SPb. Math. Society Preprint 1999-08 06 Dec 1999

Efficient Construction of Local Parameters of Irreducible Components of an Algebraic Variety

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 an $(n-s)$-dimensional algebraic variety V defined over a perfect infinite field k and irreducible over this field which is a subvariety of the projective space of dimension n. We prove that the local ring of V has a regular sequence (respectively if characteristic $\mathrm{char}(k) = 0$ a sequence of local parameters) represented by s non–homogeneous polynomials the product of degrees of which is less than the degree of the variety multiplied to a constant depending on n. In the case when V is an irreducible component of an algebraic variety given by a system of homogeneous polynomial equations of degrees less than d over a field of zero–characteristic the degrees of all these local parameters are less then d multiplied to a constant depending on n. These constants depending on n are estimated.

Introduction

Let k be an infinite perfect field and $\mathbb{P}^n(\overline{k})$ be the n–dimensional projective space over algebraic closure $\overline{k}$ with the homogeneous coordinates $X_0, \ldots, X_n$. Let $V \subset \mathbb{P}^n(\overline{k})$ be an algebraic variety irreducible and defined over k of dimension $n-s$ where $1 \leq s \leq n$ and degree $\deg V = D$. Let the variety V be the set of zeroes of the homogeneous prime ideal $\mathfrak{P} \subset k[X_0, \ldots, X_n]$. We prove that the local ring of V has a regular sequence (respectively if characteristic $\mathrm{char}(k) = 0$ a sequence of local parameters) represented by s non–homogeneous polynomials the product of degrees of which is less than D multiplied to a constant depending on n. In the case when V is an irreducible component of an algebraic variety given by a system of homogeneous polynomial equations of degrees less than d over a field of zero–characteristic the degrees of all these local parameters are less then d multiplied to a constant depending on n. These constants depending on n are estimated.

For arbitrary polynomials $g_1, \ldots, g_m \in \overline{k}[X_0, \ldots, X_n]$ we shall denote by $\mathcal{Z}(g_1, \ldots, g_m)$ the set of all common zeroes of these polynomials in $\mathbb{P}^n(\overline{k})$ (in what follows we shall use the similar notations for the sets of common zeroes of others polynomials or polynomial ideals in projective or affine spaces). For an arbitrary algebraic variety $W \subset \mathbb{P}^n(\overline{k})$ we shall denote by $\mathcal{I}(W) \subset k[X_0, \ldots, X_n]$ the homogeneous ideal corresponding to W (the similar notations will be used for ideals of affine algebraic varieties and for ideals in the rings of polynomials over other fields of coefficients).

It will be convenient to use in the paper the following definitions.

DEFINITION 1 *Let $0 < j \leq s$ be an integer. Consider a sequence of homogeneous polynomials $f_i \in \mathfrak{P}$, $1 \leq i \leq j$. Let $0 \leq u < j$ 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 $\mathcal{Z}(f_1, \ldots, f_u)$ such that $W \supset V$. Suppose that for every integer $0 \leq u < j$ the polynomial $f_{u+1} \in \mathfrak{P}$ 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 $f_1, \ldots, f_j$ will be called $\mathfrak{P}$–sequence (of length j).

DEFINITION 2 *Let $f_1, \ldots, f_s$ be a $\mathfrak{P}$–sequence. By definition put*

$$\delta_i(\mathfrak{P}) = \deg f_i, \quad 1 \leq i \leq s.$$

Then, see Lemma 2 Section 2, the integers $\delta_i(\mathfrak{P})$ depend only on $\mathfrak{P}$ and do not depend of the choice of the $\mathfrak{P}$–sequence. The integer $\delta_i(\mathfrak{P})$ will be called i–th degree corresponding to $\mathfrak{P}$–sequence.

Note that if $f_1, \ldots, f_j$ is a $\mathfrak{P}$–sequence then for every $0 \leq u \leq j$ every irreducible component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_u)$ containing V has dimension $n-u$. In particular when $j = s$ the algebraic variety V is an irreducible component of $\mathcal{Z}(f_1, \ldots, f_s)$. Note also that in the general case the algebraic variety $\mathcal{Z}(f_1, \ldots, f_s)$ may have irreducible components of dimension greater than $n-s$.

Now we can formulate the main results of the paper.

THEOREM 1 *Let $f_1, \ldots, f_s$ be an arbitrary $\mathfrak{P}$–sequence and hence $\delta_i = \delta_i(\mathfrak{P})$ $= \deg f_i$ for every $1 \leq i \leq s$. Then there is $C \in \mathbb{R}$ such that the inequality*

$$\delta_1 \cdot \ldots \cdot \delta_s \leq n^{2^{sC}} D. \tag{1}$$

holds.

REMARK 1 *Note that the proof of the fact that $\delta_i(\mathfrak{P})$ does not depend on the choice of $\mathfrak{P}$–sequence uses the infiniteness of k. Theorem 1 is valid also for the case of finite fields (but it is not affirmed here that δ_i does not depend on the choice of $\mathfrak{P}$–sequence). One can easily see that only minor changes are required in the proof. But we don't consider now the most general situation.*

Theorem 1 will be obtained as a consequence of Theorem 4 which is formulated in Section 1. Note also that one can compute explicitly the constant C in (1) as well as constants from other assertions below using proofs in the paper.

THEOREM 2 *Let characteristic of the field $\mathrm{char}(k) = 0$. Then there are homogeneous polynomials $g_1, \ldots, g_s \in \mathfrak{P}$, a smooth point point $x \in V$, and a linear form $L \in k[X_0, \ldots, X_n]$ such that*

- $L(x) \neq 0$,
- *$g_1/L^{\deg g_1}, \ldots, g_s/L^{\deg g_s}$ is a system of local parameters (definition of local parameters, see, e.g., in [6]), of the algebraic variety V in the point x,*
- $\deg g_i \leq n^{2^{sC}} \delta_i(\mathfrak{P})$, $1 \leq i \leq s$, *for an absolute constant $0 < C \in \mathbb{R}$.*

As a consequence of Theorem 2 and Lemma 1 we get the following result.

THEOREM 3 *Let characteristic of the field $\mathrm{char}(k) = 0$. Let $\phi_1, \ldots, \phi_m \in k[X_0, \ldots, X_n]$, $m \geq 1$, be arbitrary homogeneous polynomials. Let the degree $\deg \phi_i < d$ for all $1 \leq i \leq m$. Let V be an arbitrary irreducible and defined over k component of the algebraic variety*

$$\mathcal{Z}(\phi_1, \ldots, \phi_m) \subset \mathbb{P}^n(\overline{k})$$

of all common zeroes of these polynomials in $\mathbb{P}^n(\overline{k})$. Let $\dim V = n - s$ where $1 \leq s \leq n$. Then there are homogeneous polynomials $g_1, \ldots, g_s \in \mathfrak{P}$, a smooth point point $x \in V$, and a linear form $L \in k[X_0, \ldots, X_n]$ such that

- $L(x) \neq 0$,
- *$g_1/L^{\deg g_1}, \ldots, g_s/L^{\deg g_s}$ is a system of local parameters of the algebraic variety V in the point x,*
- $\deg g_i \leq n^{2^{sC}} d$, $1 \leq i \leq s$, *for an absolute constant $0 < C \in \mathbb{R}$.*

Using the the theorems of the present paper, [2], [4] we get in [5] the following results. 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 $C(n)d^n$.

1 Plan for the proof of Theorem 1

Denote by K a purely transcendental extension of k of sufficiently large transcendency degree. Now we shall suppose that this transcendency degree is at least $(n+1)^2$. In what follows for any homogeneous ideal $\mathfrak{a}$ of $k[X_0, \ldots, X_n]$ we shall denote by $\mathfrak{a}$ also the ideal generated by $\mathfrak{a}$ in $K[X_0, \ldots, X_n]$ (i.e, the ideal $\mathfrak{a} \otimes_k K$). We shall use the notations $\mathcal{Z}(\mathfrak{a})$ also for the set of all common zeroes of the ideal $\mathfrak{a}$ in the projective space over $\overline{K}$. It will not lead to ambiguities.

We shall consider the category of finitely generated graded $K[X_0, \ldots, X_n]$–modules. Such a module M is a direct sum of its homogeneous components M_m for $0 \leq m \in \mathbb{Z}$. We shall denote by $|M|_m = \dim_K M_m$ the dimension over K of the homogeneous component M_m. For every M there exists [6] a polynomial $\chi \in \mathbb{Q}[Z]$ such that $|M|_m = \chi(m)$ for all sufficiently large m. Denote for brevity $\Lambda = K[X_0, \ldots, X_n]$.

Let $0 \leq v \leq n$ be an integer. Let $U_{v+1}, \ldots, U_n \in K[X_0, \ldots, X_n]$ be linear forms such that the family of their coefficients has elements from the basis of transcendence of the field K over k. Therefore this family of coefficients has transcendency degree $(n+1)(n-v)$ over k. Denote by $\mathfrak{u}_v$ the ideal of $K[X_0, \ldots, X_n]$ generated by $U_{v+1}, \ldots, U_n$.

Let $0 \leq j \leq s$ be an integer and $\mathfrak{p}_j \subset k[X_0, \ldots, X_n]$ be an arbitrary homogeneous prime ideal such that $f_i \in \mathfrak{p}_j \subset \mathfrak{P}$ for all $1 \leq i \leq j$ and $\dim \mathcal{Z}(\mathfrak{p}_j) = n - j$ in $\mathbb{P}^n(\overline{k})$. In particular $\mathfrak{p}_s = \mathfrak{P}$.

By the Bertini theorem for the linear system of hyperplane sections (which is valid for the case of fields of arbitrary characteristic, see [10]) the set $\mathcal{Z}(\mathfrak{p}_j + \mathfrak{u}_v)$ considered as a subset of $\mathbb{P}^n(\overline{K})$

- is empty if $j > v$,
- consists of $\deg \mathcal{Z}(\mathfrak{p}_j)$ points of $\mathbb{P}^n(\overline{K})$ (and the intersection of $\mathcal{Z}(\mathfrak{p}_j)$ with the linear space $\mathcal{Z}(\mathfrak{u}_j)$ is transversal in each point) if $j = v$,
- is an irreducible over the perfect closure of the field K algebraic variety defined over K of dimension $v - j$ if $j < v$.

Set $\mathfrak{p}_{j,v} = \mathcal{I}(\mathcal{Z}(\mathfrak{p}_j + \mathfrak{u}_v)) \subset K[X_0, \ldots, X_n]$. So $\mathfrak{p}_{j,v}$ is a prime ideal if $j < v$. Actually in what follows we shall use only the simple fact that the dimension of every irreducible component of $\mathcal{Z}(\mathfrak{p}_{j,v})$ is $v - j$ if $j \leq v$.

Theorem 1 will be deduced from the following one.

THEOREM 4 *Let $0 \leq j \leq s$ be an integer. Let conditions of Theorem 1 be satisfied. Set also $\delta_0 = 1$. Let $\mathfrak{p}_j$ be an arbitrary prime ideal of $k[X_0, \ldots, X_n]$*

such that $f_i \in \mathfrak{p}_j \subset \mathfrak{P}$ *for all* $1 \le i \le j$ *and* $\dim \mathcal{Z}(\mathfrak{p}_j) = n - j$ *in* $\mathbb{P}^n(\overline{k})$. *Then the following conditions are satisfied.*

(i) There is a constant b_j *(which depends only on* n, s *and* j*) such that the inequality*

$$\delta_j \le b_j \left(\frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} \right)^{1/(s-j+1)}$$

holds (note that if $j \le 1$ *then the product in the denominator of the right part of this inequality is empty and hence is equal to 1).*

(ii) There is a constant a_j *(which depends only on* n, s *and* j*) such that the inequality*

$$a_j \deg \mathcal{Z}(\mathfrak{p}_j) > \delta_1 \cdot \ldots \cdot \delta_j$$

holds.

(iii) There is a constant $c_j > 0$ *(which depends only on* n, s *and* j*) such that the inequality*

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge c_j \delta_1 \cdot \ldots \cdot \delta_j$$

holds for all $m \ge 2^{-1} a_j^{-1} \delta_j$.

Besides that, if $n \ge 2$ *then there is* C, $0 < C \in \mathbb{R}$ *such that for every* n, s *and* j *the constants* a_j, b_j, c_j^{-1} *are bounded from above by* $n^{2^{(j+1)^C}}$.

As a consequence of Theorem 4 we get the following result which proves the conjecture posed in [1].

THEOREM 5 *Let* $s \ge 1$. *Under conditions of Theorem 4 for every* $1 \le j \le s$ *the inequality*

$$\delta_1 \cdot \ldots \cdot \delta_j \le b_1 \cdot \ldots \cdot b_j D^{j/s}$$

holds. Hence there is $C \in \mathbb{R}$ *such that for every* n, s *and every prime ideal* $\mathfrak{p}_j$ *of* $k[X_0, \ldots, X_n]$ *such that* $f_i \in \mathfrak{p}_j \subset \mathfrak{P}$ *for all* $1 \le i \le j$ *and* $\dim \mathcal{Z}(\mathfrak{p}_j) = n - j$ *in* $\mathbb{P}^n(\overline{k})$ *the inequality*

$$\deg \mathcal{Z}(\mathfrak{p}_j) \le n^{2^{(j+1)^C}} D^{j/s}$$

holds.

PROOF Set $d_j = b_1 \cdot \ldots \cdot b_j$ for all $0 \le j \le s$. Note that $d_j \ge 1$ for all j. By the induction hypothesis we can suppose that

$$\delta_1 \cdot \ldots \cdot \delta_{j-1} \le d_{j-1} D^{(j-1)/s}.$$

Then assertion (i) of Theorem 4 implies

$$\begin{aligned}
&\delta_1 \cdot \ldots \cdot \delta_j \le (\delta_1 \cdot \ldots \cdot \delta_{j-1}) b_j \left(\frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} \right)^{1/(s-j+1)} \le \\
&b_j (\delta_1 \cdot \ldots \cdot \delta_{j-1})^{1-1/(s-j+1)} D^{1/(s-j+1)} \le \\
&b_j d_{j-1} D^{((j-1)/s)(1-1/(s-j+1))+1/(s-j+1)} = d_j D^{j/s}.
\end{aligned}$$

The estimation $d_j \le n^{2^{(j+1)^C}}$ follows immediately from the estimation for b_j from Theorem 4. Theorem 5 (modulo Theorem 4) is proved.

Let s, $1 \le s \le n$ be arbitrary. Theorem 4 will be proved by induction on $j \ge 0$. Additionally we shall choose $a_j \ge n+1$ for all j. The base of induction is $j = 0$. Set

$$a_0 = n+1, \quad c_0 = b_0 = 1. \tag{2}$$

In this case assertions (i)–(iii) are trivial since $\mathfrak{p}_0 = \{0\}$ and the products of δ_i in the right sides of (i)–(iii) are empty (and hence are equal to 1).

The constants a_j, b_j, c_j can be estimated using the information obtained from the proof of Theorem 4. Theorem 1 follows from Theorem 4 immediately (the cases $n = 1$ or $s = 1$ of Theorem 1 are trivial). But first of all in the next two sections some preliminary facts will be proved.

2 Properties of $\mathfrak{P}$–sequences

Let the homogeneous prime ideal $\mathfrak{P}$ and the integer s be as in the Introduction.

DEFINITION 3 *Let $0 < j \le s$ be an integer. Consider a sequence of homogeneous polynomials $f_i \in \mathfrak{P}$, $1 \le i \le j$. Let $0 \le u < j$ be an integer. Denote as above by $\mathcal{W} = \mathcal{W}(\mathfrak{P}, u)$ the set of all irreducible components W defined over k of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_u)$ such that $W \supset V$. Suppose that for every integer $0 \le u < j$ the polynomial $f_{u+1} \in \mathfrak{P}$ is such that for every irreducible component $W \in \mathcal{W}$ the algebraic variety*

$$W \not\subset \mathcal{Z}(f_{u+1})$$

and if $u \ge 1$ then $\deg f_{u+1} \ge \deg f_u$. Then any such sequence $f_1, \ldots, f_j$ will be called weak $\mathfrak{P}$–sequence (of length j).

Note that every $\mathfrak{P}$–sequence is a weak $\mathfrak{P}$–sequence.

LEMMA 1 *Let $g_1, \ldots, g_j$ and $h_1, \ldots, h_j$ be two weak $\mathfrak{P}$–sequences. Then there is a weak $\mathfrak{P}$–sequence $q_1, \ldots, q_j$ such that $\deg q_v = \min\{\deg g_v, \deg h_v\}$ and the polynomial q_v belongs to the union of ideals $(g_1, \ldots, g_j) \cup (h_1, \ldots, h_j)$ for all $1 \le v \le j$. Besides that, if $\deg g_i \le \deg h_i$ for all $1 \le i \le i_1$ for some $i_1 \le j$ then one can take $q_i = g_i$ for all $1 \le i \le i_1$.*

PROOF Denote $\deg g_u = \mu_u$, $\deg h_u = \nu_u$ for all $1 \le u \le j$. Set $g_{0,u} = g_u$ and $h_{0,u} = h_u$ for all $1 \le u \le j$.

