Efficient Smooth Stratification of an Algebraic Variety in Zero Characteristic and its Applications

Alexander L. Chistov

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

1999

Abstract

Consider a projective algebraic variety V which is given as a set of common zeros of a family of homogeneous polynomials of degrees less than d in $n+1$ variables with coefficients from a field k of zero–characteristic. We prove that V can be represented as a union (respectively disjoint union) of at most $C(n)d^n$ (respectively $C(n)d^{n(n+1)/2}$) smooth quasiprojective algebraic varieties with degrees (herewith degree of a quasiprojective algebraic variety is degree of its closure in the Zariski topology) bounded from above by $C(n)d^n$ where $C(n) < 2^{2^{n^C}}$ for an absolute constant $C > 0$. Further, in the case of zero–characteristic algorithms for constructing regular sequences and sequences of local parameters for irreducible components of V are described. The complexity of these algorithms is polynomial in the size of input and $C(n)d^n$. Finally, in the case when k is a subfield of $\mathbb{R}$ an algorithm is suggested to compute the dimension of the set $V(\mathbb{R})$ of $\mathbb{R}$-points of V with the complexity polynomial in the size of input and $C(n)d^n$.

Introduction

Let k be a field of zero–characteristic and $\mathbb{P}^n(\overline{k})$ be n–dimensional projective space over algebraic closure $\overline{k}$ with the homogeneous coordinates $X_0, \ldots, X_n$. Consider a projective algebraic variety V which is given as a set of common zeros of a family of homogeneous polynomials of the degree less than d in $n+1$ variables $X_0, \ldots, X_n$ with coefficients from k.

DEFINITION 1 Smooth cover *of the algebraic variety V is a finite family*

$$V_\alpha, \quad \alpha \in A, \tag{1}$$

of quasiprojective smooth algebraic varieties $V_\alpha \subset \mathbb{P}^n(\overline{k})$, $\alpha \in A$ such that V is represented as a union $V = \cup_{\alpha \in A} V_\alpha$. Further, we shall require that all irreducible components of V_α have the same dimension (which depends only on α). Smooth stratification *of the algebraic variety V is a smooth cover V_α, $\alpha \in A$, of V such that additionally for any two $\alpha_1, \alpha_2 \in A$ if $\alpha_1 \neq \alpha_2$ then $V_{\alpha_1} \cap V_{\alpha_1} = \emptyset$.*

REMARK 1 Let l_1 and l_2 be two distinct lines in $\mathbb{P}^2$. Then the family of two quasiprojective algebraic varieties l_1 and $l_2 \setminus l_1$ defines a smooth stratification of $l_1 \cup l_2$. This example shows that some varieties V_α may contain smooth points and singular points of V simultaneously.

In this paper we introduce a new representation of quasiprojective algebraic varieties which is convenient from the algorithmic point of view. Using this representation we prove the existence of a smooth cover and a smooth stratification (1) such that for every $\alpha \in A$ the degree of the closure in the Zariski topology $\deg \overline{V}_\alpha$ is bounded from above by $2^{2^{n^C}} d^n$ where $C > 0$ is an absolute constant. Besides that, the number of elements $\#A$ is bounded from above by $2^{2^{n^C}} d^n$ for the case of smooth cover and by $2^{2^{n^C}} d^{n(n+1)/2}$ for the case of smooth stratification. For more details see Theorem 2 and Theorem 4 from Section 2. The constant C (as well as other constants below) can be computed explicitly from the proofs given in the paper and in [7].

Using results of the present paper, [8], [9] one can suggest in the case of zero–characteristic algorithms for constructing a smooth cover (respectively a smooth stratification) of V within the time polynomial in the size of input and $2^{2^{n^C}} d^n$ (respectively $2^{2^{n^C}} d^{n(n+1)/2}$) for an absolute constant $C > 0$, see Remark 3 below. If there will be interest to this subject we hope to describe these algorithms in one of the next papers. Here one should probably translate into English, may be in a revised form, the bulky paper [8]. The method of [8] is essentially classical. The algorithm of [8] has polynomial complexity and uses instructive ideas (from the point of view of theory of computation) combining algebra and analysis.

In the algorithmic part of the paper in the case of zero–characteristic and when k is finitely generated over $\mathbb{Q}$ we suggest a method for constructing sequences of local parameters for components of algebraic varieties within the time polynomial in the size of input and $2^{2^{n^C}} d^n$ where $C > 0$ is an absolute constant, see Theorem 1. In the case when k is a subfield of $\mathbb{R}$ the existence of a smooth cover proved in Theorem 2 allows to construct an algorithm for computing dimension of a real algebraic variety $V(\mathbb{R})$ within the time polynomial in the size of input and $2^{2^{n^C}} d^n$, see Theorem 3.

In the present paper the proofs are based on the results of [7], [6]. In [7] an efficient construction (in mathematical sense without algorithms) of regular sequences and sequences of local parameters in the local rings of components of algebraic varieties is described. Using efficient estimations for degrees of local parameters from [7] and the results of [6] we suggest an algorithm for constructing regular sequences and sequences of local parameters in the local ring of a component of dimension $n-s$ of an algebraic variety V within the time polynomial in the size of input and $n^{2^{s^C}} d^n$.

Now we give the precise statements. Let homogeneous polynomials $f_1, \dots, f_m \in k[X_0, \dots, X_n]$ be given, $n \geq 1$, $m \geq 1$. Consider the closed algebraic set or algebraic variety (in this paper we do not distinguish these two concepts)

$$V = \{(x_0 : \ldots : x_n) : f_i(x_0, \ldots, x_n) = 0, \ x_i \in \overline{k}, \ \forall 1 \leq i \leq m\} \subset \mathbb{P}^n(\overline{k}) .$$

This is a set of all common zeros of polynomials $f_1, \ldots, f_m$ in $\mathbb{P}^n(\overline{k})$, where $\overline{k}$ is an algebraic closure of k. In what follows we shall denote for brevity this set by $\mathcal{Z}(f_1, \ldots, f_m)$. 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 $V = \mathcal{Z}(f_1, \ldots, f_m)$.

Now let the field $k = \mathbb{Q}(t_1, \dots, t_l, \theta)$ where $t_1, \dots, t_l$ are algebraically independent over the field $\mathbb{Q}$ and θ is algebraic over $\mathbb{Q}(t_1, \dots, t_l)$ with the minimal polynomial $F \in \mathbb{Q}[t_1, \dots, t_l, Z]$ and leading coefficient $\mathrm{lc}_Z F$ of F is equal to 1. We shall represent each polynomial $f = f_i$ in the form

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

where $a_0, a_{i_0,\ldots,i_n,j} \in \mathbb{Z}[t_1, \ldots, t_l]$, $\gcd_{i_0,\ldots,i_n,j}(a_0, a_{i_0,\ldots,i_n,j}) = 1$. 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 lengths of coefficients from $\mathbb{Z}$ of polynomials $a_0, a_{i_0,\ldots,i_n,j}$ and the degree

$$\deg_{t_\gamma}(f) = \max_{i_0,\ldots,i_n,j} \{\deg_{t_\gamma}(a_0), \deg_{t_\gamma}(a_{i_0,\ldots,i_n,j})\} ,$$

where $1 \leq \gamma \leq l$. In the similar way we shall define degrees and lengths of integer coefficients of other polynomials, in particular $\deg_{t_\gamma} F$ and $l(F)$ are defined. We shall suppose that we have the following bounds

$$\begin{gathered} \deg_{X_0,\ldots,X_n}(f_i) < d, \ \deg_{t_\gamma}(f_i) < d_2, \ l(f_i) < M, \\ \deg_Z(F) < d_1, \ \deg_{t_\gamma}(F) < d_1, \ l(F) < M_1 . \end{gathered}$$

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

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

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

REMARK 2 In what follows we shall assume without loss of generality that the polynomials $f_1, \ldots, f_m$ are linearly independent over k. Hence $\dim V \leq n-1$.

Let W be a defined over k and irreducible over k projective algebraic variety in $\mathbb{P}^n(\overline{k})$ and dimension $\dim W = n-s$. Let $\mathfrak{P} = \mathcal{I}(W) \subset k[X_0,\ldots,X_n]$ be the homogeneous prime ideal corresponding to W. Recall that in [7] $\mathfrak{P}$–sequences were introduced. Namely, consider a sequence of homogeneous polynomials $g_1,\ldots,g_j \in \mathfrak{P}$, $1 \le j \le s$. Let $0 \le u < j$ be an integer. Denote by $\mathcal{W} = \mathcal{W}(\mathfrak{P}, u)$ the set of all defined over k and irreducible over k components W' of the algebraic variety $\mathcal{Z}(g_1,\ldots,g_u)$ such that $W' \supset V$. Suppose that for every integer $0 \le u \le j-1$ the polynomial $g_{u+1} \in \mathfrak{P}$ is a polynomial g of the least degree such that for every irreducible component $W' \in \mathcal{W}$ the algebraic variety $W' \not\subset \mathcal{Z}(g)$. Then any such sequence $g_1,\ldots,g_j$ is called *$\mathfrak{P}$–sequence (of length j)*.

Note that if $g_1,\ldots,g_j$ is a $\mathfrak{P}$–sequence then for every $0 \le u \le j$ every irreducible component of the algebraic variety $\mathcal{Z}(g_1,\ldots,g_u)$ containing V has dimension $n-u$. In particular when $j = s$ the algebraic variety V is an irreducible component of $\mathcal{Z}(g_1,\ldots,g_s)$.

Recall also that $g_1,\ldots,g_s$ is a sequence of local parameters of the algebraic variety W in a smooth point $x_0 \in W$ if and only if $g_1,\ldots,g_s$ generate the ideal of W in the local ring $\mathcal{O}_{x_0,\mathbb{P}^n(\overline{k})}$ of the point x_0 in $\mathbb{P}^n(\overline{k})$. Further, $g_1,\ldots,g_s$ is a sequence of local parameters of the algebraic variety W if and only if there exists a smooth point $x_0 \in W$ such that $g_1,\ldots,g_s$ is a sequence of local parameters of the algebraic variety W in the point x_0.

THEOREM 1 *Let a smooth point $x_0 \in V$ be given (the fact that x_0 is a smooth point of V can be verified using the algorithms from [6]). This means that an index $0 \le i_0 \le n$ is known such that $X_{i_0}(x_0) \ne 0$ and an isomorphism of fields*

$$k(x_0) = k((X_1/X_{i_0})(x_0),\ldots,(X_n/X_{i_0})(x_0)) = k[\eta] \simeq k[Z]/(\Phi) \qquad (2)$$

is given where $\eta = \sum_{0\le i\le n} c_i (X_i/X_{i_0})(x_0)$, the coefficients $c_i \in \mathbb{Z}$ are given and $\Phi \in k[Z]$ is minimal polynomial of η over k with leading coefficient $\mathrm{lc}_Z\,\Phi = 1$ (so the point x_0 is defined up to a conjugation over k). Let W be a uniquely defined irreducible over k component of V such that $x_0 \in W$. Let $\mathfrak{P} = \mathcal{I}(W) \subset k[X_0,\ldots,X_n]$ be homogeneous prime ideal corresponding to W. Let $\dim W = n-s$ where $1 \le s \le n$. Then the following assertions hold.

(i) One can construct a $\mathfrak{P}$–sequence $g_1,\ldots,g_s \in k[X_0,\ldots,X_n]$. Therefore $\deg g_i \le d$ for all $1 \le i \le s$ and by [7]

$$\deg g_1 \cdot \ldots \cdot \deg g_s \le n^{2^{s^C}} \deg W$$

for an absolute constant $0 < C \in \mathbb{R}$. The working time of the algorithm for constructing this $\mathfrak{P}$–sequence is polynomial in d^n, d_1, d_2, M, M_1, m and the size of the point x_0.

(ii) One can construct homogeneous polynomials $h_1,\ldots,h_s \in k[X_0,\ldots,X_n]$ and a point $x \in W$ such that x is a smooth point of V, the coordinate $X_{i_0}(x) \ne 0$ and $h_1/X_{i_0}^{\deg h_1},\ldots,h_s/X_{i_0}^{\deg h_s}$ is a system of local parameters of W in the point x, the degrees

$$\deg_{X_0,\ldots,X_n} h_i \le n^{2^{s^C}} \deg g_i \le n^{2^{s^C}} d, \quad 1 \le i \le s,$$

for an absolute constant $0 < C \in \mathbb{R}$. The working time of the algorithm for constructing the polynomials $h_1, \ldots, h_s$ is polynomial in $n^{2^{s^C}} d^n$, d_1, d_2, M, M_1, m and the size of the point x_0 where $0 < C \in \mathbb{R}$ is an absolute constant.

Note here that using the algorithms from [6] one can construct a a set S containing a representative system of the family of sets of smooth points of all irreducible components of V such that the size of every point from the set S is bounded from above by a polynomial in d^n, d_1, d_2, M, M_1, m and the number of points $\#S \le d^n$.

Before formulating our next result we need to describe how we shall represent quasiprojective algebraic varieties in this paper. Let W be a quasiprojective algebraic variety in $\mathbb{P}^n(\overline{k})$ and W is defined over k. Then represent

$$W = W^{(1)} \setminus \cup_{2 \le i \le a} W^{(i)}, \tag{3}$$

where all $W^{(i)}$, $1 \le i \le a$ are projective algebraic varieties in $\mathbb{P}^n(\overline{k})$ defined over k. Each algebraic variety $W^{(i)}$, $1 \le i \le a$ is given as a union of some irreducible components of the algebraic variety $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)}) \subset \mathbb{P}^n(\overline{k})$ where homogeneous polynomials $f_1^{(i)}, \ldots, f_{m(i)}^{(i)} \in k[X_0, \ldots, X_n]$ are given (here one should not confuse the upper index (i) with the derivative). For every $1 \le s \le n$ denote by $V_s^{(i)}$ (respectively $W_s^{(i)}$) the union of all irreducible components of dimension $n-s$ of $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)})$ (respectively $W^{(i)}$). Therefore $W_s^{(i)}$ is a union of some irreducible components of $V_s^{(i)}$. For every $1 \le s \le n$ the family of linear forms $L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)} \in k[X_0, \ldots, X_n]$ with integer coefficients is given such that the number of points

$$\# V_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}) < +\infty \tag{4}$$

is finite, every point $\xi \in V_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)})$ is a smooth point of the algebraic variety $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)})$, and the intersection of the tangent spaces in the point ξ of $V_s^{(i)}$ and $\mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)})$ is transversal, i.e.,

$$T_{\xi, V_s^{(i)}} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}) = \{\xi\}. \tag{5}$$

The set of points

$$\Xi_s^{(i)} = W_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)})$$

is given. Hence the following property holds. Let $\xi \in V_s^{(i)} \cap \mathcal{Z}(L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)})$ and V' be the uniquely defined irreducible over k component of the algebraic variety $V_s^{(i)}$ such that $\xi \in V'$. Then $\xi \in \Xi_s^{(i)}$ if and only if V' is a component of $W^{(i)}$.

Thus formally the accepted in this paper representation of W is a triple

$$(f, L, \Xi), \tag{6}$$

where f is a family of polynomials

$$f_j^{(i)}, \quad 1 \le j \le m(i),\ 1 \le i \le a, \tag{7}$$

L is a family of linear forms

$$L_{s,j}^{(i)}, \quad s+1 \le j \le n,\ 1 \le s \le n,\ 1 \le i \le a, \tag{8}$$

and Ξ is a family of finite sets of points

$$\Xi_s^{(i)}, \quad 1 \le s \le n,\ 1 \le i \le a. \tag{9}$$

Denote also

$$\Xi^{(i)} = \bigcup_{1 \le s \le n} \Xi_s^{(i)}. \tag{10}$$

Note that (4) and (5) can be always verified using the algorithms from [6]. Note also that for a given point $y \in \mathbb{P}^n(\overline{k})$ one can decide whether $y \in W_s^{(i)}$ using the algorithms from [6] and [3]. Namely, construct linearly independent linear forms $M_{s+2}, \ldots, M_n$ which are linear combinations of $L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)}$ such that $M_j(y) = 0,\ s+2 \le j \le n$. Construct systems of polynomial equations giving all the curves V'' which are irreducible components of the intersection

$$\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)}) \cap \mathcal{Z}(M_{s+2}, \ldots, M_n)$$

such that $V'' \cap \Xi_s^{(i)} \neq \emptyset$. Then $y \in W_s^{(i)}$ if and only if $y \in V''$ for some curve V''.

Thus, for a given point $y \in \mathbb{P}^n(\overline{k})$ one can decide also within the polynomial time whether $y \in W^{(i)}$, $1 \le i \le a$, and whether $y \in W$.

Besides that, for an algebraic variety W' which is similar to W and is given in the similar way one can decide whether $W' = W$ within the polynomial time. Let us prove this fact when W and W' are projective algebraic varieties. In this case it is sufficient to check that $W \setminus W' = \emptyset$ and $W' \setminus W = \emptyset$. To check that, e.g., $W \setminus W' = \emptyset$ it is sufficient to prove this equality in the neighborhood of every point $\xi \in \Xi^{(1)}$. At first decide as above whether $\xi \in W'$ and if $\xi \in W'$ construct a point $\xi_1 \in W' \cap W$ which is infinitesimal close to ξ and ξ_1 is a smooth point of W', see above. Now if $W \setminus W' = \emptyset$ in the infinitesimal (relative to the field of definition of the point ξ_1) neighborhood of the point ξ_1 then $W \setminus W' = \emptyset$ in the infinitesimal neighborhood of the point ξ. The equality $W \setminus W' = \emptyset$ in the infinitesimal neighborhood of the point ξ_1 can be verified by solving a system of polynomial equations and inequalities with absolute values, see [4], [5].

