Efficient Construction of Local Parameters of Irreducible Components of an Algebraic Variety in Nonzero Characteristic

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

2005

Abstract

Consider an $(n-s)$-dimensional algebraic variety W defined over an infinite field k of nonzero characteristic p and irreducible over this field. Let W be a subvariety of the projective space of dimension n. We prove that the local ring of W has a sequence of local parameters represented by s non–homogeneous polynomials with the product of degrees less than the degree of the variety multiplied to a constant depending on n. This allows to prove the existence of effective smooth cover and smooth stratification of an algebraic variety in the case of ground field of nonzero characteristic. The paper extends the analogous results of the author obtained earlier from zero to nonzero characteristic of the ground field.

Introduction

Let k be an infinite field of characteristic p. Let $\mathbb{P}^n(\overline{k})$ be the n–dimensional projective space over algebraic closure $\overline{k}$ of the field k with the homogeneous coordinates $X_0, \ldots, X_n$. Let $W \subset \mathbb{P}^n(\overline{k})$ be an algebraic variety defined over k and irreducible over k. Suppose that the dimension $\dim W = n - s$ where $1 \le s \le n$ and the degree $\deg W = D$. Let the variety W be the set of all zeroes of the homogeneous prime ideal $\mathfrak{P} \subset k[X_0, \ldots, X_n]$. In [2] we prove that the local ring of W has a regular sequence (respectively if $p = 0$ a sequence of local parameters) represented by s non–homogeneous polynomials with the product of degrees bounded from above by D multiplied to a constant depending on n (this is proved in [2] only for the case of perfect ground field; but from here in the obvious way the same assertion follows in the general case, see below). Further, see [2], in the case when W 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 in [2].

The aim of the present paper is to extend the results of [2] related to the bounds on the degrees of local parameters of W to the case of nonzero characteristic. Namely for arbitrary p we prove that W has a sequence of local parameters represented by s non–homogeneous polynomials with the product of degrees bounded from above by D multiplied to a constant depending only on n, see Theorem 1. In the case when W is an irreducible component of an algebraic variety given by a system of homogeneous polynomial equations of degrees less than d, and W is defined over k and irreducible over k the degrees of all these local parameters are less than d multiplied to a constant depending only on n, see Theorem 2. These constants depending on n are estimated.

Denote by $k^{p^{-\infty}}$ the perfect closure of k. For every integer $\nu \ge 0$ denote by $k^{p^{-\nu}}$ the subfield of all the elements $z \in k^{p^{-\infty}}$ such that $z^{p^{\nu}} \in k$.

Notice here that in the general case one can represent an algebraic variety V given by a system of homogeneous polynomial equations with coefficients from k of degrees less than d only as a union of defined over $k^{p^{-\infty}}$ and irreducible over $k^{p^{-\infty}}$ components. By [1] actually

(*) for every $0 \le s \le n$ all the irreducible components of V of codimension s defined over $k^{p^{-\infty}}$ are defined also over $k^{p^{-\nu}}$ for an integer $\nu \ge 0$ such that $p^{\nu} \le d^{2s}$.

Hence if k is perfect the variety V is represented as a union of defined over k and irreducible over k components.

Now using Theorem 1 and Theorem 2 we get an analog of Theorem 2 [3]. Recall the last result from [3]. 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. In [3] 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 the 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 $C > 0$. A minor correction of assertion (vi) of Theorem 2 [3] see in [4] (it is related to the estimations of the lengths of the coefficients from the ground field of the polynomials giving the strata). By Remark 4 from [3] at present the result similar to Theorem 2 [3] is also true for the case of the perfect ground field of nonzero characteristic. In Theorem 3 below we consider even the case when k is not necessarily perfect.

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

Recall some definitions from [2].

DEFINITION 1 *Let W and $\mathfrak{P}$ be as above. 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 by $\mathcal{W} = \mathcal{W}(\mathfrak{P}, u)$ the set of all defined over k and irreducible over k components E of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_u)$ such that $E \supset W$. Suppose that for every integer $0 \le u < j$ the polynomial $f_{u+1} \in \mathfrak{P}$ is a polynomial g of the least degree such that for every irreducible component $E \in \mathcal{W}$ the algebraic variety*

$$E \not\subset \mathcal{Z}(g).$$

Then any such sequence $f_1, \ldots, f_j$ will be called $\mathfrak{P}$–sequence (of length j). By Proposition 1, see below, there exists a $\mathfrak{P}$-sequence $f_1, \ldots, f_s$.

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

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

Then, see [2] 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 $\delta_i(\mathfrak{P})$ is called the i–th degree corresponding to $\mathfrak{P}$–sequence.

Note that if $f_1, \ldots, f_j$ is a $\mathfrak{P}$–sequence then for every $0 \le u \le j$ every irreducible component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_u)$ containing W is of dimension $n - u$. In particular when $j = s$ the algebraic variety W 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 $n - s$.

The following result follows from Theorem 1 [2].

PROPOSITION 1 *Let k be an infinite field. Then there exists some $\mathfrak{P}$–sequence $f_1, \ldots, f_s$. Hence $\delta_i = \delta_i(\mathfrak{P}) = \deg f_i$ for every $1 \le i \le s$. Further, see [2] Theorem 1, for arbitrary p there is $C \in \mathbb{R}$ such that the inequality*

$$\delta_1 \cdot \ldots \cdot \delta_s \le n^{2^{s^C}} D \tag{1}$$

holds.

PROOF The case when k is perfect is exactly Theorem 1 [2]. In the general case we extend k till $k^{p^{-\infty}}$ and get a $\mathfrak{P}$–sequence $f_1, \ldots, f_s$ with coefficients from $k^{p^{-\infty}}$. Since W is defined over k and irreducible over k, one can represent $f_i = \sum_{1\le j\le N_i} \lambda_{i,j} g_{i,j}$, where all $\lambda_{i,j} \in k^{p^{-\infty}}$ and $g_{i,j} \in \mathfrak{P}$ are nonzero homogeneous polynomials (with coefficients from k), and $\deg g_{i,j} = \deg f_i$ for all i, j. Therefore, W is an irreducible component of the algebraic variety

$$\mathcal{Z}\Big(\sum_{1\le j\le N_1} \mu_{1,j} g_{1,j}, \ldots, \sum_{1\le j\le N_s} \mu_{s,j} g_{s,j} \Big)$$

for appropriate $\mu_{i,j} \in k$, $1 \le i \le s$, $1 \le j \le N_i$. This gives the required $\mathfrak{P}$-sequence with coefficients from k. The proposition is proved.

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 [2] 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.*

Now we are going to formulate the results of the present paper. Theorem 1 and Theorem 2, see below, generalize Theorem 2 and Theorem 3 from [2] to the case of nonzero characteristic.