Let $0 \le v \le j$ be an integer. Suppose that we have already constructed recursively the polynomials q_u for all $u \le v$ and the polynomials $g_{v,v+1}, \ldots, g_{v,j}$, $h_{v,v+1}, \ldots, h_{v,j}$ satisfying the following properties

- $\deg g_{v,u} = \mu_u$ for all $v+1 \le u \le j$,
- $\deg h_{v,u} = \nu_u$ for all $v+1 \le u \le j$,
- $q_1, \ldots, q_v, g_{v,v+1}, \ldots, g_{v,j}$ is a weak $\mathfrak{P}$–sequence,
- $q_1, \ldots, q_v, h_{v,v+1}, \ldots, h_{v,j}$ is a weak $\mathfrak{P}$–sequence.

Let $\deg g_{v,v+1} \leq \deg h_{v,v+1}$ (the case of the opposite strict inequality is considered analogously). Then set $q_{v+1} = g_{v,v+1}$ and $g_{v+1,u} = g_{v,u}$ for all $v+2 \leq u \leq j$. Further, we shall construct polynomials $\widetilde{h}_{v+2}, \ldots, \widetilde{h}_j$ satisfying the following conditions.

- the polynomial $\widetilde{h}_u$ belongs to the ideal $(h_{v,v+1}, \ldots, h_{v,j})$ for every $v+2 \leq u \leq j$,
- $q_1, \ldots, q_{v+1}, \widetilde{h}_{v+2}, \ldots, \widetilde{h}_j$ is a weak $\mathfrak{P}$–sequence,
- $\deg \widetilde{h}_u = \nu_u$ for all $v+2 \leq u \leq j$.

To construct the polynomials $\widetilde{h}_{v+2}, \ldots, \widetilde{h}_j$ we need one more recursion. Let $v+3 \leq u \leq j+1$ be an integer. Suppose that we have already constructed the polynomials $\widetilde{h}_i$ for $u \leq i \leq j$. Suppose also that

$$\widetilde{h}_i = h_{v,i} + \sum_{v+1 \leq w \leq i-1} r_{v,i,w} h_{v,w}$$

where $r_{v,i,w} \in k[X_0, \ldots, X_n]$ are homogeneous polynomials and $\deg r_{v,i,w} = \nu_i - \nu_w$ for all i and w. Suppose that $q_1, \ldots, q_{v+1}, \widetilde{h}_u, \ldots, \widetilde{h}_j$ is a weak $\mathfrak{P}$–sequence. So in the case when $u = j+1$ nothing is constructed.

Let us show that we can construct the polynomial $\widetilde{h}_{u-1}$ such that the described properties will be satisfied if we replace u by $u-1$. Indeed, the algebraic variety $\mathcal{Z}(\mathfrak{P})$ is an irreducible component of the set

$$\begin{aligned}
&\mathcal{Z}(q_1, \ldots, q_v, h_{v,v+1}, \ldots, h_{v,j}) \cap \mathcal{Z}(q_{v+1}) = \\
&\mathcal{Z}(q_1, \ldots, q_v, h_{v,v+1}, \ldots, h_{v,u-1}, \widetilde{h}_u, \ldots, \widetilde{h}_j) \cap \mathcal{Z}(q_{v+1}) = \\
&\mathcal{Z}(q_1, \ldots, q_{v+1}, \widetilde{h}_u, \ldots, \widetilde{h}_j) \cap \mathcal{Z}(h_{v,v+1}, \ldots, h_{v,u-1})
\end{aligned}$$

Hence, there are homogeneous polynomials r_w of degrees $\deg r_w = \nu_{u-1} - \nu_w$ for all $v+1 \leq w \leq u-1$ such that $r_{u-1} = 1$ and every polynomial r_w, $v+1 \leq w \leq u-2$, is not vanishing on the algebraic variety $\mathcal{Z}(\mathfrak{P})$. Then $\mathcal{Z}(\mathfrak{P})$ is an irreducible component of the algebraic variety

$$\mathcal{Z}(q_1, \ldots, q_{v+1}, \widetilde{h}_u, \ldots, \widetilde{h}_j) \cap \mathcal{Z}(r_{v+1} h_{v,v+1}, \ldots, r_{u-1} h_{v,u-1}).$$

Therefore, there are elements $\alpha_{v+1}, \ldots, \alpha_{u-2} \in k$ such that

$$q_1, \ldots, q_{v+1}, h_{v,u-1} + \sum_{v+1 \leq w \leq u-2} \alpha_w r_w h_{v,w}, \widetilde{h}_u, \ldots, \widetilde{h}_j$$

is a weak $\mathfrak{P}$–sequence. Thus, we can set $r_{v,u-1,w} = \alpha_w r_w$ for all $v+1 \leq w \leq u-2$. Our assertion is proved. Hence by this second recursion we can construct the required polynomials $\widetilde{h}_i$, $v+2 \leq i \leq j$.

Set $h_{i+1,u} = \widetilde{h}_u$ for all $v+2 \leq u \leq j$. Thus, we can effect the next step of the first recursion. Finally, we shall construct the required polynomials $q_1, \ldots, q_j$. The first assertion of the lemma is proved. The second one follows immediately from the construction described in the proof of the first assertion. The lemma is proved.

LEMMA 2 *Let $g_1, \dots, g_j$ be a $\mathfrak{P}$–sequence and $h_1, \dots, h_j$ be a weak $\mathfrak{P}$–sequence. Then* $\deg g_i \le \deg h_i$ *for all* $1 \le i \le j$. *In particular if $h_1, \dots, h_j$ is a $\mathfrak{P}$–sequence then* $\deg g_i = \deg h_i$ *for all* $1 \le i \le j$, *i.e., for any $\mathfrak{P}$–sequence $g_1, \dots, g_j$ and an integer i such that $1 \le i \le j$ the degree* $\deg g_i$ *depends only on $\mathfrak{P}$ and i, and does not depend in the choice of polynomials $g_1, \dots, g_j$.*

PROOF This follows immediately from Definition 1 and Lemma 1. The lemma is proved.

3 Estimations for characteristic functions of a prime ideal and its reductions

We shall use the notations $\mathfrak{p}_j$, $\mathfrak{p}_{j,v}$ introduced in Section 1. It is not necessary to suppose in this section that $\mathfrak{p}_j \subset \mathfrak{P}$. So we shall suppose only that $\mathfrak{p}_j$ is a prime ideal and $\dim \mathcal{Z}(\mathfrak{p}_j) = n - j$ for all $0 \le j \le n$. Recall that $\mathfrak{p}_j = \mathfrak{p}_{j,n}$.

LEMMA 3 *Let $0 \le j < v \le n$ be integers. Then for every $m \ge 1$ the inequality*

$$|\Lambda/\mathfrak{p}_{j,v}|_m \ge \sum_{0 \le i \le v-j-1} \binom{m+i-1}{i} |\Lambda/\mathfrak{p}_{j,v-i}|_0 + \sum_{1 \le i \le m} \binom{v-j-1+m-i}{v-j-1} |\Lambda/\mathfrak{p}_{j,j}|_i$$

holds (herewith $|\Lambda/\mathfrak{p}_{j,v-i}|_0 = 1$ for all i, j, v).

PROOF Let $w \ge 1$ be an integer. Consider the exact sequence of vector spaces

$$0 \to (\Lambda/\mathfrak{p}_{j,v})_{w-1} \to (\Lambda/\mathfrak{p}_{j,v})_w \to (\Lambda/(\mathfrak{p}_{j,v} + (U_v)))_w \to 0 \tag{3}$$

which is induced by the multiplication to U_v. We have

$$|\Lambda/(\mathfrak{p}_{j,v} + (U_v))|_w \ge |\Lambda/\mathfrak{p}_{j,v-1}|_w$$

by the definition of the ideals $\mathfrak{p}_{j,v}$ and $\mathfrak{p}_{j,v-1}$. Hence,

$$|\Lambda/\mathfrak{p}_{j,v}|_w \ge |\Lambda/\mathfrak{p}_{j,v}|_{w-1} + |\Lambda/\mathfrak{p}_{j,v-1}|_w.$$

Summing these inequalities for $1 \le w \le m$ we get the following one

$$|\Lambda/\mathfrak{p}_{j,v}|_m \ge |\Lambda/\mathfrak{p}_{j,v}|_0 + \sum_{1 \le w \le m} |\Lambda/\mathfrak{p}_{j,v-1}|_w. \tag{4}$$

If $j = v-1$ the required assertion is proved. Let $j < v-1$. Applying the similar construction (with v replaced by $v-1$) to every summand of the sum from the right part of (4) and iterating in the same way as far as it is possible we get the required inequality. The lemma is proved.

LEMMA 4 *Let $0 \le v \le j \le n$ be integers. Let*

$$|\Lambda/\mathfrak{p}_{j-v,j-v}|_\mu \ge \gamma$$

for some $\mu \geq 1$. Then for every $m \geq \mu$ the inequality

$$|\Lambda/\mathfrak{p}_{j-v,j}|_m \geq \binom{v+m-\mu}{v}\gamma$$

holds. Hence, if $\mu_1 \in \mathbb{R}$, $\mu - 1 < \mu_1 \leq \mu$ and $m \geq 2\mu_1$ then

$$|\Lambda/\mathfrak{p}_{j-v,j}|_m \geq (2^v v!)^{-1} m^v \gamma.$$

PROOF We can suppose without loss of generality that $v > 0$. Considering the exact sequence similar to (3) we get

$$|\Lambda/\mathfrak{p}_{j-v,j-v}|_m \leq |\Lambda/\mathfrak{p}_{j-v,j-v}|_{m+1}$$

for every m. Therefore, Lemma 3 implies that

$$|\Lambda/\mathfrak{p}_{j-v,j}|_m \geq \left(\binom{v-1}{v-1} + \ldots + \binom{v-1+m-\mu}{v-1}\right)\gamma = \binom{v+m-\mu}{v}\gamma.$$

The second assertion follows from the first one immediately since $m \geq 2\mu - 1$ in this case. The lemma is proved.

4 Proof of the first assertion of Theorem 4

We shall use the notations from Section 1. Let $0 < j \leq s$. We shall suppose by induction that Theorem 4 is already proved for all prime ideals $\mathfrak{p}_u$ with $u < j$. So the constants a_u, b_u and c_u are defined for all $0 \leq u < j$. In this section our aim is to prove assertion (i) of Theorem 4 for j and define the constant b_j.

Let $\mathfrak{p}_{j-1}$ be an arbitrary prime ideal of $k[X_0, \ldots, X_n]$ such that $f_i \in \mathfrak{p}_{j-1} \subset \mathfrak{P}$ for all $1 \leq i \leq j-1$ and $\dim \mathcal{Z}(\mathfrak{p}_{j-1}) = n-j+1$ in $\mathbb{P}^n(\overline{k})$. Recall that $\mathfrak{p}_{j-1} = \mathfrak{p}_{j-1,n}$. Set μ to be the least integer such that $\mu \geq 2^{-1}a_{j-1}^{-1}\delta_{j-1}$. Applying Lemma 4 we get

$$|\Lambda/\mathfrak{p}_{j-1}|_m \geq \binom{n-j+1+m-\mu}{n-j+1} c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1} \tag{5}$$

for all $m \geq \mu$.

We shall use the upper bound for the characteristic function of a homogeneous prime ideal obtained in [11] for the case of zero–characteristic. This result was improved and extended for the case of non–zero characteristic in [1]. Recall that $\deg \mathcal{Z}(\mathfrak{P}) = D$. It is proved in [1] that for all $m \geq 0$ the inequality

$$|\Lambda/\mathfrak{P}|_m \leq \binom{n-s+m}{n-s} D \tag{6}$$

holds.

Denote by S_{j-1} the set of all homogeneous prime ideals $\mathfrak{p}_{j-1} \subset k[X_0, \ldots, X_n]$ such that $\dim \mathcal{Z}(\mathfrak{p}_{j-1}) = n-j+1$ and the ideals

$$(f_1, \ldots, f_{j-1}) \subset \mathfrak{p}_{j-1} \subset \mathfrak{P}.$$

Considering the epimorphism $(\Lambda/\mathfrak{p}_{j-1})_m \to (\Lambda/\mathfrak{P})_m$ we see that (5) and (6) imply that if

$$\binom{n-j+1+m-\mu}{n-j+1} c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1} > \binom{n-s+m}{n-s} D \tag{7}$$

then there is a homogeneous polynomial $g \in (\mathfrak{P})_m \setminus (\mathfrak{p}_{j-1})_m$ for every $m \geq \mu$ and each prime ideal $\mathfrak{p}_{j-1} \in S_{j-1}$. Hence it follows from (7) that there is a homogeneous polynomial

$$g \in (\mathfrak{P})_m \setminus \bigcup_{\mathfrak{p}_{j-1} \in S_{j-1}} (\mathfrak{p}_{j-1})_m \tag{8}$$

for every $m \geq \mu$. Note that (7) is equivalent to the inequality

$$\prod_{1 \leq i \leq n-s} \frac{m-\mu+i}{m+i} \prod_{n-s<i \leq n-j+1} (m-\mu+i) > c_{j-1}^{-1} \frac{(n-j+1)!}{(n-s)!} \frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}}.$$

If $m \geq (n+1)\mu$ then each factor of the first product of the considered inequality is greater than $n/(n+1)$. Hence if

$$m \geq \max\left\{ \left(c_{j-1}^{-1} \frac{(n-j+1)!}{(n-s)!} \left(\frac{n+1}{n} \right)^n \right)^{1/(s-j+1)} \times \left(\frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} \right)^{1/(s-j+1)} + \mu, (n+1)\mu \right\} \tag{9}$$

than (7) holds and $m \geq \mu$. Therefore, if (9) holds than there is a homogeneous polynomial g satisfying (8). Note that by the definition of $\mathfrak{P}$–sequence we have $\deg g \geq \delta_j$.

Suppose that the maximum in the right part of (9) is the first term in the braces. Then

$$\delta_j \leq 3 \left(\frac{4(n-j+1)!}{(n-s)!c_{j-1}} \right)^{1/(s-j+1)} \left(\frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} \right)^{1/(s-j+1)}. \tag{10}$$

Suppose that the maximum in the right part of (9) is $(n+1)\mu$. In this case

$$\delta_j \leq (n+1)(2^{-1}a_{j-1}^{-1}\delta_{j-1}+1) \leq 2^{-1}\delta_j + n + 1$$

since $a_{j-1} \geq n+1$ and $\delta_j \geq \delta_{j-1}$. Therefore $\delta_j \leq 2n+2$. Hence $\delta_i \leq 2n+2$ for every $1 \leq i \leq j$. Thus,

$$\delta_j \leq (2n+2)^{1+(j-1)/(s-j+1)} \left(\frac{D}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} \right)^{1/(s-j+1)} \tag{11}$$

in this case.

Set

$$b_j = \max\left\{ 3n \left(4c_{j-1}^{-1} \right)^{1/(s-j+1)}, (2n+2)^{1+(j-1)/(s-j+1)} \right\}. \tag{12}$$

Then it follows from previous considerations that for b_j defined by this formula the first assertion of Theorem 4 holds. Thus, the first assertion of Theorem 4 is proved.

In the case when $s = j$ set $a_j = b_j + 1$. Thus, assertion (ii) of Theorem 4 is proved for j in the case when $s = j$.

5 Proof of the second assertion of Theorem 4

We shall use the notations from Section 1. Let $0 < j \leq s$. We shall suppose by induction that Theorem 4 is already proved for all prime ideals $\mathfrak{p}_u$ with $u < j$. So a_u, b_u, c_u are defined for all $0 \leq u < j$. In this section our aim is to prove assertion (ii) of Theorem 4 and define the constant a_j.

The case when $s = j$ was considered in the previous section. So we shall suppose without loss of generality that $s > j$.

Let $\mathfrak{p}_{j-1}$, $\mathfrak{p}_j$ be arbitrary homogeneous prime ideals such as in previous sections. Recall that $\mathfrak{p}_{j-1} = \mathfrak{p}_{j-1,n}$. Set μ to be the least integer such that $\mu \geq 2^{-1}a_{j-1}^{-1}\delta_{j-1}$. Applying Lemma 4 we get

$$|\Lambda/\mathfrak{p}_{j-1}|_m \geq \binom{n-j+1+m-\mu}{n-j+1} c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1} \tag{13}$$

for all $m \geq \mu$.

