.

Let the real structure of $\overline{k}$ be given by the isomorphism $\overline{k} \simeq \widetilde{K}[\sqrt{-1}]$ where $\widetilde{K}$ is a real closed field. By the definition the real structure on the field $\overline{k(\varepsilon_1)}$ is induced by the real structure on the field of fractional power series in ε_1 with coefficient from $\overline{k}$. The real elements from this field are fractional power series with coefficients from $\widetilde{K}$.

Let us show that there exists a point $x^* \in C_1$ in $\mathbb{A}^n(\overline{k(\varepsilon_1)})$ such that $|x^*|^2 = \varepsilon_1^2$ and $x \neq \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1) \in l$. Besides that, this point x^* will be defined by a through homomorphism

$$\overline{k}[C_1] \hookrightarrow \overline{k}[[\tau_1]] \to \overline{k}[[\varepsilon_1^{1/m}]]$$

such that $\tau_1 \mapsto \tau^* \in \widetilde{K}[[\varepsilon_1^{1/m}]]$. Here $\overline{k}[[\varepsilon_1^{1/m}]]$ is the ring of formal power series in $\varepsilon_1^{1/m}$.

To prove this assertion represent $w_{i,j} = u_{i,j} + \sqrt{-1}v_{i,j}$ where $u_{i,j}, v_{i,j} \in \widetilde{K}$ for all i, j. Set

$$u_i = u_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} u_{i,j}\tau_1^j, \; v_i = v_{i,m}\tau_1^m + \sum_{m<j\in\mathbb{Z}} v_{i,j}\tau_1^j, \; 1 \le i \le n.$$

So $w_i = u_i + \sqrt{-1} v_i$ for $1 \le i \le n$.

The functions w_i are algebraic over the field $\overline{k}(\tau_1)$ and hence they are algebraic over the field $\widetilde{K}(\tau_1)$ for $1 \le i \le n$. We have the embedding $\overline{k}[C_1] \hookrightarrow \widetilde{K}[\sqrt{-1}]((\tau_1))$ of $\overline{k}[C_1]$ into the field of formal power series $\widetilde{K}[\sqrt{-1}]((\tau_1))$. Therefore, the functions $u_i - \sqrt{-1} v_i$ are also algebraic over the field $\widetilde{K}(\tau_1)$. Hence u_i, v_i are algebraic over $\widetilde{K}(\tau_1)$ and over $\overline{k}(\tau_1)$ for all $1 \le i \le n$.

There exists a formal power series $\tau^* \in \widetilde{K}((\varepsilon_1^{1/m}))$ such that

$$\tau^* = (\sum_{1 \le i \le n} |w_{i,m}|^2)^{-1/(2m)} \varepsilon_1^{1/m} + \sum_{m < j \in \mathbb{Z}} \tau_j^* \varepsilon_1^{j/m}, \ \tau_j^* \in \widetilde{K}$$

and the substitution $\tau_1 \mapsto \tau^*$ defines the homomorphism $\psi : \overline{k}[[\tau_1]] \to \overline{k}[[\varepsilon_1^{1/m}]]$ for which $\sum_{1 \le i \le n} (u_i^2 + v_i^2)|_{\tau_1 = \tau^*} = \varepsilon_1^2$ (it is just the inversion of a function in the ring of formal power series).

The element $\tau^* \in \overline{k(\varepsilon_1)}$ since ψ is a homomorphism and $\sum_{1 \le i \le n} (u_i^2 + v_i^2)$ and τ_1 are algebraically independent over $\overline{k}$. Now set $x_i^* = w_i|_{\tau_1 = \tau^*}$ for $1 \le i \le n$. Then similarly $x_i^* \in \overline{k(\varepsilon_1)}$ for $1 \le i \le n$. Set $x^* = (x_1^*, \ldots, x_n^*)$. Then $x^* \in C_1$, $|x^*|^2 = \varepsilon_1^2$ and $x \ne \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1) \in l$ since ψ is a homomorphism. Our assertion is proved.

Set $y^* = \varepsilon_1 \mathrm{st}_{\varepsilon_1}(x^*/\varepsilon_1)$. Since $x^* \in W^{(1)} \cap \mathcal{Z}(h_{s+1})$ there exists a point $z^* \in \mathbb{A}^n(\overline{K_2})$ such that $(x^*, y^*, z^*, h_{s+1}(z^*)^{-1})$ gives a solution of system (15). The lemma is proved.

Return to the description of the algorithm. Decide whether system (15) has a solution. If system (15) has no solutions then by Lemma 8 we can set $M_i = L_i$ for $i = 0, s+2, \ldots, n$. Suppose that system (15) has a solution. Construct such a solution $(x^*, y^*, z^*, h_{s+1}(z^*)^{-1}) \in \mathbb{A}^{3n+1}(\overline{K_2})$, see [2], [3]. Recall that $L = \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n)$. Construct, see the proof of Lemma 8, the line

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

Construct a linear forms L_1 in $X_1, \ldots, X_n$ such that L_1 is not identically zero on the line l. Denote $L' = \mathcal{Z}(L_1, L_{s+2}, L_{s+3}, \ldots, L_n)$. This is a linear subspace such that $L' + l = L$.

Define the line

$$l' = \{x^* t \ : \ t \in \overline{K_2}\}.$$

Construct the linear subspace $L' + l'$. Then the subspace $L' + l'$ is infinitely close to $L' + l$ since x^*, y^* are obtained from a solution of (15). The subspace $L' + l' = \mathcal{Z}(L'_{s+2}, \ldots, L'_n)$ in $\mathbb{A}^n(\overline{K_2})$ where $L'_j = L_j - \delta_j L_1$ and δ_j are infinitesimal relative to the field k for $s+2 \le j \le n$. Construct such linear forms $L'_{s+2}, \ldots, L'_n \in \overline{K_2}[X_1, \ldots, X_n]$. Set also $L'_0 = L_0$.