REMARK 3 Basing on [8] one can suggest a polynomial–time algorithm to decide whether given two smooth point of W belong to the same irreducible component of W defined over k or $\overline{k}$. In particular one can decide whether W is an irreducible algebraic variety. Using the results of [8], [9] one can suggest also an algorithm to decide whether $W_1 \subset W_2$ for two projective algebraic varieties W_1 and W_2 given in the form described here. We shall not describe these algorithms in the present paper. Analyzing the proof of Theorem 2, see below, one can see that these algorithms allow to construct smooth cover (respectively smooth stratification) of V within the time polynomial in size of input and $2^{2^{n^C}} d^n$ (respectively $2^{2^{n^C}} d^{n(n+1)/2}$) for an absolute constant $C > 0$. Note also that if a smooth cover of V is constructed then Theorem 3, see below, is trivial.

THEOREM 2 *There is a smooth cover (respectively a smooth stratification) V_α, $\alpha \in A$, of the algebraic variety V such that every quasiprojective algebraic variety V_α is defined over k, irreducible over k, and represented in the accepted way. Let $\dim V_\alpha = n - s$ where $1 \le s \le n$, and $s = s(\alpha)$ depends on α. Let (6) be the constructed representation of V_α. Denote $h_{\alpha,j} = f_j^{(1)}$, $1 \le j \le m(1)$, and $\Delta_\alpha = f_1^{(2)}$ if $a \ge 2$, see (7). Then the constructed representation of V_α satisfies the following properties.*

(i) For the case of smooth cover $a = 2$ if $s < n$, and $a = 1$ if $s = n$. For the case of smooth stratification $a \le 2^{2^{n^C}} d^{n(n+1)/2}$ for an absolute constant $0 < C \in \mathbb{R}$.

(ii) $m(1) = s$ and if $a \ge 2$ then $m(2) = 1$. Hence if $a \ge 2$ then V_α is an irreducible component of the algebraic variety $\mathcal{Z}(h_{\alpha,1}, \dots, h_{\alpha,s}) \setminus \mathcal{Z}(\Delta_\alpha)$ in the case of the smooth cover (respectively an open in the Zariski topology subset of an irreducible component of the latter algebraic variety in the case of smooth stratification).

(iii) There are linearly independent linear forms $Y_0, \dots, Y_n \in k[X_0, \dots, X_n]$ such that $X_i = \sum_{0 \le j \le n} x_{i,j} Y_j$, all the coefficients $x_{i,j} \in k$, all $x_{i,j}$ are integers with lengths $O(2^{n^C} + n \log d)$ for an absolute constant $C > 0$, and

$$\Delta_\alpha = \det(\partial h_{\alpha,i}/\partial Y_j)_{1 \le i,j \le s} = \det(\sum_{0 \le v \le n} x_{v,j} \partial h_{\alpha,i}/\partial X_v)_{1 \le i,j \le s}.$$

Hence V_α is a smooth algebraic variety by the implicit function theorem. Besides that, in the case of smooth cover one can take $Y_i = X_{\sigma(i)}$ for some permutation σ of the set $0, \dots, n$.

(iv) The lengths of integer coefficients of all linear forms from the family L is $O(2^{n^C} + n \log d)$ for an absolute constant $0 < C \in \mathbb{R}$.

(v) For all $\alpha \in A$, $1 \le j \le s(\alpha)$ degrees $\deg_{X_0,\dots,X_n} h_{\alpha,j}$ are less than $n^{2^{s(\alpha)^C}} d$ for an absolute constant $0 < C \in \mathbb{R}$. In the case of smooth stratification for all $i > 2$, j degrees $\deg_{X_0,\dots,X_n} f_j^{(i)}$ are less than $2^{2^{n^C}} d$.

(vi) For all $\alpha \in A$, $1 \le j \le s(\alpha)$ lengths of coefficients of polynomials $h_{\alpha,j}$ are bounded from above by a polynomial in $n^{2^{s(\alpha)^C}} d^n$, d_1, d_2, M, M_1, m for an absolute constant $0 < C \in \mathbb{R}$. Further, in the case of smooth stratification lengths of coefficients of all polynomials from the family f are bounded from above by a polynomial in $2^{2^{n^C}} d^n$, d_1, d_2, M, M_1, m for an absolute constant $0 < C \in \mathbb{R}$.

(vii) The number of elements $\#A$ of A is bounded from above by $2^{2^{n^C}} d^n$ for the case of smooth cover (respectively $2^{2^{n^C}} d^{n(n+1)/2}$ for the case of smooth stratification) for an absolute constant $0 < C \in \mathbb{R}$.

REMARK 4 *Note that if one obtains (at present one does not obtain) estimations for local parameters over perfect fields of non–zero characteristic similar to ones from [7] then all the assertions of Theorem 2 (except of the assertions* *about the lengths of integer coefficients) are valid also over perfect infinite fields of non–zero characteristic. The proof is without changes over such infinite fields. Respectively the case of finite fields requires only small changes in the formulation and the proof of Theorem 2.*

Note that the existence of required linear forms from the representation (6) in Theorem 2 follows, see [6], automatically from the existence of all other objects from the statement of this theorem.

The key to the proof of Theorem 2 for the case of smooth cover is Theorem 4 which is formulated in Section 2. The case of smooth stratification requires ordering irreducible algebraic varieties. This ordering is described in Section 4. Theorem 2 for the case of smooth stratification is proved in Section 5. Note also that the question whether one can construct a smooth stratification with $\#A \le 2^{2^{n^C}} d^n$ (in notation of Theorem 2) is not investigated.

Now suppose that k is a real ordered field. Assume that the field k satisfies the following property.

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

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

By R denote a real closed field which is a field extension of k. For an algebraic variety V defined over the field k denote by $V(R)$ the real algebraic variety over the field R corresponding to V (i.e., the set of points of $V(R)$ is the set of point of V with coordinates in R). Every real algebraic variety can be obtained in this way, the definition of real algebraic varieties see in [1]. The dimension $\dim V(R)$ of the real algebraic variety $V(R)$ is defined in the natural way as maximum of dimensions of its smooth points, see [1].

THEOREM 3 *Let k be a real ordered field satisfying condition (A) and R be a real closed field containing k. Then one can compute dimension $\dim V(R)$ of the set of R-points of the algebraic variety V within the time polynomial in $2^{2^{n^C}} d^n$, d_1, d_2, M, M_1, m for an absolute constant $0 < C \in \mathbb{R}$. More than that, if in output of the algorithm $\dim V(R) = n - s$ then actually the working time of the algorithm is polynomial in $n^{2^{s^C}} d^n$, d_1, d_2, M, M_1, m.*

1 Algorithms for constructing regular sequences and sequences of local parameters

Using the algorithm from [6], Section 3, construct linear forms Y_0, Y_{s+1}, Y_{s+2}, ..., $Y_n \in k(x_0)[X_0, \dots, X_n]$ such that $Y_0(x_0) \ne 0$, the point x_0 is isolated in the intersection $W \cap \mathcal{Z}(Y_{s+1}, \dots, Y_n)$, and the intersection of tangent spaces of W in the point x_0 and $\mathcal{Z}(Y_{s+1}, \dots, Y_n)$ is transversal, i.e., $T_{x_0,W} \cap \mathcal{Z}(Y_{s+1}, \dots, Y_n) = \{x_0\}$.

Let V' be an arbitrary projective algebraic variety defined over k and irreducible over k and $V' = \cup_{j\in J} V'_j$ be the decomposition of V into the union of irreducible components over k. Let $x \in V'$. Then the multiplicity $\mu(x, V'_j) \geq 0$ of the point x of the algebraic variety V'_j is defined, cf. [6]. It is convenient now to define multiplicity $\mu(x, V) = \sum_{j\in J} \mu(x, V'_j)$.

LEMMA 1 *Under conditions of Theorem 1 let $1 \leq j \leq s$ and $\psi_1, \ldots, \psi_j \in k[X_0, \ldots, X_n]$ be homogeneous polynomials such that $\mathcal{Z}(\psi_1, \ldots, \psi_j) \supset W$, dimension of every irreducible component of $\mathcal{Z}(\psi_1, \ldots, \psi_j)$ containing W is $n-j$ and $\deg \psi_i \leq D$ for all $1 \leq i \leq j$. Let $\psi \in k[X_0, \ldots, X_n]$ be a homogeneous polynomial and $\deg \psi \leq D$. Then one can decide whether ψ is vanishing on W. If ψ is not vanishing on W one can construct a point $x' \in W$ and linear forms $L'_{s+1}, \ldots, L'_n \in k(x_0)[X_0, \ldots, X_n]$ satisfying the following properties.*

(i) x' is a smooth point of V (and hence a smooth point of W).

(ii) $Y_0(x') \neq 0$.

(iii) $L'_{s+1}, L'_{s+2}, \ldots, L'_n$ are linear forms in $Y_0, Y_{s+1}, \ldots, Y_n$ with integer coefficients of lengths $O(n \log(dD))$.

(iv) The point x' is isolated in the intersection $W \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$.

(v) The intersection of tangent spaces of W in the point x' and $\mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ is transversal, i.e., $T_{x',W} \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \{x'\}$.

(vi) $\psi(x') \neq 0$.

(vii) $\mu(x', \mathcal{Z}(\psi_1, \ldots, \psi_j)) = \min_{x\in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j))$.

The working time of the algorithm for constructing the point x' and linear forms $L'_{s+1}, \ldots, L'_n$ is polynomial in the size of input and $(dD)^n$.

PROOF Construct a real structure on the field k, see [4], [5]. Let $\varepsilon_1 > 0$ be an infinitesimal relative to the field k and $\varepsilon_2 > 0$ be an infinitesimal relative to the field $k(\varepsilon_1)$. Set $K = k(\varepsilon_1, \varepsilon_2)$. So the field K is equipped with a real structure and one can consider systems of algebraic equations and inequalities with squares of absolute values over K and solve them over $\overline{K}$, see [4], [5]. The same is true if one replaces K by $k(\varepsilon_1)$. Let $x_0 = (x_{0,0} : \ldots : x_{0,n})$ where all $x_{0,j} \in k(x_0)$, $0 \leq j \leq n$. Consider the system of equations and inequalities with coefficients from K in the variables $X_0, \ldots, X_n$, Z

$$\begin{cases} \sum_{0\leq i\leq n} |X_i - x_{0,i}|^2 < \varepsilon_1, & \\ f_i = 0, & 1 \leq i \leq m, \\ \psi Z - 1 = 0. & \end{cases} \tag{11}$$

Then, cf. [5], [6], system (11) has no solutions in $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1)})$ if and only if the polynomial ψ is vanishing on W. In what follows in the proof of this lemma we shall suppose that system (11) has a solution.

Suppose $x'' \in W$ and linear forms $L''_{s+1}, \ldots, L''_n \in k(x_0)[X_0, \ldots, X_n]$ satisfy the properties which are obtained from (i)–(v) by replacing x' and $L'_{s+1}, \ldots, L'_n$ by x'' and $L''_{s+1}, \ldots, L''_n$. Hence

$$\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j)) \geq \min_{x\in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j)). \tag{12}$$

Note that if we know in advance that $x'' \in W$ then we can always verify whether the point x'' and linear forms $L''_{s+1}, \ldots, L''_n$ satisfy properties (i)–(vi) (where x' and linear forms L'_j are replaced by x'' and linear forms L''_j) using algorithms from [6]. We can compute also the multiplicity $\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j))$.

Let us show that we can decide whether the equality take place in (12) and if (12) is a strict inequality we can construct a new point x''' and new linear forms $L'''_{s+1}, \ldots, L'''_n$ similar to x'' and $L''_{s+1}, \ldots, L''_n$ such that $\psi(x''') \neq 0$ and

$$\mu(x''', \mathcal{Z}(\psi_1, \ldots, \psi_j)) < \mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j)).$$

Indeed, let $x''_0, \ldots, x''_n \in \overline{k}$ be such that $x'' = (x''_0 : \ldots : x''_n)$. Compute using the algorithm from [6] the dimension $r = \dim_{x''} \mathcal{Z}(\psi_1, \ldots, \psi_j)$ in the point x'', i.e., the maximum of dimensions of irreducible components W_2 of the algebraic variety $\mathcal{Z}(\psi_1, \ldots, \psi_j)$ such that $x'' \in W_2$. Construct using the algorithm from [6] linear forms $M_0, M_{r+1}, M_{r+2}, \ldots, M_n$ with integer coefficients of lengths $O(n \log D)$ such that

$$\mathcal{Z}(\psi_1, \ldots, \psi_j) \cap \mathcal{Z}(M_0, M_{r+1}, M_{r+2}, \ldots, M_n) = \emptyset$$

in a neighborhood of the point x''.

Consider the system of equations and inequalities with coefficients from K in the variables $X_0, \ldots, X_n$, $Z_0, \ldots, Z_n$, Z

$$\left\{ \begin{array}{ll} \sum_{0 \leq i \leq n} |X_i - x''_i|^2 \leq \varepsilon_1, & \\ \sum_{0 \leq i \leq n} |Z_i - x''_i|^2 \leq \varepsilon_1, & \\ \sum_{0 \leq i \leq n} |X_i - Z_i|^2 \geq \varepsilon_2, & \\ M_i(X_0 - Z_0, \ldots, X_n - Z_n) = 0, & i = 0, r+1, r+2, \ldots, n, \\ f_i = 0, & 1 \leq i \leq m, \\ \psi_i(Z_0, \ldots, Z_n) = 0, & 1 \leq i \leq j, \\ \psi Z - 1 = 0. & \end{array} \right. \qquad (13)$$

Then, cf. [5], [6], system (13) has no solutions in $\mathbb{A}^{2n+3}(\overline{K})$ if and only if (12) is the equality.

Suppose that system (13) has a solution. Then construct this solution $x^*_0, \ldots, x^*_n$, $z^*_0, \ldots, z^*_n$, z^*. Suppose that system (13) has no solutions then construct a solution $x^*_0, \ldots, x^*_n$, z^* of system (11).

Denote $x^* = (x^*_0 : \ldots : x^*_n) \in \mathbb{P}^n(\overline{K})$. Then $\psi(x^*) \neq 0$ and, cf. [6],

$$\mu(x^*, \mathcal{Z}(\psi_1, \ldots, \psi_j)) < \mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_j))$$

in the case when system (13) has a solution and

$$\mu(x^*, \mathcal{Z}(\psi_1, \ldots, \psi_j)) = \min_{x \in W} \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_j))$$

in the case when system (13) has no solutions. Set $L^*_i = L''_i - (L''_i/Y_0)(x^*)Y_0$ for $s+1 \leq i \leq n$. Then the point x^* and linear forms $L^*_{s+1}, \ldots, L^*_n$ satisfy properties which are required for the point x''' and $L'''_{s+1}, \ldots, L'''_n$ but $x^* \in \mathbb{P}^n(\overline{K})$ and corresponding linear forms have coefficients from the field $\overline{K}$.

Represent linear forms L^*_i, $s+1 \leq i \leq n$ as linear combinations of $Y_0, Y_{s+1}, \ldots, Y_n$ with coefficients $l_{i,j} \in \overline{K}$, herewith $l_{i,j}$ is a coefficient in Y_j of L^*_i. Further, cf. [5], [6], we can replace in the linear forms L^*_i, $s+1 \leq i \leq n$ one arbitrary coefficient $l_{i,j}$ by an integer coefficient with length $O(n\log(dD))$ and obtain linear forms $\widetilde{L}_{s+1},\ldots,\widetilde{L}_n$ and a point $\widetilde{x}$ satisfying the same properties as linear forms $L^*_{s+1},\ldots,L^*_n$ and the point x^*. More precisely, suppose that we would like to replace the coefficient $l_{0,s+1}$ by an integer. We enumerate possible integer values of this replaced coefficient and check each time whether the required properties hold. The intersection

$$V\cap\mathcal{Z}(L^*_{s+2},\ldots,L^*_n)$$

has a uniquely defined irreducible component Q such that $x^*\in Q$ and Q is a curve which is contained in W. This curve Q can be constructed by the algorithm from [3]. We choose $\widetilde{x}\in Q$. So we have a criterion to check whether $\widetilde{x}\in W$. One see also immediately using the criteria to count multiplicity of a point from [6] that the number of points $y\in Q$ such that

$$\mu(x^*,\mathcal{Z}(\psi_1,\ldots,\psi_j))<\mu(y,\mathcal{Z}(\psi_1,\ldots,\psi_j))$$

is bounded from above by a polynomial in $(Dd)^n$. In the similar way one can consider the cases when one of the properties analogous to (i)–(vi) is not satisfied.

Hence replacing subsequently all the coefficients of the linear forms $L^*_{s+1},\ldots$, L^*_n by integer coefficients with lengths $O(n\log(dD))$ we shall obtain finally the required linear forms $L'''_{s+1},\ldots,L'''_n$ and the point x'''. Note also here that in the case when system (13) has no solutions and $\psi(x')\neq 0$ we can take just $x'''=x'$ and $L'''_j=L'_j$ for all j.

Now take as a base $x''=x_0$ and apply the described procedure recursively, i.e., replace each time when x''' is constructed x'' by x''' and return to the beginning. Thus, finally we shall come to the case when system (13) has no solutions. In this case set $x'=x'''$ and $L'_i=L'''_i$, $s+1\le i\le n$. The estimation for the working time of the described algorithm follows immediately from the estimations for working times of the applied algorithms. The lemma is proved.

REMARK 5 *Suppose that under conditions of Lemma 1 an integer $1\le j_1\le j$ and x_0 is a smooth point of the algebraic variety $\mathcal{Z}(\psi_1,\ldots,\psi_{j_1})$. Then one can add to the properties (i)–(vii) in the formulation of Lemma 1 the following one.*

(viii) The point x' is a smooth point of $\mathcal{Z}(\psi_1,\ldots,\psi_{j_1})$.

The proof of this variant of the lemma is similar to the initial one since by [6] we have a criterion to decide whether a point is smooth.

Now our aim is to prove Theorem 1. At first we shall prove assertion (i).

Set $\delta^{(0)}=1$, $j_0=0$. Further, recursively on step $a\ge 1$ we shall construct the following objects.