For all $m \geq 0$ by [1] the inequality

$$|\Lambda/\mathfrak{p}_j|_m \leq \binom{n-j+m}{n-j} \deg \mathcal{Z}(\mathfrak{p}_j)$$

holds. Hence for all $m \geq 0$ we have

$$|\Lambda/(\mathfrak{p}_{j-1}+\mathfrak{p}_j)|_m \leq |\Lambda/\mathfrak{p}_j|_m \leq \binom{n-j+m}{n-j} \deg \mathcal{Z}(\mathfrak{p}_j). \tag{14}$$

Denote by S_{j-1} the set of all homogeneous prime ideals $\mathfrak{p}_{j-1} \subset k[X_0, \ldots, X_n]$ such that $\dim \mathcal{Z}(\mathfrak{p}_{j-1}) = n-j+1$ and the ideals

$$(f_1, \ldots, f_{j-1}) \subset \mathfrak{p}_{j-1} \subset \mathfrak{P}.$$

Considering the epimorphism $(\Lambda/\mathfrak{p}_{j-1})_m \to (\Lambda/(\mathfrak{p}_{j-1}+\mathfrak{p}_j))_m$ we see that (13) and (14) imply that if

$$\binom{n-j+1+m-\mu}{n-j+1} c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1} > \binom{n-j+m}{n-j} \deg \mathcal{Z}(\mathfrak{p}_j) \tag{15}$$

then there is a homogeneous polynomial $g \in (\mathfrak{p}_j)_m \setminus (\mathfrak{p}_{j-1})_m$ for every $m \geq \mu$ and each prime ideal $\mathfrak{p}_{j-1} \in S_{j-1}$. Hence it follows from (15) that there is a homogeneous polynomial

$$g \in (\mathfrak{p}_j)_m \setminus \bigcup_{\mathfrak{p}_{j-1} \in S_{j-1}} (\mathfrak{p}_{j-1})_m \subset (\mathfrak{P})_m \setminus \bigcup_{\mathfrak{p}_{j-1} \in S_{j-1}} (\mathfrak{p}_{j-1})_m \tag{16}$$

for every $m \geq \mu$. Note that (15) is equivalent to the inequality

$$(m-\mu+n-j+1) \prod_{1 \leq i \leq n-j} \frac{m-\mu+i}{m+i} > \frac{(n-j+1)\deg \mathcal{Z}(\mathfrak{p}_j)}{c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1}}.$$

If $m \geq (n+1)\mu$ then $(m-\mu+i)/(m+i) > n/(n+1)$ for every $1 \leq i \leq n-j$. Hence if

$$m \geq \max\Big\{ \frac{n-j+1}{c_{j-1}} \left(\frac{n+1}{n}\right)^n \frac{\deg \mathcal{Z}(\mathfrak{p}_j)}{\delta_1 \cdot \ldots \cdot \delta_{j-1}} + \mu,\ (n+1)\mu \Big\} \tag{17}$$

than (15) holds and $m \geq \mu$. Therefore, if (17) holds than there is a homogeneous polynomial g satisfying (16). Note that by the definition of $\mathfrak{P}$–sequence we have $\deg g \geq \delta_j$.

Suppose that the maximum in the right part of (17) is the first term in the braces. Then

$$\delta_j < \frac{12(n-j+1)\deg \mathcal{Z}(\mathfrak{p}_j)}{c_{j-1}\delta_1 \cdot \ldots \cdot \delta_{j-1}}. \tag{18}$$

Hence

$$12(n-j+1)c_{j-1}^{-1}\deg \mathcal{Z}(\mathfrak{p}_j) > \delta_1 \cdot \ldots \cdot \delta_j.$$

Suppose that the maximum in the right part of (17) is $(n+1)\mu$. In this case

$$\delta_j \leq (n+1)(2^{-1}a_{j-1}^{-1}\delta_{j-1}+1) \leq 2^{-1}\delta_j + n + 1$$

since $a_{j-1} \geq n+1$ and $\delta_j \geq \delta_{j-1}$. Therefore $\delta_j \leq 2n+2$. Hence $\delta_i \leq 2n+2$ for every $1 \leq i \leq j$. Thus,

$$(2n+2)^j \deg \mathcal{Z}(\mathfrak{p}_j) \geq \delta_1 \cdot \ldots \cdot \delta_j \tag{19}$$

in this case.

Thus, if $j < s$ set

$$a_j = \max\left\{12(n-j+1)c_{j-1}^{-1},\, (2n+2)^j + 1\right\} \tag{20}$$

and if $j = s$ set

$$a_s = b_s + 1. \tag{21}$$

Then it follows from previous considerations that for a_j defined by these formulas the second assertion of Theorem 4 holds. Thus, the second assertion of Theorem 4 is proved.

6 Proof of the third assertion of Theorem 4

We shall use the notations from Section 1. Let $0 < j \leq s$. We shall suppose by induction that Theorem 4 is already proved for all prime ideals $\mathfrak{p}_u$ with $u < j$ and assertion (ii) is already proved for j. So a_u are defined for all $0 \leq u \leq j$, the constants b_u and c_u are defined for all $1 \leq u < j$. In this section our aim is to prove assertion (iii) of Theorem 4 and define the constant c_j.

Let v, $1 \leq v \leq j$ be an integer. Let $\mathfrak{p}_{j-v}$ be an arbitrary homogeneous prime ideal such that $(f_1, \ldots, f_{j-v}) \subset \mathfrak{p}_{j-v} \subset \mathfrak{p}_j$. By the induction hypothesis and Lemma 4 for every $m \geq a_{j-v}^{-1}\delta_{j-v}$ the inequality

$$|\Lambda/\mathfrak{p}_{j-v,j}|_m > (2^v v!)^{-1} c_{j-v}\delta_1 \cdot \ldots \cdot \delta_{j-v} m^v \tag{22}$$

holds. Suppose that

$$(2^v v!)^{-1} c_{j-v}\delta_1 \cdot \ldots \cdot \delta_{j-v} m^v > |\Lambda/\mathfrak{p}_{j,j}|_m. \tag{23}$$

Considering the epimorphism $(\Lambda/\mathfrak{p}_{j-v,j})_m \to (\Lambda/\mathfrak{p}_{j,j})_m$ we see that (22) and (23) imply that there is a homogeneous polynomial $g \in (\mathfrak{p}_{j,j})_m \setminus (\mathfrak{p}_{j-v,j})_m$. Hence $\dim \mathcal{Z}(\mathfrak{p}_{j-v,j}) \cap \mathcal{Z}(g) < \dim \mathcal{Z}(\mathfrak{p}_{j-v,j})$ and $\deg g = m$.

Let us show that every point from $\mathcal{Z}(\mathfrak{p}_{j,j})$ does not belong to any component W of $\mathcal{Z}(f_1,\ldots,f_j)$ which does not contain $\mathcal{Z}(\mathfrak{p}_j)$. Indeed, otherwise, this point belongs to the intersection of $\mathcal{Z}(\mathfrak{p}_j)\cap W$, i.e., belongs to some algebraic variety W_1 of dimension less than $n-j$ defined over k. But the generic linear space $\mathcal{Z}(\mathfrak{u}_j)$ does not intersect any algebraic variety defined over k of dimension less than $n-j$. This contradiction proves our assertion.

By the definition of $\mathfrak{P}$–sequence the algebraic variety $\mathcal{Z}(\mathfrak{p}_j)$ is an irreducible component of the algebraic variety $\mathcal{Z}(\mathfrak{p}_{j-v})\cap\mathcal{Z}(f_{j-v+1},\ldots,f_j)$. Hence, each point from $\mathcal{Z}(\mathfrak{p}_{j,j})$ is an isolated point of the algebraic variety $\mathcal{Z}(\mathfrak{p}_{j-v,j})\cap\mathcal{Z}(f_{j-v+1},\ldots,f_j)$.

LEMMA 5 *There are homogeneous polynomials* $\widetilde{f}_{j-v+2},\ldots,\widetilde{f}_j\in k[X_0,\ldots,X_n]$ *such that each point from* $\mathcal{Z}(\mathfrak{p}_{j,j})$ *is an isolated point of the algebraic variety*

$$\mathcal{Z}(\mathfrak{p}_{j-v,j})\cap\mathcal{Z}(g)\cap\mathcal{Z}(\widetilde{f}_{j-v+2},\ldots,\widetilde{f}_j)$$

and the degrees $\deg\widetilde{f}_i=\delta_i$ *for all* $j-v+2\le i\le j$.

PROOF Actually the proof of this lemma is similar to the one of Lemma 1 but we give it in detail for completeness. Let $j-v+3\le u\le j+1$ be an integer. Suppose that we have already constructed the polynomials $\widetilde{f}_i$ for $u\le i\le j$. Suppose also that

$$\widetilde{f}_i=f_i+\sum_{j-v+1\le w\le i-1}h_{i,w}f_w$$

where $h_{i,w}\in k[X_0,\ldots,X_n]$ are homogeneous polynomials and $\deg h_{i,w}=\delta_i-\delta_w$ for all i and w. Suppose that every irreducible component W of the algebraic variety

$$\mathcal{Z}(\mathfrak{p}_{j-v,j})\cap\mathcal{Z}(g)\cap\mathcal{Z}(\widetilde{f}_u,\ldots,\widetilde{f}_j)$$

such that $W\cap\mathcal{Z}(\mathfrak{p}_{j,j})\ne\emptyset$ has dimension $\dim W=u-j+v-2$. So in the case when $u=j+1$ nothing is constructed.

Let us show that we can construct the polynomial $\widetilde{f}_{u-1}$ such that the described properties will be satisfied if we replace u by $u-1$. Let W be an introduced above irreducible component. Each point from $\mathcal{Z}(\mathfrak{p}_{j,j})\cap W$ is an isolated point of the algebraic variety

$$W\cap\mathcal{Z}(f_{j-v+1},\ldots,f_j)=W\cap\mathcal{Z}(f_{j-v+1},\ldots,f_{u-1},\widetilde{f}_u,\ldots,\widetilde{f}_j)=$$
$$W\cap\mathcal{Z}(f_{j-v+1},\ldots,f_{u-1}).$$

Hence, there are homogeneous polynomials $\widetilde{h}_w$ of degrees $\deg\widetilde{h}_w=\delta_{u-1}-\delta_w$ for all $j-v+1\le w\le u-1$ such that $\widetilde{h}_{u-1}=1$ and every polynomial $\widetilde{h}_w$, $j-v+1\le w\le u-2$, is not vanishing in each point of $\mathcal{Z}(\mathfrak{p}_{j,j})$. Then each point from $\mathcal{Z}(\mathfrak{p}_{j,j})\cap W$ is an isolated point of the algebraic variety

$$W\cap\mathcal{Z}(\widetilde{h}_{j-v+1}f_{j-v+1},\ldots,\widetilde{h}_{u-1}f_{u-1})$$

for every irreducible component W. Therefore, there are elements $\alpha_{j-v+1},\ldots,\alpha_{u-2}\in k$ such that

$$W\cap\mathcal{Z}(f_{u-1}+\sum_{j-v+1\le w\le u-2}\alpha_w\widetilde{h}_wf_w)\ne W$$

for every irreducible component W introduced above. Thus, we can set $h_{u-1,w} = \alpha_w \widetilde{h}_w$ for all $j-v+1 \le w \le u-2$. Our assertion is proved. Hence recursively we can construct the required polynomials $\widetilde{f}_i$, $j-v+2 \le i \le j$. The lemma is proved.

Now by Lemma 5, the Bézout inequality and (i) we have the following inequalities

$$\begin{aligned}
&\deg \mathcal{Z}(\mathfrak{p}_{j-v,j}) \deg g \deg \widetilde{f}_{j-v+2} \cdot \ldots \cdot \deg \widetilde{f}_j \ge \deg \mathcal{Z}(\mathfrak{p}_{j,j}),\\
&\delta_1 \cdot \ldots \cdot \delta_{j-v} \ge \deg \mathcal{Z}(\mathfrak{p}_{j-v,j}),\\
&\deg \mathcal{Z}(\mathfrak{p}_{j,j}) > a_j^{-1}\delta_1 \cdot \ldots \cdot \delta_j .
\end{aligned}$$

Recall that $\deg g = m$ and by Lemma 5 the degree $\deg \widetilde{f}_w = \delta_w$ for $j-v+2 \le w \le j$. Hence,

$$\delta_1 \cdot \ldots \cdot \delta_{j-v} m \delta_{j-v+2} \cdot \ldots \cdot \delta_j > a_j^{-1}\delta_1 \cdot \ldots \cdot \delta_j .$$

So $m > a_j^{-1}\delta_{j-v+1}$. Thus, we have proved the following fact.

LEMMA 6 *Let $1 \le v \le j \le s$ be integers. Suppose that an integer m satisfies the inequality $a_{j-v}^{-1}\delta_{j-v} \le m \le a_j^{-1}\delta_{j-v+1}$. Then*

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge (2^v v!)^{-1} c_{j-v} \delta_1 \cdot \ldots \cdot \delta_{j-v} m^v . \tag{24}$$

Set $v = 1$ if $a_{j-1}^{-1}\delta_{j-1} < 2^{-1}a_j^{-1}\delta_j$. If $a_{j-1}^{-1}\delta_{j-1} \ge 2^{-1}a_j^{-1}\delta_j$ then set

$$v = 1 + \max\{w \,:\, a_{j-w}^{-1}\delta_{j-w} \ge 2^{-1}a_j^{-1}\delta_{j-w+1} \,\&\, 1 \le w \le j\}. \tag{25}$$

Later on we shall consider two cases. In the first case we shall suppose that

$$\delta_{j-v+1} > 2a_j , \tag{26}$$

in the second one that

$$\delta_{j-v+1} \le 2a_j . \tag{27}$$

Let (26) holds. Then $v \le j$ since $a_j > 1$. Further,

$$a_j^{-1}\delta_{j-v+1} - 2^{-1}a_j^{-1}\delta_{j-v+1} = 2^{-1}a_j^{-1}\delta_{j-v+1} > 1.$$

Hence there is an integer m such that

$$2^{-1}a_j^{-1}\delta_{j-v+1} \le m \le a_j^{-1}\delta_{j-v+1}. \tag{28}$$

So by (25) and since $v \le j$ the inequality

$$a_{j-v}^{-1}\delta_{j-v} < m \le a_j^{-1}\delta_{j-v+1} \tag{29}$$

holds for this m. Now Lemma 6 and (28) imply

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge (2^v v!)^{-1} c_{j-v} \delta_1 \cdot \ldots \cdot \delta_{j-v} 2^{-v} a_j^{-v} \delta_{j-v+1}^v . \tag{30}$$

Again by (25) the inequalities

$$2^{-1}a_j^{-1}a_{j-w}\delta_{j-w+1} \le \delta_{j-w}$$

are satisfied for all $1 \le w \le v-1$. Therefore,

$$2^{v-w-1}a_j^{v-w-1}a_{j-w-1}^{-1}\cdot\ldots\cdot a_{j-v+1}^{-1}\delta_{j-v+1} \ge \delta_{j-w} \tag{31}$$

for all $0 \le w \le v-2$. It follows from (30) and (31) that

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge (2^v v!)^{-1}c_{j-v}\delta_1\cdot\ldots\cdot\delta_{j-v+1}2^{-v}a_j^{-v}\times$$
$$\prod_{0\le w\le v-2}\frac{\delta_{j-w}}{2^{v-w-1}a_j^{v-w-1}a_{j-w-1}^{-1}\cdot\ldots\cdot a_{j-v+1}^{-1}} =$$
$$(2^v v!)^{-1}c_{j-v}2^{-(v^2+v)/2}a_j^{(-v^2-v)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_{j-v+1}^{v-1}\delta_1\cdot\ldots\cdot\delta_j$$

for all $m \ge 2^{-1}a_j^{-1}\delta_{j-v+1}$.