Now by Proposition 2 we have

$$\#V' \cap \mathcal{Z}(L_{s+2}, \dots, L_n) \le \#V' \cap \mathcal{Z}(L'_{s+2}, \dots, L'_n) < +\infty.$$

Further, there exist two points $x, x^* \in V' \cap \mathcal{Z}(L'_{s+2}, L'_{s+3}, \dots, L'_n)$ such that their standard parts in $\mathbb{P}^n(\overline{k})$ are equal to x. Therefore,

$$N = \#V' \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \dots, L_n) < \#V' \cap \mathcal{Z}(L'_{s+2}, L'_{s+3}, \dots, L'_n) = N'.$$

Set $M_0 = L_0$. Now our aim is to apply the analog of the second auxiliary algorithm from [3] to the linear forms $L'_0, L'_{s+2}, \dots, L'_n$ and construct linear forms $M_{s+2}, \dots, M_n$ in $X_1, \dots, X_n$ which have integer coefficients with lengths $O(n \log d)$ such that $\#V' \cap \mathcal{Z}(M_{s+2}, \dots, M_n) \ge N'$ and $V' \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$. Note here that the second condition can be checked effectively during this auxiliary algorithm. Indeed, suppose we replace one coefficient, say in M_{s+2} (we do not introduce new notations for linear forms which appear during the second auxiliary algorithm but use for them the notation $M_{s+2}, \dots, M_n$). Then as it is known from the previous step of the implemented algorithm $\#V' \cap \mathcal{Z}(M_0, M_{s+3}, \dots, M_n) < +\infty$ and, therefore, the points from this set can be computed as it was described above. Further we can substitute the coordinates of these points in M_{s+1} with the replaced coefficient and therefore decide whether $V' \cap \mathcal{Z}(M_0, M_{s+2}, \dots, M_n) = \emptyset$ for new obtained linear forms.

If this second condition is satisfied then $\#V' \cap \mathcal{Z}(M_{s+2}, \dots, M_n) < +\infty$ and the first condition can be also verified as it was described above. Thus, we can apply the analog of the second auxiliary algorithm from [3] to the linear forms $L'_0, L'_{s+2}, \dots, L'_n$ and construct the required linear forms $M_{s+2}, \dots, M_n$ in $X_1, \dots, X_n$.

After that, return recursively to the beginning of the algorithm described replacing the forms $L_0, L_{s+2}, \dots, L_n$ by $M_0, M_{s+2}, \dots, M_n$. Since $N' > N$ there are at most d^{s+1} such returns in the algorithm.

So we shall obtain finally by Lemma 8 a family of linear forms $M_0, M_{s+2}, M_{s+3}, \dots, M_n$ such that $M_0 = L_0$, the forms $M_{s+2}, \dots, M_n \in k[X_1, \dots, X_n]$ have integer coefficients with lengths $O(n \log d)$,

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset,$$
$$\mathrm{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \dots, M_n) = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. We shall suppose replacing as described above the forms $L_0, L_{s+2}, \dots, L_n$ by $M_0, M_{s+2}, \dots, M_n$ that these properties are satisfied for $L_0, L_{s+2}, \dots, L_n$, i.e. the forms $L_{s+2}, L_{s+3}, \dots, L_n \in k[X_1, \dots, X_n]$ have integer coefficients with lengths $O(n \log d)$ and

$$V' \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \dots, L_n) = \emptyset,$$
$$\mathrm{con}(x, V') \cap \mathcal{Z}(L_0, L_{s+2}, L_{s+3}, \dots, L_n) = \emptyset$$

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

Construct, see above, all the points x_u, $1 \le u \le N$, from the set

$$V' \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n)$$

in $\mathbb{P}^n(\overline{k})$. We can suppose without loss of generality that $x_1 = x$. Construct a linear form L_{s+1} in $X_1, \ldots, X_n$ with coefficients from $\mathbb{Z}$ of the length $O(n \log d)$ such that $L_{s+1}(x_u) \ne 0$ for all $2 \le j \le N$. Denote by

$$p_x \,:\, V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_{s+1} : L_{s+2} : \ldots : L_n)$$

the linear projection.

5 Background lemmas

Let $W \subset \mathbb{P}^n(\overline{k})$ be an irreducible algebraic variety of the dimension $\dim W = n - s - 1$ and $L_{s+1}, L_{s+2}, \ldots, L_n \in \overline{k}[X_1, \ldots, X_n]$ be linear forms. Consider the following conditions. The intersection

$$W \cap \mathcal{Z}(L_{s+1}, \ldots, L_n) \setminus \{x\} = \emptyset. \tag{16}$$

The equality (16) holds and the projection

$$p \,:\, W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_{s+1} : L_{s+2} : \ldots : L_n)$$

is a dominant morphism, i.e. the closure in the Zariski topology

$$\overline{p(W \setminus \{x\})} = \mathbb{P}^{n-s-1}(\overline{k}). \tag{17}$$

The intersection

$$\mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+1}, L_{s+2}, \ldots, L_n) \setminus \{x\} = \emptyset \quad \text{if} \quad x \in W. \tag{18}$$

LEMMA 9 *Let $W \subset \mathbb{P}^n(\overline{k})$ be an irreducible algebraic variety of the dimension $\dim W = n - s - 1$ and the linear forms $L_{s+1}, L_{s+2}, \ldots, L_n \in \overline{k}[X_1, \ldots, X_n]$ satisfy condition (16). Let*

$$1 < \# W \cap \mathcal{Z}(L_{s+2}, \ldots, L_n) < +\infty$$

in $\mathbb{P}^n(\overline{k})$. Then the morphism p is dominant, i.e. the equality (17) holds.

PROOF Indeed, we should show that the closure F in the Zariski topology of the image $p(W \setminus \{x\})$ coincides with $\mathbb{P}^{n-s-1}(\overline{k})$. By Proposition 2 for every $\lambda_{s+2}, \ldots, \lambda_n \in \overline{k(\varepsilon)}$ which are infinitesimal relative to the field k the set

$W \cap \mathcal{Z}(L_{s+2} - \lambda_{s+2}L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) \setminus \{x\} \neq \emptyset$ in $\mathbb{P}^n(\overline{k(\varepsilon)})$. Therefore, $p^{-1}((1 : \lambda_{s+2} : \ldots : \lambda_n))$ is not empty in $\mathbb{P}^{n-s}(\overline{k(\varepsilon)})$. Therefore,

$$F(\overline{k(\varepsilon)}) = \mathbb{P}^{n-s-1}(\overline{k(\varepsilon)}),$$

and hence, $F = \mathbb{P}^{n-s-1}(\overline{k})$. The lemma is proved.

Lemma 9 implies that condition (17) is satisfied for any component W of V' such that there exists $x_u \in W$, $u \geq 2$, and the linear forms $L_{s+1}, L_{s+2}, \ldots, L_n$ constructed in Section 4.

Denote by $\mathcal{H}$ the set of all families H of $n-s$ linear forms $H_{s+1}, H_{s+2}, \ldots, H_n \in \overline{k}[X_1, \ldots, X_n]$. We can identify $\mathcal{H}$ with the algebraic variety $\mathbb{A}^{(n-s)n}(\overline{k})$.