- Integers $j_a\ge 1$ and $\delta^{(a)}\ge 1$.
- A $\mathfrak{P}$–sequence $g_1,g_2,\ldots,g_{j_a}$ such that degree $\deg g_{j_a}=\delta^{(a)}$.
- A point $x_a\in W$ (which is given in the similar way as the point x_0) such that x_a is a smooth point of V, $Y_0(x_a)\neq 0$, and

$$\mu(x_a,\mathcal{Z}(g_1,\ldots,g_{j_a}))=\min_{x\in W}\mu(x,\mathcal{Z}(g_1,\ldots,g_{j_a})). \tag{14}$$

- Linear forms $L_{a,s+1}, L_{a,s+2}, \dots, L_{a,n}$ in $Y_0, Y_{s+1}, \dots, Y_n$ with integer coefficients of lengths $O(n \log(d\delta^{(a)}))$ such that $Y_0(x_a) \neq 0$, the point x_a is isolated in the intersection $W \cap \mathcal{Z}(L_{a,s+1}, \dots, L_{a,n})$ and the intersection of tangent spaces of W in the point x_a and $\mathcal{Z}(L_{a,s+1}, \dots, L_{a,n})$ is transversal, i.e., $T_{x_0,W} \cap \mathcal{Z}(L_{a,s+1}, \dots, L_{a,n}) = \{x_a\}$.

Step a is final if and only if $j_a = s = n - \dim W$.

Suppose that step $a-1$ is not final or $a = 1$. Let us describe step a of the recursion. Let $x_{a-1,0}, \dots, x_{a-1,n} \in \overline{k}$ be such that $x_{a-1} = (x_{a-1,0} : \ldots : x_{a-1,n})$.

Denote for brevity $j_{a-1} = r$. By (14) with a replaced by $a-1$ for every irreducible component W_1 of the algebraic variety $\mathcal{Z}(g_1, \dots, g_r)$ such that $x_{a-1} \in W_1$ we have $W_1 \supset W$ and the dimension $\dim W_1 = n - r$. Construct using the algorithm from [6], Section 6 (here we leave a simple exercise for the reader) linear forms $M_0, M_{r+1}, M_{r+2}, \dots, M_n$ with integer coefficients of lengths $O(n \log(\delta + 1))$ such that x_{a-1} is an isolated point of the intersection

$$\mathcal{Z}(g_1, \dots, g_r) \cap \mathcal{Z}(M_{r+1}, M_{r+2}, \dots, M_n)$$

in $\mathbb{P}^n(\overline{k})$, the linear form $M_0(x_{a-1}) \neq 0$, and the intersection

$$\mathcal{Z}(g_1, \dots, g_r) \cap \mathcal{Z}(M_{r+1} - \varepsilon_1 M_0, M_{r+2}, M_{r+3} \dots, M_n) = T$$

contains $\mu(x_{a-1}, \mathcal{Z}(g_1, \dots, g_r))$ different points in $\mathbb{P}^n(\overline{k(\varepsilon_1)})$ which are infinitesimal close to x_{a-1}. All the points from T are smooth points of the algebraic variety $\mathcal{Z}(g_1, \dots, g_r)$, see [6].

Enumerate $\delta = \delta^{(a-1)}, \delta^{(a-1)}+1, \dots$. For the considered value of δ construct a basis of the vector space of all homogeneous polynomials $g \in k[X_0, \dots, X_n]$ of degree δ such that $g(x_i) = 0$ for all $0 \le i \le a-1$. This can be effected by solving a linear system over k using representations of points x_i similar to (2) which are constructed on previous steps of the recursion. Denote by S the set of elements of the constructed basis.

If S is empty proceed to the next value of δ, i.e. to $\delta + 1$. Suppose that the set S is non–empty. Enumerate elements $g \in S$. For $g \in S$ apply Lemma 1 with $j = j_{a-1}$, $\psi_i = g_i$, $1 \le i \le j$, $\psi = g$ and decide whether g is vanishing on W.

Suppose that g is not vanishing on W. Then applying Lemma 1 construct a point x' and linear forms $L'_{s+1}, \dots, L'_n$. Set $x_a = x'$ and $L_{a,j} = L'_j$, $s+1 \le j \le n$. Using the algorithm from [3] construct representation similar to (2) for the point x_a. In this case set $j_a = j_{a-1}$, $\delta^{(a)} = \delta^{(a-1)}$.

Suppose that g is vanishing on W. Let $z \in T$. Let $z_0, \dots, z_n \in \overline{k(\varepsilon_1)}$ and $z = (z_0 : \ldots : z_n)$. Consider the system of equations and inequalities with coefficients from K in the variables $X_0, \dots, X_n$, Z

$$\begin{cases} \sum_{0 \le i \le n} |X_i - z_i|^2 < \varepsilon_2, & \\ g_i = 0, & 1 \le i \le r, \\ gZ - 1 = 0. & \end{cases} \tag{15}$$

System (15) has no solutions in $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$ if and only if g is vanishing on the irreducible component W_1 of $\mathcal{Z}(g_1, \dots, g_r)$ such that $z \in W_1$, cf. [4], [5]. Decide for every $z \in T$ whether system (15) has no solutions in $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$ and construct the subset $T(g) \subset T$ consisting of all points $z \in Z$ such that (15) has a solution in $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2)})$.

Then proceed to the next element $g \in S$. If all the elements from S are enumerated then construct the subset $S_1 \subset S$ consisting of all polynomials g vanishing on W and decide whether $\cup_{g \in S_1} T(g) = T$. If $\cup_{g \in S_1} T(g) \neq T$ then there is an irreducible component W_1 of $\mathcal{Z}(g_1, \ldots, g_r)$ and $z \in T$ such that $z \in W_1$ and all the polynomials from S are vanishing on W_1. Recall that $W_1 \supset W$. Hence there is no $\mathfrak{P}$–sequence $g_1, \ldots, g_{j_{a-1}}, \widetilde{g}$ such that $\widetilde{g}$ belongs to the linear space with the basis S. So we proceed to the next value of δ, i.e., to $\delta + 1$, in this case.

Suppose that $\cup_{g \in S_1} T(g) = T$. Then construct, cf. [5], [6], considering systems similar to (15) a linear combination

$$q = \sum_{g \in S_1} c_g g,$$

where c_g are integers with lengths $O(r \log(\delta + 1))$ such that q is not vanishing on every irreducible components W_1 of $\mathcal{Z}(g_1, \ldots, g_r)$ for which $x_{a-1} \in W_1$. Set $j_a = j_{a-1} + 1$, $\delta^{(a)} = \delta$ and $g_{j_a} = q$. Applying Lemma 1 (with $\psi = 1$) construct the required point x_a and linear forms $L_{a,s+1}, \ldots, L_{a,n}$. Using the algorithm from [3] construct representation similar to (2) for the point x_a. This finishes the description of step a and of all the algorithm.

Note that $a \leq \delta^{(a)} \binom{\delta^{(a)}+n}{n}$. Now the estimation for the working time of the described algorithm follows immediately from [7] and estimations for working times of the applied algorithms. Assertion (i) of Theorem 1 is proved.

Now our aim is to prove assertion (ii) of Theorem 1. Using (i) construct a $\mathfrak{P}$–sequence $g_1, \ldots, g_s$. Let $0 \leq r < s$ be an integer. Suppose that we have already constructed by recursion on r a point $x \in W$ which is a smooth point of $\mathcal{Z}(g_1, \ldots, g_s)$ and homogeneous polynomials

$$h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s} \in k[X_0, \ldots, X_n]$$

such that

(a) x is a smooth point of $\mathcal{Z}(h_1, \ldots, h_r)$,

(b) W is an irreducible component of $\mathcal{Z}(h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s})$,

(c) x is a smooth point of $\mathcal{Z}(h_1, \ldots, h_r, g_{r,r+1}, \ldots, g_{r,s})$,

(d) $g_{r,j} = \sum_{1 \leq v \leq j} q_{r,j,v} g_v$ where $q_{r,j,v} \in k[X_0, \ldots, X_n]$ are homogeneous polynomials and $\deg q_{r,j,v} = \deg g_j - \deg g_v$ for all $1 \leq v \leq j$.

(so in the case of the base of the recursion $r = 0$ a smooth point $x = x_0 \in W$ is given and we set $g_{0,j} = g_j$ for every $1 \leq j \leq s$). Our aim is to construct the polynomial h_{r+1} and homogeneous polynomials $g_{r+1,r+2}, \ldots, g_{r+1,s}$ such that properties (a)–(d) will be satisfied if one replace r by $r+1$ (may be with another point x).

Let $X_{i_0}(x) \neq 0$. We shall assume without loss of generality effecting if necessary a permutation of coordinates $\mathbb{P}^n(\overline{k})$ that $i_0 = 0$.

Denote $\psi_i = h_i / X_0^{\deg h_i}$, $1 \leq i \leq r$ and $\rho_j = g_{r,j} / X_0^{\deg g_{r,j}}$, $r + 1 \leq j \leq s$.

By $Z_i = X_i / X_0 - (X_i / X_0)(x)$, $1 \leq i \leq n$, denote the coordinate functions of the affine space $\mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. So $\psi_j, \rho_w \in \overline{k}[Z_1, \ldots, Z_n]$ for all j, w.

Construct using the algorithm from [6] the tangent space $T_{x,W}$ of the algebraic variety W in the point x. More precisely, construct linear forms $Y_1, \ldots, Y_s \in k(x)[Z_1, \ldots, Z_n]$ (recall that $k(x)$ is the field generated over k by the affine coordinate $(X_i/X_0)(x)$, $1 \le i \le n$, of the point x) such that $T_{x,W} = \mathcal{Z}(Y_1, \ldots, Y_s)$ and $d_x \psi_i = Y_i$ for every $1 \le i \le r$. Consider arbitrary polynomials $\varphi_j \in \overline{k}[Z_1, \ldots, Z_n]$, $r+1 \le j \le s$, and indices $1 \le i_{s+1} < \ldots < i_n \le n$ such that

$$\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s$$

is a system of local parameters of the algebraic variety W in the point x, the differentials $d_x \varphi_i = Y_i$ for every $r+1 \le i \le s$, and

$$\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{i_{s+1}}, \ldots, Z_{i_n}$$

is a system of local parameters of the algebraic variety $\{x\}$ consisting of one point x. We shall suppose without loss of generality that $i_j = j$ for all $s+1 \le j \le n$.

Effecting if necessary a permutation of coordinates $Z_1, \ldots, Z_s$ we shall assume without loss of generality that the minor of the Jacobi matrix in the point x

$$\det\left(\left(\partial \psi_i / \partial Z_j\right)(x)\right)_{1 \le i,j \le r} \ne 0. \tag{16}$$

Consider the ring of formal power series

$$\Omega = \overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]]. \tag{17}$$

This ring coincides with the ring of formal power series in $Z_1, \ldots, Z_n$ over $\overline{k}$. Therefore it contains the ring $k[X_1/X_0, \ldots, X_n/X_0]$. Each element F of the ring Ω can be represented in the form

$$F = \sum_{i_1, \ldots, i_n \ge 0} F_{i_1, \ldots, i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}, \tag{18}$$

where all $F_{i_1, \ldots, i_n} \in \overline{k}$. By

$$\widetilde{\mathfrak{P}} = (\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s)$$

denote the ideal of the ring Ω generated by the elements $\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s$. Let $F \in k[X_1/X_0, \ldots, X_n/X_0]$. Then

$$F \in \widetilde{\mathfrak{P}} \quad \text{if and only if} \quad \mathcal{Z}(F) \supset V \setminus \mathcal{Z}(X_0). \tag{19}$$

For an arbitrary formal power series F denote

$$\operatorname{ord} F = \min\{i_{r+1} + \ldots + i_s \ : \ F_{0,\ldots,0,i_{r+1},\ldots,i_n} \ne 0\}.$$

So $\operatorname{ord} F$ is a non–negative integer or $+\infty$.

Let (18) holds for a formal power series F. Set

$$\nu_0 = \nu_0(x, F) = \min\{i_{r+1} + \ldots + i_n \ : \ F_{0,\ldots,0,i_{r+1},\ldots,i_n} \ne 0\},$$
$$\operatorname{lf}(x, F) = \sum_{i_{r+1} + \ldots + i_n = \nu_0} F_{0,\ldots,0,i_{r+1},\ldots,i_n} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}.$$

So $\mathrm{lf}(x,F) \in \overline{k}[\varphi_{r+1},\dots,\varphi_s, Z_{s+1},\dots,Z_n]$. Denote by

$$\mathrm{Lf}(x,F) \in \overline{k}[Y_{r+1},\dots,Y_s, Z_{s+1},\dots,Z_n]$$

the polynomial such that $\mathrm{Lf}(x,F)(\varphi_{r+1},\dots,\varphi_s,Z_{s+1},\dots,Z_n) = \mathrm{lf}(x,F)$.

Introduce the operators $\mathcal{D}_j$, $r+1 \le j \le s$ of differentiation on the ring Ω by the formulas

$$\mathcal{D}_j(F) = \det \begin{pmatrix} \partial\psi_1/\partial Z_1 & \dots & \partial\psi_1/\partial Z_r & \partial\psi_1/\partial Z_j \\ \vdots & \vdots & \vdots & \vdots \\ \partial\psi_r/\partial Z_1 & \dots & \partial\psi_r/\partial Z_r & \partial\psi_r/\partial Z_j \\ \partial F/\partial Z_1 & \dots & \partial F/\partial Z_r & \partial F/\partial Z_j \end{pmatrix}.$$

Hence if $F \in \overline{k}[Z_1,\dots,Z_n]$ then degree relative to $Z_1,\dots,Z_n$

$$\deg \mathcal{D}_i(F) \le \deg F + \deg h_1 + \ldots + \deg h_r - r - 1. \tag{20}$$

If $F \in k[X_1/X_0,\dots,X_n/X_0]$ then $\mathcal{D}_i(F) \in k[X_1/X_0,\dots,X_n/X_0]$ for every $r+1 \le i \le s$. By Theorems 1, 2 and Lemma 18 from [7] we have

$$\mathrm{ord}\,\rho_{r+1} \le 1 + \frac{\deg h_1 \cdot \ldots \cdot \deg h_r \deg g_{r+1} \cdot \ldots \cdot \deg g_s}{\deg W} \le n^{2^{s^{C_0}}}$$

for an absolute constant $C_0 > 0$.

Let $\mu_0 = \min\{\mu(z, \mathcal{Z}(\psi_1,\dots,\psi_r,\rho_{r+1})) : z \in W\}$. Construct by Lemma 1 the point x' similar to x and such that

$$\mu(x', \mathcal{Z}(\psi_1,\dots,\psi_r,\rho_{r+1})) = \mu_0.$$

Replacing the point x by x' we shall suppose without loss of generality that $x = x'$.

LEMMA 2 *Let $\nu = \mathrm{ord}\,\rho_{r+1}$. Represent ρ_{r+1} as an element of the ring Ω*

$$\rho_{r+1} = \sum_{i_1,\dots,i_n \ge 0} a_{i_1,\dots,i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n},$$

where all $a_{i_1,\dots,i_n} \in \overline{k}$. Then $\nu = \nu_0(x,\rho_{r+1})$ or which is equivalent $\mathrm{lf}(x,\rho_{r+1}) \in \overline{k}[\varphi_{r+1},\dots,\varphi_s]$.

PROOF By R denote the local ring of the algebraic variety $\mathcal{Z}(h_1,\dots,h_r) \setminus \mathcal{Z}(X_0) = \mathcal{Z}(\psi_1,\dots,\psi_r)$ in the point x. So R is a regular local ring and hence is a factorial ring. There is a natural inclusion

$$R \longrightarrow \overline{k}[[\varphi_{r+1},\dots,\varphi_s, Z_{s+1},\dots,Z_n]] = \Omega_1,$$

where Ω_1 is a ring of formal power series in $\varphi_{r+1},\dots,\varphi_s$, $Z_{s+1},\dots,Z_n$ over $\overline{k}$. There is a natural epimorphism $p : \Omega \to \Omega_1$. Let $z \in R$ and $\widetilde{z}$ be an element of the ring Ω such that $p(\widetilde{z}) = z$. Set $\nu_0(x,z) = \nu_0(x,\widetilde{z})$ and $\mathrm{lf}(x,z) = p(\mathrm{lf}(x,\widetilde{z}))$. Then $\nu_0(x,z)$ and $\mathrm{lf}(x,z)$ do not depend on the choice of $\widetilde{z}$. Let $\overline{\rho}_{r+1} \in R$ be the image of ρ_{r+1}. We need to prove that $\mathrm{lf}(x,\overline{\rho}_{r+1}) \in \overline{k}[\varphi_{r+1},\dots,\varphi_s]$. Represent

$$\overline{\rho}_{r+1} = \lambda \prod_{i \in I} \eta_i^{e_i},$$

where η_i are irreducible elements of R and λ is an invertible element of R. Choose elements $\widetilde{\eta}_i \in \overline{k}(Z_1, \ldots, Z_n) \cap \Omega$ such that $p(\widetilde{\eta}_i) = \eta_i$ for every $i \in I$. Then $\mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})$ coincides with $\cup_{i \in I} \mathcal{Z}(\widetilde{\eta}_i, \psi_1, \ldots, \psi_r)$ in a neighborhood in the Zariski topology of x. Further, the multiplicity

$$\mu(x, \mathcal{Z}(\widetilde{\eta}_i, \psi_1, \ldots, \psi_r)) = \nu_0(x, \eta_i)$$

as it follows from the definition of multiplicity using Hilbert–Samuel polynomial, see [11]. Henceforth,

$$\mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) = \sum_{i \in I} \nu_0(x, \eta_i). \tag{21}$$

We have $\mathrm{lf}(x, \overline{\rho}_{r+1}) = \mathrm{lf}(x, \lambda) \prod_{i \in I} \mathrm{lf}(x, \eta_i)^{e_i}$. So it is sufficient to prove that $\mathrm{lf}(x, \eta_i) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ for every $i \in I$.