Now consider the second case when (27) holds. Suppose that $v \le j$. Then $\delta_1 \le \ldots \le \delta_{j-v+1} \le 2a_j$ and as in the first case (31) is satisfied for all $0 \le w \le v-2$. Hence for every $m \ge 1$

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge 1 \ge \frac{\delta_1}{2a_j}\cdot\ldots\cdot\frac{\delta_{j-v+1}}{2a_j}\times$$
$$\prod_{0\le w\le v-2}\frac{\delta_{j-w}}{2a_j2^{v-w-1}a_j^{v-w-1}a_{j-w-1}^{-1}\cdot\ldots\cdot a_{j-v+1}^{-1}} =$$
$$(2a_j)^{-j}2^{(-v^2+v)/2}a_j^{(-v^2+v)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_{j-v+1}^{v-1}\delta_1\cdot\ldots\cdot\delta_j.$$

Finally, suppose that $v = j+1$. Then as in the first case (31) is satisfied for all $0 \le w \le v-2$. Recall that $\delta_0 = 1$. Hence for every $m \ge 1$

$$|\Lambda/\mathfrak{p}_{j,j}|_m \ge 1 \ge \prod_{0\le w\le v-2}\frac{\delta_{j-w}}{2^{v-w-1}a_j^{v-w-1}a_{j-w-1}^{-1}\cdot\ldots\cdot a_{j-v+1}^{-1}} =$$
$$2^{(-v^2+v)/2}a_j^{(-v^2+v)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_{j-v+1}^{v-1}\delta_1\cdot\ldots\cdot\delta_j =$$
$$2^{-(j^2+j)/2}a_j^{-(j^2+j)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_0^j\delta_1\cdot\ldots\cdot\delta_j.$$

Set for $1 \le v \le j$

$$\begin{aligned} c'_{j,v} &= (2^v v!)^{-1}c_{j-v}2^{-(v^2+v)/2}a_j^{(-v^2-v)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_{j-v+1}^{v-1},\\ c''_{j,v} &= (2a_j)^{-j}2^{(-v^2+v)/2}a_j^{(-v^2+v)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_{j-v+1}^{v-1}. \end{aligned} \tag{32}$$

Set

$$c'''_j = 2^{-(j^2+j)/2}a_j^{-(j^2+j)/2}a_{j-1}a_{j-2}^2\cdot\ldots\cdot a_0^j. \tag{33}$$

By definition, put

$$c_j = \min_{1\le v\le j}\{c'_{j,v}, c''_{j,v}, c'''_j\}. \tag{34}$$

Then it follows from previous considerations that for c_j defined by this formula the third assertion of Theorem 4 holds. Thus, the third assertion of Theorem 4 is proved.

The required in the formulation of Theorem 4 estimations for constants a_j, b_j and c_j^{-1} now follow immediately from (2), (12), (20), (21), (32), (33) and (34). Theorem 4 and Theorem 1 are completely proved.

7 Some facts from elimination theory

Let $n \geq 0$. Consider $n+1$ homogeneous polynomials $F_0, \ldots, F_n$ in $n+1$ variables $X_0, \ldots, X_n$ of degrees $\deg F_i = d_i$, $0 \leq i \leq n$ with indeterminante coefficients, i.e., the family of all coefficients of these polynomials is algebraically independent over $\mathbb{Z}$. Denote by $\mathcal{R}$ the ring generated by the coefficients of $F_0, \ldots, F_n$ over $\mathbb{Z}$. By definition *the resultant (or the resultant form) of homogeneous polynomials* $F_0, \ldots, F_n$ is a unique up to a factor ± 1 irreducible element $R \in \mathcal{R}$ (it exists, see [7]) satisfying the following condition. Let $\widetilde{F}_0, \ldots, \widetilde{F}_n$ be arbitrary homogeneous polynomials in $X_0, \ldots, X_n$ of degrees $\deg \widetilde{F}_i = d_i$, $0 \leq i \leq n$ with coefficients from the field K_1. So the coefficients of $\widetilde{F}_0, \ldots, \widetilde{F}_n$ correspond to coefficients of $F_0, \ldots, F_n$. Let $\widetilde{R} \in K_1$ be obtained by substitution of the coefficients of $\widetilde{F}_0, \ldots, \widetilde{F}_n$ in R and the natural homomorphism $\mathbb{Z} \to K_1$. Then $\widetilde{R} = 0$ if and only if $\mathcal{Z}(\widetilde{F}_0, \ldots, \widetilde{F}_n) \neq \emptyset$ in $\mathbb{P}^n(\overline{K_1})$. The element $\widetilde{R}$ is called *the resultant of homogeneous polynomials* $\widetilde{F}_0, \ldots, \widetilde{F}_n$. The factor ± 1 in the definition of the resultant can be chosen canonically using Lemma 7, see Definition 4 below. We shall denote the resultant with canonically chosen sign

$$\widetilde{R} = \mathrm{Res}_{X_0, \ldots, X_n}(\widetilde{R}_0, \ldots, \widetilde{R}_n).$$

Denote by $(F_0, \ldots, F_n)$ the ideal of $\mathcal{R}[X_0, \ldots, X_n]$ generated by $F_0, \ldots, F_n$. The main property of the resultant R, see [7], cf. [8], [9], is that for all sufficiently large integers N and all $0 \leq i \leq n$

$$RX_i^N \in (F_0, \ldots, F_n). \tag{35}$$

In [7] this property is proved if one replaces $\mathbb{Z}$ by a primitive field (and K_1 is a field of the same characteristic), and it will be sufficient for our aims later.

LEMMA 7 *Let $n \geq 1$. Denote by R_1 the resultant of n homogeneous polynomials $F_0(X_0, \ldots, X_{n-1}, 0), \ldots, F_{n-1}(X_0, \ldots, X_{n-1}, 0)$ in n variables $X_0, \ldots, X_{n-1}$. Then*

$$R = \pm R_1^{d_n} \prod_{\xi} F_n(\xi), \tag{36}$$

where $\xi = (\xi_0, \ldots, \xi_{n-1}, 1)$ and $(\xi_0 : \ldots : \xi_{n-1} : 1)$ runs over all the roots of the system $F_0 = \ldots = F_{n-1} = 0$ in $\mathbb{P}^n(\overline{\mathcal{K}})$, herewith $\mathcal{K}$ is the field of fractions of $\mathcal{R}$.

PROOF Denote by $F^{(i)}$ the family of coefficients of F_i. Note that the resultant R considered as a polynomial in $F^{(n)}$ is equal to $\prod_\xi F_n(\xi)$ up to a factor from the field generated over $\mathbb{Q}$ by $F^{(0)}, \ldots, F^{(n-1)}$. Therefore,

$$\deg_{F^{(n)}} \prod_{\xi} F_n(\xi) = d_0 \cdot \ldots \cdot d_{n-1}.$$

Hence, for $i = n$ (and therefore, by symmetry for every $0 \leq i \leq n$) the polynomial R is homogeneous in $F^{(i)}$ of degree

$$\deg_{F^{(i)}} R = \Big(\prod_{0 \leq j \leq n} d_j \Big) / d_i. \tag{37}$$

Further, denote by $R^{(n-1)}(Z_{n-1}, Z_n)$ the resultant of n homogeneous in $X_0, \ldots, X_{n-1}$ polynomials

$$F_i(X_0, \ldots, X_{n-2}, Z_n X_{n-1}, Z_{n-1} X_{n-1}), \quad 0 \le i \le n-1.$$

So $R^{(n-1)}(Z_{n-1}, Z_n)$ is a homogeneous polynomial with respect to every family $F^{(0)}, \ldots, F^{(n-1)}$. By the definition of the resultant $R^{(n-1)}(1, \xi_{n-1}) = 0$ for every ξ. Therefore all elementry symmetric functions of roots ξ_{n-1} of $R^{(n-1)}(1, Z_n)$ which are rational functions in $F^{(0)}, \ldots, F^{(n-1)}$ have degree 0 with respect to every $F^{(i)}$, $0 \le i \le n-1$, (the degree of a rational function is the difference of degrees of its numerator and denominator). The same is true by symmetry for elementry symmetric functions of ξ_i for all $0 \le i \le n-1$. Hence (we leave the details to the reader)

$$\deg_{F^{(i)}} \prod_{\xi} F_n(\xi) = 0, \quad 0 \le i \le n-1. \tag{38}$$

We suppose that (39), see below, is proved by induction for polynomials in n variables. Then (39), implies that $R^{(n-1)}$ is a homogeneous polynomial in Z_{n-1}, Z_n. Hence R_1 is leading coefficient in Z_n of $R^{(n-1)}(1, Z_n)$. Therefore $R_1 \xi_i$ is integral over the ring of polynomials generated over $\mathbb{Z}$ by $F^{(0)}, \ldots, F^{(n-1)}$ for $i = n-1$ and by symmetry for all $0 \le i \le n-1$. Recall that R_1 and R are irreducible elements of $\mathcal{R}$. Hence $R = \pm R_1^N \prod_\xi F_n(\xi)$ for an integer $N \ge 0$. Now from (37) applied to R and R_1, and by (38) we get that $N = d_n$. The lemma is proved.

REMARK 2 *Lemma 7 remains true if one replaces in its formulation the generic polynomial F_n by an arbitrary homogeneous polynomial $\widetilde{F}_n$ with* $\deg F_n = d_n$ *and the resultant R by* $\mathrm{Res}_{X_0,\ldots,X_n}(F_1, \ldots, F_{n-1}, \widetilde{F}_n)$. *The proof is without changes.*

DEFINITION 4 *Let $n = 0$ and $F_0 = aX_0^{d_0}$. Set the resultant* $\mathrm{Res}_{X_0}(F_0) = a$. *Let $n \ge 1$ and the resultant is defined recursively for n homogeneous polynomials in n variables $X_0, \ldots, X_{n-1}$. By definition, put the resultant*

$$\mathrm{Res}_{X_0,\ldots,X_n}(F_0, \ldots, F_n) = R_1^{d_n} \prod_{\xi} F_n(\xi),$$

where R_1 and the product over ξ are the same as in (36).

The resultant satisfies the following isobaric relation.

LEMMA 8 *Let $n \ge 0$. Denote $D = d_0 \cdot \ldots \cdot d_n$. Let $0 \ne \lambda \in \overline{K}$ be an arbitrary element. Denote by R_2 the resultant of homogeneous polynomials $F_0(X_0, \ldots, X_{n-1}, \lambda X_n), \ldots, F_n(X_0, \ldots, X_{n-1}, \lambda X_n)$. Then*

$$R_2 = \lambda^D R \tag{39}$$

PROOF We shall prove (39) using induction on n. The base $n = 0$ is easy. Let $n \ge 1$ and (39) holds for polynomials with the number of variables less than $n+1$. Let $(\xi_0 : \ldots : \xi_{n-1} : 1)$ be a root of the system $F_0 = \ldots = F_{n-1} = 0$. Then $(\lambda\xi_1 : \ldots : \lambda\xi_{n-1} : 1)$ is a root of the system

$$F_0(X_0, X_1, \ldots, X_{n-1}, \lambda X_n) = \ldots = F_{n-1}(X_0, X_1, \ldots, X_{n-1}, \lambda X_n) = 0.$$

Now (39) follows from (36) (note that equality (39) for n homogeneous polynomials is used in the proof of (36), and it is possible by the induction hypothesis). The lemma is proved.

Let $f_0, \dots, f_n$ be homogeneous polynomials in $X_0, \dots, X_n$. Let σ be a permutation of $0, \dots, n$. Then it follows from the definition of the resultant given at the beginning of the section that

$$\mathrm{Res}_{X_0,\dots,X_n}(f_{\sigma(0)}, \dots, f_{\sigma(n)}) = \pm \mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_n), \tag{40}$$

$$\mathrm{Res}_{X_{\sigma(0)},\dots,X_{\sigma(n)}}(f_0, \dots, f_n) = \pm \mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_n). \tag{41}$$

Let g_n be a homogeneous polynomial in $X_0, \dots, X_n$. Then (36) and Remark 2 imply

$$\begin{aligned} &\mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_{n-1}, f_n g_n) = \\ &\mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_{n-1}, f_n)\, \mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_{n-1}, g_n) \end{aligned} \tag{42}$$

Let $\deg f_n \geq \deg f_i$ for some $0 \leq i \leq n-1$. Let g_i be a homogeneous polynomial in $X_0, \dots, X_n$ of degree $\deg g_i = \deg f_n - \deg f_i$. Then (36) and Remark 2 imply

$$\mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_{n-1}, f_n + g_i f_i) = \mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_{n-1}, f_n) \tag{43}$$

Let $\deg f_n = 0$ and $D = \deg f_0 \cdot \ldots \cdot \deg f_{n-1}$. Then (36) and Remark 2 imply

$$\mathrm{Res}_{X_0,\dots,X_n}(f_0, \dots, f_n) = f_n^D. \tag{44}$$

8 Generic projections and their specializations

Let the ideal $\mathfrak{P}$ and the algebraic variety $\mathcal{Z}(\mathfrak{P})$ be as in previous sections. Consider the linear forms

$$U_i = \sum_{0 \leq j \leq n} u_{i,j} X_j, \quad i = 0, s, s+1, \dots, n,$$

introduced in Section 1. So $u_{i,j} \in K$, $i = 0, s, s+1, \dots, n$, $0 \leq j \leq n$ is a family of algebraically independent over k elements. Denote for brevity the family

$$\mathcal{U} = \{u_{i,j}\}_{i=0,s,s+1,\dots,n,\ 0 \leq j \leq n}.$$

We shall denote by $k[\mathcal{U}]$ (respectively $k(\mathcal{U})$) the ring (respectively the field) generated over k by the elements of $\mathcal{U}$ and shall use other similar notations.

There is a unique (up to a non–zero factor from k) irreducible polynomial

$$H_{\mathfrak{P}} \in k[\mathcal{U}, Z_0, Z_s, Z_{s+1}, \dots, Z_n]$$

homogeneous relative to $Z_0, Z_s, \dots, Z_n$ such that $H_{\mathfrak{P}}(\mathcal{U}, U_0, U_s, \dots, U_n)$ is vanishing on $\mathcal{Z}(\mathfrak{P})$ considered as a subvariety of $\mathbb{P}^n(\overline{K})$. It is known that $H_{\mathfrak{P}}$ considered as a polynomial in $Z_0, Z_s, \dots, Z_n$ is separable and has degree $\deg_{Z_0,Z_s,\dots,Z_n} H_{\mathfrak{P}} = \deg V$, cf. also the proof of Lemma 9 below.

DEFINITION 5 *The polynomial $H_{\mathfrak{P}}$ is called the form corresponding to the generic projection of V.*

LEMMA 9 *The degree* $\deg_{u_{i,0},u_{i,s},\ldots,u_{i,n}} H_{\mathfrak{P}} = \deg V$ *for every* $i = 0, s, s+1, \ldots, n$.

PROOF Denote for brevity $H = H_{\mathfrak{P}}$ and set

$$\mathcal{U}' = \{u_{i,j}\}_{i=0,s,s+1,\ldots,n-1,\, 0\le j\le n}.$$

Consider the system of homogeneous polynomials equations in $X_0, \ldots, X_n$ with coefficients from the field $k(\mathcal{U}')(Z_s, \ldots, Z_{n-1})$

$$f = 0,\ f \in \mathfrak{P},\ U_s - Z_s U_0 = \ldots = U_{n-1} - Z_{n-1}U_0 = 0. \tag{45}$$

For every solution ξ of (45) we have $U_0(\xi) \neq 0$ since all U_i are generic linear forms and $\dim \mathcal{Z}(\mathfrak{P}) = n - s$. Since all $U_i - Z_i U_0$ are generic linear forms there are $\deg \mathcal{Z}(\mathfrak{P})$ different solutions ξ (all of them of multiplicity one) of system (45). Denote for brevity $D = \deg \mathcal{Z}(\mathfrak{P})$. Further,

$$k(\mathcal{U}')(Z_s, \ldots, Z_{n-1}) = k(\mathcal{U}')((U_s/U_0)(\xi), \ldots, (U_{n-1}/U_0)(\xi)).$$

Therefore transcendency degree of the field generated by affine coordinates of the point ξ is $n-s$. Hence ξ is a generic point of $\mathcal{Z}(\mathfrak{P})$ considered as an algebraic variety defined over the field $k(\mathcal{U})$.

By definition, put

$$H_1 = \prod_{\xi} (Z_n - (U_n/U_0)(\xi)), \tag{46}$$

where ξ runs over all the roots in $\mathbb{P}^n(\overline{k(\mathcal{U}', Z_s, \ldots, Z_{n-1})})$ of system (45). Note that

$$(U_n/U_0)(\xi) = \sum_{0\le j\le n} (X_j/U_0)(\xi) u_{n,j} \tag{47}$$

where $(X_j/U_0)(\xi) \in \overline{k(\mathcal{U}', Z_s, \ldots, Z_{n-1})}$. Further, H_1 is a symmetric function of solutions ξ. Hence,

$$H_1 \in k(\mathcal{U}')(Z_s, \ldots, Z_{n-1})[Z_n, u_{n,0}, u_{n,s}, \ldots, u_{n,n}]$$

and $\deg_{Z_n} H_1 = \deg_{u_{n,0},u_{n,s},\ldots,u_{n,n}} H_1 = D$.