Denote by $\mathcal{H}_1$ the subset of $\mathcal{H}$ consisting of all families H of $n-s$ linear forms $H_{s+1}, H_{s+2}, \ldots, H_n$ such that

$$W \cap \mathcal{Z}(H_{s+1}, H_{s+2}, \ldots, H_n) = \{x\}.$$

LEMMA 10 *Let $W \subset \mathbb{P}^n(\overline{k})$ be an irreducible algebraic variety of the dimension $\dim W = n-s-1$ such that there are linear forms $L_{s+1}, L_{s+2}, \ldots, L_n \in \overline{k}[X_1, \ldots, X_n]$ satisfying (16) and (17). Then $\mathcal{H}_1$ contains a non-empty open subset of $\mathcal{H}$ in the Zariski topology.*

PROOF Indeed, denote by

$$\pi : \mathbb{P}^n \setminus \{x\} \to \mathbb{P}^{n-1}, \ (X_0 : \ldots : X_n) \mapsto (X_1 : \ldots : X_n)$$

the linear projection Note that the closure in the Zariski topology of the image $\pi(W \setminus \{x\})$ is an irreducible variety of the dimension $n-s-1$ since the closure in the Zariski topology of $p(W \setminus \{x\})$ is $\mathbb{P}^{n-s-1}$. Hence there exist homogeneous polynomials $F_1, \ldots, F_s \in K[X_1 \ldots, X_n]$ such that $\dim \mathcal{Z}(F_1, \ldots, F_s) = n-s-1$ in $\mathbb{P}^{n-1}$ and $\pi(W \setminus \{x\}) \subset \mathcal{Z}(F_1, \ldots, F_s)$. The condition

$$T = \mathcal{Z}(F_1, \ldots, F_s, H_{s+1}, H_{s+2}, \ldots, H_n) = \emptyset$$

in $\mathbb{P}^{n-1}(\overline{k})$ implies that $W \cap \mathcal{Z}(H_{s+1}, H_{s+2}, \ldots, H_n) \setminus \{x\} = \emptyset$. But $T = \emptyset$ is equivalent to the condition that at least one coefficient of the corresponding U–resultant is not equal to zero. Now the assertion of the lemma follows from the fact that the coefficients of the U–resultant are polynomials in coefficients of linear forms $H_{s+1}, H_{s+2}, \ldots, H_n$. The lemma is proved.

LEMMA 11 *Let $W \subset \mathbb{P}^n(\overline{k})$ be an irreducible algebraic variety of the dimension $\dim W = n-s-1$ such that there are linear forms $L_{s+1}, L_{s+2}, \ldots, L_n \in$*

$\overline{k}[X_1, \ldots, X_n]$ *satisfying condition (18). Let* $x \in W$. *Then there exists a non–empty open subset* U_4 *of* $\mathbb{P}^{n-s-1}(\overline{k})$ *such that* $U_4 \subset \mathbb{P}^{n-s-1}(\overline{k}) \setminus \mathcal{Z}(L_{s+1})$ *and if* $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$ *then*

$$\mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \{x\}.$$

PROOF We have $\dim \pi(\mathrm{con}(x, W) \setminus \{x\}) \leq n - s - 2$ and

$$\pi(\mathrm{con}(x, W) \setminus \{x\}) \cap \mathcal{Z}(L_{s+1}, \ldots, L_n) = \emptyset.$$

Thus, there exists a non–empty open subset $U_4 \subset \mathbb{P}^{n-s-1}(\overline{k}) \setminus \mathcal{Z}(L_{s+1})$ such that if $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$ then

$$\pi(\mathrm{con}(x, W) \setminus \{x\}) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \emptyset.$$

Therefore, if $(1 : \lambda_{s+1} : \ldots : \lambda_n) \in U_4$ then

$$\mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \ldots, L_n - \lambda_n L_{s+1}) = \{x\}.$$

The lemma is proved.

Let W be an irreducible algebraic variety from the formulation of Lemma 10 and H be a family of $n - s$ linear forms $H_{s+1}, H_{s+2}, \ldots, H_n$ in $X_1, \ldots, X_n$ with coefficients from $\overline{k}$. Let $H \in \mathcal{H}_1$. Denote by $p(H) : W \setminus \{x\} \to \mathbb{P}^{n-s-1}$ the projection corresponding to p if we replace $L_{s+1}, L_{s+2}, \ldots, L_n$ by $H_{s+1}, H_{s+2}, \ldots, H_n$. Set

$$\begin{aligned} &U_3(H) = \{z \in \mathbb{P}^{n-s} : \#p(H)^{-1}(z) < +\infty\}, \\ &\delta(H) = \sup\{\#p(H)^{-1}(z) : z \in U_3(H)\}, \\ &U(H) = \{z \in U_3(H) : \#p(H)^{-1}(z) = \delta(H)\}, \\ &\delta = \sup\{\#p(H)^{-1}(z) : z \in U_3(H), H \in \mathcal{H}_1\}. \end{aligned} \tag{19}$$

Note that if $H \in \mathcal{H}_1$ and the projection $p(H)$ is not dominant then by Lemma 9 $\delta(H) = 0$ and $U_3(H) = U(H)$ contains a non–empty open in the Zariski topology subset of $\mathbb{P}^{n-s-1}(\overline{k})$.

Denote by $\widetilde{H}$ the family $\widetilde{H}_{s+1}, \widetilde{H}_{s+2}, \ldots, \widetilde{H}_n$ which is a the generic element of $\mathcal{H}_1$, i.e. the field K generated by the coefficients of linear forms from $\widetilde{H}$ over k is purely transcendental over $\overline{k}$ of the transcendency degree $(n - s)n$.

LEMMA 12 *Let* W *be as in the formulation of Lemma 10 and* $H \in \mathcal{H}_1$ *be such that the projection* $p(H)$ *is a dominant morphism. Then* $0 < \delta(H) < +\infty$ *and* $U(H)$ *contains a non–empty open in the Zariski topology subset* U *of* $\mathbb{P}^{n-s-1}(\overline{k})$ *such that for every* $x^* \in U$ *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

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

is an 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 Let $Y \in \overline{k}[X_0, \dots, X_n]$ be a linear form. Consider the linear projection

$$p_1 : W \setminus \{x\} \longrightarrow \mathbb{P}^{n-s}(\overline{k}), \quad (X_0 : \dots : X_n) \mapsto (Y : H_{s+1} : H_{s+2} : \dots : H_n).$$

Since $p(H)$ is a dominant morphism there exists an irreducible homogeneous polynomial $G \in \overline{k}[Y, H_{s+1}, H_{s+2}, \dots, H_n]$ such that the closure of $p_1(W)$ in the Zariski topology $\overline{p_1(W)} = \mathcal{Z}(G)$ and $p_1(W)$ contains an open subset of the closed set $\mathcal{Z}(G)$.