Suppose that $\mathrm{lf}(x, \overline{\rho}_{r+1}) \notin \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$. Then there is $i_0 \in I$ such that

$$\mathrm{lf}(x, \eta_{i_0}) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n] \setminus \overline{k}[\varphi_{r+1}, \ldots, \varphi_s].$$

Let ε_i be an infinitesimal relative to the field $k(\varepsilon_{s+1}, \ldots, \varepsilon_{i-1})$ for every $s+1 \leq i \leq n$. By $x'' \in W(\overline{k(\varepsilon_{s+1}, \ldots, \varepsilon_n)})$ denote the point which is infinitely close to x such that $Z_j(x'') = \varepsilon_j$, $s+1 \leq j \leq n$. By R'' denote the local ring of the algebraic variety W in the point x''. Hence $\overline{\rho}_{r+1}, \eta_i \in R''$, $i \in I$, and λ is an invertible element of R''. Consider the ring of formal power series

$$\Omega'' = \overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1} - Z_{s+1}(x''), \ldots, Z_n - Z_n(x'')]]. \tag{22}$$

For an element $F \in \Omega''$ define $\nu_0(x'', F)$ and $\mathrm{lf}(x'', F)$ replacing in the definition of $\nu_0(x, F)$ and $\mathrm{lf}(x, F)$ the ring Ω by Ω'' and $Z_{s+1}, \ldots, Z_n$ by $Z_{s+1} - Z_{s+1}(x''), \ldots, Z_n - Z_n(x'')$.

Hence $\nu_0(x'', \eta_i) \leq \nu_0(x, \eta_i)$, $i \in I$ and $\nu_0(x'', \eta_{i_0}) < \nu_0(x, \eta_{i_0})$ by the choice of i_0 and the point x''. On the other hand, similarly to (21) we have

$$\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) \leq \sum_{i \in I} \nu_0(x'', \eta_i).$$

Thus $\mu(x'', \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1})) < \mu(x, \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+1}))$. This contradiction proves the lemma.

LEMMA 3 *Let $F \in R$ be an element such that $\mathrm{lf}(x, F) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ and hence $\mathrm{Lf}(x, F) \in \overline{k}[Y_{r+1}, \ldots, Y_s]$. Then there is $r+1 \leq j \leq s$ such that $\mathrm{ord}(\mathcal{D}_j(F)) = \mathrm{ord}(F) - 1$ and*

$$\mathrm{lf}(x, \mathcal{D}_j(F)) = \sum_{r+1 \leq i \leq s} \frac{\partial\, \mathrm{Lf}(x, F)}{\partial Y_i}(\varphi_{r+1}, \ldots, \varphi_s)\, \mathrm{lf}(x, \mathcal{D}_j(\varphi_i)).$$

Hence $\mathrm{lf}(x, \mathcal{D}_j(F)) \in \overline{k}[\varphi_{r+1}, \ldots, \varphi_s]$ for this j.

PROOF By the definition of operators $\mathcal{D}_i$, (16) and since any linear combination of $\psi_{r+1}, \ldots, \psi_s$ is a local parameter in the point x the vectors

$$(\mathcal{D}_{r+1}(\psi_i)(x), \ldots, \mathcal{D}_s(\psi_i)(x)) \in (\overline{k})^{s-r}, \quad r+1 \leq i \leq s,$$

are linearly independent over $\overline{k}$. From here the assertions of the Lemma follow immediately.

Constructing first terms of the expansion of ρ_{r+1} in the ring of formal power series $k(x)[[Y_1,\dots,Y_s,Z_{s+1},\dots,Z_n]]$ compute $\mathrm{Lf}(x,\rho_{r+1})$ and $\nu_0(x,\rho_{r+1})$. Suppose that for some $0\le\alpha\le\nu_0(x,\rho_{r+1})-2$ we have already constructed indices $r+1\le j_1,\dots,j_\alpha\le s$ such that

$$\begin{aligned}&\mathrm{ord}\,\mathcal{D}_{j_\alpha}\dots\mathcal{D}_{j_1}\rho_{r+1}=\nu_0(x,\rho_{r+1})-\alpha,\\&\mathrm{Lf}(x,\mathcal{D}_{j_\alpha}\dots\mathcal{D}_{j_1}\rho_{r+1})\in k(x)[Y_{r+1},\dots,Y_s]\end{aligned}$$

(the base of the recursion is $\alpha=0$). At the next step of the recursion apply Lemma 3 to $F=\mathcal{D}_{j_\alpha}\dots\mathcal{D}_{j_1}\rho_{r+1}$ and compute an index $j_{\alpha+1}$ such that the formulated properties will be satisfied for $\alpha+1$. Finally we shall obtain indices $r+1\le j_1,\dots,j_\beta\le s$, $\beta=\nu_0(x,\rho_{r+1})-1$. Then set

$$\begin{aligned}&\psi_{r+1}=\mathcal{D}_{j_\beta}\dots\mathcal{D}_{j_1}\rho_{r+1}\in k(x)[Z_1,\dots,Z_n],\\&h_{r+1}=\psi_{r+1}X_0^{\deg_{Z_1,\dots,Z_n}\psi_{r+1}}\in k[X_0,\dots,X_n].\end{aligned}$$

Thus h_{r+1} is vanishing on W and x is smooth point of the algebraic variety $\mathcal{Z}(h_1,\dots,h_{r+1})$.

Let us show how to construct all the polynomials $g_{r+1,j}$ and $q_{r+1,j,v}$ such that conditions (b) and (d) hold with r replaced by $r+1$. Suppose that we have already construct the homogeneous polynomials $g_{r+1,j}$, $q_{r+1,j,v}$ for all $\alpha\le j\le s$, $1\le v\le j$ for some $r+3\le\alpha\le s+1$ and dimension of every irreducible component containing the point x of the algebraic variety

$$\mathcal{Z}(h_1,\dots,h_{r+1},g_{r+1,\alpha},\dots,g_{r+1,s})=S_\alpha$$

is $n-r-s+\alpha-2$. The algebraic variety W is an irreducible component of

$$\begin{aligned}&\mathcal{Z}(h_1,\dots,h_{r+1},g_{r,r+1},\dots,g_{r,s})=\\&\mathcal{Z}(h_1,\dots,h_{r+1},g_{r,r+1},\dots,g_{r,\alpha-1},g_{r+1,\alpha},\dots,g_{r+1,s})=\\&S_\alpha\cap\mathcal{Z}(g_{r,r+1},\dots,g_{r,\alpha-1}).\end{aligned}$$

By [6] we can compute the dimension of an algebraic variety (which is given by a system of polynomial equations) in the point x, i.e. the maximum of dimensions of irreducible components of the considered algebraic variety containing the point x. Therefore, cf. [4], [5], we can construct the homogeneous polynomials $g_{r+1,\alpha-1}$, $q_{r+1,\alpha-1,v}$, $1\le v\le\alpha-1$, such that $\deg q_{r+1,\alpha-1,v}=\deg g_{\alpha-1}-\deg g_v$, and the polynomial $g_{r+1,\alpha-1}$ is not vanishing on every irreducible component containing the point x of the algebraic variety S_α.

Hence dimension of every irreducible component containing the point x of the algebraic variety $S_{\alpha-1}$ is $n-r-s+\alpha-3$.

Thus, using decreasing recursion on α we shall construct all the polynomials $g_{r+1,v}$ and $q_{r+1,j,v}$ such that conditions (b) and (d) hold with r replaced by $r+1$. Finally applying Lemma 1 and Remark 5 in the case when $\psi=1$, the sequence $\psi_1,\dots,\psi_j$ is $h_1,\dots,h_{r+1},g_{r+1,r+2},\dots,g_{r+1,s}$ (so $j=s$) and $j_1=r+1$ construct a point x' and replace x by x'. Now conditions (a)–(d) hold with r replaced by $r+1$.

Thus, we shall construct finally the required in assertion (ii) of Theorem 1 homogeneous polynomials $h_1,\dots,h_s$. The fact that $\mathrm{Lf}(x,\rho_{r+1})\in\overline{k}[Y_{r+1},\dots,Y_s]$

and the inequality $\operatorname{ord} \rho_{r+1} \leq n^{2^{s^{C_0}}}$ are important for the estimation of the working time of the described algorithm. The inequalities $\deg h_i < n^{2^{s^C}} \deg g_i$, $1 \leq i \leq s$, follows from the estimate for $\operatorname{ord} \rho_{r+1}$ and (20), cf. Lemma 19 [7]. The estimation for the working time of the described algorithm now follows immediately from estimations for working times of the applied algorithms. Theorem 1 is completely proved.

2 Refinement of the cover

To prove Theorem 2 for the case of smooth cover we need to formulate a more precise result. Let V_α, $\alpha \in A_1$ be a family of defined over k and irreducible over k quasiprojective algebraic varieties in $\mathbb{P}^n(\overline{k})$. Let $\dim V_\alpha = n - s$ where $1 \leq s = s(\alpha) \leq n$. For every $\alpha \in A_1$ let homogeneous polynomials $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$ and indices $0 \leq i_1 < \ldots < i_s \leq n$ (these homogeneous polynomials and indices depend on α) be given. Denote

$$\Delta_\alpha = \det(\partial h_v / \partial X_{i_w})_{1 \leq v, w \leq s}.$$

Let V_α be a defined over k and irreducible over k component of the algebraic variety

$$\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(\Delta_\alpha)$$

for every $\alpha \in A_1$.

THEOREM 4 *Let V be the same algebraic variety as in the Introduction. Let W_β, $\beta \in B$ be a family of defined over k and irreducible over k projective algebraic varieties. Let $\dim W_\beta = n - s(\beta)$ where $1 \leq s(\beta) \leq n$. Let homogeneous polynomials $g_{\beta,1}, \ldots, g_{\beta,m(\beta)} \in k[X_0, \ldots, X_n]$. Denote $\mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}) = S_\beta$. Let*

$$W_\beta \subset \mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}) = S_\beta \subset V$$

for every $\beta \in B$. Suppose that

$$V \setminus \bigcup_{\beta \in B} W_\beta \subset \bigcup_{\alpha \in A_1} V_\alpha. \tag{23}$$

Then for every $\beta \in B$ there is a finite family of defined over k and irreducible over k projective algebraic varieties $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$ with $\dim W_{\beta,\gamma} = n - s(\gamma)$, $1 \leq s(\gamma) \leq n$, satisfying the following properties.

(a) For every $\beta \in B$, $\gamma \in \Gamma_\beta$ the inclusion

$$W_{\beta,\gamma} \subset W_\beta$$

holds.

(b) The inclusion

$$V \setminus \bigcup_{\beta \in B} \bigcup_{\gamma \in \Gamma_\beta} W_{\beta,\gamma} \subset \bigcup_{\alpha \in A_1} V_\alpha$$

holds.

(c) For every $\beta \in B$, $\gamma \in \Gamma_\beta$ there exist indices $\alpha_1, \ldots, \alpha_r \in A_1$ (here these indices and r depend on γ) such that $\dim W_{\beta,\gamma} < \dim V_{\alpha_i}$ for all $1 \le i \le r$ and $W_{\beta,\gamma}$ is an irreducible component of the algebraic variety

$$\mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}, \Delta_{\alpha_1}, \ldots, \Delta_{\alpha_r}).$$

(d) The inequality

$$(\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\beta)} \deg W_\beta \ge \sum_{\gamma \in \Gamma_\beta} (\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\gamma)} \deg W_{\beta,\gamma}$$

holds.

(e) For every $\beta_1, \beta_2 \in B$, $\gamma_1 \in \Gamma_{\beta_1}$, $\gamma_2 \in \Gamma_{\beta_2}$, if $(\beta_1, \gamma_1) \ne (\beta_2, \gamma_2)$ then $W_{\beta_1,\gamma_1} \not\subset W_{\beta_2,\gamma_2}$.

(f) For every $\alpha \in A_1$ for every $\beta \in B$, $\gamma \in \Gamma_\beta$ the inequality $\dim V_\alpha \cap W_{\beta,\gamma} < \dim W_{\beta,\gamma}$ holds.

PROOF We can take if necessary $\Gamma_\beta = \emptyset$ for some β. Hence we can suppose without loss of generality in what follows that $W_{\beta_1} \not\subset W_{\beta_2}$ if $\beta_1 \ne \beta_2$, and $W_{\beta_1} \not\subset \cup_{\alpha \in A_1} V_\alpha$ for all $\beta_1, \beta_2 \in B$. Denote by $\mathcal{F}$ the family of embeddings $W_\beta \subset S_\beta$, $\beta \in B$.

Now we describe the general plan of the proof. The construction of the required family $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$, $\beta \in B$ is effected recursively in a finite (this will be proved) number of steps starting from the first step. At the i-th step we construct a tree $\mathcal{T}_i$ and a family $\mathcal{F}_i$ of embeddings $W_\beta \subset S_\beta$, $\beta \in B_i$, herewith $\mathcal{F}_i$ and B_i are similar to $\mathcal{F}$ and B. The tree $\mathcal{T}_{i-1}$ is a subtree of $\mathcal{T}_i$ for every $i \ge 1$ (the tree $\mathcal{T}_0$ will be defined). We construct also a subset $E_i \subset B_i$ such that for every $\beta_1, \beta_2 \in B_i \setminus E_i$ we have $W_{\beta_1} \not\subset W_{\beta_2}$ if $\beta_1 \ne \beta_2$, and $W_{\beta_1} \not\subset \cup_{\alpha \in A_1} V_\alpha$. The set of leaves of the tree $\mathcal{T}_i$ is B_i. For every $\beta \in B_i$ the embedding $W_\beta \subset S_\beta$ is assigned to the leaf β. Denote $\dim W_\beta = n - s(\beta)$, $\beta \in B_i$.

The inclusion

$$V \setminus \bigcup_{\beta \in B_i \setminus E_i} W_\beta \subset \bigcup_{\alpha \in A_1} V_\alpha \tag{24}$$

will be proved. For every $\beta \in B$ denote by $\Gamma_{i,\beta}$ the set of all $\gamma \in B_i \setminus E_i$ which are descendants of β or coincide with β. For every $\beta \in B$ for every $\gamma \in \Gamma_{i,\beta}$ the inclusion

$$W_\gamma \subset W_\beta \tag{25}$$

will be satisfied. We shall prove that for every $\gamma \in \Gamma_{i,\beta}$ there exist indices $\alpha_1, \ldots, \alpha_r \in A_1$ (here these indices and r depend on γ) such that $\dim W_\gamma < \dim V_{\alpha_i}$ for all $1 \le i \le r$ and

$$S_\gamma = \mathcal{Z}(g_{\beta,1}, \ldots, g_{\beta,m(\beta)}, \Delta_{\alpha_1}, \ldots, \Delta_{\alpha_r}). \tag{26}$$

The inequality

$$(\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\beta)} \deg W_\beta \ge \sum_{\gamma \in \Gamma_{i,\beta}} (\max_{1 \le i \le r} \deg \Delta_{\alpha_i})^{n-s(\gamma)} \deg W_{\beta,\gamma} \tag{27}$$

will be ascertained.

Set $\mathcal{F}_0 = \mathcal{F}$, $B_0 = B$ and $E_0 = \emptyset$. The tree $\mathcal{T}_0$ has the root v^* (here we introduce a new element). All the leaves $\beta \in B$ of this tree are sons of v^*. Set $\Gamma_{0,\beta} = \{\beta\}$ for every $\beta \in B$. For $i = 0$ inclusion (24) follows here from (23). The inclusion (25) is trivial. The inequality (26) holds in this case. The equality (27) is also fulfilled with $r = 0$.

Let $i \geq 0$. The i-th step is final (or if $i = 0$ no construction is required) if and only if for every $u \in B_i \setminus E_i$ the algebraic variety W_u is an irreducible component of S_u and for every $\alpha \in A_1$ the inequality $\dim V_\alpha \cap W_u < \dim W_u$ holds. Let N be the number of the last step of the considered construction. By definition, put $\Gamma_\beta = \Gamma_{N,\beta}$ for every $\beta \in B$ and $W_{\beta,\gamma} = W_\gamma$ for every $\beta \in B$, $\gamma \in \Gamma_\beta$. Then the required assertions (a)–(d) follow from (25), (24), (26) and (27) for $i = N$. The assertion (e) of the theorem holds since for every two distinct $\beta_1, \beta_2 \in B_N \setminus E_N$ we have $W_{\beta_1} \not\subset W_{\beta_2}$. The last assertion (f) is satisfied since for every $\alpha \in A_1$, $\beta \in B_N \setminus E_N$ the inequality $\dim V_\alpha \cap W_\beta < \dim W_\beta$ holds.

We shall suppose without loss of generality that our construction contains at least one step.

Now we go to details. Suppose that the $(i-1)$-th step is not final or $i = 1$. Let us describe how to effect the i-th step. We suppose that $\mathcal{T}_{i-1}$, $\mathcal{F}_{i-1}$ and E_{i-1} are already constructed and (24), (25), (26), (27) are proved for $i - 1$ if $i > 1$. In the case $i - 1 = 0$ (24), (25), (26), (27) also hold as we have seen.

Since the $(i-1)$-th step is not final or $i = 1$ at least one of the following conditions holds:

(a) there are $u \in B_{i-1} \setminus E_{i-1}$ and a defined over k and irreducible over k component W of S_u such that $W_u \subset W$ and $W_u \neq W$.

(b) there is $\alpha \in A_1$ such that $\dim V_\alpha \cap W_u = \dim W_u$.

Under condition (a) $W \not\subset \bigcup_{\beta \in B_{i-1} \setminus E_{i-1}} W_\beta$. Hence by (24) (for $i - 1$) there is $\alpha \in A_1$ such that $V_\alpha \cap W$ contains a non–empty open in the Zariski topology subset of W. Hence the closure in the Zariski topology $\overline{V}_\alpha \supset W$ and

$$\overline{V}_\alpha \supset W_u. \tag{28}$$

The second condition $\dim V_\alpha \cap W_u = \dim W_u$ also implies (28). Choose an index α such that (28) holds and under condition (a) $\overline{V}_\alpha \supset W$.