Therefore there is $0 \neq H_2 \in k[\mathcal{U}'][Z_s, \ldots, Z_{n-1}]$ such that all the elements $(X_j/U_0)(\xi)H_2$, $0 \le j \le n$, are integral over $k[\mathcal{U}'][Z_s, \ldots, Z_{n-1}]$. Hence the polynomial

$$H_3 = H_1 H_2^D \in k[\mathcal{U}][Z_s, \ldots, Z_n]. \tag{48}$$

By (46) we have $H_3(Z_s, \ldots, Z_{n-1}, (U_n/U_0)(\xi)) = 0$. Hence by (45) we get $H_3((U_s/U_0)(\xi), \ldots, (U_{n-1}/U_0)(\xi), (U_n/U_0)(\xi)) = 0$. But ξ is a generic point of $\mathcal{Z}(\mathfrak{P})$. Thus the rational function $H_3((U_s/U_0), \ldots, (U_n/U_0))$ is vanishing on a non–empty open in the Zariski topology subset of $\mathcal{Z}(\mathfrak{P})$. Hence the polynomial $H_{\mathfrak{P}}(\mathcal{U}, 1, Z_s, \ldots, Z_n)$ divides H_3. But $\deg_{Z_n} H_{\mathfrak{P}} = D = \deg_{Z_n} H_1 = \deg_{Z_n} H_3$. So H_1 divides $H_{\mathfrak{P}}(\mathcal{U}, 1, Z_s, \ldots, Z_n)$ in the ring

$$k(\mathcal{U}')(Z_s, \ldots, Z_{n-1})[Z_n, u_{n,0}, u_{n,s}, \ldots, u_{n,n}].$$

Hence $\deg_{u_{n,0},u_{n,s},\ldots,u_{n,n}} H_{\mathfrak{P}} = \deg_{u_{n,0},u_{n,s},\ldots,u_{n,n}} H_1 = D$. The assertion of the lemma for $i = n$ is proved. For $i = 0, s, s+1, \ldots, n-1$ it follows from the symmetry of all these indices. The lemma is proved.

Let $n \geq s \geq 1$. Let $g_1, \ldots, g_s \in k[X_0, \ldots, X_n]$ be homogeneous polynomials such that $\dim \mathcal{Z}(g_1, \ldots, g_s) = n - s$ in $\mathbb{P}^n(\overline{k})$. Denote $D = \deg g_1 \cdot \ldots \cdot \deg g_s$. Let $\mathfrak{P}_i$, $i \in I$ be the family of all homogeneous prime ideals such that

$$(g_1, \ldots, g_s) \subset \mathfrak{P}_i \subset k[X_0, \ldots, X_n]$$

and $\dim \mathcal{Z}(\mathfrak{P}_i) = n - s$ in $\mathbb{P}^n(\overline{k})$.

Let $L_i = \sum_{0 \leq j \leq n} l_{i,j} X_j$, $i = 0, s, s+1, \ldots, n$, be a family of linear forms in $X_0, \ldots, X_n$ with coefficients $l_{i,j}$ from a field extension of k. Denote for brevity the family of coefficients

$$\mathcal{L} = \{l_{i,j}\}_{i=0,s,s+1,\ldots,n,\, 0 \leq j \leq n}. \tag{49}$$

We shall denote by $k[\mathcal{L}]$ (respectively $k(\mathcal{L})$) the ring (respectively the field) generated over k by the elements of $\mathcal{L}$.

Let

$$\mathcal{Z}(g_1, \ldots, g_s) \cap \mathcal{Z}(L_s, \ldots, L_n) = \emptyset, \tag{50}$$

$$\mathcal{Z}(g_1, \ldots, g_s) \cap \mathcal{Z}(L_0, L_s, L_{s+1}, \ldots, L_{n-1}) = \emptyset \tag{51}$$

in $\mathbb{P}^n(\overline{k(\mathcal{L})})$. Consider the linear projection

$$\begin{array}{l} \pi_i : \mathcal{Z}(\mathfrak{P}_i) \to \mathbb{P}^{n-s+1}(\overline{k(\mathcal{L})}), \\ (X_0 : \ldots : X_n) \mapsto (L_0 : L_s : L_{s+1} : \ldots : L_n). \end{array} \tag{52}$$

Let us show that $\pi_i(\mathcal{Z}(\mathfrak{P}_i)) = \mathcal{Z}(H_i)$ where

$$H_i \in k(\mathcal{L})[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$$

is a unique up to a factor from $k(\mathcal{L})$ separable polynomial. Indeed, $k(\mathcal{L})$ is a separable extension of k. Therefore, we can represent $\mathcal{Z}(\mathfrak{P}_i) = \cup_{j \in J_i} W_j$, where W_j are pairwise different defined over $k(\mathcal{L})$ and irreducible over $k(\mathcal{L})$ components of $\mathcal{Z}(\mathfrak{P}_i)$. Condition (50) implies, see, e.g., [2], that there is a unique irreducible polynomial $H_j \in k(\mathcal{L})[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$, such that $\pi_i(W_j) = \mathcal{Z}(H_j)$ in $\mathbb{P}^n(\overline{k(\mathcal{L})})$. The extension $k(\mathcal{L})(W_j) \supset k(\mathcal{L})$ is separable. Let $p = \mathrm{char}(k) > 0$. Then W_j is irreducible over the field $k(\mathcal{L})^{1/p}$, and the fields $k(\mathcal{L})(W_j)$ and $k(\mathcal{L})^{1/p}$ are linearly disjoint in the field $k(\mathcal{L})^{1/p}(W_j)$ over $k(\mathcal{L})$. Hence if a polynomial $0 \neq H^{(1)} \in k(\mathcal{L})^{1/p}[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$ is such that $H^{(1)}(L_0, L_s, L_{s+1}, \ldots, L_n)$ is vanishing on W_j, then there is a polynomial $0 \neq H^{(2)} \in k(\mathcal{L})[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$ such that $H^{(2)}(L_0, L_s, L_{s+1}, \ldots, L_n)$ is vanishing on W_j, and $\deg H^{(2)} \leq \deg H^{(1)}$. Thus, all the polynomials H_j are separable in any characteristic. Let J_i' be a maximal subset of J_i such that all the algebraic varieties $\pi_i(W_j)$, $j \in J_i'$ are pairwise distinct. Then $H_i = \prod_{j \in J_i'} H_j$ and hence H_i is separable. The required assertion is proved.

DEFINITION 6 *The polynomial H_i is called the form corresponding to the projection of $\mathcal{Z}(\mathfrak{P}_i)$ defined by the linear forms $L_0, L_s, L_{s+1}, \ldots, L_n$.*

So $H_i(L_0, L_s, L_{s+1}, \ldots, L_n)$ is vanishing on $\mathcal{Z}(\mathfrak{P}_i)$ considered as a subvariety of $\mathbb{P}^n(\overline{k(\mathcal{L})})$. In the case when $\mathcal{L} = \mathcal{U}$ set $H_i = H_{\mathfrak{P}_i}$, where $H_{\mathfrak{P}_i}$ is the form corresponding to the generic projection of $\mathcal{Z}(\mathfrak{P}_i)$ for every $i \in I$.

REMARK 3 *Actually, in what follows we shall need only two cases when $k(\mathcal{L}) = k$ or $k(\mathcal{L})$ is a pure trancendental extension of k. In the both cases the polynomial H_i is irreducible over $k(\mathcal{L})$. So we shall assume in what follows for simplicity (though it is not principal and one can consider the general case) that the following condition holds.*

(A) The field $k(\mathcal{L}) = k$ or $k(\mathcal{L})$ is a pure trancendental extension of k.

Define the equivalence on the set I as follows. Two indices i_1 and i_2 are equivalent if and only if $H_{i_1} = \lambda H_{i_2}$ for some $0 \neq \lambda \in k(\mathcal{L})$. Define J to be the factor set of I by this equivalence. For every $i \in J$ choose $i_1 \in i$ and set $H_i = H_{i_1}$.

Consider the system of homogeneous polynomials equations in $X_0, \ldots, X_n$ with coefficients from the field $k(\mathcal{L})(Z_0, Z_s, \ldots, Z_n)$

$$g_1 = \ldots = g_s = Z_0 L_s - Z_s L_0 = \ldots = Z_0 L_n - Z_n L_0 = 0. \tag{53}$$

Set

$$\Delta_0 = \mathrm{Res}_{X_0,\ldots,X_n}(g_1, \ldots, g_s, Z_0 L_s - Z_s L_0, \ldots, Z_0 L_n - Z_n L_0). \tag{54}$$

So Δ_0 is a polynomial in $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$. Substituting 0 for Z_i, $s \leq i \leq n$ in (53) we get the system which does not have non–zero solutions by (50). Hence $\Delta_0 \neq 0$ and Z_i does not divide Δ_0 for every $s \leq i \leq n$. If $\mathcal{L} = \mathcal{U}$ then by (37) we have

$$\deg_{u_{i,0}, u_{i,s}, \ldots, u_{i,n}} \Delta_0 = \deg g_1 \cdot \ldots \cdot \deg g_s = D \tag{55}$$

for every $i = s, s+1, \ldots, n$. Represent

$$\Delta_0 = Z_0^{N_0} \Delta_{\mathcal{L}}, \tag{56}$$

where $\Delta_{\mathcal{L}} \in k[\mathcal{L}][Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$ and the integer N_0 is maximal possible.

LEMMA 10 *The following statements hold.*

(a) $N_0 = (n-s)D$.

(b) Let $\mathcal{L} = \mathcal{U}$. Then the degree $\deg_{u_{i,0}, u_{i,s}, \ldots, u_{i,n}} \Delta_{\mathcal{L}} = \deg g_1 \cdot \ldots \cdot \deg g_s = D$ for every $i = 0, s, s+1, \ldots, n$.

PROOF By (55) it is sufficient to prove the assertion (b) of the lemma for $i = 0$. Consider the system of homogeneous polynomials equations in $X_0, \ldots, X_n$ with coefficients from the field $k(\mathcal{L})(Z_0, Z_s, \ldots, Z_n)$

$$g_1 = \ldots = g_s = Z_n L_0 - Z_0 L_n = Z_n L_s - Z_s L_n = \ldots = Z_n L_{n-1} - Z_{n-1} L_n = 0. \tag{57}$$

Set

$$\Delta_n = \mathrm{Res}_{X_0,\ldots,X_n}(g_1, \ldots, g_s, \\ Z_n L_0 - Z_0 L_n, Z_n L_s - Z_s L_n, \ldots, Z_n L_{n-1} - Z_{n-1} L_n).$$

Substituting 0 for Z_i, $i = 0, s, s+1, \ldots, n-1$ in (57) we get the system which does not have non–zero solutions by (51). Hence $\Delta_n \neq 0$ and Z_i does not divide Δ_n for every $i = 0, s, s+1, \ldots, n-1$.

Note that

$$Z_0(Z_nL_i - Z_iL_n) = Z_n(Z_0L_i - Z_iL_0) + Z_i(Z_nL_0 - Z_0L_n)$$

for every $s \le i \le n-1$. Hence by (40), (43), (44) and (42) we get

$$Z_n^{(n-s)D}\Delta_0 = \pm Z_0^{(n-s)D}\Delta_n.$$

Hence $N_0 = (n-s)D$. Further, if $\mathcal{L} = \mathcal{U}$ then for every $i = 0, s, s+1, \ldots, n-1$ the equalities similar to (55)

$$\deg_{u_{i,0},u_{i,s},\ldots,u_{i,n}} \Delta_n = D$$

are satisfied. Therefore $\deg_{u_{0,0},u_{0,s},\ldots,u_{0,n}} \Delta_0 = D$. The lemma is proved.

LEMMA 11 *There is a family of positive integers e_i, $i \in J$ and there is a family of homogeneous polynomials $h_1, \ldots, h_s \in k[\mathcal{L}][X_0, \ldots, X_n]$ such that*

$$\sum_{i\in J} e_i \deg_{Z_0,Z_s,Z_{s+1},\ldots,Z_n} H_i = \deg g_1 \cdot \ldots \cdot \deg g_s, \tag{58}$$

$$\Delta_{\mathcal{L}} = \mu \prod_{i\in J} H_i^{e_i},$$

$$h_1g_1 + \ldots + h_sg_s = \Delta_{\mathcal{L}}(L_0, L_s, \ldots, L_n),$$

where $0 \ne \mu \in k(\mathcal{L})$ and if $\mathcal{L} = \mathcal{U}$ then $0 \ne \mu \in k$.

PROOF By (37) Δ_0 is a homogeneous polynomial in $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$ of degree $(n-s+1)D$. Hence by Lemma 10 (a) the polynomial $\Delta_{\mathcal{L}}$ is homogeneous in $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$ of degree

$$\deg_{Z_0,Z_s,Z_{s+1},\ldots,Z_n} \Delta_{\mathcal{L}} = D. \tag{59}$$

Suppose that $\Delta_{\mathcal{L}}(z_0^*, z_s^*, z_{s+1}^*, \ldots, z_n^*) = 0$ for some $z_0^*, z_s^*, z_{s+1}^*, \ldots, z_n^*$ from a field extension of $k(\mathcal{L})$ such that $z_0^* \ne 0$. This is equivalent to the condition that the system

$$g_1 = \ldots = g_s = z_0^*L_s - z_s^*L_0 = \ldots = z_0^*L_n - z_n^*L_0 = 0.$$

has a non–zero solution $\eta = (\eta_0 : \ldots : \eta_n) \in \mathcal{Z}(g_1, \ldots, g_s)$ in projective space over algebraic closure of the field $k(\mathcal{L})(z_0^*, z_s^*, z_{s+1}^*, \ldots, z_n^*)$. Hence there is $i \in J$ such that $H_i(L_0(\eta), L_s(\eta), L_{s+1}(\eta), \ldots, L_n(\eta)) = 0$. Since $z_0^* \ne 0$ and by (50) $L_0(\eta) \ne 0$. Therefore

$$H_i(z_0^*, z_s^*, z_{s+1}^*, \ldots, z_n^*) = 0. \tag{60}$$

Conversely, (60) and $z_0^* \ne 0$ imply that there is $(\eta_0 : \ldots : \eta_n) \in \mathcal{Z}(g_1, \ldots, g_s)$ such that

$$(L_0(\eta) : L_s(\eta) : L_{s+1}(\eta) : \ldots : L_n(\eta)) = (z_0^* : z_s^* : z_{s+1}^* : \ldots : z_n^*).$$

Thus $\Delta_{\mathcal{L}}(z_0^*, z_s^*, z_{s+1}^*, \ldots, z_n^*) = 0$.

Therefore, there is a family of positive integers e_i, $i \in J$ and there is $0 \ne \mu \in k(\mathcal{L})$ such that

$$\Delta_{\mathcal{L}} = \mu \prod_{i\in J} H_i^{e_i}. \tag{61}$$

Hence (58) holds. In the case when $\mathcal{L} = \mathcal{U}$ the element $\mu \in k[\mathcal{U}]$. By Lemma 9 the degree $\deg_{u_{i,0}, u_{i,s}, \ldots, u_{i,n}} H_i = \deg \mathcal{Z}(\mathfrak{P}_i)$, for every $i = 0, s, s+1, \ldots, n$. By Lemma 10 (b) $\deg_{u_{i,0}, u_{i,s}, \ldots, u_{i,n}} \Delta_{\mathcal{L}} = D$ for every $i = 0, s, s+1, \ldots, n$. Hence by (59) and since $\deg_{Z_0, Z_s, \ldots, Z_n} H_i = \deg \mathcal{Z}(\mathfrak{P}_i)$ we get $\deg_{u_{i,0}, u_{i,s}, \ldots, u_{i,n}} \mu = 0$ for every $i = 0, s, s+1, \ldots, n$. Thus $\mu \in k$ in this case.

Further, by (35) there is an integer $N > 0$ and there are homogeneous in the variables $X_0, \ldots, X_n$ polynomials

$$A_i, B_j \in k[\mathcal{L}][Z_0, Z_s, \ldots, Z_n, X_0, \ldots, X_n], \quad 1 \leq i \leq s, \ s \leq j \leq n,$$

such that

$$\Delta_{\mathcal{L}} Z_0^{(n-s)D} L_0^N = \sum_{1 \leq i \leq s} A_i g_i + \sum_{s \leq j \leq n} (Z_0 L_j - Z_j L_0) B_i \tag{62}$$

Since the left part of (62) is a homogeneous polynomial in $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$ we shall suppose without loss of generality that all A_i and B_j are homogeneous polynomials in $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$.