By the theorem about 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 induces the birational isomorphism $W \setminus \{x\} \longrightarrow \mathcal{Z}(G)$ 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 $\mathcal{Z}(G)$ and p_2 induces the isomorphism $U_1 \to p_2(U_1)$.

Denote $U_2 = \mathcal{Z}(G) \setminus \mathcal{Z}(H_{s+1}, H_{s+2}, \dots, H_n)$. There exists a projection $p_3 : U_2 \longrightarrow \mathbb{P}^{n-s}(\overline{k})$ such that $p = p_3 \circ p_2$ (on the open subset where the right and left parts are defined). Denote by $R = \mathrm{Res}_Y(G, G'_Y)$ the discriminant of the polynomial G relatively to Y. Then $0 \neq R$ is a homogeneous polynomial since G is a separable homogeneous polynomial.

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 U_2 and the differential of p_3 in the point y

$$d_y p_3 : T_{y, U_2} \longrightarrow T_{x, \mathbb{P}^{n-s}}$$

is an isomorphism of tangent spaces $T_{y, p_1(W)}$ and $T_{x, \mathbb{P}^{n-s}}$ of the varieties U_2 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 $R(x^*) \neq 0$.

Denote by F the closure in the Zariski topology of the set $p_3(U_2 \setminus p_2(U_1))$ Set $U = \mathbb{P}^{n-s-1}(\overline{k}) \setminus (\mathcal{Z}(R) \cup F)$ (hence $U \neq \emptyset$). Then for every $x^* \in U$

(a) the cardinality $\# p(H)^{-1}(x^*) = \deg_Y G$,

(b) for every $y \in p(H)^{-1}(x^*)$ 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 an 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.

Let $\varepsilon > 0$ be an infinitesimal relative to the field K. Now if $z^* \in U(H)$ there is a point $z \in U$ in $\mathbb{P}^{n-s-1}(\overline{K(\varepsilon)})$ which is infinitesimal close to z^*. Hence, by Proposition 2 $\# p(H)^{-1}(z^*) \leq \# p(H)^{-1}(z)$. Therefore, $\delta(H) = \deg_Y G$ and $U \subset U(H)$. The lemma is proved.

LEMMA 13 *Let W be as in the formulation of Lemma 10. For every $z \in U(\widetilde{H})$ the equalities*

$$\delta = \delta(\widetilde{H}) = \# p(\widetilde{H})^{-1}(z)$$

hold. Therefore, δ is an integer which depends only on W and x.

PROOF The equality $\delta(\widetilde{H}) = \# p(\widetilde{H})^{-1}(z)$ follows from Lemma 12. Further, if $H \in \mathcal{H}_1$ and $z \in U_3(H)$ are arbitrary then we can set the coefficients of the forms $H_j - \widetilde{H}_j$ to be infinitesimals for all j and by Proposition 2 the point $z \in U_3(\widetilde{H})$ and $\# p(\widetilde{H})^{-1}(z) \geq \# p(H)^{-1}(z)$. Hence, $\delta = \delta(\widetilde{H})$. The lemma is proved.

LEMMA 14 *Let $q : V_1 \to V_2$ be a dominant regular morphism of irreducible algebraic varieties V_1 and V_2 defined over the field k. Let $\dim V_1 = \dim V_2$. Let $z \in V_2$ and*

$$\# q^{-1}(z) = [k(V_1) : k(V_2)],$$

i.e. the number of elements of the inverse image of the point z coincides with the degree of the extension of the fields of rational functions of V_1 and V_2. Then there is an open in the Zariski topology subset $U' \subset V_2$ such that $z \in U'$ and the morphism

$$q^{-1}(U') \to U'$$

induced by q is finite.

PROOF Denote $[k(V_1) : k(V_2)] = \alpha$. Denote by $\widetilde{V}_i$, $i = 1, 2$, the normalization of the algebraic variety V_i in the field $k(V_1)$, see [9], [3]. So we have the commutative diagram of morphisms of algebraic varieties

$$\begin{array}{ccc} \widetilde{V}_1 & \xrightarrow{\widetilde{q}} & \widetilde{V}_2 \\ {\scriptstyle \pi_1}\big\downarrow & & {\scriptstyle \pi_2}\big\downarrow \\ V_1 & \xrightarrow{q} & V_2 \end{array}$$

where π_1 and π_2 are finite morphisms and $\widetilde{q}$ is a birational isomorphism induced by q. We have $\# \pi_2^{-1}(z) \leq \alpha$ since π_2 is finite. By the Zariski main theorem $\widetilde{q}$ is invertible in some neighborhood in the Zariski topology of every point $z' \in \pi_2^{-1}(z)$ if $\widetilde{q}^{-1}(z') \neq \emptyset$. Hence, $\# \pi_2^{-1}(z) \geq \# \pi_1^{-1}(q^{-1}(z))$. But $\# q^{-1}(z) = \alpha$. Therefore, $\# \pi_2^{-1}(z) = \# \pi_1^{-1}(q^{-1}(z))$ and $\widetilde{q}$ is invertible in some neighborhood in the Zariski topology U'' of the finite set $\pi_2^{-1}(z)$. So we have the isomorphism of algebraic varieties

$$\widetilde{q}^{-1}(U'') \simeq U''$$

induced by $\widetilde{q}$. Set $U' = V_2 \setminus \pi_2(\widetilde{V}_2 \setminus U'')$. Then $z \in U'$ and the morphism

$$\pi_1^{-1}(q^{-1}(U')) = \widetilde{q}^{-1}(\pi_2^{-1}(U')) \to U'$$

is finite. Hence, the morphism $q^{-1}(U') \to U'$ is also finite. The lemma is proved.

LEMMA 15 *Let $W \subset \mathbb{P}^n(\overline{k})$ be an irreducible algebraic variety of the dimension* $\dim W = n-s-1$ *and the linear forms $L_{s+1}, L_{s+2}, \dots, L_n \in \overline{k}[X_1, \dots, X_n]$ satisfy (16), (17) and (18). Then*

(i) there exists a non–empty open in the Zariski topology subset U of $\mathbb{P}^{n-s}(\overline{k})$ such that for every $x^* \in U$ the cardinality $\#p^{-1}(x^*) = \delta > 0$, and δ is an integer defined in (19) which depends only on W and x.