Suppose that $\mathcal{Z}(\Delta_\alpha) \supset W_u$ (so condition (a) holds). Then by definition there is a unique son u_1 of u in the tree $\mathcal{T}_i$ (we suppose without loss of generality that this new index u_1 is not an integer and does not belong to any set of indices B_ι introduced previously). To this son u_1 assign the embedding $W_u \subset S_u \cap \mathcal{Z}(\Delta_\alpha)$. So $W_{u_1} = W_u$ and $S_{u_1} = S_u \cap \mathcal{Z}(\Delta_\alpha)$. The set of leaves of $\mathcal{T}_i$ is by definition $B_{i-1} \cup \{u_1\} \setminus \{u\}$ and $E_i = E_{i-1}$. Hence for every two distinct $\beta_1, \beta_2 \in B_i \setminus E_i$ we have $W_{\beta_1} \not\subset W_{\beta_2}$. Thus, the tree $\mathcal{T}_i$ is constructed in this case. The required (24), (25), (26), (27) for i follow from the same assertions for $i - 1$ in this case. Note here that $W \not\subset S_{u_1}$ in the considered case.

Suppose that $\mathcal{Z}(\Delta_\alpha) \not\supset W_u$. Represent

$$\mathcal{Z}(\Delta_\alpha) \cap W_u = \bigcup_{\beta \in B_u} W_\beta,$$

where W_β, $\beta \in B_u$ is the family of all defined over k and irreducible over k components of the algebraic variety $\mathcal{Z}(\Delta_\alpha) \cap W_u$ (we suppose without loss of generality that all indices from B_u are not integers and do not belong to any set of indices B_ι introduced previously).

Denote by E_u the subset of all $\beta \in B_u$ such that there is $\beta_1 \in B_{i-1} \setminus (E_{i-1} \cup \{u\})$ with $W_\beta \subset W_{\beta_1}$ or $W_\beta \subset \cup_{\alpha \in A_1} V_\alpha$.

By definition the set of sons of u in the tree $\mathcal{T}_i$ is B_u. To each $\beta \in B_u$ assign the embedding $W_\beta \subset S_u \cap \mathcal{Z}(\Delta_\alpha) = S_\beta$. By definition the set of leaves of the tree $\mathcal{T}_i$ is

$$B_i = (B_{i-1} \cup B_u) \setminus \{u\}.$$

By definition put

$$E_i = (E_{i-1} \cup E_u) \setminus \{u\}.$$

Hence for every two distinct $\beta_1, \beta_2 \in B_i \setminus E_i$ we have $W_{\beta_1} \not\subset W_{\beta_2}$. Thus, the tree $\mathcal{T}_i$ is constructed in this case.

Note that $B_i \setminus E_i = (B_{i-1} \setminus (E_{i-1} \cup \{u\})) \cup (B_u \setminus E_u)$. Hence

$$W_u \setminus \left(\bigcup_{\beta \in B_u \setminus E_u} W_\beta \cup \bigcup_{\beta \in B_{i-1} \setminus (E_{i-1} \cup \{u\})} W_\beta \right) \subset W_u \setminus \mathcal{Z}(\Delta_\alpha) \subset V_\alpha$$

in the considered case. Hence (24) for i follows from the same inclusion for $i-1$. The required (25), (26), (27) for i follow from the same assertions for $i-1$ and the Bézout theorem in this case.

To prove that our construction consists of only a finite number of steps we introduce an invariant $a(\mathcal{F})$ corresponding to the family $\mathcal{F}$ (or similar one) of embeddings $W_\beta \subset S_\beta$, $\beta \in B$ from the formulation of the theorem (herewith B is not fixed in this invariant).

By $\mathbb{Z}_+ = \{z \in \mathbb{Z} : z \geq 0\}$ denote the set of all non–negative integers. Set $Z(j) = \mathbb{Z}_+^{j+2}$ for $j \in \mathbb{Z}_+$. Consider the lexicographic order on $Z(j)$. Namely, let $x = (x_1, \ldots, x_{j+2})$, $y = (y_1, \ldots, y_{j+2})$ be two elements from $Z(j)$. Then $x > y$ if and only if there is i such that $1 \leq i \leq j+2$ and

$$x_1 = y_1, \ \ldots, \ x_{i-1} = y_{i-1} \quad \text{and} \quad x_i > y_i.$$

By definition put $Z^* = Z(1) \times Z(2) \times \ldots \times Z(n)$. Consider the lexicographic order on the set Z^*. Namely, let $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$ be two elements from Z^*. Then $x > y$ if and only if there is i such that $1 \leq i \leq n$ and

$$x_1 = y_1, \ \ldots, \ x_{i-1} = y_{i-1} \quad \text{and} \quad x_i > y_i.$$

Note that every strictly descending sequence of elements of Z^* is finite, i.e., Z^* satisfies descending chain condition.

By $S_{\beta,i}$ denote the union of all irreducible components W of S_β such that dimension $\dim W = n - i$ and $W \supset W_\beta$. So if $S_{\beta,i} \neq \emptyset$ then $0 \leq i \leq s(\beta)$. Set $\deg S_{\beta,i} = s_{\beta,i}$ and $\deg W_\beta = w_\beta$ for all i, β.

In what follows we shall suppose without loss of generality that $B \cap \mathbb{Z} = \emptyset$ introducing if necessary new indices. By $B^{(j)}$, $1 \leq j \leq n$, denote the set of all $\beta \in B$ such that $s(\beta) = j$. By definition, put

$$w_j = \sum_{\beta \in B^{(j)}} w_\beta, \quad 1 \leq j \leq n,$$

$$s_{j,i} = \sum_{\beta \in B^{(j)}} s_{\beta,i}, \quad 0 \leq i \leq j, \ 1 \leq j \leq n,$$

$$a_j = (w_j, s_{j,0}, s_{j,1}, \ldots, s_{j,j}) \in Z(j), \quad 1 \le j \le n,$$
$$a(\mathcal{F}) = (a_1, \ldots, a_n) \in Z^*.$$

Now note that for every $i \geq 1$ if the described construction of the family $W_{\beta,\gamma}$, $\gamma \in \Gamma_\beta$, $\beta \in B$ consists of at least i steps then $a(\mathcal{F}_{i-1}) > a(\mathcal{F}_i)$. Hence by the descending chain condition there is only a finite number N of steps. The theorem is proved.

REMARK 6 *Note that if under conditions of Theorem 4 additionally for every $\alpha \in A_1$, $\beta \in B$ we have $W_\beta \not\supset V_\alpha$ then for every $\alpha \in A_1$, $\beta \in B$, $\gamma \in \Gamma_\beta$ the inequality* $\dim V_\alpha \cap W_{\beta,\gamma} < \dim V_\alpha$ *holds.*

3 Proof of Theorem 2 for the case of smooth cover

Under conditions of Theorem 4 we shall suppose without loss of generality that for every distinct $\beta_1, \beta_2 \in B$ the intersection $\Gamma_{\beta_1} \cap \Gamma_{\beta_2} = \emptyset$. Denote $W_\gamma = W_{\beta,\gamma}$ for every $\beta \in B$, $\gamma \in \Gamma_\beta$.

In what follows we use new notations which is different from ones of the proof of Theorem 4. Let $i \geq 1$ be an integer. By A_i, B_i and Γ_i denote respectively the sets A_1, B and $\cup_{\beta \in B} \Gamma_\beta$ in old notation of Theorem 4. Then in the construction of Theorem 4 we have in input the pair of families

$$V_\alpha,\ \alpha \in A_i, \quad W_\beta \subset S_\beta,\ \beta \in B_i, \tag{29}$$

and in output the pair of families

$$V_\alpha,\ \alpha \in A_i, \quad W_\gamma \subset S_\gamma,\ \gamma \in \Gamma_i. \tag{30}$$

The construction of the required smooth cover V_α, $\alpha \in A$ is effected recursively in a finite number of steps starting from the first step. By W_γ, $\gamma \in \Gamma_0$ denote the family of all defined over k and irreducible over k components of V and set $S_\gamma = \mathcal{Z}(f_1, \ldots, f_m)$ for every $\gamma \in \Gamma_0$. Set $A_0 = \emptyset$. We can assume without loss of generality that $\Gamma_0 \neq \emptyset$.

Let us describe the i-th step, $i \geq 1$. At the beginning of this step the pair of families (30) with i replaced by $i-1$ is constructed and $\Gamma_{i-1} \neq \emptyset$. Set

$$B_i = \Gamma_{i-1}, \quad A_i = A_{i-1} \cup \Gamma_{i-1}$$

(we can suppose without loss of generality here that $A_{i-1} \cap \Gamma_{i-1} = \emptyset$ introducing if necessary new indices). Let $\dim W_\beta = n - s(\beta)$ where $1 \leq s(\beta) \leq n$ for every $\beta \in B_i$. Applying Theorem 1 for every $\beta \in B_i$ construct a family of homogeneous polynomials $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$, indices $0 \leq i_1 < \ldots < i_s \leq n$ (these homogeneous polynomials and indices depend on β, $s = s(\beta)$) and the polynomial

$$\Delta_\beta = \det(\partial h_v / \partial X_{i_w})_{1 \leq v,w \leq s}$$

such that $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ is an irreducible component of the algebraic variety

$$\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(\Delta_\beta).$$

Hence $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ is a smooth quasiprojective algebraic variety. Set $V_\beta = W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ for every $\beta \in B_i$.

Then applying Theorem 4 to (29) we get the pair of families (30). If $\Gamma_i = \emptyset$ then V_α, $\alpha \in A_i$ is the required smooth cover. If $\Gamma_i \neq \emptyset$ we proceed to the $(i+1)$-th step.

By the assertion (f) of Theorem 4 there is at most n steps in the described construction. The required in Theorem 2 estimations for degrees and sizes of coefficients follow immediately from Theorem 1 and Theorem 4, see also the remarks about representation (6) in the Introduction. The theorem for the case of smooth cover is proved.

4 Construction of a partial order on a set of irreducible algebraic varieties

Let W_β, $\beta \in B$ be a family of defined over k and irreducible over k algebraic varieties which are given in the form (6) from the Introduction. So $\dim W_\beta = n - s(\beta)$, $1 \le s(\beta) \le n$. Let $W_{\beta_1} \neq W_{\beta_2}$ for all $\beta_1 \neq \beta_2$. In this section we shall construct a partial order and a linear order on the set $\{W_\beta : \beta \in B\}$ or which is equivalent on B.

By B_s denote the subset of all $\beta \in B$ such that $\dim W_\beta = n - s$, $1 \le s \le n$. For every $1 \le s_1 < s_2 \le n$ for every $\beta_1 \in B_{s_1}$, $\beta_2 \in B_{s_2}$ set $\beta_1 < \beta_2$. Thus we get a partial order on B which we shall call preliminary. Now it is sufficient to construct a partial order and a linear order on every set B_s, $1 \le s \le n$. So in what follows without loss of generality we shall suppose that s is fixed.

For every $\beta \in B_s$ consider, see Theorem 1, a family of homogeneous polynomials $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$, indices $0 \le i_1 < \ldots < i_s \le n$ (these homogeneous polynomials and indices depend on β) and the polynomial

$$\Delta_\beta = \det(\partial h_v / \partial X_{i_w})_{1 \le v, w \le s}$$

such that $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ is an irreducible component of the algebraic variety

$$\mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(\Delta_\beta).$$

Hence $W_\beta \setminus \mathcal{Z}(\Delta_\beta)$ is a smooth quasiprojective algebraic variety. We shall denote also $h_i = h_{\beta,i}$, $1 \le i \le s$, when the dependence on β will be essential. Define the family

$$\mathcal{H} = \{h_{\beta,i}\}_{\beta \in B_s,\, 1 \le i \le s}.$$

Let $\delta_s = \max_{\beta \in B_s, 1 \le i \le s} \deg h_{\beta,i}$. In what follows we shall suppose without loss of generality that $\deg h_{\beta,i} = \delta_s$ for all $\beta \in B_s$, $1 \le i \le s$, multiplying if necessary each $h_{\beta,i}$ by a monomial which is not vanishing on W_β.

Define the function

$$\sigma(\mathcal{H}) : B_s \times B_s \longrightarrow \{0, 1\}$$

as follows. Denote for brevity $\sigma = \sigma(\mathcal{H})$. Set $\sigma(\beta, \beta') = 1$ (respectively $\sigma(\beta, \beta') = 0$) if and only if all the polynomials $h_{\beta,1}, \ldots, h_{\beta,s}$ are vanishing (respectively at least one of the polynomials $h_{\beta,1}, \ldots, h_{\beta,s}$ is not vanishing) on the algebraic variety $W_{\beta'}$. For every $(\beta, \beta') \in B_s \times B_s$ such that $\sigma(\beta, \beta') = 0$ define also an index $i_0 = i_0(\beta, \beta')$ for which h_{β,i_0} is not vanishing on $W_{\beta'}$.

For every $\tau \in B_s$ define the sets

$$B'_\tau = B'_\tau(\mathcal{H}) = \{(\beta', \beta) \in B_s \times B_s \,:\, \sigma(\beta', \tau) = 1 \,\&$$
$$\sigma(\tau, \beta) = 1 \,\&\, \sigma(\beta', \beta) = 0\,\}$$
$$B_\tau = B_\tau(\mathcal{H}) = \{\beta \,:\, \exists \beta'(\,(\beta', \beta) \in B'_\tau\,)\,\}.$$

Let us prove that we can construct a family

$$\widetilde{\mathcal{H}} = \{\widetilde{h}_{\beta,i}\}_{\beta \in B_s,\, 1 \le i \le s}$$

similar to $\mathcal{H}$ such that replacing $\mathcal{H}$ by $\widetilde{\mathcal{H}}$ we get a new family $\mathcal{H}$ for which additionally (35) holds, see below. Let $\tau \in B_s$. At first let us show how to construct a new family $\widetilde{\mathcal{H}}$ and the function $\sigma(\widetilde{\mathcal{H}})$ similar to $\mathcal{H}$ and $\sigma(\mathcal{H})$ such that for every $\tau \in B_s$ for every $\beta \in B_\tau(\mathcal{H})$

$$\sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 0, \tag{31}$$

and for every $\tau, \beta \in B_s$

$$\sigma(\widetilde{\mathcal{H}})(\tau, \beta) \le \sigma(\mathcal{H})(\tau, \beta). \tag{32}$$

Set

$$\widetilde{h}_{\tau,i} = h_{\tau,i} \quad \text{for all} \quad \tau \in B_s,\ 1 \le i \le s - 1. \tag{33}$$

It remains to define $\widetilde{h}_{\tau,s}$ for all τ.

Construct a function $\rho : B_\tau \to B_s$ satisfying the condition that

$$(\rho(\beta), \beta) \in B'_\tau$$

for every $\beta \in B_\tau$. We shall denote also $\rho = \rho(\tau, \mathcal{H})$.

Set for all $\tau \in B_s$

$$\widetilde{h}_{\tau,s} = h_{\tau,s} + \sum_{\beta \in B_\tau} c_\beta h_{\rho(\beta), i_0(\rho(\beta),\beta)}, \tag{34}$$

where c_β, $\beta \in B_\tau$, are some elements of k (one should choose them) such that the required properties (31), (32) hold and the function

$$\widetilde{\Delta}_\tau = \det(\partial \widetilde{h}_u / \partial X_{i_v})_{1 \le u,v \le s}$$

is not vanishing on W_τ (here the indices $0 \le i_1 < \ldots < i_s \le n$ are the same as they were defined above for Δ_τ). Besides that, we choose $c_\beta \in \mathbb{Z}$ with lengths $\mathrm{l}(c_\beta) = O(\log(2 + \#B_s))$ for all $\beta \in B_\tau$.

For every $\tau \in B_s$ define the sets $B'_\tau(\widetilde{\mathcal{H}})$, $B_\tau(\widetilde{\mathcal{H}})$ and the function $\rho(\tau, \widetilde{\mathcal{H}})$ replacing in the definitions of $B'_\tau(\mathcal{H})$, $B_\tau(\mathcal{H})$ and $\rho(\mathcal{H})$ the family $\mathcal{H}$ by $\widetilde{\mathcal{H}}$.

LEMMA 4 *For every $\tau \in B_s$ the set $B_\tau(\widetilde{\mathcal{H}}) = \emptyset$.*

PROOF Let us show that if $\beta' \notin B_\tau(\mathcal{H})$ then $\sigma(\mathcal{H})(\tau, \beta') = \sigma(\widetilde{\mathcal{H}})(\tau, \beta')$. Indeed, we have $\sigma(\mathcal{H})(\tau, \beta') \ge \sigma(\widetilde{\mathcal{H}})(\tau, \beta')$ for all τ, β'. Therefore, it is sufficient to consider the case when $\sigma(\mathcal{H})(\tau, \beta') = 1$. The condition $\beta' \notin B_\tau(\mathcal{H})$ implies that for every $\beta \in B_\tau(\mathcal{H})$ the polynomial $h_{\rho(\beta), i_0(\rho(\beta),\beta)}$ is vanishing on $W_{\beta'}$. Hence by (33) and (34) $\sigma(\widetilde{\mathcal{H}})(\tau, \beta') = 1$ which proves our assertion.

Now suppose that $\beta \in B_\tau(\widetilde{\mathcal{H}}) \neq \emptyset$ for some τ. Set $\beta_1 = \rho(\tau, \widetilde{\mathcal{H}})(\beta)$. Then $\sigma(\mathcal{H})(\beta_1, \beta) = 1$ since, otherwise, $\sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 0$.

If $\beta \notin B_{\beta_1}(\mathcal{H})$ then as we have proved $\sigma(\widetilde{\mathcal{H}})(\beta_1, \beta) = 1$. This leads to a contradiction.

Therefore $\beta \in B_{\beta_1}(\mathcal{H})$. Set $\beta_2 = \rho(\beta_1, \mathcal{H})(\beta)$. So $\sigma(\mathcal{H})(\beta_2, \beta) = 0$ and $\sigma(\mathcal{H})(\beta_2, \beta_1) = 1$. On the other hand,

$$\sigma(\mathcal{H})(\beta_1, \tau) = \sigma(\widetilde{\mathcal{H}})(\beta_1, \tau) = 1.$$

Hence $\sigma(\mathcal{H})(\beta_2, \tau) = 1$. Recall that

$$\sigma(\mathcal{H})(\tau, \beta) = \sigma(\widetilde{\mathcal{H}})(\tau, \beta) = 1.$$

Hence $\sigma(\mathcal{H})(\beta_2, \beta) = 1$. This contradiction proves the lemma.