Substituting in (62) L_j for Z_j, $j = 0, s, s+1, \ldots, n$, we get that there are homogeneous in the variables $X_0, \ldots, X_n$ polynomials

$$C_i \in k[\mathcal{L}][L_0, L_s, \ldots, L_n, X_0 \ldots, X_n], \quad 1 \leq i \leq s$$

such that

$$\Delta_{\mathcal{L}}(L_0, L_s, \ldots, L_n) L_0^{(n-s)D+N} = \sum_{1 \leq i \leq s} C_i g_i.$$

Let us show that L_0 is not a zero–divisor in the ring $k[\mathcal{L}][X_0, \ldots, X_n]/(g_1, \ldots, g_s)$. Note that every non–zero element $\nu \in k[\mathcal{L}]$ is not a zero–divisor of $k[\mathcal{L}][X_0, \ldots, X_n]/(g_1, \ldots, g_s)$ since the last ring is a free $k[\mathcal{L}]$–module. So it is sufficient to prove that L_0 is not a zero–divisor in the ring $k(\mathcal{L})[X_0, \ldots, X_n]/(g_1, \ldots, g_s)$. Suppose contrary. The ideal

$$(g_1, \ldots, g_s) \subset k(\mathcal{L})[X_0, \ldots, X_n]$$

is unmixed. Hence $\mathcal{Z}(L_0)$ contains an irreducible component of $\mathcal{Z}(g_1, \ldots, g_s)$. But this contradicts to condition (51). The required assertion is proved. Therefore, there are homogeneous in $X_0, \ldots, X_n$ polynomials

$$h_i \in k[\mathcal{L}][X_0, \ldots, X_n], \quad 1 \leq i \leq s$$

such that

$$\Delta_{\mathcal{L}}(L_0, L_s, \ldots, L_n) = h_1 g_1 + \ldots + h_s g_s.$$

Now the assertion of the lemma follows from (59) and (61). The lemma is proved.

LEMMA 12 *Let $\mathfrak{P} \subset k[X_0, \ldots, X_n]$ be a homogeneous prime ideal such that $\dim \mathcal{Z}(\mathfrak{P}) = n - s$ in $\mathbb{P}^n(\overline{k})$ where $n \geq s \geq 1$. Let $L_i = \sum_{0 \leq j \leq n} l_{i,j} X_j$, $i = 0, s, s+1, \ldots, n$, be a family of linear forms in $X_0, \ldots, X_n$ with coefficients $l_{i,j}$ from a field extension of k. Let (49) hold. Let $\lambda_s, \ldots, \lambda_n \in \overline{k(\mathcal{L})}$. Let*

$$\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(L_s, \ldots, L_n) = \emptyset, \tag{63}$$

$$\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(L_0, L_s, L_{s+1}, \ldots, L_{n-1}) = \emptyset, \tag{64}$$

$$\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(L_s - \lambda_s L_0, \ldots, L_n - \lambda_n L_0) = \emptyset \tag{65}$$

in $\mathbb{P}^n(\overline{k(\mathcal{L})})$. *Then there are homogeneous polynomials* $g_1, \ldots, g_s \in k[X_0, \ldots, X_n]$ *such that* $\dim \mathcal{Z}(g_1, \ldots, g_s) = n - s$ *in* $\mathbb{P}^n(\overline{k})$, $\mathcal{Z}(\mathfrak{P}) \subset \mathcal{Z}(g_1, \ldots, g_s)$, *equalities (50), (51) and*

$$\mathcal{Z}(g_1, \ldots, g_s) \cap \mathcal{Z}(L_s - \lambda_s L_0, \ldots, L_n - \lambda_n L_0) = \emptyset \tag{66}$$

hold.

PROOF Suppose that $0 \leq r \leq s-1$ and we have already constructed polynomials $g_1, \ldots, g_r$ such that

$$\begin{array}{l} \dim \mathcal{Z}(g_1, \ldots, g_r, L_s, \ldots, L_n) = s - 1 - r, \\ \mathcal{Z}(g_1, \ldots, g_r, L_0, L_s, L_{s+1}, \ldots, L_{n-1}) = s - 1 - r, \\ \dim \mathcal{Z}(g_1, \ldots, g_r, L_s - \lambda_s L_0, \ldots, L_n - \lambda_n L_0) = s - 1 - r, \\ \mathcal{Z}(\mathfrak{P}) \subset \mathcal{Z}(g_1, \ldots, g_r) \end{array} \tag{67}$$

in $\mathbb{P}^n(\overline{k(\mathcal{L})})$ (here the case when $r = 0$ follows from (63), (64) and (65)). Represent

$$\begin{array}{l} \mathcal{Z}(g_1, \ldots, g_r, L_s, \ldots, L_n) = \cup_{i \in I_1} W_i, \\ \mathcal{Z}(g_1, \ldots, g_r, L_0, L_s, L_{s+1}, \ldots, L_{n-1}) = \cup_{i \in I_2} W_i, \\ \mathcal{Z}(g_1, \ldots, g_r, L_s - \lambda_s L_0, \ldots, L_n - \lambda_n L_0) = \cup_{i \in I_3} W_i, \end{array}$$

where all W_i, $i \in I_1 \cup I_2 \cup I_3$ are irreducible algebraic varieties defined over the field $\overline{k(\mathcal{L})}$ of dimension $s - 1 - r$. By (63), (64) and (65) $W_i \cap \mathcal{Z}(\mathfrak{P}) = \emptyset$ for every $i \in I_1 \cup I_2 \cup I_3$. Hence there is a point $w_i \in W_i \setminus \mathcal{Z}(\mathfrak{P})$ for every $i \in I_1 \cup I_2 \cup I_3$. There is a homogeneous polynomial $g \in \mathfrak{P}$ such that $g(w_i) \neq 0$ for every $i \in I_1 \cup I_2 \cup I_3$. Set $g_{r+1} = g$. Then (67) is satisfied if one replaces r by $r + 1$. Thus, recursively we shall construct the required polynomials $g_1, \ldots, g_s$. The lemma is proved.

Now let (63) holds. Let, see Remark 3, condition (A) hold. Replace in (52) π_i and $\mathfrak{P}_i$ by π and $\mathfrak{P}$ respectively. Condition (63) implies, see e.g. [2], that $\pi(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(H_0)$ where

$$H_0 \in k(\mathcal{L})[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$$

is a unique up to a factor from $k(\mathcal{L})$ irreducible polynomial. So H_0 is the form corresponding to the projection of $\mathcal{Z}(\mathfrak{P})$ defined by the linear forms L_0, L_s, $L_{s+1}, \ldots, L_n$. Hence $H_0(L_0, L_s, L_{s+1}, \ldots, L_n)$ is vanishing on $\mathcal{Z}(\mathfrak{P})$ considered as a subvariety of $\mathbb{P}^n(\overline{k(\mathcal{L})})$.

LEMMA 13 *Let (63) and (64) hold. Let condition (A) hold. Let* $H_{\mathfrak{P}} \in k[\mathcal{U}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$ *be the form corresponding to the generic projection of* $\mathcal{Z}(\mathfrak{P})$. *Let the homogeneous polynomial in* $Z_0, Z_s, Z_{s+1}, \ldots, Z_n$

$$H_{\mathfrak{P}}(\mathcal{L}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n) \in k(\mathcal{L})[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$$

be obtained from $H_{\mathfrak{P}}$ *by substituting* $l_{i,j}$ *for* $u_{i,j}$ *for all* $0 \leq j \leq n$, $i = 0, s, s+1, \ldots, n$. *Then there are an integer* $r > 0$ *and an element* $0 \neq \lambda \in k(\mathcal{L})$ *such that*

$$H_{\mathfrak{P}}(\mathcal{L}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n) = \lambda H_0^r.$$

PROOF Since H_0 is irreducible by Remark 3 it is sufficient to prove that

$$\mathcal{Z}(H_{\mathfrak{P}}(\mathcal{L}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n)) \setminus \mathcal{Z}(H_0) = \emptyset. \tag{68}$$

Suppose contrary. Then dimension of the set in the left part of (68) is at least $n - s$. Therefore there is a point

$$(\lambda_0 : \lambda_s : \ldots : \lambda_n) \in \mathcal{Z}(H_{\mathfrak{P}}(\mathcal{L}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n)) \setminus \pi(\mathcal{Z}(\mathfrak{P}))$$

in $\mathbb{P}^{n-s+1}(\overline{k(\mathcal{L})})$ such that $\lambda_0 \neq 0$ or $\lambda_n \neq 0$. Since indices 0 and n are symmetric in the statement of the lemma we can assume without loss of generality that $\lambda_0 \neq 0$. More than that, we shall suppose that $\lambda_0 = 1$. Hence (65) holds. Applying Lemma 12 construct the homogeneous polynomials $g_1, \ldots, g_s$. Let us apply Lemma 11 in two cases: to the family $\mathcal{L}$ and when $\mathcal{L} = \mathcal{U}$. In the case $\mathcal{L} = \mathcal{U}$ denote

$$\Delta_{\mathcal{U}} = \Delta(\mathcal{U}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n).$$

So by Lemma 11 we get

$$\Delta_{\mathcal{L}} = \mu \prod_{i \in J} H_i^{e_i},$$

$$\Delta(\mathcal{U}, Z_0, Z_s, \ldots, Z_n) = \mu' \prod_{i \in J'} H_{\mathfrak{P}_i}(\mathcal{U}, Z_0, Z_s, \ldots, Z_n)^{\varepsilon_i},$$

where μ', J', ε_i corresponding to $\mathcal{U}$ are similar to μ, J, e_i corresponding to $\mathcal{L}$. By the definition of resultant, (54), (56) and Lemma 10 (a) the polynomial $\Delta_{\mathcal{L}}(Z_0, Z_s, Z_{s+1}, \ldots, Z_n)$ is obtained by substituting $l_{i,j}$ for $u_{i,j}$ in $\Delta(\mathcal{U}, Z_0, Z_s, Z_{s+1}, \ldots, Z_n)$ for all $0 \leq j \leq n$, $i = 0, s, s+1, \ldots, n$. Hence,

$$\Delta(\mathcal{L}, Z_0, Z_s, \ldots, Z_n) = \Delta_{\mathcal{L}}.$$

By Lemma 11 $0 \neq \mu' \in k$. There exists i such that $H_{\mathfrak{P}} = H_{\mathfrak{P}_i}$. Therefore,

$$H_{\mathfrak{P}}(\mathcal{L}, Z_0, Z_s, \ldots, Z_n) = \nu \prod_{i \in J''} H_i^{\alpha_i}, \tag{69}$$

where $0 \neq \nu \in k(\mathcal{L})$, $J'' \subset J$, and integers $\alpha_i > 0$ for all $i \in J''$.

Let us show that

$$\Delta_{\mathcal{L}}(1, \lambda_s, \ldots, \lambda_n) \neq 0. \tag{70}$$

Substitute in system (53) 1 for Z_0 and λ_i for Z_i, $s \leq i \leq n$. The obtained system has no non–zero solutions by (66). Now (70) follows from the definition of resultant and (54), (56). The required assertion is proved.

Hence $H_i(1, \lambda_s, \ldots, \lambda_n) \neq 0$ for every $i \in J$. By (69) $H_{\mathfrak{P}}(\mathcal{L}, 1, \lambda_s, \ldots, \lambda_n) \neq 0$. This contradiction proves the lemma.

REMARK 4 *Note that it is not necessary to use in the proof of Lemma 13 that $0 \neq \mu' \in k$. It is sufficient to apply only the fact that $\mu' \in k[\mathcal{U}]$ since in the latter case automatically $\mu'(\mathcal{L}) \neq 0$ under conditions of Lemma 13. So it is not necessary to prove Lemma 9 for the proof of Lemma 13.*

LEMMA 14 *Let $\xi \in \mathbb{P}^n(\overline{k})$ and $\xi \notin \mathcal{Z}(\mathfrak{P})$. Then*

$$H_{\mathfrak{P}}(\mathcal{U}, U_0, U_s, \ldots, U_n)(\xi) \neq 0.$$

PROOF Let $Y_1, \ldots, Y_n \in \overline{k}[X_0, \ldots, X_n]$ be linearly independent linear forms such that $Y_i(\xi) = 0$ for every $0 \leq i \leq n$. Represent

$$U_j - (U_j/U_0)(\xi)U_0 = \sum_{1 \leq i \leq n} v_{j,i} Y_i, \quad s \leq j \leq n,$$

where all $v_{j,i} \in \overline{k}(\mathcal{U})$. Let us show that the family of coefficients $v_{j,i}$, $s \leq j \leq n$, $1 \leq i \leq n$, is algebraically independent over $\overline{k}$. Indeed, in the case when $\xi = (1 : 0 : \ldots : 0)$ it is easy, and the general case is reduced to this one by a linear automorphism of $\mathbb{P}^n(\overline{k})$.

Let $p : \mathbb{P}^n(\overline{k}) \setminus \{\xi\} \to \mathbb{P}^{n-1}(\overline{k})$ be the linear projection with the center ξ. We have

$$p(\mathcal{Z}(\mathfrak{P})) \cap \mathcal{Z}(\sum_{1 \leq i \leq n} v_{s,i} Y_i, \ldots, \sum_{1 \leq i \leq n} v_{n,i} Y_i) = \emptyset$$

since the family $v_{j,i}$, $s \leq j \leq n$, $1 \leq i \leq n$, is algebraically independent. Therefore,

$$\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(U_s - (U_s/U_0)(\xi)U_0, \ldots, U_n - (U_n/U_0)(\xi)U_0) = \emptyset.$$

Hence the point with coordinates $(U_0(\xi) : U_s(\xi) : \ldots : U_n(\xi))$ does not belong to the projection $\pi(\mathcal{Z}(\mathfrak{P}))$ where π is a projection defined by linear forms $U_0, U_s, \ldots, U_n$. The lemma is proved.

9 Elimination in general position and localization

LEMMA 15 *Let m and N be positive integers. Let k be an arbitrary field. Let $S \subset \overline{k}^m$ be a dense in the Zariski topology subset. Let polynomials $\Phi_1, \ldots, \Phi_N \in k[Z_1, \ldots, Z_m]$ (here $Z_1, \ldots, Z_m$ are independent variables). Let*

$$\Phi = (\Phi_1, \ldots, \Phi_N) : \overline{k}^m \longrightarrow \overline{k}^N$$

be the morphism defined by polynomials $\Phi_1, \ldots, \Phi_N$. Let V_1 (respectively V_2) be the vector subspace of $\overline{k}^N$ over $\overline{k}$ generated by $\Phi(\overline{k}^m)$ (respectively $\Phi(S)$). Then $V_1 = V_2$.

PROOF Let $\lambda_1, \ldots, \lambda_N \in \overline{k}$. By definition of the Zariski topology if the equalities $\sum_{1 \leq i \leq N} \lambda_i \Phi_i(x) = 0$ hold for all $x \in S$ then $\sum_{1 \leq i \leq N} \lambda_i \Phi_i(x) = 0$ for all $x \in \overline{k}^m$. Hence $V_1 = V_2$. The lemma is proved.

LEMMA 16 *Let $\mathfrak{P} \subset k[X_0, \ldots, X_n]$ be a homogeneous prime ideal such that $\dim \mathcal{Z}(\mathfrak{P}) = n - s$ in $\mathbb{P}^n(\overline{k})$ where $n \geq s \geq 1$. Let $f_1, \ldots, f_s \in k[X_0, \ldots, X_n]$ be homogeneous polynomials such that $\mathcal{Z}(\mathfrak{P})$ is an irreducible and defined over k component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_s)$ in $\mathbb{P}^n(\overline{k})$. Let*

$$L_i = \sum_{0 \leq j \leq n} l_{i,j} X_j, \quad i = 0, s, s+1, \ldots, n,$$

be a family of linear forms in $X_0, \ldots, X_n$ with coefficients $l_{i,j}$ from k. Let the family $\mathcal{L}$ be defined by (49). Let H_0 be the form corresponding to the projection

of $\mathcal{Z}(\mathfrak{P})$ defined by the linear forms $L_0, L_s, L_{s+1}, \ldots, L_n$. Let (63) and (64) hold. Then there are homogeneous polynomials $h_1, \ldots, h_s \in k[X_0, \ldots, X_n]$, a homogeneous polynomial $q \in k[X_0, \ldots, X_n] \setminus \mathfrak{P}$, and an integer $r > 0$ such that

$$r \deg_{Z_0, Z_s, Z_{s+1}, \ldots, Z_n} H_0 \le \deg f_1 \cdot \ldots \cdot \deg f_s, \tag{71}$$

$$h_1 f_1 + \ldots + h_s f_s = q H_0(L_0, L_s, L_{s+1}, \ldots, L_n)^r \tag{72}$$

PROOF Let X_{n+i}, $1 \le i \le s$ be new variables. Set $g_i = f_i - X_{n+i}^{\deg f_i}$. For every $0 \le i \le s$ define the algebraic variety

$$V_i = \mathcal{Z}(g_1, \ldots, g_i, f_{i+1}, \ldots, f_s) \subset \mathbb{P}^{n+i}(\overline{k}),$$

where $\mathbb{P}^{n+i}(\overline{k})$ has the coordinates $X_0, \ldots, X_{n+i}$. Denote by V_i' the union of all defined over k and irreducible over k components W of V_i such that $W \supset \mathcal{Z}(\mathfrak{P})$, herewith the last inclusion is induced by the inclusion of projective spaces $\mathbb{P}^{n+i} \supset \mathcal{Z}(X_{n+1}, \ldots, X_{n+i}) = \mathbb{P}^n$.