(ii) if for some point $x^* \in \mathbb{P}^{n-s}(\overline{k})$ the cardinality $\#p^{-1}(x^*) = \delta$ then 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

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

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.

(iii) if for some point $x^* \in \mathbb{P}^{n-s}(\overline{k})$ the cardinality $\#p^{-1}(x^*) < +\infty$ then $\#p^{-1}(x^*) \le \delta$.

PROOF The family $L_{s+1}, \dots, L_n$ belongs to $\mathcal{H}_1$. Set in Lemma 12 the family H to be $L_{s+1}, \dots, L_n$. We shall use the notations Y, p_1, p_2, p_3, G, R, U from the proof of Lemma 12 and U_4 from Lemma 11. Let us show that $\deg_Y G = \delta$. Set the coefficients of the forms $\widetilde{H}_j - L_j$ to be infinitesimals relative the field k for all j. So the map of the standard part

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

is defined. Thus, by Proposition 2 for every $x^* \in U \cap U(\widetilde{H}) \cap U_4$ for every $y^* \in p(\widetilde{H})^{-1}(x^*)$ the element $y = \mathrm{st}\, y^* \in p^{-1}(x^*)$ or $x = \mathrm{st}\, y^*$. The differential of p in the point $y \in p^{-1}(x^*)$ is an isomorphism. If $y \in p^{-1}(x^*)$ then by the implicit function theorem there exists a unique $y' \in p(\widetilde{H})^{-1}(x^*)$ such that $\mathrm{st}(y') = y$. Hence, in this case $y' = y^*$.

Let us show that there exists no y^* such as above for which $x = \mathrm{st}\, y^*$. Indeed, suppose contrary, that $x = \mathrm{st}\, y^*$. Denote $y^* = (y_1^*, \dots, y_n^*) \in \mathbb{A}^n(\overline{k})$ and $x^* = (1 : \lambda_{s+1} : \ldots : \lambda_n)$. Set $|y^*| = (\sum_{1 \le i \le n} |y_i^*|^2)^{1/2}$. Then

$$x \ne \mathrm{st}(y^*/|y^*|) \in \mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2} - \lambda_{s+1} L_{s+1}, \dots, L_n - \lambda_n L_{s+1})$$

since if $F \in \overline{k}[X_1, \dots, X_n]$, $F(y^*) = 0$ and F_r is the form of the least degree of F then $F_r(\mathrm{st}(y^*/|y^*|)) = 0$. A contradiction is obtained which proves our assertion.

Thus,

$$\delta = \#p(\widetilde{H})^{-1}(x^*) = \#p^{-1}(x^*) = \deg_Y G$$

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

Now (iii) follows from (i) and the definition of δ.

To prove (ii) note that by Lemma 14 (with k replaced by $\overline{k}$) for every point x^* with $\#p^{-1}(x^*) = \delta = [\overline{k}(W) : \overline{k}(\mathbb{P}^{n-s-1})]$ (here the inclusion $\overline{k}(\mathbb{P}^{n-s-1}) \subset \overline{k}(W)$ of fields rational functions is induced by p) there exists an open set U' in the Zariski topology such that $x^* \in U'$ and the morphism $p^{-1}(U') \to U'$ induced by p is finite. Now there exists a linear form Y such that the corresponding p_1 is birational, $\#p_1(p^{-1}(x^*)) = \delta$. We have for this form $(\mathrm{lc}_Y G)(x^*) \neq 0$ since the morphism $p^{-1}(U') \to U'$ is finite and $x^* \in U'$. Hence $p_3^{-1}(x^*) < +\infty$. Therefore, $p_3^{-1}(x^*) = p_1(p^{-1}(x^*)) = \delta$. Hence, $R(x^*) \neq 0$.

Further, if $R(x^*) \neq 0$, $\#p^{-1}(x^*) = \delta$ 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, by the Zariski main theorem the local rings

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

Thus, p_1 is an isomorphism in the neighbourhood of each point $y \in p^{-1}(x^*)$. From here and (a) and (b) proved above assertion (ii) follows immediately. The Lemma is proved.

COROLLARY 3 *Under the conditions of Lemma 15 the multiplicity* $\mu(x, V_{s+1}) = \deg V_{s+1} - \delta$.

PROOF This follows immediately from the definition of the multiplicity (1) given in the Introduction and lemmas proved in this Section.

REMARK 5 *As it follows from Corollary 4 from Lemma 16, see below, Lemma 15 and Corollary 3 are also valid when the condition (17) is not satisfied. In this case* $\delta = 0$ *and* $W = \mathrm{con}(x, W)$.

LEMMA 16 *Let* W *be an irreducible an irreducible algebraic variety of the dimension* $n-s-1$ *and linear forms* $L_0, L^{(i)}_{s+2}, \ldots, L^{(i)}_n \in \overline{k}[X_0, \ldots, X_n]$, $i = 0, 1$ *be such that*

$$\begin{aligned}
&L^{(i)}_{s+2}, \ldots, L^{(i)}_n \in \overline{k}[X_1, \ldots, X_n],\\
&W \cap \mathcal{Z}(L_0, L^{(0)}_{s+2}, \ldots, L^{(0)}_n) = \emptyset,\\
&\mathrm{con}(x, W) \cap \mathcal{Z}(L_0, L^{(0)}_{s+2}, \ldots, L^{(0)}_n) = \emptyset \quad \textit{if} \quad x \in W,\\
&W \cap \mathcal{Z}(L^{(1)}_{s+2}, \ldots, L^{(1)}_n) < +\infty
\end{aligned}$$

in $\mathbb{P}^n(\overline{k})$. Further, let all the points of $W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) \setminus \{x\}$ be smooth and the differentials of the projection

$$p^{(0)} : W \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}), \quad (X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+2}^{(0)} : \ldots : L_n^{(0)})$$

are isomorphisms in all the points from $W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) \setminus \{x\}$. Then

$$\# W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) \geq \# W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots, L_n^{(1)}).$$

PROOF Suppose contrary, that

$$\# W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) < \# W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots, L_n^{(1)}).$$

Let $\varepsilon > 0$ be an infinitesimal relative to the field k. So the map of the standard part

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

is defined.