THEOREM 1 *Let k be an infinite field of arbitrary characteristic p. Let $W = \mathcal{Z}(\mathfrak{P})$ and $\mathfrak{P}$ be as above. Then there are homogeneous polynomials $g_1, \ldots, g_s \in \mathfrak{P}$, a smooth point point $x \in W$, 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 W at the point x,*
- *$\deg g_i \le n^{2^{s^C}} \delta_i(\mathfrak{P})$, $1 \le i \le s$, for an absolute constant $0 < C \in \mathbb{R}$ (it does not depend on p).*

As a consequence of Theorem 1 and [2] Lemma 5 we get the following result.

THEOREM 2 *Let $\phi_1, \ldots, \phi_m \in k[X_0, \ldots, X_n]$, $m \ge 1$, be arbitrary homogeneous polynomials. Let the degrees $\deg \phi_i < d$ for all $1 \le i \le m$. Assume that there is a defined over k and irreducible over k component W 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 $\dim W = n - s$ where $1 \le s \le n$. Then there are homogeneous polynomials $g_1, \ldots, g_s \in \mathfrak{P}$, a smooth point point $x \in W$, 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 W at the point x,*
- *$\deg g_i \le n^{2^{s^C}} d$, $1 \le i \le s$, for an absolute constant $0 < C \in \mathbb{R}$ (it does not depend on p).*

Now we are going to formulate an analog of Theorem 2 [3]. But at first we need to recall some definitions from [3]. Let $f_1, \dots, f_m \in k[X_0, \dots, X_n]$, $m \ge 1$, be arbitrary homogeneous polynomials (one should not confuse the with the ones from the Definition 1, Definition 2 and Proposition 1). Let the degrees $\deg f_i < d$ for all $1 \le i \le m$. Put $V = \mathcal{Z}(f_1, \dots, f_m) \subset \mathbb{P}^n(\overline{k})$ to be the algebraic variety of all the common zeroes of the polynomials $f_1, \dots, f_m$ in the projective space $\mathbb{P}^n(\overline{k})$.

DEFINITION 3 *Smooth cover of the algebraic variety V is a finite family*

$$V_\alpha, \quad \alpha \in A, \tag{2}$$

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

In [3] we introduce a new method to represent algebraic varieties. Only the case of zero–characteristic is considered in [3]. Now we extend this representation for nonzero characteristic. In the statement of Theorem 3 below the ground field k is finitely generated over a primitive subfield (hence it is not necessarily perfect). Namely we represent $k = \mathbb{F}_p(t_1, \dots, t_l, \theta)$, $l \ge 0$, where $t_1, \dots, t_l$ are algebraically independent over the field of p elements $\mathbb{F}_p$, and θ is algebraic and separable over the field $\mathbb{F}_p(t_1, \dots, t_l)$ element. The minimal polynomial $F \in \mathbb{F}_p(t_1, \dots, t_l)[Z]$ of the element θ over $\mathbb{F}_p(t_1, \dots, t_l)$ is given. The leading coefficient $\mathrm{lc}_Z F$ of the polynomial F with respect to Z is 1. In the case when k is finite, i.e., $l = 0$, we shall require that k has sufficiently many elements. Namely, the number of elements $\#k$ is bounded from below by a polynomial in $2^{2^{n^C}} d^{n^2}$ for an appropriate $C > 0$ (where $\deg f_i < d$, see above). One can always extend the finite ground field till a field $k(t_1)$, or, in the other way, till a finite field k' with sufficient many elements, and after that apply Theorem 3.

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

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

where $a_0, a_{i_0, \dots, i_n, j} \in \mathbb{F}_p[t_1, \dots, t_l]$, $\mathrm{GCD}_{i_0, \dots, i_n, j}(a_0, a_{i_0, \dots, i_n, j}) = 1$. Let us define the length $l(a)$ of an element $a \in \mathbb{F}_p$ by the formula $l(a) = [\log p / \log 2] + 1$. Similarly the length of coefficients $l(f)$ of the polynomial f is defined to be $l(f) = [\log p / \log 2] + 1$ and the degree

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

where $1 \le \gamma \le l$. In the similar way we shall define degrees and lengths of coefficients from $\mathbb{F}_p$ of other polynomials, in particular $\deg_{t_\gamma} F$ and $l(F) = [\log p / \log 2] + 1$ are defined.
We shall suppose that we have the following bounds

$$\deg_{X_0, \dots, X_n}(f_i) < d, \ \deg_{t_\gamma}(f_i) < d_2,$$
$$\deg_Z(F) < d_1, \ \deg_{t_\gamma}(F) < d_1.$$

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

$$L(f_i) < (\binom{d+n}{n} d_1 + 1) d_2^l ([\log p / \log 2] + 1).$$

Similarly $L(F) < d_1^{l+1}([\log p/\log 2] + 1)$. Unless we state otherwise, in what follows we suppose l to be fix.

Actually, in [3] only minor modifications are required. The first of them is related to the estimation of the degrees of inseparability of the fields of definition of the strata. The second one is connected to the choice of coefficients of linear forms and other polynomials, see below. In place of integer coefficients we choose the coefficients from a small subring Λ of the field k. If the transcendency degree of k over the primitive subfield $\mathbb{F}_p$ of p element is nonzero, then we choose an element $\lambda^{(0)} \in k$ which is transcendental over $\mathbb{F}_p$ (say $\lambda^{(0)} = t_1$) and put $\Lambda = \mathbb{F}_p[\lambda^{(0)}] \subset k$. If the transcendency degree of k over $\mathbb{F}_p$ is zero, then set $\Lambda = k$ (recall that in this case we assume that k has sufficiently many elements, see above). The size $\mathrm{L}(a)$ of an arbitrary element $a \in \Lambda$ is defined, see above (e.g., if $\Lambda = \mathbb{F}_p[\lambda^{(0)}]$ then $\mathrm{L}(a) = (\deg_{\lambda^{(0)}}(a) + 1)([\log p/\log 2] + 1)$).

Let W be a quasiprojective algebraic variety in $\mathbb{P}^n(\overline{k})$ and W is defined over k. Then represent

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

where all $W^{(i)}$, $1 \le i \le a$ are projective algebraic varieties in $\mathbb{P}^n(\overline{k})$ defined over k. Each algebraic variety $W^{(i)}$, $1 \le i \le a$ is given as a union of some irreducible components of the algebraic variety $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)}) \subset \mathbb{P}^n(\overline{k})$, where homogeneous polynomials $f_1^{(i)}, \ldots, f_{m(i)}^{(i)} \in k[X_0, \ldots, X_n]$ are given. For every $1 \le s \le n$ denote by $V_s^{(i)}$ (respectively $W_s^{(i)}$) the union of all irreducible components of dimension $n-s$ of $\mathcal{Z}(f_1^{(i)}, \ldots, f_{m(i)}^{(i)})$ (respectively $W^{(i)}$). Therefore, $W_s^{(i)}$ is a union of some irreducible components of $V_s^{(i)}$. For every $1 \le s \le n$ the family of linear forms $L_{s,s+1}^{(i)}, \ldots, L_{s,n}^{(i)} \in k[X_0, \ldots, X_n]$ with coefficients from Λ is given such that the number of points

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

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

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

The set of points

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

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

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

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

where f is a family of polynomials

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

L is a family of linear forms

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

and Ξ is a family of finite sets of points

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

Denote also

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

Note that here W is defined over k. We shall use also this representation for other fields of definition.