Let W be an arbitrary defined over k irreducible component of V_i', $0 \le i \le s$. We claim that $\dim W = n - s + i$. Indeed, otherwise,

$$\dim W \cap \mathcal{Z}(X_{n+1}, \ldots, X_{n+i}) > n - s \tag{73}$$

which contradicts to the inclusions

$$\mathcal{Z}(f_1, \ldots, f_s) \supset W \cap \mathcal{Z}(X_{n+1}, \ldots, X_{n+i}) \supset \mathcal{Z}(\mathfrak{P})$$

and the condition that $\mathcal{Z}(\mathfrak{P})$ is an irreducible component of $\mathcal{Z}(f_1, \ldots, f_s)$. The required assertion is proved.

Represent for every $0 \le i \le s$

$$V_i = \cup_{w \in J_i} W_w,$$

where all W_w are defined over k and irreducible over k algebraic varieties, J_i is a finite set. Set

$$J_i' = \{w \in J_i : W_w \subset V_i'\}, \quad J_i'' = J_i \setminus J_i'.$$

For every $w \in J_i$ by $\mathfrak{P}_w$ denote the homogeneous prime ideal in $k[X_0, \ldots, X_{n+i}]$ such that $\mathcal{Z}(\mathfrak{P}_w) = W_w$.

Now we shall suppose that transcendency degree of the field K introduced in Section 1 is at least $4(n+1)^2$. Let $u_{i,j} \in K$, $0 \le i, j \le 2n+1$ be a family which has elements from the basis of transcendence of the field K over k. Therefore this family has transcendency degree $4(n+1)^2$ over k. For every $0 \le i \le s$ define the family of linear forms

$$U_j^{(i)} = \sum_{0 \le v \le n+i} u_{j,v} X_v, \quad j = 0, s, s+1, \ldots, n+i.$$

For every $0 \le i \le s$ set the family of coefficients

$$\mathcal{U}^{(i)} = \{u_{j,v}\}_{j=0,s,s+1,\ldots,n+i,\ 0 \le v \le n+i}.$$

For every $0 \le i \le s$ for every $w \in J_i'$ denote by

$$H_w \in k[\mathcal{U}^{(i)}, Z_0, Z_s, \ldots, Z_{n+i}]$$

the form corresponding to generic projection of W_w.

Let us show that for every $0 \leq i \leq s$ there are integers $e_w > 0$, $w \in J_i'$, a family of polynomials

$$h_{i,1}, \ldots, h_{i,s} \in k[\mathcal{U}^{(i)}, X_0, \ldots, X_{n+i}]$$

homogeneous in $X_0, \ldots, X_{n+i}$, and a polynomial

$$q_i \in k[\mathcal{U}^{(i)}, X_0, \ldots, X_{n+i}]$$

homogeneous in $X_0, \ldots, X_{n+i}$ such that

$$\sum_{w \in J_i'} e_w \deg_{Z_0, Z_s, Z_{s+1}, \ldots, Z_n} H_w \leq \deg f_1 \cdot \ldots \cdot \deg f_s, \tag{74}$$

$$h_{i,1} g_1 + \ldots + h_{i,i} g_i + h_{i,i+1} f_{i+1} + \ldots + h_{i,s} f_s =$$
$$q_i \prod_{w \in J_i'} H_w(\mathcal{U}^{(i)}, U_0^{(i)}, U_s^{(i)}, U_{s+1}^{(i)}, \ldots, U_{n+i}^{(i)})^{e_w} \tag{75}$$

and q_i is not vanishing on $\mathcal{Z}(\mathfrak{P})$. We shall prove this assertion using decreasing induction on i.

Let $i = s$. Note that $\dim \mathcal{Z}(g_1, \ldots, g_s) = n$ since $\mathcal{Z}(g_1, \ldots, g_s, X_0, \ldots, X_n) = \emptyset$ in $\mathbb{P}^{n+s}(\overline{k})$. Replace in the formulation of Lemma 11 n by $n+s$. Applying this lemma to the family of linear forms $L_j = U_j^{(s)}$, $j = 0, s, s+1 \ldots n+s$ we get that there are integers $e_w > 0$, $w \in J_s$, a family of polynomials

$$h_{s,1}, \ldots, h_{s,s} \in k[\mathcal{U}^{(s)}, X_0, \ldots, X_{n+s}]$$

homogeneous in $X_0, \ldots, X_{n+s}$, and an element $0 \neq \mu_s \in k$ such that

$$\sum_{w \in J_s'} e_w \deg_{Z_0, Z_s, Z_{s+1}, \ldots, Z_n} H_w \leq \deg f_1 \cdot \ldots \cdot \deg f_s,$$
$$h_{s,1} g_1 + \ldots + h_{s,s} g_s = \mu_s \prod_{w \in J_s} H_w(\mathcal{U}^{(s)}, U_0^{(s)}, U_s^{(s)}, U_{s+1}^{(s)}, \ldots, U_{n+s}^{(s)})^{e_w}.$$

By Lemma 14 applied to the point $\xi \in \mathcal{Z}(\mathfrak{P}) \setminus \mathcal{Z}(\mathfrak{P}_w)$ for every $w \in J_s''$ the polynomial

$$H_w(\mathcal{U}^{(s)}, U_0^{(s)}, U_s^{(s)}, U_{s+1}^{(s)}, \ldots, U_{n+s}^{(s)}) \in k[\mathcal{U}^{(s)}, X_{n+1}, \ldots, X_{n+s}]$$

is not vanishing on $\mathcal{Z}(\mathfrak{P})$. Set

$$q_s = \mu_s \prod_{w \in J_s''} H_w(\mathcal{U}^{(s)}, U_0^{(s)}, U_s^{(s)}, U_{s+1}^{(s)}, \ldots, U_{n+s}^{(s)})^{e_w}.$$

Therefore, now (74) and (75) hold for $i = s$.

Suppose that $-1 \leq i < s$. Suppose that (74) and (75) hold for $i+1$. In the case when $i > -1$ we shall deduce (74) and (75) for i. In the case $i = -1$ we shall prove the assertion of the lemma. If $i > -1$ set the linear forms $M_0 = U_0^{(i)}$, $M_s = X_{n+i+1}$, and

$$M_j = U_{j-1}^{(i)}, \quad s+1 \leq j \leq n+i+1.$$

In the case $i=-1$ set $M_0=L_0$ and $M_j=L_j$, $s\le j\le n$. By

$$\mathcal{M}=\{m_{j,v}\}_{j=0,s,s+1,\dots,n+i+1,\,0\le v\le n+i+1}$$

denote the family of coefficients of the linear forms M_j, $j=0,s,s+1,\dots,n+i+1$, herewith $m_{j,v}$ is the coefficient of M_j in X_v.

Let $i>-1$. Let us show that $\dim W_w\cap\mathcal{Z}(X_{n+i+1})<\dim W_w$ for every $w\in J'_{i+1}$. Suppose contrary. Then (73) holds with i replaced by $i+1$ and $W=W_w$. This leads to a contradiction as we have seen above. The required assertion is proved.

Let us show that for every $w\in J'_{i+1}$

$$\begin{aligned} W_w\cap\mathcal{Z}(M_s,\dots,M_{n+i+1})&=\emptyset,\\ W_w\cap\mathcal{Z}(M_0,M_{s+1},\dots,M_{n+i})&=\emptyset. \end{aligned}\tag{76}$$

Indeed, if $i>-1$ these equalities hold since all M_j with $j\ne s$ are linear forms with the transcendental coordinates, and the point with the coordinates $X_0=\ldots=X_{n+i}=0$, $X_{n+i+1}=1$ does not belong to V_{i+1}, cf. the proof of Lemma 14. In the case $i=-1$ these equalities coincide with (63) and (64).

Let

$$\begin{aligned} &\pi\,:\,V'_{i+1}\to\mathbb{P}^{n+i-s+2}(\overline{k(\mathcal{M})}),\\ &(X_0:\ldots:X_{n+i+1})\mapsto(M_0:M_s:M_{s+1}:\ldots:M_{n+i+1}) \end{aligned}$$

be the linear projection. By (76) the projection $\pi\,:\,V'_{i+1}\to\pi(V'_{i+1})$ is finite.

For every $w\in J'_{i+1}$ denote by $\widetilde{H}_w\in k(\mathcal{M})[Z_0,Z_s,\dots,Z_{n+i+1}]$ the form corresponding to the projection of W_w defined by the linear forms

$$M_0,M_s,M_{s+1},\dots,M_{n+i+1}.\tag{77}$$

If $i>-1$ we shall suppose without loss of generality that

$$\widetilde{H}_w\in k[\mathcal{U}^{(i)},Z_0,Z_s,\dots,Z_{n+i+1}]$$

is an irreducible polynomial in all variables $\mathcal{U}^{(i)}$, $Z_0,Z_s,\dots,Z_{n+i+1}$ for every $w\in J'_{i+1}$.

Let $i>-1$. For every $w\in J'_{i+1}$ represent $W_w\cap\mathcal{Z}(X_{n+i+1})=\cup_{\beta\in C_w}W_\beta$ where all W_β are defined over k and irreducible over k algebraic varieties and C_w is a finite set. Denote by H_β the form corresponding to generic projection of W_β.

We have $\pi(W_w\cap\mathcal{Z}(X_{n+i+1}))=\pi(W_w)\cap\mathcal{Z}(X_{n+i+1})$. Therefore, for every $w\in J'_{i+1}$

$$\widetilde{H}_w(\mathcal{U}^{(i)},M_0,0,M_{s+1},\dots,M_{n+i+1})=\nu_w\prod_{\beta\in C_w}H_\beta^{r_\beta},\tag{78}$$

where $0\ne\nu_w\in k[\mathcal{U}^{(i)}]$ and integers $r_\beta>0$ for all $\beta\in C_w$.

Let $i\ge-1$. Recall that equalities (76) hold. For every $w\in J'_{i+1}$ applying Lemma 13 (with n replaced by $n+i+1$) to the homogeneous prime ideal $\mathfrak{P}_w$ and linear forms (77) we get

$$H_w(\mathcal{M},Z_0,Z_s,\dots,Z_{n+i+1})=\lambda_w\widetilde{H}_w^{r_w},$$

where $0 \neq \lambda_w \in k(\mathcal{M})$ and integers $r_w > 0$. Therefore,

$$H_w(\mathcal{M}, M_0, M_s, M_{s+1}, \ldots, M_{n+i+1}) = \lambda_w \widetilde{H}_w(M_0, M_s, M_{s+1}, \ldots, M_{n+i+1})^{r_w} \tag{79}$$

(here we consider all $\widetilde{H}_w$ as elements of $k(\mathcal{M})[Z_0, Z_s, \ldots, Z_{n+i+1}]$). If $i > -1$ then $\lambda_w \in k[\mathcal{U}^{(i)}]$ since $\widetilde{H}_w$ is an irreducible polynomial.

Now consider the product in the right part of equality (75) for $i+1$ which is proved by the induction hypothesis. Represent

$$\prod_{w \in J'_{i+1}} H_w(\mathcal{U}^{(i+1)}, U_0^{(i+1)}, U_s^{(i+1)}, U_{s+1}^{(i+1)}, \ldots, U_{n+i+1}^{(i+1)})^{e_w} = \sum_{(i_0, \ldots, i_{n+i+1}) \in T} \Phi_{i_0, \ldots, i_{n+i+1}} X_0^{i_0} \cdot \ldots \cdot X_{n+i+1}^{i_{n+i+1}},$$

where $T \subset \mathbb{Z}^{n+i+2}$ is a finite set and all polynomials

$$\Phi_{i_0, \ldots, i_{n+i+1}} \in k[\mathcal{U}^{(i+1)}].$$

Let m be the number of variables of the ring of polynomials $k[\mathcal{U}^{(i+1)}]$ and $N = \#T$ be the number of elements of T. Let S be the subset of all $x \in k^m$ (here k^m has coordinates from the family $\mathcal{U}^{(i+1)}$) such that the polynomial $q_{i+1}(x, X_0, \ldots, X_{n+i+1})$ is not vanishing on $\mathcal{Z}(\mathfrak{P})$. Then S is dense in the Zariski topology in $\overline{k}^m$ since q_{i+1} is not vanishing on $\mathcal{Z}(\mathfrak{P})$ by the induction hypothesis and since k is infinite.

Apply Lemma 15 to the set S and the polynomial map

$$\Phi = (\Phi_{i_0, \ldots, i_{n+i+1}})_{(i_0, \ldots, i_{n+i+1}) \in T} : \overline{k}^m \to \overline{k}^N.$$

Let $u_1, \ldots, u_t \in S$ be elements such that $\Phi(u_1), \ldots, \Phi(u_t)$ is a basis of the vector space generated by $\Phi(\overline{k}^m)$. Then there are $y_\alpha \in k(\mathcal{M})$, $1 \leq \alpha \leq t$ such that

$$\prod_{w \in J'_{i+1}} H_w(\mathcal{M}, M_0, M_s, M_{s+1}, \ldots, M_{n+i+1})^{e_w} = \sum_{1 \leq \alpha \leq t} \frac{y_\alpha}{q_{i+1}(u_\alpha, X_0, \ldots, X_{n+i+1})} \times \Big(\sum_{1 \leq v \leq i+1} h_{i+1,v}(u_\alpha, X_0, \ldots, X_{n+i+1}) g_v + \sum_{i+2 \leq v \leq s} h_{i+1,v}(u_\alpha, X_0, \ldots, X_{n+i+1}) f_v \Big), \tag{80}$$

where $q_{i+1}(u_\alpha, X_0, \ldots, X_{n+i+1})$ is not vanishing on $\mathcal{Z}(\mathfrak{P})$ for every $1 \leq \alpha \leq t$.

Let $i > -1$. Represent $y_\alpha = z_\alpha / z$ where $z_\alpha, z \in k[\mathcal{U}^{(i)}]$, $1 \leq \alpha \leq t$. Substituting in (80) 0 for X_{n+i+1} (recall that X_{n+i+1} is vanishing on $\mathcal{Z}(\mathfrak{P})$) and combining it with (78), (79) we get

$$\prod_{w \in J'_{i+1}} (\lambda_w \nu_w) \prod_{w \in J'_{i+1}} \prod_{\beta \in C_w} H_\beta^{e_w r_w r_\beta} =$$

$$\sum_{1\le v\le i} g_v \sum_{1\le\alpha\le t} \frac{z_\alpha h_{i+1,v}(u_\alpha, X_0,\dots,X_{n+i},0)}{z q_{i+1}(u_\alpha, X_0,\dots,X_{n+i},0)} + \sum_{i+1\le v\le s} f_v \sum_{1\le\alpha\le t} \frac{z_\alpha h_{i+1,v}(u_\alpha, X_0,\dots,X_{n+i},0)}{z q_{i+1}(u_\alpha, X_0,\dots,X_{n+i},0)} \tag{81}$$

Now note that for every $w_1 \in J'_i$ there are $w \in J'_{i+1}$, $\beta \in C_w$ such that $W_{w_1} = W_\beta$. Hence the left part of (81) is divisible by $H_{w_1}(\mathcal{U}^{(i)}, U_0^{(i)}, U_s^{(i)}, U_{s+1}^{(i)},\dots,U_n^{(i)})$. For every $w \in J'_{i+1}$ denote by D_w the subset of indices $\beta \in C_w$ such that the polynomial H_β is not vanishing on $\mathcal{Z}(\mathfrak{P})$. By Lemma 14 for every $w \in J'_{i+1}$, $\beta \in C_w$ if $\mathcal{Z}(\mathfrak{P}) \not\subset W_\beta$ then H_β is not vanishing on $\mathcal{Z}(\mathfrak{P})$. Thus, in this case $\beta \in D_w$. Set

$$q_i = z \prod_{w\in J'_{i+1}} (\lambda_w \nu_w) \prod_{1\le\alpha\le t} q_{i+1}(u_\alpha, X_0,\dots,X_{n+i},0) \prod_{w\in J'_{i+1}} \prod_{\beta\in D_w} H_\beta^{e_w r_w r_\beta}.$$

Then q_i is not vanishing on $\mathcal{Z}(\mathfrak{P})$ and (81) implies that the required equality (75) holds. Finally, (74) follows from (81), (78), (79) and inequality (74) with i replaced by $i+1$ which is proved by the induction hypothesis.

It remains to prove the assertion of the lemma when $i = -1$. In this case it follows in the similar way directly from (80), (79) and inequality (74) with $i = 0$ which is proved by the induction hypothesis. The lemma is proved.