We have, c.f. [4], $+\infty > \# W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0, \ s+2 \leq j \leq n\} \geq \# W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots, L_n^{(1)})$ (here one can use Proposition 2 if only for a moment one considers $1/\varepsilon$ as an infinitesimal). Let $x^* \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0, \ s+2 \leq j \leq n\}$. Then $\mathrm{st}(x^*) \in W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)})$ by Proposition 2. The differentials of the projection $p^{(0)}$ are isomorphisms in all the point from $W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) \setminus \{x\}$. Thus, by the implicit function theorem (applied to formal power series) for every $x'' \in W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) \setminus \{x\}$ there exists a unique $x^* \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0, \ s+2 \leq j \leq n\}$ such that $\mathrm{st}(x^*) = x''$. Hence, $x \in W$ and there exists at least one $x' \in W \cap \{L_j^{(0)} + \varepsilon L_j^{(1)} = 0, \ s+2 \leq j \leq n\}$ such that $\mathrm{st}(x') = x$.

Denote $x' = (x'_1, \ldots, x'_n) \in \mathbb{A}^n$. Set $|x'| = (\sum_{1 \leq i \leq n} |x'_i|^2)^{1/2}$. We have $\mathrm{st}(x') = x$ and, therefore,

$$x \neq \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, W) \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)})$$

since if $F \in \overline{k}[X_1, \ldots, X_n]$, $F(x') = 0$ and F_r is the form of the least degree of F then $F_r(\mathrm{st}(x'/|x'|)) = 0$. A contradiction is obtained. The lemma is proved.

COROLLARY 4 *Let W and $L_{s+2}^{(i)}, \ldots, L_n^{(i)}$, $i = 1, 2$, be as in the formulation of Lemma 16. Let*

$$W \cap \mathcal{Z}(L_{s+2}^{(0)}, \ldots, L_n^{(0)}) = \{x\}.$$

Then

$$W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots, L_n^{(1)}) = \{x\}.$$

More than that, in this case $W = \mathrm{con}(x, W)$.

PROOF It is necessary to prove only the last statement. Consider the projection $\pi : \mathbb{P}^n(\overline{k}) \setminus \{x\} \to \mathbb{P}^{n-1}(\overline{k})$ defined in the proof of Lemma 10.

Let us show that the closure W_1 in the Zariski topology of $\pi(W \setminus \{x\})$ has the dimension $n-s-2$. Indeed, otherwise this dimension is equal to $n-s-1$. Hence there exist linear forms $H_{s+1}, H_{s+2}, \ldots, H_n$ in $\overline{k}[X_1, \ldots, X_n]$ such that

$$W_1 \cap \mathcal{Z}(H_{s+1}, \ldots, H_n) = \emptyset.$$

Therefore, the morphism of $W \setminus \{x\} \to \mathbb{P}^{n-s-1}(\overline{k})$, $(X_0 : \ldots : X_n) \mapsto (H_{s+1} : \ldots : H_n)$ is dominant. Hence there exists $z_1, \ldots, z_n \in \overline{k}$ such that

$$W \cap \mathcal{Z}(H_{s+2} - z_{s+2}H_{s+1}, \ldots, H_n - z_n H_{s+1}) \setminus \{x\}$$

is a non–empty finite set. Now set $L_j^{(1)} = H_j - z_j H_{s+1}$, $s+2 \le j \le n$. Hence $\# W \cap \mathcal{Z}(L_{s+2}^{(1)}, \ldots, L_n^{(1)}) \setminus \{x\} \ge 1$ which is a contradiction. Our assertion is proved.

Now the irreducible algebraic variety $\pi^{-1}(W_1) \supset W \setminus \{x\}$ and $\dim \pi^{-1}(W_1) = \dim W$. Hence $W = \mathrm{con}(x, W) = \pi^{-1}(W_1) \cup \{x\}$. The corollary is proved.

6 Conclusion of the description of the algorithm for computing the multiplicity

Our aim now is to construct a family of linear forms $M_0, M_{s+2}, M_{s+3}, \ldots, M_n$ such that $M_0 = L_0$, the forms $M_{s+2}, M_{s+3}, \ldots, M_n \in k[X_1, \ldots, X_n]$ have the coefficients from $\mathbb{Z}$ of the length $O(n \log d)$,

$$V' \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \ldots, M_n) = \emptyset,$$

$$\mathrm{con}(x, V') \cap \mathcal{Z}(M_0, M_{s+2}, M_{s+3}, \ldots, M_n) = \emptyset$$

in $\mathbb{P}^n(\overline{k})$, all the points from $V' \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots, M_n) \setminus \{x\}$ are smooth points of the variety V', and the intersection of tangent spaces

$$T_{x_1, V'} \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots, M_n) = \{x_1\}$$

for every point $x_1 \in V' \cap \mathcal{Z}(M_{s+2}, M_{s+3}, \ldots, M_n) \setminus \{x\}$.

Recall that in Section 4 the points x_u, $1 \le u \le N$ are constructed, herewith $x_1 = x$. 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 [2], [3], which induces a real structure on $\overline{k}$.

Let the infinitesimals $\varepsilon_0, \varepsilon_1, \varepsilon_2$ and the field $K_2 = k(\varepsilon_0, \varepsilon_1, \varepsilon_2)$ be as Section 4.

Let $Y_0, \ldots, Y_n$, $Z_0, \ldots, Z_n$, $T_0, \ldots, T_n$, Z, T be new variables. For every $2 \le u \le N$ consider the following system of equations and inequalities with coefficients in K_2

$$\left\{\begin{array}{ll}
h_i = 0, & 1 \le i \le s+1, \\
h_i(Y_0, \ldots, Y_n) = 0, & 1 \le i \le s+1, \\
h_i(Z_0, \ldots, Z_n) = 0, & 1 \le i \le s, \\
h_i(T_0, \ldots, T_n) = 0, & 1 \le i \le s, \\
h_{s+1}(Z_0, \ldots, Z_n)Z - 1 = 0, & \\
h_{s+1}(T_0, \ldots, T_n)T - 1 = 0, & \\
\sum_{0 \le i \le n} |X_i - Z_i|^2 \le \varepsilon_2, & \\
\sum_{0 \le i \le n} |Y_i - T_i|^2 \le \varepsilon_2, & \\
L_j(X_0 - Y_0, \ldots, X_n - Y_n) = 0, & s+1 \le j \le n, \\
L_{s+1}(X_0 - x_{u,0}, \ldots, X_n - x_{u,n}) = 0, & \\
\sum_{0 \le i \le n} |X_i - x_{u,i}|^2 \le \varepsilon_0, & \\
\sum_{0 \le i \le n} |Y_i - x_{u,i}|^2 \le \varepsilon_0, & \\
\sum_{0 \le i \le n} |Y_i - X_i|^2 \ge \varepsilon_1, &
\end{array}\right. \tag{20}$$

We have the following analog of Lemma 2.