Now we are able to formulate the analog of Theorem 2 [3].

THEOREM 3 *Let the ground field $k = \mathbb{F}_p(t_1, \dots, t_l, \eta)$ be given as above. Let homogeneous polynomials $f_1, \dots, f_m \in k[X_0, \dots, X_n]$ and the algebraic variety $V = \mathcal{Z}(f_1, \dots, f_m)$ be as above. There is a smooth cover (respectively a smooth stratification) V_α, $\alpha \in A$, of the algebraic variety V such that every quasiprojective algebraic variety V_α is defined over $k^{p^{-n(\alpha)}} = k_\alpha$ for an integer $n \ge 0$, irreducible over k_α, and represented in the accepted way (with the ground field k_α in place of k). Let $\dim V_\alpha = n - s$ where $1 \le s \le n$, and $s = s(\alpha)$ depends on α. Let (6) be the constructed representation of V_α. Denote $h_{\alpha,j} = f_j^{(1)}$, $1 \le j \le m(1)$, and $\Delta_\alpha = f_1^{(2)}$ if $a \ge 2$, see (7). Then the constructed representation of V_α satisfies the following properties.*

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

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

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

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

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

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

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

(vi) For all $\alpha\in A$, $1\le j\le s(\alpha)$ the polynomials

$$h_{\alpha,1},\dots,h_{\alpha,s(\alpha)}\in k^{p^{-\nu(\alpha)}}[X_0,\dots,X_n], \tag{11}$$

where $p^{\nu(\alpha)}\le n^{2^{s(\alpha)^C}}d^{2ns(\alpha)}$ for an absolute constant $0<C\in\mathbb{R}$. Further, the lengths of coefficients of polynomials $h_{\alpha,j}^{p^{\nu(\alpha)}}$ are bounded from above by a polynomial in $n^{2^{s(\alpha)^C}}d^{ns(\alpha)}$, d_1, d_2, M, M_1, m for an absolute constant $0<C\in\mathbb{R}$. Finally, in the case of smooth stratification $p^{n(\alpha)}\le 2^{2^{n^C}}d^{2n^2}$ for an absolute constant $0<C\in\mathbb{R}$; for all $i>2$, j the lengths of coefficients of all polynomials from the family $(f_j^{(i)})^{p^{n(\alpha)}}$, $1\le j\le m(i)$, $1\le i\le a$, see (7), are bounded from above by a polynomial in $2^{2^{n^C}}d^{n^2}$, d_1, d_2, M, M_1, m for an absolute constant $0<C\in\mathbb{R}$.

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

SKETCH OF THE PROOF This follows from Remark 4 [3]. Namely, applying Theorem 1 and Theorem 2 in place of Theorem 1 [3] (we do not need at present to construct regular sequences and sequences of local parameters as in assertions (i) and (ii) of the last theorem, and we use only the existence of them) the reader can repeat all the constructions from the proof of Theorem 2 [3] with small modifications and obtain all the assertions of Theorem 3.

Let us consider in more details assertion (vi). It is sufficient here to prove only two first statements related to the polynomials $h_{\alpha,1},\dots,h_{\alpha,s(\alpha)}$. Indeed, if they are proved for strata of all dimensions then the last assertion from (vi) follows immediately from (ii).

The statements related to the polynomials $h_{\alpha,1},\dots,h_{\alpha,s(\alpha)}$ are proved by the induction on $s(\alpha)$ using the construction from the proof of Theorem 2 [3]. Here one should use (*), see above. We leave the details to the reader. The theorem is proved.

1 Preliminary definitions and lemmas

In the present and the next sections our aim is to prove Theorem 1. We shall follow the construction from Section 10 [2] and extend it to the case of nonzero characteristic. Since the case of zero–characteristic is considered in [2], we shall assume in what follows without loss of generality that $p=\mathrm{char}(k)>0$. Besides that, cf. the proof of Proposition 1, we shall assume without loss of generality that the field k is perfect.

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

$$W \cap \mathcal{Z}(Y_0, Y_{s+1}, \ldots, Y_n) = \emptyset, \tag{12}$$

$$W \cap \mathcal{Z}(Y_0, Y_i, Y_{s+1}, \ldots, Y_{n-1}) = \emptyset, \quad 1 \leq i \leq s. \tag{13}$$

Consider the projections

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

and

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

All the projections π and $\pi_i : W \to \pi_i(W)$, $1 \leq i \leq s$, are finite by (12). Let $H_i \in k[Z_0, Z_s, Z_{s+1}, \ldots, Z_n]$ be the form corresponding to the projection π_i of W for every $1 \leq i \leq s$, see Definition 6 from Section 8 [2], i.e., it is a nonzero polynomial of the least degree such that $H_i(Y_0, Y_i, Y_{s+1}, \ldots, Y_n)$ vanishes on W. The following lemma is similar to Lemma 17 [2].

LEMMA 1 *Let $x \in W$ be a smooth point in $\mathbb{P}^n(\overline{k})$. Then there is a family of linearly independent linear forms $Y_0, \ldots, Y_n \in k[X_0, \ldots, X_n]$ satisfying (12) and (13) and such that*

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

(ii) $\pi^{-1}(\pi(x))$ *consists of* $\deg W$ *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 $\deg H_i = D$, the polynomial $H_i \in k(Z_0, Z_{s+1}, \ldots, Z_n)[Z_s]$ is separable for every $1 \leq i \leq s$ and $\varphi_1, \ldots, \varphi_s$ is a system of local parameters of the algebraic variety W at the point x (this means by definition that $\varphi_1, \ldots, \varphi_s$ generate the ideal of W 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) and by, e.g., the remarks before the Definition 6 Section 8 from [2] the degree $\deg_{Z_s} H_i = \deg H_i = D = \deg W$. Hence the polynomial $H_i \in k(Z_0, Z_{s+1}, \ldots, Z_n)[Z_s]$ is separable. By (ii) the differential $d_x\pi$ at the point x of the projection π is an isomorphism. The implicit function theorem implies now $\varphi_1, \ldots, \varphi_s$ is a system of local parameters of W at the point x. The lemma is proved.