10 Construction of local parameters

Let the homogeneous prime ideal $\mathfrak{P}$ be the same as in previous sections, the algebraic variety $V = \mathcal{Z}(\mathfrak{P})$ in $\mathbb{P}^n(\overline{k})$ and $D = \deg V$. Let $s \ge 1$. Let $Y_0,\dots,Y_n \in k[X_0,\dots,X_n]$ be linearly independent linear forms satisfying the following conditions

$$V \cap \mathcal{Z}(Y_0, Y_{s+1},\dots,Y_n) = \emptyset, \tag{82}$$

$$V \cap \mathcal{Z}(Y_0, Y_i, Y_{s+1},\dots,Y_{n-1}) = \emptyset, \quad 1 \le i \le s. \tag{83}$$

Consider the projections

$$\pi : V \to \mathbb{P}^{n-s}(\overline{k}),$$
$$(X_0 : \dots : X_n) \mapsto (Y_0 : Y_{s+1} : \dots : Y_n),$$

and

$$\pi_i : V \to \mathbb{P}^{n-s+1}(\overline{k}),$$
$$(X_0 : \dots : X_n) \mapsto (Y_0 : Y_i : Y_{s+1} : \dots : Y_n),\ 1 \le i \le s.$$

All the projections π and $\pi_i : V \to \pi_i(V)$, $1 \le i \le s$, are finite by (82). Let $H_i \in k[Z_0, Z_s, Z_{s+1},\dots,Z_n]$ be the form corresponding to the projection π_i of V for every $1 \le i \le s$.

LEMMA 17 *Let $x \in V$ be a smooth point in $\mathbb{P}^n(\overline{k})$. Then there is a family of linearly independent linear forms $Y_0,\dots,Y_n \in k[X_0,\dots,X_n]$ satisfying (82) and (83) and such that*

(i) $Y_0(x) \neq 0$,

(ii) $\pi^{-1}(\pi(x))$ *consists of* $\deg V$ *different points,*

(iii) the number of elements $\#(Y_i/Y_0)(\pi^{-1}(\pi(x))) = \#\pi^{-1}(\pi(x))$ *for every* $1 \leq i \leq s$.

Let $L \in k[X_0, \ldots, X_n]$ *be a linear form such that* $L(x) \neq 0$. *Set*

$$\varphi_i = H_i(Y_0, Y_i, Y_{s+1}, \ldots, Y_n)/L^{\deg H_i}, \quad 1 \leq i \leq s.$$

Then $\deg H_i = D$ *for every* $1 \leq i \leq s$ *and* $\varphi_1, \ldots, \varphi_s$ *is a system of local parameters of the algebraic variety* V *in the point* x *(this means by definition that* $\varphi_1, \ldots, \varphi_s$ *generate the ideal of* V *in the local ring* $\mathcal{O}_{x,\mathbb{P}^n(\overline{k})}$ *of the point* x *in* $\mathbb{P}^n(\overline{k})$*).*

PROOF The existence of the linear forms $Y_0, \ldots, Y_n$ satisfying all the requirements follows from the fact that generic linear forms in $X_0, \ldots, X_n$ satisfy these requirements.

By (iii) $\deg H_i = D = \deg V$. By (ii) the differential $d_x\pi$ in the point x of the projection π is an isomorphism. By the Zariski main theorem the point $\pi_i(x)$ is smooth on $\pi_i(V)$. The implicit function theorem implies now $\varphi_1, \ldots, \varphi_s$ is a system of local parameters of V in the point x. The lemma is proved.

Let characteristic of the field k be zero. Suppose that a $\mathfrak{P}$–sequence $f_1, \ldots, f_s$ is given. Now we are going to describe a construction of local parameters in a point of an algebraic variety V. Let $0 \leq r < s$ be an integer. Suppose that we have already constructed by recursion on r a smooth point $x \in V$ and homogeneous polynomials

$$g_1, \ldots, g_r, f_{r,r+1}, \ldots, f_{r,s} \in k[X_0, \ldots, X_n]$$

such that

(a) x is a smooth point of $\mathcal{Z}(g_1, \ldots, g_r)$,

(b) V is an irreducible component of $\mathcal{Z}(g_1, \ldots, g_r, f_{r,r+1}, \ldots, f_{r,s})$,

(c) x is a smooth point of $\mathcal{Z}(g_1, \ldots, g_r, f_{r,r+1}, \ldots, f_{r,s})$,

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

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

Let $L = X_i$ for some $0 \leq i \leq n$ and $L(x) \neq 0$. Effecting if necessary a permutation of coordinates we shall assume without loss of generality that $L = X_0$.

Denote $\psi_i = g_i/X_0^{\deg g_i}$, $1 \leq i \leq r$ and $\rho_j = f_{r,j}/X_0^{\deg f_{r,j}}$, $r+1 \leq j \leq s$. Consider the system of local parameters $\varphi_1, \ldots, \varphi_s$ from Lemma 17. By conditions (a)–(d) there exist indices $1 \leq i_{r+1} < \ldots < i_s \leq s$ such that

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

is a system of local parameters of V in the point x. We shall suppose without loss of generality that $i_j = j$ for all $r+1 \le j \le s$.

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

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

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

$$\det\left(\left(\partial\psi_i/\partial Z_j\right)(x)\right)_{1\le i,j\le r} \ne 0. \tag{84}$$

Consider the ring of formal power series

$$\overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]]. \tag{85}$$

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 (85) can be represented in the form

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

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 (85) 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

$$F \in \widetilde{\mathfrak{P}} \quad \text{if and only if} \quad \mathcal{Z}(F) \supset V \setminus \mathcal{Z}(X_0). \tag{86}$$

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 $+\infty$. Introduce the operators $\mathcal{D}_j$, $r+1 \le j \le s$, of differentiation on the ring (85) by the formulas

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

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

$$\deg \mathcal{D}_i(F) \le \deg F + \deg g_1 + \ldots + \deg g_r - r - 1. \tag{87}$$

If $F \in k[X_1/X_0, \ldots, X_n/X_0]$ then $\mathcal{D}_i(F) \in k[X_1/X_0, \ldots, X_n/X_0]$ for every $r+1 \le i \le s$.

By the definition of the operators $\mathcal{D}_i$, by (84) and since any linear combination of $\varphi_{r+1}, \ldots, \varphi_s$ is a local parameter in the point x the vectors

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

are linearly independent over $\overline{k}$. This implies that for every element F of the ring of formal power series (85) if $\mathrm{ord}(F) > 0$ then there is $r+1 \leq i \leq s$ such that

$$\mathrm{ord}(\mathcal{D}_i(F)) = \mathrm{ord}(F) - 1. \tag{88}$$

Define δ to be the least integer such that

$$\delta \geq \frac{\deg g_1 \cdot \ldots \cdot \deg g_r \deg f_{r+1} \cdot \ldots \cdot \deg f_s}{\deg V}.$$

LEMMA 18 *The inequality* $\mathrm{ord}\, \rho_{r+1} \leq \delta$ *holds.*

PROOF Suppose contrary. Denote by $\psi_{i,1}$, $1 \leq i \leq r$, $\varphi_{j,1}$, $r+1 \leq j \leq s$ the forms of the least degree (or which is the same the non–zero homogeneous in $Z_1, \ldots, Z_n$ components of the least degree) in the ring $\overline{k}[Z_1, \ldots, Z_n]$ of the polynomials ψ_i, $1 \leq i \leq r$, φ_j, $r+1 \leq j \leq s$ respectively.

By Lemma 16 and (82), (83) for every $r+1 \leq j \leq s$ there are polynomials $q, h_1, \ldots, h_s \in \overline{k}[Z_1, \ldots, Z_n]$ such that

$$h_1\psi_1 + \ldots + h_r\psi_r + h_{r+1}\rho_{r+1} + \ldots + h_s\rho_s = q\varphi_j^\delta$$

and the polynomial q is not vanishing on $V \setminus \mathcal{Z}(X_0)$. Replacing if necessary the point x by a point $x_1 \in V$ from a sufficiently small neighborhood in the Zariski topology of the point x (it is reduced to a linear automorphism $X_i \mapsto X_i + \lambda_i X_0$, $\lambda_i \in \overline{k}$, $1 \leq i \leq n$, of $\mathbb{P}^n(\overline{k})$) we can assume without loss of generality that $q(x) \neq 0$. So q is an invertible element of the ring of formal power series (85). Therefore there exist polynomials $\widetilde{h}_i \in \overline{k}[Z_1, \ldots, Z_n]$ which are approximations of the elements h_i/q from the ring (85) such that

$$\widetilde{h}_1\psi_1 + \ldots + \widetilde{h}_r\psi_r + \widetilde{h}_{r+1}\rho_{r+1} + \ldots + \widetilde{h}_s\rho_s = \Phi_j,$$

where $\Phi_j \in \overline{k}[Z_1, \ldots, Z_n]$ is a polynomial with the form of the least degree in the ring (85) φ_j^δ. Hence the form of the least degree of the polynomial Φ_j in the ring $\overline{k}[Z_1, \ldots, Z_n]$ is $\varphi_{j,1}^\delta$.

By our assumption and (86) applied to $F = \rho_{r+1}$ all homogeneous component of degree less than $\delta + 1$ of the product $\widetilde{h}_{r+1}\rho_{r+1}$ belong to the ideal

$$\widetilde{\mathfrak{P}}_r = (\psi_1, \ldots, \psi_r)$$

of the ring (85) generated by the elements $\psi_1, \ldots, \psi_r$. Therefore we can assume without loss of generality that $\widetilde{h}_{r+1} = 0$.

Hence the linear forms $\psi_{i,1}$, $1 \leq i \leq r$, $\varphi_{j,1}$, $r+1 \leq j \leq s$ belong to the radical of the ideal generated by the forms of the least degree of the elements from the ideal

$$(\psi_1, \ldots, \psi_r, \rho_{r+2}, \ldots, \rho_s) \subset \overline{k}[Z_1, \ldots, Z_n].$$

But this radical is by definition the ideal of the tangent cone of the algebraic variety $W = \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+2}, \ldots, \rho_s)$ in the point x. Denote this tangent

cone by $\mathrm{con}(x, W)$. It is known that $\dim \mathrm{con}(x, W) = \dim_x W$ where $\dim_x W$ is the maximum of dimensions of irreducible components of W containing the point x (the direct proof of this fact can be found in [4]).

Now we have $\dim_x W = n - s + 1$ by conditions (a)–(d). On the other hand, there are s linearly independent linear forms from the ideal of $\mathrm{con}(x, W)$. Hence $\dim \mathrm{con}(x, W) \leq n - s < \dim_x W$. This contradiction proves the lemma.

Set $a = \mathrm{ord}(\rho_{r+1})$. Then $0 < a < +\infty$ by Lemma 18 and (86). We have $\mathcal{D}_j(\widetilde{\mathfrak{P}}_r) \subset \widetilde{\mathfrak{P}}_r$ for all $r + 1 \leq j \leq s$. Hence by (88) we get that there are indices $r + 1 \leq i_1, \ldots, i_a \leq s$ such that

$$\mathcal{D}_{i_{a-1}} \ldots \mathcal{D}_{i_1}(\rho_{r+1}) \in \widetilde{\mathfrak{P}} \tag{89}$$

and

$$\mathcal{D}_{i_a} \ldots \mathcal{D}_{i_1}(\rho_{r+1}) \notin \widetilde{\mathfrak{P}}. \tag{90}$$

By (89) and (86) the polynomial $\mathcal{D}_{i_{a-1}} \ldots \mathcal{D}_{i_1}(\rho_{r+1})$ is vanishing on $V \setminus \mathcal{Z}(X_0)$. By (90) and (86) the polynomial $\mathcal{D}_{i_a} \ldots \mathcal{D}_{i_1}(\rho_{r+1})$ is not vanishing on $V \setminus \mathcal{Z}(X_0)$. By definition of the operator $\mathcal{D}_{i_a}$ and (90) there is a non–empty open in the Zariski topology subset $S \subset V$ such that every point $y \in S$ is a smooth point of V and the differentials in the point y

$$d_y\psi_1, \ldots, d_y\psi_r, d_y\mathcal{D}_{i_{a-1}} \ldots \mathcal{D}_{i_1}(\rho_{r+1})$$

are linearly independent over $\overline{k}$.

Set $d_{r+1} = \deg_{Z_1,\ldots,Z_n} \mathcal{D}_{i_{a-1}} \ldots \mathcal{D}_{i_1}(\rho_{r+1})$ and

$$g_{r+1} = \mathcal{D}_{i_{a-1}} \ldots \mathcal{D}_{i_1}(\rho_{r+1}) X_0^{d_{r+1}}. \tag{91}$$

Then $g_{r+1} \in k[X_0, \ldots, X_n]$ is a homogeneous polynomial. Further, for every $y \in S$ the point y is smooth on the algebraic variety $\mathcal{Z}(g_1, \ldots, g_{r+1})$ and $\dim_y \mathcal{Z}(g_1, \ldots, g_{r+1}) = n - r - 1$.

There are two weak $\mathfrak{P}$–sequences $\theta_{1,1}, \ldots, \theta_{1,s}$ and $\theta_{2,1}, \ldots, \theta_{2,s}$ such that

- the polynomials $\theta_{1,1}, \ldots, \theta_{1,r+1}$ coincides with $g_1, \ldots, g_{r+1}$ up to a permutation,
- the polynomials $\theta_{2,i} = \eta f_i$, $1 \leq i \leq s$, for a homogeneous polynomial η which is not vanishing on V,
- $\deg \theta_{1,i} \leq \deg \eta$ for all $1 \leq i \leq r + 1$,
- $\deg \theta_{1,i} > \deg \theta_{2,s}$ for all $r + 2 \leq i \leq s$.

Applying Lemma 1 to these $\mathfrak{P}$-sequences we get the third $\mathfrak{P}$-sequence $\theta_{3,1}, \ldots, \theta_{3,s}$. Set $f_{r+1,j} = \theta_{3,j}/\eta$, $r + 2 \leq j \leq s$. Replace in conditions (a)–(d) r by $r + 1$ and the point x by a point y. Then by Lemma 1 there is a point $y \in S$ such that (a)–(d) are satisfied for the constructed homogeneous polynomials $g_1, \ldots, g_{r+1}, f_{r+1,r+2}, \ldots, f_{r+1,s}$ in the point y. This finishes the description of the recursion step.

Thus, finally we shall construct a system of local parameters $\psi_1, \ldots, \psi_s$ of the algebraic variety V in some point $x \in V$.

LEMMA 19 *There is a constant* $0 \leq C \in \mathbb{R}$ *and there are* $e_j \in \mathbb{R}$, $1 \leq j \leq s$ *such that the inequalities*

$$\deg g_j \leq e_j \deg f_j, \quad 1 \leq j \leq s, \tag{92}$$

$$e_j \leq n^{2^{s^C}}, \quad 1 \leq j \leq s \tag{93}$$

hold

PROOF Suppose that inequalities (92) hold for all $1 \leq j \leq r$ where $0 \leq r < s$. Then by Lemma 18 and Theorem 4 we have

$$a \leq \delta \leq 1 + e_1 \cdot \ldots \cdot e_r \delta_1 \cdot \ldots \cdot \delta_s / \deg V \leq 1 + a_s e_1 \cdot \ldots \cdot e_r .$$

Hence by (87) and (91) we get

$$\deg g_{r+1} \leq \delta_{r+1} + a_s e_1 \cdot \ldots \cdot e_r (-1 - r + \sum_{1 \leq j \leq r} e_j \delta_j).$$

Set

$$e_{r+1} = 1 + a_s e_1 \cdot \ldots \cdot e_r \sum_{1 \leq j \leq r} e_j .$$

Then (92) holds for $j = r + 1$. Now the existence of the constant C such that inequalities (92) and (93) hold for all $1 \leq j \leq s$ follows from Theorem 4 (the cases when $n = 1$ or $s = 1$ are trivial). The lemma and Theorem 2 are proved.

References

[1] **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.

[2] **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].

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

[4] **Chistov A. L.:** *"Polynomial-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: Zapiski Nauchn. Semin. St.–Petersburg. Otdel. Mat. Inst. Steklov (POMI), v. 258.

[5] **Chistov A. L.:** *"Efficient Smooth Stratification of an Algebraic Variety in Zero Characteristic and its Applications"*, St.Petersburg Mathematical Society Preprint # 1999-11, http://www.pdmi.ras.ru/spbmo/preprint/1999/index.html#11

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

[7] **Hodge W. V. D., Pedoe D.** *"Methods of algebraic geometry"*, v. 1, Cambridge, 1947.

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

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

[10] **Nakai Y.** Mem. Coll. Sci. Univ. Kyoto A 26 (1950) # 2, p.185–187.

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