Now replacing the family $\mathcal{H}$ by $\widetilde{\mathcal{H}}$ we shall suppose in what follows that

$$B_\tau(\mathcal{H}) = \emptyset \quad \text{for all} \quad \tau \in B_s. \tag{35}$$

Define the equivalence relation on the set B_s as follows. Two elements $\beta, \tau \in B_s$ are equivalent if and only if $\sigma(\beta, \tau) = 1$ and $\sigma(\tau, \beta) = 1$ (the transitiveness of this relation follows from (35)). Construct the factor set $\overline{B}_s$ of B_s by this equivalence. Denote by $\pi : B_s \longrightarrow \overline{B}_s$, $\pi(\beta) = \overline{\beta}$, the natural projection. By (35) the function σ can be represented in the form $\sigma = \overline{\sigma} \circ (\pi \times \pi)$ for a uniquely defined function $\overline{\sigma} : \overline{B}_s \times \overline{B}_s \longrightarrow \{0, 1\}$.

Introduce a partial order on $\overline{B}_s$ as follows. Let $u, v \in \overline{B}_s$. Then $u \geq v$ if and only if $\overline{\sigma}(u, v) = 1$ (the transitiveness of this partial order follows from (35)).

For every $u, v \in \overline{B}_s$, $\beta \in u$, $\tau \in v$ such that $u > v$ by definition put $\beta > \tau$. Thus we get a partial order on B_s. The required partial order on B is by definition the minimal partial order (it is a subset of $B \times B$) containing all the constructed partial orders on B_s, $1 \leq s \leq n$, and the preliminary partial order on B described at the beginning of the section.

It is known that every partial order on a finite set can be continued till a linear order. So we continue the constructed partial order on B till a linear order. The obtained linear order is the required linear order on B.

Consider a family of linearly independent linear forms

$$Y_i = \sum_{0 \leq j \leq n} y_{i,j} X_j, \quad 0 \leq i \leq n \tag{36}$$

where $y_{i,j} \in k$ for all i, j. Represent also

$$X_i = \sum_{0 \leq j \leq n} x_{i,j} Y_j, \quad 0 \leq i \leq n \tag{37}$$

where $x_{i,j} \in k$ for all i, j. For every $u \in \overline{B}_s$ consider homogeneous polynomials

$$h_{u,i} = \sum_{\beta \in u} c_{\beta,i} h_{\beta,i}, \quad 1 \leq i \leq s, \tag{38}$$

where $c_{\beta,i} \in k$ for all β, i. Set

$$\Delta_u = \det(\partial h_{u,i} / \partial Y_j)_{1 \leq i,j \leq s} = \det(\sum_{0 \leq v \leq n} x_{v,j} \partial h_{u,i} / \partial X_v)_{1 \leq i,j \leq s}.$$

We get immediately (considering at first all $x_{i,j}$ and $c_{\beta,i}$ as variables) that there are linear forms (36) and homogeneous polynomials (38) such that

- for every $\tau \in B_s$ the algebraic variety $W_\tau \subset \mathcal{Z}(h_{u,1}, \dots, h_{u,s})$ if and only if $u \geq \overline{\tau}$ with respect to the constructed partial order on $\overline{B}_s$.
- for every $\tau \in u$ the polynomial Δ_u is not vanishing on W_τ (and hence $W_\tau \setminus \mathcal{Z}(\Delta_u)$ is an irreducible component of $\mathcal{Z}(h_{u,1}, \dots, h_{u,s}) \setminus \mathcal{Z}(\Delta_u)$).

Besides that, one can choose additionally all $x_{i,j}, c_{\beta,i} \in \mathbb{Z}$ with lengths $O(n + \log(1 + \#B_s))$.

5 Proof of Theorem 2 for the case of smooth stratification

We shall prove Theorem 2 in a slightly more general situation. Namely, let projective algebraic varieties $V^{(i)}$, $1 \leq i \leq b$, be similar to $W^{(i)}$, $1 \leq i \leq a$ from the Introduction. Let homogeneous polynomials $g_j^{(i)}$, $1 \leq i \leq b$, $1 \leq j \leq \mu(i)$, be similar to the polynomials $f_j^{(i)}$, $1 \leq i \leq a$, $1 \leq j \leq m(i)$ from the Introduction. Hence $V^{(i)}$, $1 \leq i \leq b$, is a union of some irreducible components of the algebraic variety $\mathcal{Z}(g_1^{(i)}, \dots, g_{\mu(i)}^{(i)})$. Suppose that $V^{(1)} = V$ and $g_j^{(1)} = f_j$, $1 \leq j \leq m = \mu(1)$. Set

$$V' = V^{(1)} \setminus \bigcup_{2 \leq i \leq b} V^{(i)}.$$

Let degrees and lengths of integer coefficients of homogeneous polynomials $g_j^{(i)}$, $1 \leq i \leq b$, $1 \leq j \leq \mu(i)$, satisfy the same estimates as degrees and lengths of integer coefficients of $f_1, \dots, f_m$ do. Replacing in Definition 1 V by V' we get the definition of smooth cover and smooth stratification of a quasiprojective algebraic variety. Let us replace in the formulation of Theorem 2 the algebraic variety V by V'. We shall prove Theorem 2 in the case of smooth stratification in this new formulation for the quasiprojective algebraic variety V'.

Of course the new formulation of Theorem 2 is a consequence of the initial one (for V) though there is a difference. Namely, it may happen that $\dim V' < \dim V$ and in this case the new formulation of Theorem 2 is important for applying the inductive assumption, see below.

We shall denote in this section the required smooth stratification of the algebraic variety V' by V'_α, $\alpha \in A$. Let $\dim V'_\alpha = n - s(\alpha)$ where $1 \leq s(\alpha) \leq n$ for every $\alpha \in A$. We shall prove that there is an absolute constant $C_1 > 0$ such that if $\dim V' \leq n - s$ where $1 \leq s \leq n$ then

$$\sum_{\alpha \in A} d^{n-s(\alpha)} \deg \overline{V'_\alpha} \leq n^{2^{(n(n-s+1))^{C_1}}} d^{(n+s)(n-s+1)/2}, \tag{39}$$

where $\overline{V'_\alpha}$ is the closure in the Zariski topology of V'_α.

In our construction we shall use induction on $\dim V'$. The base $\dim V' = -1$, i.e., $V' = \emptyset$, is trivial.

The construction of the smooth stratification V'_α, $\alpha \in A$ is effected recursively in a finite number of steps starting from the first step (this recursion is not the induction on $\dim V'$).

By W_γ, $\gamma \in \Gamma_0$ denote the family of all defined over k and irreducible over k components of V (to avoid ambiguities we shall suppose without loss of generality that all elements of Γ_0 are not integers). Replace in Section 4 the family W_β, $\beta \in B$ by W_γ, $\gamma \in \Gamma_0$ and construct a linear order on Γ_0 using the method from this section. For every $\gamma \in \Gamma_0$ construct also homogeneous polynomials $h_j = h_{\overline{\gamma},j} \in k[X_0, \ldots, X_n]$, $1 \le j \le s$ and the polynomial $\Delta_{\overline{\gamma}}$, where $\overline{\gamma} \in \overline{(\Gamma_0)}_s$, см. Раздел 4. We shall denote also $h_{\gamma,j} = h_{\overline{\gamma},j}$, $1 \le j \le s = s(\gamma)$, when the dependence on γ will be important. Denote $\Delta_\gamma = \Delta_{\overline{\gamma}}$ for every $\gamma \in \Gamma_0$. Set

$$W'_{0,\gamma} = W_\gamma \setminus \left(\bigcup_{\tau<\gamma,\, \tau\in\Gamma_0} W_\tau \cup \bigcup_{2\le j\le b} V^{(j)} \right)$$

for every $\gamma \in \Gamma_0$ (here and below in similar situations $\tau < \gamma$ means with respect to the introduced linear order on Γ_0). Set $A_0 = \emptyset$. We can suppose without loss of generality that $\Gamma_0 \ne \emptyset$.

Let us describe the objects known at the beginning of the i-th step, $i \ge 1$.

- The family V_α, $\alpha \in A_{i-1}$ of defined over k and irreducible over k quasiprojective algebraic varieties in $\mathbb{P}^n(\overline{k})$ is constructed. Let $\dim V_\alpha = n-s$ where $1 \le s = s(\alpha) \le n$. For every $\alpha \in A_{i-1}$ the homogeneous polynomials

$$h_1, \ldots, h_s \in k[X_0, \ldots, X_n] \tag{40}$$

  and linear forms $Y_0, \ldots, Y_n \in k[X_0, \ldots, X_n]$ are given (these homogeneous polynomials depend on α, $s = s(\alpha)$ and we shall denote also $h_j = h_{\alpha,j}$ when the dependence on α will be important). The inequalities

$$\deg h_{\alpha,j} \le n^{2^{s(\alpha)^{C_2}}} d \quad 1 \le j \le s(\alpha), \tag{41}$$

  holds for every $\alpha \in A_{i-1}$ where $C_2 > 0$ is an absolute constant. We shall suppose that (36) and (37), Section 4 hold. Denote

$$\Delta_\alpha = \det(\partial h_v/\partial Y_w)_{1\le v,w\le s} = \det(\sum_{0\le u\le n} x_{u,w}\partial h_v/\partial X_u)_{1\le v,w\le s}.$$

  The algebraic variety V_α is an irreducible component of the algebraic variety

$$\mathcal{Z}(h_{\alpha,1}, \ldots, h_{\alpha,s}) \setminus \mathcal{Z}(\Delta_\alpha)$$

  for every $\alpha \in A_{i-1}$. For every $\alpha \in A_{i-1}$ denote $W_\alpha = \overline{V_\alpha}$ where $\overline{V_\alpha}$ is the closure in the Zariski topology of V_α.

- For every $\alpha \in A_{i-1}$ the defined over k and irreducible over k quasiprojective algebraic variety

$$V'_\alpha \subset V_\alpha \setminus \bigcup_{2\le j\le b} V^{(j)}$$

  is constructed such that V'_α is a non–empty open in the Zariski topology subset of V_α (hence V'_α is smooth and $V_\alpha \not\subset \bigcup_{2\le j\le b} V^{(j)}$).

- The subset $\Gamma_{i-1} \subset \Gamma_0$ is constructed such that the number of elements $\#\Gamma_{i-1} \le 1 - i + \#\Gamma_0$ and for every $\gamma \in \Gamma_{i-1}$ for every $\gamma_1 \in \Gamma_0 \setminus \Gamma_{i-1}$ the inequality $\gamma > \gamma_1$ holds, i.e., for every $j > 0$ the set Γ_j is contained in the set which is obtained by deleting from Γ_{j-1} the minimal element.

- For every $\gamma \in \Gamma_{i-1}$ the defined over k and irreducible over k quasiprojective algebraic variety

$$W'_{i-1,\gamma} \subset W_\gamma \setminus \bigcup_{2\le j\le b} V^{(j)}$$

is constructed such that $W'_{i-1,\gamma}$ is a non–empty open in the Zariski topology subset of W_γ (in particular $W'_{i-1,\gamma} \not\subset \bigcup_{2\le j\le b} V^{(j)}$).

The following properties are satisfied at the beginning of the i-th step.

$$\bigcup_{\alpha\in A_{i-1}} V'_\alpha \cup \bigcup_{\gamma\in\Gamma_{i-1}} W'_{i-1,\gamma} = V', \tag{42}$$

$$W_\tau \setminus \bigcup_{2\le j\le b} V^{(j)} \subset \bigcup_{\alpha\in A_{i-1}} V'_\alpha \quad \text{for every} \quad \tau \in A_{i-1}, \tag{43}$$

$$V'_{\alpha_1} \cap V'_{\alpha_2} = \emptyset \quad \text{for every distinct} \quad \alpha_1, \alpha_2 \in A_{i-1}, \tag{44}$$

$$W_\alpha \cap W'_{i-1,\gamma} = \emptyset \quad \text{for every} \quad \alpha \in A_{i-1},\ \gamma \in \Gamma_{i-1}, \tag{45}$$

$$W_\gamma \setminus \bigcup_{2\le j\le b} V^{(j)} \subset \bigcup_{\tau\le\gamma,\ \tau\in\Gamma_{i-1}} W'_{i-1,\tau} \cup \bigcup_{\alpha\in A_{i-1}} V'_\alpha \tag{46}$$

for every $\gamma \in \Gamma_{i-1}$.

One sees that these properties hold for $i-1=0$.

Let us describe the i-th step, $i \ge 1$. We shall suppose without loss of generality in what follows that all newly introduced indices (respectively sets of indices) are different from all indices (respectively are disjoint with all sets of indices) considered previously.

Let γ_i be the least element of Γ_{i-1}. By W'_τ, $\tau \in D_i$ denote the family of all defined over k and irreducible over k components of the algebraic variety $W'_{i-1,\gamma_i} \cap \mathcal{Z}(\Delta_{\gamma_i})$. Hence

$$W'_{i-1,\gamma_i} \cap \mathcal{Z}(\Delta_{\gamma_i}) = \bigcup_{\tau\in D_i} W'_\tau.$$

For all $\tau \in D_i$ set

$$W_\tau = \overline{W'_\tau},$$

where $\overline{W'_\tau}$ denotes the closure in the Zariski topology of W'_τ.

LEMMA 5 *Let $\tau \in D_i$. Then W'_τ is a defined over k and irreducible over k component of the algebraic variety*

$$\mathcal{Z}(f_1, \ldots, f_m,\, h_{\gamma_i,1}, \ldots, h_{\gamma_i,s(\gamma_i)},\, \Delta_{\gamma_i}) \setminus \left(\bigcup_{\alpha\in A_{i-1}} W_\alpha \cup \bigcup_{2\le j\le b} V^{(j)} \right). \tag{47}$$

Besides that, the dimension of the algebraic variety (47) is at most $-1+\dim W_{\gamma_i}$.

PROOF By (45), (46) we have

$$W'_{i-1,\gamma_i} = W_{\gamma_i} \setminus \left(\bigcup_{\alpha\in A_{i-1}} W_\alpha \cup \bigcup_{2\le j\le b} V^{(j)} \right).$$

Hence

$$W'_\tau = W_\tau \setminus \left(\bigcup_{\alpha \in A_{i-1}} W_\alpha \cup \bigcup_{2 \le j \le b} V^{(j)} \right).$$

Hence it is sufficient to prove the last assertion of the lemma.

It is sufficient to prove that for every irreducible component W of the algebraic variety (47) $\dim W < \dim W_{\gamma_i}$. By (42), (44) for every $\gamma < \gamma_i$, $\gamma \in \Gamma_0$, there is $\alpha \in A_{i-1}$ such that $W_\alpha = W_\gamma$. Hence for every irreducible component W of the algebraic variety (47) there is $\gamma \ge \gamma_i$ such that $W \subset W_\gamma$. If $\dim W_\gamma < \dim W_{\gamma_i}$ then the lemma is proved. Suppose that $\dim W_\gamma \ge \dim W_{\gamma_i}$. Then $\dim W_\gamma = \dim W_{\gamma_i}$ and

$$W_\gamma \not\subset \mathcal{Z}(h_{\gamma_i,1}, \ldots, h_{\gamma_i,s(\gamma_i)}, \Delta_{\gamma_i})$$

by the construction of the linear order on Γ_0. Hence $W_\gamma \ne W$ and

$$\dim W_{\gamma_i} = \dim W_\gamma > \dim W.$$

The lemma is proved.

By S_{γ_i} denote the algebraic variety (47). Using the inductive assumption construct a smooth stratification V'_α, $\alpha \in A_{\gamma_i}$ of the quasiprojective algebraic variety S_{γ_i}. (we can suppose without loss of generality that $(A_{i-1} \cup \Gamma_{i-1}) \cap A_{\gamma_i} = \emptyset$). We suppose also that corresponding V_α, Δ_α and homogeneous polynomials (40) (depending on α) are constructed for every $\alpha \in A_{\gamma_i}$.

For every $\gamma \in \Gamma_{i-1} \setminus \{\gamma_i\}$ set

$$W'_{i,\gamma} = W'_{i-1,\gamma} \setminus \overline{S_{\gamma_i}},$$

where $\overline{S_{\gamma_i}}$ is closure of S_{γ_i}. Since

$$W'_{i-1,\gamma} \cap \left(\bigcup_{\alpha \in A_{i-1}} W_\alpha \cup \bigcup_{2 \le j \le b} V^{(j)} \right) = \emptyset$$

we have $W'_{i,\gamma} = W'_{i-1,\gamma} \setminus S_{\gamma_i}$ for every $\gamma \in \Gamma_{i-1} \setminus \{\gamma_i\}$.

Set $V'_{\gamma_i} = W'_{i-1,\gamma_i} \setminus \mathcal{Z}(\Delta_{\gamma_i}) = W'_{i-1,\gamma_i} \setminus S_{\gamma_i}$ and $V_{\gamma_i} = W_{\gamma_i} \setminus \mathcal{Z}(\Delta_{\gamma_i})$. Recall that the homogeneous polynomials $h_{\gamma_i,1}, \ldots, h_{\gamma_i,s(\gamma_i)}$ have been constructed.

By definition, put

$$\Gamma_i = \{\gamma \in \Gamma_{i-1} \,:\, W'_{i,\gamma} \ne \emptyset \ \&\ \gamma \ne \gamma_i\},$$
$$A_i = A_{i-1} \cup A_{\gamma_i} \cup \{\gamma_i\}.$$

Let us prove properties (42)–(46) with $i-1$ replaced by i. Indeed, these new properties follows immediately from (42)–(46) (for $i-1$) and definitions.