LEMMA 17 *Let V' and the projection $p_x : V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k})$ be as in Section 4. If for every $2 \le u \le N$ there do not exist solutions of system (20) in $\mathbb{A}^{4n+2}(\overline{K_2})$ then all the points $\{x_u\}_{2 \le u \le N}$ of the variety V' are smooth and the differentials of the projection p_x in points $\{x_u\}_{2 \le u \le N}$ are isomorphisms.*

PROOF Let $\varepsilon_3 > 0$ be an infinitesimal relative to the field $k(\varepsilon_0)$ such that ε_1 is an infinitesimal relative to the field $k(\varepsilon_0, \varepsilon_3)$. Suppose that at least one point x_{u_0} is not smooth or it is smooth but the differential of the projection p in the point x_{u_0} is not an isomorphism. Denote $p_x(x_{u_0}) = w \in \mathbb{P}^{n-s-1}(\overline{k})$.

Suppose that there exists only one component W of V' such that $x_{u_0} \in W$. Denote by $A(W)$ the set of indices u such that $x_u \in W$, $1 \le u \le N$, and set $p = p_x|_{W \setminus \{x\}}$, $N(W) = \#A(W)$. Apply Lemma 15. Then by this lemma $N(W) - 1 < \delta$ and there exists $w^* \in \mathbb{P}^{n-s-1}(\overline{k(\varepsilon_3)})$ such that $\mathrm{st}_{\varepsilon_3}(w^*) = w$ and $\#p^{-1}(w^*) = \delta$. By Proposition 2 there exist two different elments $x', y' \in \#p^{-1}(w^*)$ such that $\mathrm{st}_{\varepsilon_3}(x') = \mathrm{st}_{\varepsilon_3}(y') = x_{u_1}$ for some $u_1 \in A(W)$.

Recall that $L = \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n)$. Denote $\mathrm{st} = \mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_3}$. Let us show that $u_1 \ne 1$. Indeed, otherwise $x \ne \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, W) \subset \mathrm{con}(x, V')$ since if $F \in \overline{k}[X_1, \ldots, X_n]$, $F(x') = 0$ and F_r is the form of the least degree of F then $F_r(\mathrm{st}(x'/|x'|)) = 0$. Further

$$(L_j - (L_j/L_{s+1})(w^*)L_{s+1})(x'/|x'|) = 0$$

and $(L_j/L_{s+1})(w^*)$ is an infinitesimal for every $s+2 \le j \le n$. Therefore, we have $L_j(\mathrm{st}(x'/|x'|)) = 0$ for every $s+2 \le j \le n$. Hence $x \ne \mathrm{st}(x'/|x'|) \in \mathrm{con}(x, V') \cap L$. This contradiction proves our assertion.

Hence $u \ge 2$. From the fact that $x', y' \in W \subset V'$ we get the existence of $z', t' \in \mathbb{P}^n(\overline{k(\varepsilon_3, \varepsilon_2)})$ such that $h_i(z') = h_i(t') = 0$ for $1 \le i \le s$, $h_{s+1}(z') \ne 0$, $h_{s+1}(t') \ne 0$ and $\mathrm{st}_{\varepsilon_2}(z') = x'$, $\mathrm{st}_{\varepsilon_2}(t') = y'$. Thus, system (20) with $u = u_1$ has a solution in $\mathbb{P}^n(\overline{k(\varepsilon_3, \varepsilon_2)})$. Now the the isomorphism of the fields with real structures $\overline{k(\varepsilon_3, \varepsilon_2)} \simeq \overline{k(\varepsilon_0^a, \varepsilon_2)}$ induced by $\varepsilon_3 \mapsto \varepsilon_0^a$ for sufficiently great $0 < a \in \mathbb{Z}$ gives a solution of system (20) with $u = u_1$ in $\mathbb{P}^n(\overline{k(\varepsilon_0, \varepsilon_2)})$.

If there exist two different components W_1 and W_2 of W then there exists a point $w^* \in \mathbb{P}^{n-s-1}(\overline{k(\varepsilon_3)})$ such that $w^* \notin p(W_1 \cap W_2)$ and $\mathrm{st}_{\varepsilon_3}(w^*) = w$. Then by Proposition 2 there exist two different $x', y' \in \# p^{-1}(w^*)$ such that $x' \in W_1$, $y' \in W_2$, $\mathrm{st}_{\varepsilon_3}(x') = \mathrm{st}_{\varepsilon_3}(y') = x_{u_0}$. Further the proof is similar to the considered case of one component W. The lemma is proved.

Return to the description of the algorithm. Construct a solution of system (20) for some u or ascertain that for every $2 \le u \le N$ there exists no solutions of system (20) in $\mathbb{A}^{4n+2}(\overline{K_2})$. In the last case by Lemma 17 all the points $\{x_u\}_{2 \le u \le N}$ of the variety V' are smooth and the differentials of the projection p_x in the points $\{x_u\}_{2 \le u \le N}$ are isomorphisms.

Suppose that there exists a solution

$$(x'_0, \dots, x'_n, y'_0, \dots, y'_n, z'_0, \dots, z'_n, t'_0, \dots, t'_n, z, t) \in \mathbb{A}^{4n+2}(\overline{K_2})$$

of some system (20) with $u = u_0$. Denote $x' = (x'_0 : \dots : x'_n)$ and $y' = (y'_0 : \dots : y'_n)$. So $x', y' \in \mathbb{P}^n(\overline{K_2})$. Compute $x^* = \mathrm{st}_{\varepsilon_2}(x')$ and $y^* = \mathrm{st}_{\varepsilon_2}(y')$. Then $x^*, y^* \in V'$ since the polynomials $h_1, \dots, h_s$ are vanishing in these points and the polynomial h_{s+1} is not vanishing in the points $(z'_0, \dots, z'_n)$ and $(t'_0, \dots, t'_n)$ which are infinitesimal close to x^* and y^* respectively. Set

$$L'_i = L_i - (L_i/L_{s+1})(x^*) L_{s+1}, \; s+2 \le i \le n.$$

Compute all the points from the set $V' \cap \mathcal{Z}(L'_{s+2}, \dots, L'_n)$ in $\mathbb{P}^n(\overline{K_2})$. Denote $N' = \# V' \cap \mathcal{Z}(L'_{s+2}, \dots, L'_n)$. By Proposition 2 for every $x'' \in V' \cap \mathcal{Z}(L'_{s+2}, \dots, L'_n)$ there exists $1 \le u \le N$ such that $(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(x'') = x_u$. So $N' \ge N$. Further, $x^*, y^* \in V' \cap \mathcal{Z}(L'_{s+2}, \dots, L'_n)$, $x^* \ne y^*$ and $(\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(x^*) = (\mathrm{st}_{\varepsilon_0} \circ \mathrm{st}_{\varepsilon_1})(y^*)$. Therefore, $N' \ge N+1 > N$.