Suppose that a $\mathfrak{P}$–sequence $f_1, \ldots, f_s$ is given. In this an the next sections we describe a construction of local parameters at a point of the algebraic variety W.

We shall construct the polynomials $g_1, \ldots, g_s$ from the statement of Theorem 1. Let $0 \le r < s$ be an integer. Suppose that we have already constructed by the recursion on r a smooth point $x \in W$ 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) W 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) $f_{r,j} = \sum_{1 \le v \le j} q_{r,j,v} f_v$ 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 $1 \le v \le j$.

(so in the case of the base of the recursion $r = 0$ a smooth point $x \in W$ is given and we set $f_{0,j} = f_j$ for every $1 \le j \le s$). 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 $0 \le i \le n$ and $L(x) \ne 0$. Performing if necessary a permutation of coordinates we shall assume without loss of generality that $L = X_0$.

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

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

is a system of local parameters of W at 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 $\mathbb{A}^n(\overline{k}) = \mathbb{P}^n(\overline{k}) \setminus \mathcal{Z}(X_0)$. *In what follows for all polynomials $w \in \overline{k}[Z_1, \ldots, Z_n]$ (respectively $w \in \overline{k}[X_0, \ldots, X_n]$) the degree* $\deg w$ *is the degree with respect to $Z_1, \ldots, Z_n$ (respectively $X_0, \ldots, X_n$).*

So $\varphi_i, \psi_j, \rho_w \in \overline{k}[Z_1, \ldots, Z_n]$ for all i, j, w. Let us 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 at the point x

$$\Delta = \det\left(\left(\partial\psi_i/\partial Z_j\right)(x)\right)_{1 \le i,j \le r} \ne 0. \tag{14}$$

Notice that $\Delta \in \overline{k}[Z_1, \ldots, Z_n]$, and the degree $\deg \Delta \le -r + \deg \psi_1 + \ldots + \deg \psi_r$.

Consider the ring of formal power series

$$\overline{k}[[\psi_1, \ldots, \psi_r, \varphi_{r+1}, \ldots, \varphi_s, Z_{s+1}, \ldots, Z_n]] = \Omega_0. \tag{15}$$

This ring coincides with the ring of formal power series in $Z_1, \dots, Z_n$ over $\overline{k}$. Therefore it contains the ring $k[X_1/X_0, \dots, X_n/X_0]$. Each element F of the ring (15) can be represented in the form

$$F = \sum_{i_1,\dots,i_n \geq 0} F_{i_1,\dots,i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}, \tag{16}$$

where all $F_{i_1,\dots,i_n} \in \overline{k}$. Put

$$\Omega = \overline{k}[[\psi_1, \dots, \psi_r, Z_{s+1}, \dots, Z_n]] \subset \Omega_0.$$

Hence Ω is a subring of Ω_0.

The differentiations $\partial/\partial\psi_i$, $1 \leq i \leq r$, and $\partial/\partial\varphi_i$, $r+1 \leq j \leq s$, are defined in the natural way on the ring Ω_0. The differentiations $\partial/\partial Z_i$, $1 \leq i \leq s$ are defined in the natural way on the ring $\overline{k}[[Z_1, \dots, Z_n]]$. We define the differentiations $\partial/\partial Z_i$, $1 \leq i \leq s$, on Ω_0 using the natural identification $\Omega_0 = \overline{k}[[Z_1, \dots, Z_n]]$.

Set

$$\widetilde{\mathfrak{P}} = (\psi_1, \dots, \psi_r, \varphi_{r+1}, \dots, \varphi_s) \subset \Omega_0,$$
$$\mathfrak{q} = \widetilde{\mathfrak{Q}} = (\psi_1^p, \dots, \psi_r^p, \varphi_{r+1}^p, \dots, \varphi_s^p) \subset \Omega_0,$$
$$\widetilde{\mathfrak{P}}_r = (\psi_1, \dots, \psi_r) \subset \Omega_0,$$

i.e., $\widetilde{\mathfrak{P}}$ (respectively $\widetilde{\mathfrak{Q}}$, $\widetilde{\mathfrak{P}}_r$) is the ideal of the ring Ω_0 generated by the elements $\psi_1, \dots, \psi_r$, $\varphi_{r+1}, \dots,$ φ_s (respectively $\psi_1^p, \dots, \psi_r^p, \varphi_{r+1}^p, \dots, \varphi_s^p$, respectively $\psi_1, \dots, \psi_r$).

Let $F \in k[X_1/X_0, \dots, X_n/X_0]$. Then

$$F \in \widetilde{\mathfrak{P}} \quad \text{if and only if} \quad \mathcal{Z}(F) \supset W \setminus \mathcal{Z}(X_0). \tag{17}$$

Let (16) holds. Let $i \geq 0$ be an integer. Put by definition

$$\mathcal{J}^{(i)} = \{(i_1, \dots, i_n) \in \mathbb{Z}^n \,:\, i_1 + \ldots + i_s = i\},$$
$$F^{(i)} = \sum_{(i_1,\dots,i_n) \in \mathcal{J}^{(i)}} F_{i_1,\dots,i_n} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n},$$
$$\overline{\mathcal{J}} = \{(i_1, \dots, i_n) \in \mathbb{Z}^n \,:\, i_1 = \ldots = i_r = 0 \,\&\, i_{r+1}, \dots, i_n \geq 0\},$$
$$\overline{\mathcal{J}}^{(i)} = \{(i_1, \dots, i_n) \in \overline{\mathcal{J}} \,:\, i_{r+1} + \ldots + i_s = i\},$$
$$\overline{F} = \sum_{(i_1,\dots,i_n) \in \overline{\mathcal{J}}} F_{i_1,\dots,i_n} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n},$$
$$\overline{F}^{(i)} = \sum_{(i_1,\dots,i_n) \in \overline{\mathcal{J}}^{(i)}} F_{i_1,\dots,i_n} \varphi_{r+1}^{i_{r+1}} \cdot \ldots \cdot \varphi_s^{i_s} Z_{s+1}^{i_{s+1}} \cdot \ldots \cdot Z_n^{i_n}.$$

Hence $\overline{F}$ is obtained by the substitution of 0 in place of $\psi_1, \dots, \psi_r$ in F, and $\overline{F} = \sum_{i \geq 0} \overline{F}^{(i)}$, $F = \sum_{i \geq 0} F^{(i)}$. Further, set

$$\mathrm{ord}_{1,n} F = \min\{i_1 + \ldots + i_n \,:\, F_{i_1,\dots,i_n} \neq 0\},$$
$$\mathrm{ord}_{1,s} F = \min\{i \,:\, F^{(i)} \neq 0\},$$
$$\mathrm{ord}_{1,s,\Omega} F = \min\{i \,:\, F^{(i)} \notin \Omega\},$$

$$
\begin{aligned}
&\mathrm{ord}_{1,s,\mathfrak{q}}F = \min\{i \,:\, F^{(i)} \notin \mathfrak{q}\},\\
&\mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F = \min\{i \,:\, F^{(i)} \notin \Omega+\mathfrak{q}\},\\
&\mathrm{ord}_{r+1,s}F = \min\{i \,:\, \overline{F}^{(i)} \neq 0\},\\
&\mathrm{ord}_{r+1,s,\mathfrak{q}}F = \min\{i \,:\, \overline{F}^{(i)} \notin \mathfrak{q}\}.
\end{aligned}
$$