Let us prove the inequality (41) for all $\alpha \in A_i$. It is sufficient to consider the case when $\alpha \in A_{\gamma_i} \cup \{\gamma_i\}$. If $\alpha = \gamma_i$ then (41) follows from Theorem 1 (ii) applied to the algebraic variety W_{γ_i} which is an irreducible component of V. Let $\alpha \in A_\gamma$. Then W_α is an irreducible component of the algebraic variety (47). The estimates for $\deg h_{\gamma_i,j}$, $\deg \Delta_{\gamma_i}$ follows similarly from Theorem 1 (ii) applied to the algebraic variety W_{γ_i}. Let C be the constant from the formulation of Theorem 1 (ii). Let $C_2 > C$. Then the degrees of all polynomials which define the algebraic variety (47) are bounded from above by

$$(s(\alpha)-1)n^{2^{(s(\alpha)-1)^{C_2}}}d. \tag{48}$$

Hence for $\alpha \in A_{\gamma_i}$ the inequality (41) (with appropriate C_2 depending on C) follows from Theorem 1 (ii).

Now if $\Gamma_i \neq \emptyset$ we proceed to the next $(i+1)$-th step. If $\Gamma_i = \emptyset$ set $A = A_i$. Then V'_α, $\alpha \in A$ is a smooth stratification of V by (42), (44).

It remains to prove the inequality (39).

LEMMA 6 *The inequality*

$$\sum_{\gamma \in \Gamma_0} d^{n-s(\gamma)} \deg W_\gamma \leq d^n$$

holds.

PROOF In the proof of this lemma we shall suppose that $\deg f_i = d$ for every $1 \leq i \leq m$ replacing the family f_i, $1 \leq i \leq m$ by

$$f_i X_j^{d-\deg f_i}, \quad 1 \leq i \leq m,\ 0 \leq j \leq n.$$

Further, there are linear combinations $h_j = c_{j,1}f_1 + \ldots + c_{j,m}f_m$, $1 \leq j \leq n$ with all coefficients $c_{j,i} \in k$ such that for every $1 \leq s \leq n$ for every $\gamma \in \Gamma_0$ if $s(\gamma) \leq s$ then W_γ is an irreducible component of the algebraic variety

$$\mathcal{Z}(h_1, \ldots, h_s). \tag{49}$$

By W_γ, $\gamma \in H_s$, denote the family of all defined over k and irreducible over k irreducible components of the algebraic variety (49). By the induction on s and the Bézout theorem we get the inequality

$$\sum_{\gamma \in H_s} d^{s-s(\gamma)} \deg W_\gamma \leq d^s.$$

Now the assertion of the lemma follows from the last inequality for $s = n$. The lemma is proved.

Let N be the number of steps in the described construction. So $N \leq \#\Gamma_0$. Note that for every $\alpha \in A$ we have $W_\alpha = W_{\gamma_i}$ or $\alpha \in A_{\gamma_i}$ for some $\gamma_i \in \Gamma_0$.

Denote for brevity $s(\gamma_i) = s_i$. By the inductive assumption applied to S_{γ_i} and since the degrees of all polynomials which define the algebraic variety (47) are bounded from above by (48) the inequality

$$\sum_{\alpha \in A_{\gamma_i}} (s_i n^{2^{s_i^{C_2}}} d)^{n-s(\alpha)} \deg W_\alpha \leq n^{2^{(n(n-s_i))^{C_1}}} (s_i n^{2^{s_i^{C_2}}} d)^{(n+s_i+1)(n-s_i)/2}$$

holds for every $1 \leq i \leq N$. Hence by Lemma 6 (and its proof)

$$\sum_{\alpha \in A} d^{n-s(\alpha)} \deg W_\alpha \leq$$

$$\sum_{1 \leq i \leq N} \left(d^{n-s_i} \deg W_{\gamma_i} + \sum_{\alpha \in A_{\gamma_i}} (s_i n^{2^{s_i^{C_2}}} d)^{n-s(\alpha)} \deg W_\alpha \right) \leq$$

$$\sum_{1\le i\le N}\left(d^{n-s_i}\deg W_{\gamma_i}+n^{2^{(n(n-s_i))^{C_1}}}(s_i n^{2^{s_i^{C_2}}}d)^{(n+s_i+1)(n-s_i)/2}\right)\le$$

$$d^n+\sum_{1\le i\le N}n^{2^{(n(n-s_i))^{C_1}}}(s_i n^{2^{s_i^{C_2}}}d)^{(n+s_i+1)(n-s_i)/2}\le$$

$$d^n+n^{2^{(n(n-s))^{C_1}}}\sum_{s\le j\le n}(nn^{2^{n^{C_2}}}d)^{(n+j+1)(n-j)/2}d^j\le$$

$$n^{2^{(n(n-s+1))^{C_1}}}d^{(n+s)(n-s+1)/2}.$$

for an appropriate $C_1>0$. Thus the inequality (39) is proved. The required in Theorem 2 estimations for degrees and sizes of coefficients follow immediately from Theorem 1, see also the remarks about representation (6) in the Introduction. Theorem 2 for the case of smooth stratification is proved.

6 Computing dimension of a real algebraic variety

Let k be a real ordered field with a real closure R and V be the algebraic variety from the Introduction. Hence $V(R)$ is a set of points of a real algebraic variety. Our aim is to compute the dimension of $V(R)$ and prove Theorem 3. It is sufficient to find the dimension of $n+1$ affine algebraic varieties $V(R)\setminus\mathcal{Z}(X_i)$, $0\le i\le n$. We shall show how to compute $\dim V(R)\setminus\mathcal{Z}(X_0)$. Dimensions of other considered affine algebraic varieties are computed in the similar way. For an arbitrary subset $S\subset\mathbb{P}^n(\overline{R})$ by $\overline{S}$ denote the closure of S in the Zariski topology in $\mathbb{P}^n(\overline{R})$. Denote $V_0=\overline{V(R)\setminus\mathcal{Z}(X_0)}$. We have $\dim V_0=\dim V(R)\setminus\mathcal{Z}(X_0)$ and V_0 is a projective algebraic variety. So it is sufficient to compute $\dim V_0$.

Let $\dim V_0(R)=n-r$ where $1\le r\le n$. Then there is a smooth point $\xi=(1:\xi_1:\ldots:\xi_n)$ of $V_0(R)$ of dimension $n-r$, see [1].

Now consider the smooth cover V_α, $\alpha\in A$ of V from Theorem 2. By A' denote the subset of all $\alpha\in A$ such that $V_\alpha(R)\setminus\mathcal{Z}(X_0)\ne\emptyset$. We have $\overline{V_\alpha}=\overline{V_\alpha(R)}$ since V_α is smooth for every $\alpha\in A'$. Therefore,

$$\bigcup_{\alpha\in A'}\overline{V_\alpha}=\bigcup_{\alpha\in A'}\overline{V_\alpha(R)}=\overline{(V\setminus\mathcal{Z}(X_0))(R)}=V_0.$$

Hence V_0 is defined over k and there is a unique defined over k and irreducible over k component W' of V_0 such that ξ is a smooth point of W'. Besides that $\dim W'=n-r$. Further, there is $\alpha\in A'$ such that $\overline{V_\alpha}=W'$. Therefore by Theorem 2 there are homogeneous polynomials $h_1,\ldots,h_r\in k[X_0,\ldots,X_n]$ and indices $1\le i_1<\ldots<i_r\le n$ (one can take $i_1\ge 1$ since there are smooth points in $W'\setminus\mathcal{Z}(X_0)$) satisfying the following property. Denote

$$\Delta=\det(\partial h_v/\partial X_{i_w})_{1\le v,w\le r}. \tag{50}$$

Then $W'\setminus\mathcal{Z}(\Delta)$ is non–empty and coincides with an irreducible component of the quasiprojective algebraic variety

$$\mathcal{Z}(h_1,\ldots,h_r)\setminus\mathcal{Z}(\Delta)$$

The degrees $\deg h_i < n^{2^{r^C}} d$, $1 \le i \le r$, for an absolute constant $C > 0$.

There is a permutation τ of the set $\{1, \ldots, n\}$ such that ξ is an isolated point of the real algebraic variety

$$V_0(R) \cap \mathcal{Z}(X_{\tau(r+1)} - \xi_{\tau(r+1)} X_0, \ldots, X_{\tau(n)} - \xi_{\tau(n)} X_0) \tag{51}$$

and the intersection of tangent spaces in the point ξ

$$T_{\xi, V_0(R)} \cap \mathcal{Z}(X_{\tau(r+1)} - \xi_{\tau(r+1)} X_0, \ldots, X_{\tau(n)} - \xi_{\tau(n)} X_0) = \{\xi\} \tag{52}$$

is transversal. In what follows we shall suppose without loss of generality as in the proof of Lemma 6 that $\deg f_j = d$ for all j. Let X_{n+1} be a new variable. Set

$$h = X_0^3 \sum_{1 \le j \le m} f_j^2 - X_{n+1} \sum_{0 \le i \le n} X_i^{2d+2}.$$

Let $1 \le s \le n$ be an integer and σ be a permutation of $\{1, \ldots, n\}$. Consider the system of polynomial equations in $X_0, \ldots, X_n, X_{n+1}$

$$\begin{cases} h = 0, \\ \partial h / \partial X_{\sigma(j)} = 0, \quad 2 \le j \le s, \end{cases} \tag{53}$$

which defines the algebraic variety $S_{\sigma,s} \subset \mathbb{P}^{n+1}(\overline{k})$, herewith $\mathbb{P}^{n+1}$ has coordinates $(X_0 : \ldots : X_n : X_{n+1})$. We shall identify $\mathcal{Z}(X_{n+1})$ with $\mathbb{P}^n$. By $V_{\sigma,s}$ denote the union of all irreducible components of $S_{\sigma,s}$ which are not contained in any finite union of hyperplanes $\mathcal{Z}(X_{n+1} - vX_0)$ where $v \in \overline{k}$ and are not contained in $\mathcal{Z}(X_0)$. Then dimension of every irreducible components of the algebraic variety $V_{\sigma,s}$ is $n - s + 1$, cf. [3]. Set $W_{\sigma,s} = V_{\sigma,s} \cap \mathcal{Z}(X_{n+1})$.

Let $\xi^*_{s+1}, \ldots, \xi^*_n \in \overline{k}$. By $C_{\sigma,s}(\xi^*_{s+1}, \ldots, \xi^*_n)$ denote the union of all irreducible components of

$$S_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)} X_0, \ldots, X_{\sigma(n)} - \xi^*_{\sigma(n)} X_0)$$

which are not contained in any finite union of hyperplanes $\mathcal{Z}(X_{n+1} - vX_0)$ where $v \in \overline{k}$ and are not contained in $\mathcal{Z}(X_0)$. Then, cf. [3], by the same argument as above for $V_{\sigma,s}$ dimension of every irreducible components of $C_{\sigma,s}(\xi^*_{s+1}, \ldots, \xi^*_n)$ is 1, i.e. $C_{\sigma,s}(\xi^*_{s+1}, \ldots, \xi^*_n)$ is a curve. Hence this curve is a union of some irreducible component of the intersection

$$V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)} X_0, \ldots, X_{\sigma(n)} - \xi^*_{\sigma(n)} X_0). \tag{54}$$

But $V_{\sigma,s} \cap \mathcal{Z}(X_0) = \mathcal{Z}(X_0, X_{\sigma(2)}, \ldots, X_{\sigma(s)}, \sum_{0 \le i \le n} X_i^{2d+2})$. Therefore,

$$V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)} X_0, \ldots, X_{\sigma(n)} - \xi^*_{\sigma(n)} X_0) \cap \mathcal{Z}(X_0) = \{(0 : \ldots : 0 : 1)\}.$$

Hence the intersection (54) is a curve and every irreducible component of (54) is not contained in any finite union of hyperplanes $\mathcal{Z}(X_{n+1} - vX_0)$ where $v \in \overline{k}$ and is not contained in $\mathcal{Z}(X_0)$. Thus,

$$C_{\sigma,s}(\xi^*_{s+1}, \ldots, \xi^*_n) = V_{\sigma,s} \cap \mathcal{Z}(X_{\sigma(s+1)} - \xi^*_{\sigma(s+1)} X_0, \ldots, X_{\sigma(n)} - \xi^*_{\sigma(n)} X_0)$$

for every $\xi^*_{s+1}, \ldots, \xi^*_n \in \overline{k}$.

Consider the system of polynomial equations

$$\begin{cases} h = 0, \\ \partial h / \partial X_{\tau(j)} = 0, \quad 2 \le j \le r, \\ X_{\tau(j)} - \xi_{\tau(j)} X_0 = 0, \quad r+1 \le j \le n, \\ X_0 - 1 = 0. \end{cases} \tag{55}$$

Recall that ξ is an isolated point of the intersection (51). Hence considering system (55), cf. [14], [4], we get that the point $\xi \in C_{\tau,r}(\xi_{r+1}, \ldots, \xi_n)$. Hence $C_{\tau,r}(\xi_{r+1}, \ldots, \xi_n) \cap \mathcal{Z}(X_{n+1})$ coincides with $\{\xi\}$ in some neighborhood of ξ in the topology of the real field R. By the implicit function theorem and the same argument $W_{\tau,r}$ coincides with W' in some neighborhood of ξ in the topology of the real field R. Therefore W' is an irreducible component of $W_{\tau,r}$, cf. [15].

Let $\varepsilon_i > 0$ be an infinitesimal relative to the field $k(\varepsilon_1, \ldots, \varepsilon_{i-1})$ for every $1 \le i \le 3$. Denote by $\widetilde{W}_{\sigma,s}$ the algebraic variety

$$V_{\sigma,s} \cap \mathcal{Z}(X_{n+1} - \varepsilon_3 X_0)$$

considered as a subvariety of $\mathbb{P}^{n+1}(\overline{k(\varepsilon_3)})$.

Let us show how to construct linear forms $Y_{s+1}, \ldots, Y_n \in k[X_0, \ldots, X_n]$ with integer coefficients with lengths $O(n \log d)$ such that the set

$$W_{\sigma,s} \cap \mathcal{Z}(Y_{s+1}, \ldots, Y_n) \setminus \mathcal{Z}(X_0) \tag{56}$$

consists of $\deg W_{\sigma,s}$ points. Hence, cf., e.g., [6], all the points of the intersection (56) are smooth points of $W_{\sigma,s}$ and intersection (56) is transversal in these points.

Let us multiply all the equations of system (53) by $X_0 X_{n+1}$ and using the algorithm from [5] construct for all $s+1 \le i \le n+1$ linear forms $L_i \in k[X_0, \ldots, X_n]$ with integer coefficients with lengths $O(n \log d)$ and integers λ_i of lengths $O(n \log d)$ such that the number of elements of the intersection

$$V_{\sigma,s} \cap \mathcal{Z}(L_{s+1} - \lambda_{s+1} X_{n+1}, \ldots, L_{n+1} - \lambda_{n+1} X_{n+1})$$

is finite and

$$V_{\sigma,s} \cap \mathcal{Z}(L_{s+1} - \lambda_{s+1} X_{n+1}, \ldots, L_{n+1} - \lambda_{n+1} X_{n+1}) \cap \mathcal{Z}(X_0 X_{n+1}) = \emptyset. \tag{57}$$

If every $\lambda_i = 0$, $s+1 \le i \le n$, then set $D_i = L_i$, $s+1 \le i \le n$. Suppose that there is $s+1 \le i_0 \le n$ such that $\lambda_{i_0} \ne 0$. Say, e.g., $\lambda_{n+1} \ne 0$. Then set $D_i = \lambda_{n+1} L_i - \lambda_i L_{n+1}$ for all $s+1 \le i \le n$.

Each irreducible component of the intersection

$$V_{\sigma,s} \cap \mathcal{Z}(D_{s+1}, \ldots, D_n)$$

is a curve which is not contained in $\mathcal{Z}(X_0 X_{n+1})$ by (57). Hence the intersection

$$W_{\sigma,s} \cap \mathcal{Z}(D_{s+1}, \ldots, D_n) \tag{58}$$

consists of a finite number of points.

Using the algorithm of [3] construct all the points

$$\xi^{(i)} = (\xi_0^{(i)} : \ldots : \xi_n^{(i)} : \varepsilon_3), \quad 1 \le i \le N_1,$$

of the intersection

$$\widetilde{W}_{\sigma,s} \cap \mathcal{Z}(D_{s+1}, \dots, D_n).$$

Then, see [5] Proposition 2, or [6] Proposition 1, each point of the intersection (58) has the form $\mathrm{st}_{\varepsilon_3}(\xi^{(i)})$ for some $1 \le i \le N_1$ where the standard part $\mathrm{st}_{\varepsilon_3}$ has the same meaning as in [5], [6] (the standard part of an element $z \in \mathbb{P}^{n+1}(\overline{k(\varepsilon_3)})$ is the element $z' \in \mathbb{P}^{n+1}(\overline{k})$ which is infinitely close to z). So we construct using Newton–Puiseux expansions, see [4], [5], [10], all the elements $\eta^{(i)}$, $1 \le i \le N_2$ of the intersection (58). Let $\eta^{(i)} = (\eta_0^{(i)} : \dots : \eta_n^{(i)})$ where $\eta_j^{(i)} \in \overline{k}$ and if $\eta_0^{(i)} \ne 0$ then $\eta_0^{(i)} = 1$ for every $1 \le i \le N_2$.