Apply the analog of the second auxiliary algorithm from [3] described in Section 4 to the linear forms $L'_{s+2}, \dots, L'_n$ and construct linear forms M_{s+2}, $\dots, M_n$ in $X_1, \dots, X_n$ with coefficients from $\mathbb{Z}$ of the length $O(n \log d)$ such that

$$\#V' \cap \mathcal{Z}(M_{s+2}, \ldots, M_n) \geq N' > N,$$
$$V' \cap \mathcal{Z}(L_0, M_{s+2}, \ldots, M_n) = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. Set also $M_0 = L_0$

After that, return recursively to the beginning of the algorithm described replacing the forms $L_0, L_{s+2}, \ldots, L_n$ by $M_0, M_{s+2}, \ldots, M_n$. Since $N' > N$ there are at most d^{s+1} such returns in the algorithm.

Thus, effecting this recursive construction till the end we can suppose without loss of generality by Lemma 17 that all the points x_u, $2 \leq u \leq N$ (if they exist) are smooth of the variety V' and the differentials of the projection p_x, see Lemma 17, in the points x_u, $2 \leq u \leq N$ are isomorphisms.

The condition that the differentials of the projection

$$\widetilde{p} : W \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+2} : \ldots : L_n)$$

are isomorphisms in all the point from $V' \cap \mathcal{Z}(L_{s+2}, \ldots, L_n) \setminus \{x\}$ follows from the condition that the differentials of the projection

$$p_x : V' \setminus \{x\} \longrightarrow \mathbb{P}^{n-s-1}(\overline{k}),\ (X_0 : \ldots : X_n) \mapsto (L_{s+1} : L_{s+2} : \ldots : L_n).$$

are isomorphisms in all the point from $W \cap \mathcal{Z}(L_{s+2}, \ldots, L_n) \setminus \{x\}$. The both conditions are equivalent to the fact that the intersection of tangent spaces $T_{x_u, V'} \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n) = \{x_u\}$ for every point $x_u \in V' \cap \mathcal{Z}(L_{s+2}, L_{s+3}, \ldots, L_n) \setminus \{x\}$. That is we have the required linear forms $M_j = L_j$, $j = 0, s+2, s+3, \ldots, n$.

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

$$\{x_u : u \in A\} = V_{s+1} \cap \mathcal{Z}(L_{s+2}, \ldots, L_n) \tag{21}$$

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

LEMMA 18 *Let $\mu(x, V_{s+1})$ be the multiplicity of the point x of the variety V_{s+1}. Then*

$$\mu(x, V_{s+1}) = \deg V_{s+1} - \#A. \tag{22}$$

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

$$\{x_u : u \in A(W)\} = W \cap \mathcal{Z}(L_{s+2}, \ldots, L_n)$$

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

Consider the set of families H of $n-s-1$ linear forms $H_{s+2},\dots,H_n$ in $X_1,\dots,X_n$ with coefficients from $\overline{k}$. So by the definition of the multiplicity there exists such a family $H=\{H_j\}_{s+2\le j\le n}$ for which $\#(W\cap\mathcal{Z}(H_{s+2},\,\dots,\,H_n)\setminus\{x\})<+\infty$ and $\mu(x,W)=\deg W-\#(W\cap\mathcal{Z}(H_{s+2},\,\dots,\,H_n)\setminus\{x\})$. The conditions of Lemma 16 are satisfied for $L_j^{(0)}=L_j$, $j=0,s+2,\dots,n$ and $L_j^{(1)}=H_j$, $j=s+2,\dots,n$. Now applying Lemma 16 we get that

$$\#(W\cap\mathcal{Z}(L_{s+2},\,\dots,\,L_n)\setminus\{x\})\ge\#(W\cap\mathcal{Z}(H_{s+2},\,\dots,\,H_n)\setminus\{x\}).$$

Hence by the definition of the multiplicity

$$\begin{aligned}&\#A(W)=\#(W\cap\mathcal{Z}(L_{s+2},\,\dots,\,L_n)\setminus\{x\})=\\&\#(W\cap\mathcal{Z}(H_{s+2},\,\dots,\,H_n)\setminus\{x\})=\deg W-\mu(x,W).\end{aligned}$$

Hence $\sum_{W\subset V_{s+1}}\mu(x,W)=\deg V_{s+1}-\#A$. But $\mu(x,V_{s+1})\ge\sum_{W\subset V_{s+1}}\mu(x,W)$ as a simple consequence of the definition of the multiplicity. Hence $\mu(x,V_{s+1})\ge\deg V_{s+1}-\#A$. Finally we have $-1+\deg V_{s+1}-\#V_{s+1}\cap\mathcal{Z}(L_{s+2},\,\dots,\,L_n)=\deg V_{s+1}-\#A$ and therefore $\mu(x,V_{s+1})=\deg V_{s+1}-\#A$. The lemma is proved.

Thus, by Lemma 18 we can compute the multiplicity $\mu(x,V_{s+1})$. 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] **Chistov A. L.** *" Polynomial–Time Computation of the Dimension of Algebraic Varieties in Zero–Characteristic"*, Journal of Symbolic Computation, 22 # 1 (1996) 1–25.

[3] **Chistov A. L.:** *"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.

[4] **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), p. 124–188 (Russian) [English transl.: J. Sov. Math. 34, (4), (1986) p. 1838–1882].

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

[6] **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) p. 127–150 (Russian).

[7] **Chistov A. L., Karpinski M.:** *"Complexity of Deciding Solvability of Polynomial Equations over p-adics"*, Research Report No. 85183-CS, Institut für Informatik der Universität Bonn, May 1997, 18 p.

[8] **Giusti M., Heintz J.:** *"La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial"*, Proc. Int. Meeting on Commutative Algebra, Cortona (1993).

[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] **Kroneker L.:** *"Grundzüge einer arithmetischen theorie der algebraischen grossen"*, J. Reine und angew. Math., 92 (1882) S. 1–122.

[12] **Lazard D.:** *"Algèbre linéaire sur* $k[x_1, \dots, x_n]$ *et élimination"*, Bul. S.M.F. 105 (1977) p. 165–190.

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

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

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

[16] **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, p. 291–295.

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