Note here that $\Omega+\mathfrak{q} \subset \Omega_0$ is a linear subspace. Hence $\mathrm{ord}_{1,n}F$ (respectively $\mathrm{ord}_{1,s}F$, $\mathrm{ord}_{1,s,\Omega}F$, $\mathrm{ord}_{1,s,\mathfrak{q}}\,F$, $\mathrm{ord}_{1,s,\Omega+\mathfrak{q}}\,F$, $\mathrm{ord}_{r+1,s}\,F$, $\mathrm{ord}_{r+1,s,\mathfrak{q}}F$) is a non–negative integer or $+\infty$. Obviously

$$
\begin{aligned}
&\mathrm{ord}_{1,n}F \le \mathrm{ord}_{1,s}F \le \mathrm{ord}_{1,s,\Omega}F \le \mathrm{ord}_{r+1,s}F \le \mathrm{ord}_{r+1,s,\mathfrak{q}}F,\\
&\mathrm{ord}_{1,s}F \le \mathrm{ord}_{1,s,\mathfrak{q}}F \le \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F \le \mathrm{ord}_{r+1,s,\mathfrak{q}}F.
\end{aligned}
$$

Besides that,

$$
\mathrm{ord}_{r+1,s,\mathfrak{q}}F \neq +\infty \quad \text{implies} \quad \mathrm{ord}_{r+1,s,\mathfrak{q}}F \le (s-r)(p-1) \tag{18}
$$

$$
\mathrm{ord}_{1,s,\mathfrak{q}}F \neq +\infty \quad \text{implies} \quad \mathrm{ord}_{1,s,\mathfrak{q}}F \le s(p-1), \tag{19}
$$

$$
\mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F \neq +\infty \quad \text{implies} \quad \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F \le s(p-1), \tag{20}
$$

Let j be equal to $\mathrm{ord}_{1,s}F$ *(respectively* $\mathrm{ord}_{1,s,\mathfrak{q}}F$*,* $\mathrm{ord}_{1,s,\Omega}F$*,* $\mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F$*,* $\mathrm{ord}_{r+1,s}F$*,* $\mathrm{ord}_{r+1,s,\mathfrak{q}}F$*). If $j=+\infty$ then by definition $F^{(j)}=0$ (respectively $F^{(j)}_{\mathfrak{q}}=0$, $F^{(j)}_{\Omega}=0$, $F^{(j)}_{\Omega+\mathfrak{q}}=0$, $\overline{F}^{(j)}=0$, $\overline{F}^{(j)}_{\mathfrak{q}}=0$).* Further, put

$$
\begin{aligned}
&F^* = F^{(j_0)}, \quad \text{where} \quad j_0 = \mathrm{ord}_{1,s}F,\\
&F^*_{\mathfrak{q}} = F^{(j_1)}, \quad \text{where} \quad j_1 = \mathrm{ord}_{1,s,\mathfrak{q}}F,\\
&F^*_{\Omega} = F^{(j_2)}, \quad \text{where} \quad j_2 = \mathrm{ord}_{1,s,\Omega}F,\\
&F^*_{\Omega+\mathfrak{q}} = F^{(j_3)}, \quad \text{where} \quad j_3 = \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F,\\
&\overline{F}^* = \overline{F}^{(j_4)}, \quad \text{where} \quad j_4 = \mathrm{ord}_{r+1,s}F,\\
&\overline{F}^*_{\mathfrak{q}} = \overline{F}^{(j_5)}, \quad \text{where} \quad j_5 = \mathrm{ord}_{r+1,s,\mathfrak{q}}F.
\end{aligned}
$$

Let us define also the leading form of an element F, see (16), with respect to $\psi_1,\ldots,\psi_r$, $\varphi_{r+1},\ldots,\varphi_s$, $Z_{s+1},\ldots,Z_n$ by the formula

$$
\mathrm{lf}(F) = \sum_{i_1+\ldots+i_n=\mathrm{ord}_{1,n}F} F_{i_1,\ldots,i_n}\psi_1^{i_1}\cdot\ldots\cdot\psi_r^{i_r}\varphi_{r+1}^{i_{r+1}}\cdot\ldots\cdot\varphi_s^{i_s}Z_{s+1}^{i_{s+1}}\cdot\ldots\cdot Z_n^{i_n}.
$$

Set

$$
\mathcal{I} = \{(i_1,\ldots,i_n) \in \mathbb{Z}^n \,:\, 0 \le i_1,\ldots,i_n < p\}, \tag{21}
$$

and for every $I=(i_1,\ldots,i_n) \in \mathcal{I}$ set $Z^I = Z_1^{i_1}\cdots Z_n^{i_n}$. One can represent an arbitrary element $F \in \overline{k}[[Z_1,\ldots,Z_n]]$ in the form

$$
F = \sum_{I\in\mathcal{I}} F_I Z^I, \tag{22}
$$

where all $F_I = F_{(i_1,\ldots,i_n)} \in \overline{k}[[Z_1^p,\ldots,Z_n^p]]$ are uniquely defined. If $F \in k[Z_1,\ldots,Z_n]$ then $F_I \in k[Z_1^p,\ldots,Z_n^p]$ and $\deg_{Z_1,\ldots,Z_n} F_I \le \deg_{Z_1,\ldots,Z_n} F$ for all $I \in \mathcal{I}$.

Let us introduce the operators $\mathcal{D}_j$, $r+1 \le j \le s$, of differentiation on the ring (15) by the formulas

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

Obviously if $F \in \widetilde{\mathfrak{P}}$ and $\mathrm{ord}_{r+1,s}F > 1$ then $\mathcal{D}_i(F) \in \widetilde{\mathfrak{P}}$ for every $r+1 \le i \le s$. We have

$$\mathcal{D}_i(\mathfrak{q}) \subset \mathfrak{q}, \quad \mathcal{D}_i(\mathfrak{P}_r) \subset \mathfrak{P}_r, \quad \mathcal{D}_i(\Omega) = \{0\}, \quad r+1 \le i \le s. \tag{23}$$

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

$$\deg \mathcal{D}_i(F) \le \deg F + \deg g_1 + \ldots + \deg g_r - r - 1. \tag{24}$$

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 $r+1 \le i \le s$.