Let us show that we can suppose without loss of generality that

$$\eta^{(i)} \notin \mathcal{Z}(X_0) \quad \text{for all} \quad 1 \le i \le N_2, \tag{59}$$

replacing if necessary linear forms $D_{s+1}, \dots, D_n$ for new ones. Indeed, denote by N_3 the number of points of the intersection (58) which do not lie in $\mathcal{Z}(X_0)$. Suppose that $N_3 < N_2$ and, e.g., $\eta^{(1)} = (0 : \eta_1^{(1)} : \dots : \eta_n^{(1)}) \in \mathcal{Z}(X_0)$ and $\eta^{(1)} = \mathrm{st}_{\varepsilon_3}(\xi^{(1)})$ where $\xi^{(1)} = (\xi_0^{(1)} : \dots : \xi_n^{(1)} : \varepsilon_3 \xi_0^{(1)})$, every $\xi_j^{(1)}$, $1 \le j \le n$ is not infinitely large relative to the field k and there is $1 \le j_0 \le n$ such that $\xi_{j_0}^{(1)}$ is not an infinitesimal relative to the field k. Solving a system of polynomial equations and inequalities with squares of absolute values construct a point $x^* \in \widetilde{W}_{\sigma,s}$ such that $x^* = (x_0^* : \dots : x_n^* : \varepsilon_3 x_0^*)$, all $x_j^* \in \overline{k(\varepsilon_1, \varepsilon_2, \varepsilon_3)}$, $0 \le j \le n$, and

$$\begin{aligned} &|x_0^*|^2 + \sum_{1 \le j \le n} |x_j^* - \xi_j^{(1)}|^2 < \varepsilon_1, \\ &|x_0^*|^2 > \varepsilon_2. \end{aligned}$$

Then construct $x_i' = \mathrm{st}_{\varepsilon_3}(x_i^*)$ for all $0 \le i \le n$. Set

$$\begin{aligned} &x' = (x_0' : x_1' : \dots : x_n') \in \mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)}), \\ &\widetilde{D}_j = D_j - (D_j/X_0)(x')X_0, \quad s+1 \le j \le n. \end{aligned}$$

Then, cf. [4], [5], the number of elements

$$\# W_{\sigma,s} \cap \mathcal{Z}(\widetilde{D}_{s+1}, \dots, \widetilde{D}_n) \setminus \mathcal{Z}(X_0) > N_3,$$

herewith all these elements are from $\mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)})$. Hence, cf. [4], [5], [6] and also Section 1, replacing subsequently all the coefficients of the linear forms $\widetilde{D}_{s+1}, \dots, \widetilde{D}_n$ by integer coefficients with lengths $O(n \log d)$ we shall obtain new linear forms $D'_{s+1}, \dots, D'_n$ similar to $D_{s+1}, \dots, D_n$ such that

$$\# W_{\sigma,s} \cap \mathcal{Z}(D'_{s+1}, \dots, D'_n) \setminus \mathcal{Z}(X_0) > N_3.$$

Then we replace the linear forms $D_{s+1}, \dots, D_n$ by $D'_{s+1}, \dots, D'_n$ and iterate the describe construction until (59) holds. The number of iterations is bounded from above by $\deg W_{\sigma,s}$ by the Bézout theorem. The required assertion is proved.

Now for every $1 \le j \le N_2$ consider the system of polynomial equations and inequalities in $X_0, \dots, X_{n+1}$, $Z_0, \dots, Z_{n+1}$, with squares of absolute values

$$\left\{\begin{array}{ll} h = 0, & \\ \partial h/\partial X_{\sigma(i)} = 0, & 2 \le i \le s, \\ h(Z_0, \dots, Z_{n+1}) = 0, & \\ \partial h(Z_0, \dots, Z_{n+1})/\partial Z_{\sigma(i)} = 0, & 2 \le i \le s, \\ X_{n+1} - \varepsilon_3 = 0, & \\ Z_{n+1} - \varepsilon_3 = 0, & \\ D_j(X_0 - Z_0, \dots, X_n - Z_n) = 0, & j \in \{0, s+1, s+2, \dots, n\}, \\ \sum_{0 \le i \le n} |X_i - \eta_i^{(j)}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Z_i - \eta_i^{(j)}|^2 \le \varepsilon_1, & \\ \sum_{0 \le i \le n} |Z_i - X_i|^2 \ge \varepsilon_2, & \\ X_0 - 1 = 0, & \\ Z_0 - 1 = 0. & \end{array}\right. \tag{60}$$

Suppose that for every $1 \le j \le N_2$ system (60) has no solutions. Then, cf. [6], the intersection (56) consists of $\deg W_{\sigma,s}$ points. In this case set $Y_j = D_j$ for every $j \in \{0, s+1, s+2, \dots, n\}$.

Suppose that there is $1 \le j \le N_2$ such that system (60) has a solution

$$(1, x_1^*, \dots, x_n^*, \varepsilon_3, 1, z_1^*, \dots, z_n^*, \varepsilon_3) \in (\overline{k(\varepsilon_1, \varepsilon_2, \varepsilon_3)})^{2n+4}.$$

Then construct $x_i' = \mathrm{st}_{\varepsilon_3}(x_i^*)$ and $z_i' = \mathrm{st}_{\varepsilon_3}(z_i^*)$ for all $1 \le i \le n$. Set

$$\begin{array}{l} x' = (1 : x_1' : \dots : x_n') \in \mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)}), \\ \widetilde{D}_j = D_j - (D_j/X_0)(x')X_0, \quad s+1 \le j \le n. \end{array}$$

Then, cf. [6], the number of elements of the set

$$\# W_{\sigma,s} \cap \mathcal{Z}(\widetilde{D}_{s+1}, \dots, \widetilde{D}_n) \setminus \mathcal{Z}(X_0) > N_2,$$

herewith the last set is a subset of $\mathbb{P}^n(\overline{k(\varepsilon_1, \varepsilon_2)})$. Hence, cf. [4], [5], [6] and also Section 1, replacing subsequently all the coefficients of the linear forms $\widetilde{D}_{s+1}, \dots, \widetilde{D}_n$ by integer coefficients with lengths $O(n \log d)$ we shall obtain new linear forms $D_{s+1}', \dots, D_n'$ similar to $D_{s+1}, \dots, D_n$ such that

$$\# W_{\sigma,s} \cap \mathcal{Z}(D_{s+1}', \dots, D_n') \setminus \mathcal{Z}(X_0) > N_2.$$

Then we replace the linear forms $D_{s+1}, \dots, D_n$ by $D_{s+1}', \dots, D_n'$ and iterate the describe construction until for every $1 \le j \le N_2$ system (60) has no solutions. The number of iterations is bounded from above by $\deg W_{\sigma,s}$ by the Bézout theorem. Thus, we shall construct finally the required linear forms $Y_{s+1}, \dots, Y_n$. The required assertion is proved.

Return to the description of the algorithm for computing $\dim V_0$. We shall enumerate $s = 1, \dots, n$ (here n is the maximal possible value of s unless the algorithm under description stops for some $s < n$). We shall suppose (it is inductive assumption) that when we consider the current value s we have proved that

$$\dim V_0 < n - s + 1. \tag{61}$$

For the considered s we shall enumerate σ defined above. For the considered s and σ construct linear forms $Y_{s+1}, \dots, Y_n$ and all the points from the intersection (56) (in the similar way as the points of (58) were constructed). We shall enumerate the points from the intersection (56). By x_0 denote the considered current point of the intersection (56). Denote by W the uniquely defined irreducible over k component of $W_{\sigma,s}$ such that $x_0 \in W$. Denote by $\mathfrak{P} \subset k[X_0, \dots, X_n]$ the homogeneous ideal of W. We shall see that the described algorithm considering s, σ and x_0 comes to one of two cases. In the first case $W' \neq W$, and in the second one $\dim V_0 = n - s$.

Now we would like to modify the algorithm for constructing regular sequences from Section 1. Namely, we replace there the algebraic variety V by $W_{\sigma,s}$. Our aim will be to decide whether there is a $\mathfrak{P}$-sequence $g_1, \dots, g_s$ with degrees $\deg g_j \leq n^{2^{s^C}} d$, $1 \leq j \leq s$, where $C > 0$ is a constant from the formulation of Theorem 2. Further, if such a $\mathfrak{P}$-sequence exists we shall construct it as well as other corresponding to it objects, in particular, a smooth point $x_a \in W$ and linear forms $L_{a,s+1}, \dots, L_{a,n}$ where the step a is final, see Section 1. Additionally we shall see that $x_a \notin \mathcal{Z}(X_0)$ (it follows from the modification of Lemma 1). The difference with Section 1 here is that the algebraic variety $W_{\sigma,s}$ is not given explicitly by a system of polynomial equations.

This modification of the algorithm from Section 1 will be described later. Now suppose that we have already applied it and found that there are no required $\mathfrak{P}$–sequences. Then if not all points from the intersection (56) are enumerated we proceed to the next point of (56). If all points from (56) are enumerated but not all σ are enumerated we proceed to the next σ. If all points from (56) and all σ are enumerated and $s < n$ we proceed to the next value of s, i.e., $s + 1$. In this case $W' \neq W$ for all σ and all points from (56) (we shall see it later from the description of the algorithm), and hence $\dim V_0 < n - s$. Therefore (61) is proved with s replaced by $s + 1$. If all points from (56), all σ are enumerated and $s = n$ then W' is not an irreducible component of $W_{\sigma,s}$ for all σ and $1 \leq s \leq n$. Therefore, as it follows from the proved above, $V_0 = \emptyset$ and $\dim V_0 = -1$ in this case.

Suppose that we have applied the modification of the algorithm from Section 1 and have constructed a $\mathfrak{P}$-sequence $g_1, \dots, g_s$. Then W is an irreducible component of the algebraic variety $\mathcal{Z}(g_1, \dots, g_s)$. Set $x = x_a$ where the step a is final in the modification of the algorithm from Section 1. Then we apply the algorithm from the second part of Section 1 (in input of this algorithm only polynomials $g_1, \dots, g_s$, the point x, and corresponding linear forms are needed) and construct homogeneous polynomials $h_1, \dots, h_s \in k[X_0, \dots, X_n]$, indices $1 \leq i_1 < \dots < i_s \leq n$, the polynomial Δ defined by (50), and a point $z \in W \setminus \mathcal{Z}(X_0)$ such that

- $z \in \mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(\Delta)$ and hence by implicit function theorem z is a smooth point of this quasiprojective algebraic variety,
- $W \setminus \mathcal{Z}(\Delta)$ is an irreducible component of $\mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(\Delta)$.

Denote by V_1 the algebraic variety $\mathcal{Z}(h_1, \dots, h_s) \setminus \mathcal{Z}(X_0\Delta)$. All the points of the algebraic variety V_1 are smooth. Hence $W(R) \setminus \mathcal{Z}(X_0\Delta)$ is a union (may be empty) of some connected component of the $V_1(R)$ (the connected components can be defined using, e.g. transfer principle, see [1] for details). Apply the algorithm from [14] and construct a finite subset S of $V_1(R)$ which has a non–empty intersection with every connected component of $V_1(R)$ with the number of elements $\#S$ bounded from above by a polynomial in d^n. Construct the subset S_1 of S consisting of all elements of S which belong to $W_{\sigma,s}$ (the point belongs to $W_{\sigma,s}$ if and only if there is an infinitely close to it point from $\widetilde{W}_{\sigma,s}$).

Further, for every point $z \in S_1$ we decide whether there is an infinitely close to z point

$$z' \in \mathcal{Z}(h_1, \ldots, h_s) \setminus \mathcal{Z}(f_1, \ldots, f_m).$$

In the case when for every point $z \in S_1$ such a point z' exists $W \neq W'$ by previous considerations, and we proceed to the next point from (56), or next σ, or next s, or decide that $\dim V_0 = -1$ as it is described above. In the case when there is no z' for some z there exists an infinitesimal neighborhood U of the point z in the algebraic variety V_1 such that $U \subset V$, cf. [4], [5]. Hence $\dim V_0 \geq n - s$. On the other hand, by (61) $\dim V_0 < n - s + 1$. Thus $\dim V_0 = n - s$.

It remains to describe the modification of the algorithm from Section 1. Construct a linear form $Y_0 \in k[X_0, \ldots, X_n]$ with integer coefficients of lengths $O(n \log d)$ such that

$$W_{\sigma,s} \cap \mathcal{Z}(Y_0, Y_{s+1}, Y_{s+2}, \ldots, Y_n) = \emptyset$$

in $\mathbb{P}^n(\overline{k})$. Recall that we replace V by $W_{\sigma,s}$. We have also the current point $x_0 \in W_{\sigma,s} \cap \mathcal{Z}(Y_{s+1}, \ldots, Y_n)$ and defined over k and irreducible over k component W of $W_{\sigma,s}$ such that $x \in W$.

First of all recall that we construct a $\mathfrak{P}$–sequence with $\deg g_i \leq n^{2^{s^C}} d$, $1 \leq i \leq s$, if it exists. So enumerating δ, see Section 1, we stop at the value $n^{2^{s^C}} d$.

In Lemma 1 the property (v) is replaced by the following one.

(v) The set $W_{\sigma,s} \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ consists of $\deg W_{\sigma,s}$ points (hence all these points are smooth points of $W_{\sigma,s}$). Further, for every point z from this set $X_0(z) \neq 0$, and the intersection of tangent spaces of $W_{\sigma,s}$ and $\mathcal{Z}(L'_{s+1}, \ldots, L'_n)$ in the point z is transversal, i.e.,

$$T_{z, W_{\sigma,s}} \cap \mathcal{Z}(L'_{s+1}, \ldots, L'_n) = \{z\}.$$

System (11) is replaced by the following one.

$$\begin{cases} \sum_{0 \leq i \leq n} |X_i - x_{r,i}|^2 < \varepsilon_1, & \\ h = 0, & \\ \partial h / \partial X_{\sigma(j)} = 0, & 2 \leq j \leq s, \\ X_{n+1} - \varepsilon_3 = 0, & \\ X_0 - 1 = 0, & \\ |\psi|^2 > \varepsilon_2. & \end{cases} \tag{62}$$

Then, cf. [5], [6], system (62) has no solutions in $\mathbb{A}^{n+2}(\overline{k(\varepsilon_1, \varepsilon_2, \varepsilon_3)})$ if and only if the polynomial ψ is vanishing on W.

System (13) is replaced by the following one.

$$\left\{\begin{array}{ll}\sum_{0\leq i\leq n}|X_i-x''_i|^2\leq\varepsilon_1, & \\ \sum_{0\leq i\leq n}|Z_i-x''_i|^2\leq\varepsilon_1, & \\ \sum_{0\leq i\leq n}|X_i-Z_i|^2\geq\varepsilon_2, & \\ M_i(X_0-Z_0,\ldots,X_n-Z_n)=0, & i=0,r+1,r+2,\ldots,n, \\ h=0, & 1\leq i\leq m, \\ \partial h/\partial X_{\sigma(j)}=0, & 2\leq j\leq s, \\ X_{n+1}-\varepsilon_3=0, & \\ X_0-1=0, & \\ \psi_i(Z_0,\ldots,Z_n)=0, & 1\leq i\leq j, \\ |\psi|^2>\varepsilon_2. & \end{array}\right. \tag{63}$$

Then, cf. [5], [6], system (63) has no solutions in $\mathbb{A}^{2n+3}(\overline{k(\varepsilon_1,\varepsilon_2,\varepsilon_3)})$ if and only if (12) is the equality.

Suppose that system (63) has a solution. Then construct a solution $\xi_0^*,\ldots,$ ξ_n^*, $z_0^*,\ldots,z_n^*$, z^* of system (63). Suppose that system (63) has no solutions Then construct a solution $\xi_0^*,\ldots,\xi_n^*$, z^* of system (62) (recall that we suppose that this system has a solution, see Section 1).

For every $0\leq i\leq n$ compute $\mathrm{st}_{\varepsilon_3}\,\xi_i^*=x_i^*$. Set

$$x^*=(x_0^*:\ldots:x_n^*).$$

Then we define the linear forms L_j^*, $s+1\leq j\leq n$ by the same formulas as in Section 1.

The last modification is related to the construction of the curve Q. In our case Q is an irreducible over $\overline{K}$ component of the intersection

$$W_{\sigma,s}\cap\mathcal{Z}(L_{s+2}^*,\ldots,L_n^*)$$

such that $x^*\in Q$. So Q is uniquely defined. Let $\varepsilon_4>0$ be an infinitesimal relative to the field $K=k(\varepsilon_1,\varepsilon_2)$ and ε_3 be infinitesimal relative to the field $K(\varepsilon_4)$. Construct solving a system of polynomial equations and inequalities a point

$$z'\in\widetilde{W}_{\sigma,s}\cap\mathcal{Z}(L_{s+2}^*,\ldots,L_n^*)$$

such that $|z'-x^*|^2=\varepsilon_4$. Compute

$$\mathrm{st}_{\varepsilon_3}(z')=z\in\mathbb{P}^n(\overline{K(\varepsilon_4)}).$$

Then z is a generic point of the algebraic variety Q. Since Q is defined over $\overline{K}$ we can construct, see [3], a system of polynomial equations with coefficients from $\overline{K}$ which gives Q. This finishes the description of all modifications to the algorithm from Section 1 for constructing regular sequences. Theorem 4 is proved.

References

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

[2] **Chardin M.:** *"Une majoration de la function de Hilbert et ses conséquences pour l'interpolation algébrique"*, Bull. Soc. Math. France 117 (1989) p. 305–318.

[3] **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].

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

[5] **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.

[6] **Chistov A. L.:** *"Polynomial–time computation of the degrees of algebraic varieties in zero–characteristic and its applications"*, St.Petersburg Mathematical Society Preprint # 1999-03, http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#03, also to appear in Russian in: Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 258.

[7] **Chistov A. L.:** *"Efficient Construction of Local Parameters of Irreducible Components of an Algebraic Variety"*, St.Petersburg Mathematical Society Preprint # 1999-08, http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#08, also to appear in Russian in: Proc. of the St.–Petersburg Mathematical Society, 1999, v. 7.

[8] **Chistov A. L.:** *"Polynomial–time computation of the Galois group over a zero–characteristic functional field with algebraically closed constant field"*, In "Mathematical methods of constructing and analysis of algorithms", Leningrad, "Nauka", 1990, p. 200–232 (Russian).

[9] **Chistov A. L.:** *"Strong version of the basic deciding algorithm for the existential theory of real fields"*, St.Petersburg Mathematical Society Preprint # 1999-10, http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#10 see also in Russian in: Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) 256 (1999) p. 168–211.

[10] **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.

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

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

[13] **Nesterenko Yu. V.** *"Estimations for the characteristic function of a prime ideal"*, Matematicheskiy Sbornik 123 (1984) 11–34 (Russian).

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

[15] **Roy M.–F., Vorobjov N.** *"Computing the Complexification of a Semialgebraic Set"*, in: Proc. of ISSAC'96 conference, 1996, p. 26–34.