LEMMA 2 *Let $F \in \mathfrak{q}$. Then, see (22), also $F_I \in \mathfrak{q}$ for every $I \in \mathcal{I}$.*

PROOF Let us represent $F = \sum_{1 \le i \le r} a_i \psi_i^p + \sum_{r+1 \le j \le s} b_j \varphi_j^p$ where all a_i, b_j are from ring (15). By (22) we have $a_i = \sum_{I \in \mathcal{I}} a_{i,I} Z^I$, $b_j = \sum_{I \in \mathcal{I}} b_{j,I} Z^I$ where all $a_{i,I}, b_{j,I} \in \overline{k}[[Z_1^p, \ldots, Z_n^p]]$. Then obviously $F_I = \sum_{1 \le i \le r} a_{i,I} \psi_i^p + \sum_{r+1 \le j \le s} b_{j,I} \varphi_j^p$ for every $I \in \mathcal{I}$. Therefore, $F_I \in \mathfrak{q}$. The lemma is proved.

LEMMA 3 *Let $F \in \widetilde{\mathfrak{P}} \cap \overline{k}[Z_1, \ldots, Z_n]$, and $\nu = \mathrm{ord}_{1,s,\mathfrak{q}}F < \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F$. Put*

$$\mathcal{I}_\nu = \{(i_1, \ldots, i_r) \in \mathbb{Z}^r \,:\, 0 \le i_1, \ldots, i_r \le p-1 \,\&\, i_1 + \ldots + i_r = \nu\}.$$

Then there exist polynomials $\Delta_{i_1,\ldots,i_r} \in \overline{k}[Z_1, \ldots, Z_n]$ for all $(i_1, \ldots, i_r) \in \mathcal{I}_\nu$ and a polynomial $\widetilde{F} \in \overline{k}[Z_1, \ldots, Z_n]$ such that

$$\Delta^\nu F = \widetilde{F} + \sum_{(i_1,\ldots,i_r) \in \mathcal{I}_\nu} \Delta_{i_1,\ldots,i_r} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r}, \tag{25}$$

where for every $(i_1, \ldots, i_r) \in \mathcal{I}_\nu$ the degree with respect to $Z_1, \ldots, Z_n$

$$\deg(\Delta_{i_1,\ldots,i_r} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r}) \le \deg(F) + \nu(-r + \deg\psi_1 + \ldots + \deg\psi_r), \tag{26}$$

and

$$\mathrm{ord}_{1,s,\mathfrak{q}}\widetilde{F} > \mathrm{ord}_{1,s,\mathfrak{q}}F, \quad \mathrm{ord}_{r+1,s}\widetilde{F} = \mathrm{ord}_{r+1,s}F. \tag{27}$$

PROOF We have

$$F^*_{\mathfrak{q}} = \sum_{(i_1,\ldots,i_r) \in \mathcal{I}_\nu} \alpha_{i_1,\ldots,i_r} \psi_1^{i_1} \cdot \ldots \cdot \psi_r^{i_r} + Q,$$

where all $\alpha_{i_1,\ldots,i_r} \in \overline{k}[[Z_{s+1}, \ldots, Z_n]]$ and $Q \in \mathfrak{q}$. Let us show that for every $(i_1, \ldots, i_r) \in \mathcal{I}_\nu$ there exist a polynomial $\Delta_{i_1,\ldots,i_r} \in \overline{k}[Z_1, \ldots, Z_n]$ and an element $\widetilde{\alpha}_{i_1,\ldots,i_r} \in \overline{k}[[Z_{s+1}, \ldots, Z_n]]$ such that

$$\Delta^\nu \alpha_{i_1,\ldots,i_r} = \Delta_{i_1,\ldots,i_r} + \widetilde{\alpha}_{i_1,\ldots,i_r}, \tag{28}$$

$$\mathrm{ord}_{1,s}\widetilde{\alpha}_{i_1,\ldots,i_r} > 0, \tag{29}$$

and (26) holds. Obviously this will imply the assertion of the lemma.

We shall assume without loss of generality that $i_1 > 0$ and $\mathrm{ord}_{1,s}\alpha_{i_1,\ldots,i_r} = 0$. Now
$$\frac{\partial F}{\partial Z_j} = \sum_{1\le i\le r} \frac{\partial F}{\partial \psi_i}\frac{\partial \psi_i}{\partial Z_j} + Q_j, \quad 1 \le j \le r,$$
where $Q_j \in \overline{k}[[Z_1,\ldots,Z_n]]$ and $\mathrm{ord}_{1,s,\mathfrak{q}}Q_j \ge \mathrm{ord}_{1,s,\mathfrak{q}}F$. Hence by Cramer's rule
$$\Delta\frac{\partial F}{\partial \psi_1} = \sum_{1\le j\le r} \Delta_{1,j}\frac{\partial F}{\partial Z_j} + Q', \quad 1 \le i \le r, \tag{30}$$
where $\Delta_{1,j} \in \overline{k}[Z_1,\ldots,Z_n]$, $1 \le j \le r$; $Q' \in \overline{k}[[Z_1,\ldots,Z_n]]$; $\mathrm{ord}_{1,s,\mathfrak{q}}Q' \ge \mathrm{ord}_{1,s,\mathfrak{q}}F$, and
$$\deg\Big(\Delta_{1,j}\frac{\partial F}{\partial Z_j}\Big) \le -r + \deg(F) + \sum_{2\le i\le r}\deg\psi_i \tag{31}$$
for every $1 \le j \le r$. Set $H = \sum_{1\le j\le r}(\Delta_{1,j}\partial F/\partial Z_j)$. Now
$$\nu - 1 = \mathrm{ord}_{1,s,\mathfrak{q}}H < \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}H$$
by (30) and since $\mathrm{ord}_{1,s}\alpha_{i_1,\ldots,i_n} = 0$. Further,
$$H^*_{\mathfrak{q}} = \Delta(x)\sum_{(i_1,\ldots,i_r)\in\mathcal{I}_\nu,\, i_1>0} i_1\alpha_{i_1,\ldots,i_r}\psi_1^{i_1-1}\psi_2^{i_2}\cdot\ldots\cdot\psi_r^{i_r} + Q'', \tag{32}$$
where $Q'' \in \overline{k}[[Z_1,\ldots,Z_n]]$ and $\mathrm{ord}_{1,s,\mathfrak{q}}Q'' \ge \mathrm{ord}_{1,s,\mathfrak{q}}F$. If $\nu = 1$ then (32) and (31) imply (28) and (29). If $\nu > 1$ we shall use the induction on ν. Applying the inductive assumption for H we get
$$\Delta^{\nu-1}(\Delta i_1\alpha_{i_1,\ldots,i_r}) = \Delta'_{i_1-1,i_2,\ldots,i_r} + \alpha'_{i_1-1,i_2\ldots,i_r},$$
where $\mathrm{ord}_{1,s}\alpha'_{i_1-1,i_2\ldots,i_r} > 0$ and by (26) (with $\nu-1$ in place of ν)
$$\begin{aligned}&\deg(\Delta'_{i_1-1,i_2,\ldots,i_r}\psi_1^{i_1-1}\psi_2^{i_2}\cdot\ldots\cdot\psi_r^{i_r}) \le\\ &\deg(H) + (\nu-1)(-r+\deg\psi_1+\ldots+\deg\psi_r) \le\\ &\deg(F) - \deg\psi_1 + \nu(-r+\deg\psi_1+\ldots+\deg\psi_r).\end{aligned}$$
Put $\Delta_{i_1,\ldots i_r} = i_1^{-1}\Delta'_{i_1-1,i_2,\ldots,i_r}$. Then (28), (29) hold. The lemma is proved.

LEMMA 4 *Let* $0 \ne F \in \widetilde{\mathfrak{P}}$ *and*
$$0 < \nu = \mathrm{ord}_{1,s,\mathfrak{q}}F = \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F < \mathrm{ord}_{r+1,s,\mathfrak{q}}F.$$
Then there is an integer $1 \le j \le r$ *such that*
$$\mathrm{ord}_{1,s,\mathfrak{q}}\Big(\frac{\partial F}{\partial Z_j}\Big) = \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}\Big(\frac{\partial F}{\partial Z_j}\Big) = \nu - 1, \tag{33}$$
where $\partial/\partial Z_j$ *is the differentiation of the ring* $k[[Z_1,\ldots,Z_n]] = \Omega_0$.

PROOF There is $(i_1,\dots,i_n)\in\mathcal{I}$, see (21), such that $F_{i_1,\dots,i_n}\neq 0$, $i_1+\dots+i_s=\nu$, $i_1+\dots+i_r<\nu$, and the sum $i_1+\dots+i_r=\nu_1$ is maximal possible. Then $\nu_1>0$ since $\mathrm{ord}_{1,s,\Omega+\mathfrak{q}}F<\mathrm{ord}_{r+1,s,\mathfrak{q}}F$. For all integers $a\geq b\geq 0$ set

$$J_{a,b}=\{(i_1,\dots,i_n)\in\mathbb{Z}^n\,:\,i_1+\dots+i_s=a\,\&\,i_1+\dots+i_r=b\},$$
$$Q=\sum_{(i_1,\dots,i_n)\in J_{\nu,\nu_1}}F_{i_1,\dots,i_n}\psi_1^{i_1}\cdot\ldots\cdot\psi_r^{i_r}\varphi_{r+1}^{i_{r+1}}\cdot\ldots\cdot\varphi_s^{i_s}Z_{s+1}^{i_{s+1}}\cdot\ldots\cdot Z_n^{i_n}.$$

Let us represent

$$\frac{\partial Q}{\partial Z_j}=\sum_{(i_1,\dots,i_n)\in\mathbb{Z}^n}Q_{j,i_1,\dots,i_n}\psi_1^{i_1}\cdot\ldots\cdot\psi_r^{i_r}\varphi_{r+1}^{i_{r+1}}\cdot\ldots\cdot\varphi_s^{i_s}Z_{s+1}^{i_{s+1}}\cdot\ldots\cdot Z_n^{i_n},$$

where all the coefficients $Q_{j,i_1,\dots,i_n}\in\overline{k}$. We have $\mathrm{ord}_{1,s}(\partial F^{(i)}/\partial Z_j)\geq i-1$ for every $i\geq 1$ and $1\leq j\leq r$, and

$$\Big(\frac{\partial}{\partial Z_j}\Big)(\mathfrak{q})\subset\mathfrak{q}\tag{34}$$

for every $1\leq j\leq r$. Hence for every $(i_1,\dots,i_n)\in J_{\nu-1,\nu_1-1}$ the coefficient of $\partial F/\partial Z_j$ at $\psi_1^{i_1}\cdot\ldots\cdot\psi_r^{i_r}\varphi_{r+1}^{i_{r+1}}\cdot\ldots\cdot\varphi_s^{i_s}Z_{s+1}^{i_{s+1}}\cdot\ldots\cdot Z_n^{i_n}$ is $Q_{j,i_1,\dots,i_n}$. Therefore, it is sufficient to prove that $Q_{j,i_1,\dots,i_n}\neq 0$ for some $1\leq j\leq r$ and $(i_1,\dots,i_n)\in J_{\nu-1,\nu_1-1}$.

Recall that $\partial/\partial\psi_i$, $1\leq i\leq r$, is the natural differentiation of the ring Ω_0. There exists $1\leq i\leq r$ such that $\partial Q/\partial\psi_i\neq 0$. Put

$$\mu=\min\{\mathrm{ord}_{1,n}(\partial Q/\partial\psi_i)\,:\,1\leq i\leq r\},$$
$$I=\{i\,:\,\mathrm{ord}_{1,n}(\partial Q/\partial\psi_i)=\mu\,\&\,1\leq i\leq r\}.$$
$$I_j=\{i\,:\,(\partial\psi_i/\partial Z_j)(x)\neq 0\,\&\,1\leq i\leq r\},\quad 1\leq j\leq r.$$

We have

$$\sum_{(i_1,\dots,i_n)\in J_{\nu-1,\nu_1-1}}Q_{j,i_1,\dots,i_n}\psi_1^{i_1}\cdot\ldots\cdot\psi_r^{i_r}\varphi_{r+1}^{i_{r+1}}\cdot\ldots\cdot\varphi_s^{i_s}Z_{s+1}^{i_{s+1}}\cdot\ldots\cdot Z_n^{i_n}=$$
$$\sum_{i\in I_j}\frac{\partial Q}{\partial\psi_i}\Big(\frac{\partial\psi_i}{\partial Z_j}\Big)^*.\tag{35}$$

Further,

$$\mathrm{lf}\Big(\sum_{i\in I_j}\frac{\partial Q}{\partial\psi_i}\Big(\frac{\partial\psi_i}{\partial Z_j}\Big)^*\Big)=\sum_{i\in I}\mathrm{lf}\Big(\frac{\partial Q}{\partial\psi_i}\Big)\Big(\frac{\partial\psi_i}{\partial Z_j}\Big)(x).\tag{36}$$

By (14) there is $1\leq j\leq r$ such that the sum in the right part of (36) is nonzero. Then by (36) the sum in the right part of (35) is nonzero. The lemma is proved.

LEMMA 5 *Let $F\in\widetilde{\mathfrak{P}}$ and $\mathrm{ord}_{r+1,s,\mathfrak{q}}F<+\infty$. Then there is $r+1\leq i\leq s$ such that*

$$\mathrm{ord}_{r+1,s,\mathfrak{q}}(\mathcal{D}_i(F))=\mathrm{ord}_{r+1,s,\mathfrak{q}}(F)-1.\tag{37}$$

PROOF Recall that $\partial/\partial\varphi_j$, $r+1\leq j\leq s$, is the natural differentiation of ring (15). Put $\nu_0=\mathrm{ord}_{r+1,s,\mathfrak{q}}F$. Since $\nu_0<+\infty$ there is $(i_1,\dots,i_n)\in\mathcal{I}\cap\mathcal{J}^{(\nu_0)}$

such that the coefficient $F_{i_1,\ldots,i_n} \neq 0$, see (16). Therefore, there is $r+1 \leq j_0 \leq s$ such that $\partial \overline{F}^* / \partial \varphi_{j_0} \neq 0$.

By the definition of the operators $\mathcal{D}_i$, by (14) and since any linear combination of $\varphi_{r+1}, \ldots, \varphi_s$ (with at least one nonzero coefficient) is a local parameter at 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 $\overline{k}$.

Set $\nu_1 = \min\{\mathrm{ord}_{1,n}(\,\partial \overline{F}^*_{\mathfrak{q}} / \partial \varphi_j\,) \,:\, r+1 \leq j \leq s\}$ and

$$J = \{j \,:\, \mathrm{ord}_{1,n}(\,\partial \overline{F}^*_{\mathfrak{q}} / \partial \varphi_j\,) = \nu_1 \,\&\, r+1 \leq j \leq s\}.$$

Hence there exists $r+1 \leq i \leq s$ such that

$$\sum_{j \in J} \mathrm{lf}\Big(\frac{\partial \overline{F}^*_{\mathfrak{q}}}{\partial \varphi_j} \Big) \mathcal{D}_i(\varphi_j)(x) \neq 0.$$

Set

$$J' = \{j \,:\, \mathcal{D}_i(\varphi_j)(x) \neq 0 \,\&\, r+1 \leq j \leq s\}.$$

But in this case

$$\sum_{j \in J} \mathrm{lf}\Big(\frac{\partial \overline{F}^*_{\mathfrak{q}}}{\partial \varphi_j} \Big) \mathcal{D}_i(\varphi_j)(x) = \mathrm{lf}\Big(\sum_{j \in J'} \frac{\partial \overline{F}^*_{\mathfrak{q}}}{\partial \varphi_j} \, \overline{\mathcal{D}_i(\varphi_j)}^* \Big) \neq 0.$$

Therefore, also $\sum_{j \in J'} (\partial \overline{F}^*_{\mathfrak{q}} / \partial \varphi_j) \, \overline{\mathcal{D}_i(\varphi_j)}^* \neq 0$. This implies

$$\overline{(\mathcal{D}_i(F))_{\mathfrak{q}}}^* = \sum_{j \in J'} \frac{\partial \overline{F}^*_{\mathfrak{q}}}{\partial \varphi_j} \, \overline{\mathcal{D}_i(\varphi_j)}^*.$$

Hence (37) holds. The lemma is proved.

Let us define δ to be the least integer such that

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

The following lemma is similar to Lemma 18 Section 10 [2]. Still due to its importance we repeat the proof.

LEMMA 6 *The inequality* $\mathrm{ord}_{r+1,s} \rho_{r+1} \leq \delta$ *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 [2] (it is valid in arbitrary characteristic) and (12), (13) 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 $W \setminus \mathcal{Z}(X_0)$. Replacing if necessary the point x by a point $x_1 \in W$ from a sufficiently small neighborhood in the Zariski topology of the point x (it is reduced to a linear automorphism $X_i \mapsto X_i + \lambda_i X_0$, $\lambda_i \in \overline{k}$, $1 \le i \le n$, of $\mathbb{P}^n(\overline{k})$) we can assume without loss of generality that $q(x) \ne 0$. So q is an invertible element of the ring of formal power series (15). 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 ring (15) 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 (15) 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 (17) applied to $F = \rho_{r+1}$ all the homogeneous components of degree less than $\delta + 1$ of the product $\widetilde{h}_{r+1}\rho_{r+1}$ belong to the ideal $\mathfrak{P}_r$, see above. Therefore we can assume without loss of generality that $\widetilde{h}_{r+1} = 0$.

Hence the linear forms $\psi_{i,1}$, $1 \le i \le r$, $\varphi_{j,1}$, $r+1 \le j \le s$ 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 by definition this radical is the ideal of the tangent cone of the algebraic variety $W = \mathcal{Z}(\psi_1, \ldots, \psi_r, \rho_{r+2}, \ldots, \rho_s)$ at 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 [5]; although the case of zero–characteristic is considered in [5] the last proof is valid in arbitrary characteristic).

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 $\dim \mathrm{con}(x, W) \le n - s < \dim_x W$. This contradiction proves the lemma.

2 Description of the main recursion.

Set $\rho = \rho_{r+1}$. Now we are ready to describe a new recursion on ρ. At the end of this recursion using the obtained element ρ we shall construct g_{r+1} and homogeneous polynomials $f_{r+1,r+2}, \ldots, f_{r+1,s}$, see Section 1. The base of the recursion is $\rho = \rho_{r+1}$. The recursion starts from the first step. At the beginning of each step $\mathrm{ord}_{1,s}\rho > 1$ and $\mathrm{ord}_{r+1,s}(\rho) < +\infty$.

Let us describe the general step of the recursion. Obviously one and only one of the following four cases holds:

1) $\mathrm{ord}_{1,s,\mathfrak{q}}(\rho) = +\infty$,

2) $\mathrm{ord}_{1,s,\mathfrak{q}}(\rho) < \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}(\rho) \le \mathrm{ord}_{r+1,s,\mathfrak{q}}(\rho) = +\infty$,

3) $\mathrm{ord}_{1,s,\mathfrak{q}}(\rho) = \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}(\rho) < \mathrm{ord}_{r+1,s,\mathfrak{q}}(\rho) = +\infty$,

4) $\mathrm{ord}_{r+1,s,\mathfrak{q}}(\rho) < +\infty$.

If 1) (respectively 2), 3), 4)) holds at the beginning of the recursion step then we shall say for brevity that this step is of type 1) (respectively 2), 3), 4)).

Assume that 1) holds. Then $\rho \in \mathfrak{q}$. Let us represent $\rho = \sum_{I \in \mathcal{I}} \rho_I Z^I$, where all $\rho_I \in \overline{k}[Z_1^p, \ldots, Z_n^p]$. Then by Lemma 2 all $\rho_I \in \mathfrak{q}$. Hence $\rho_I^{1/p} \in \overline{k}[Z_1, \ldots, Z_n] \cap \widetilde{\mathfrak{P}}$ since $\widetilde{\mathfrak{P}}$ is a prime ideal. There is $I_0 \in \mathcal{I}$ such that $\mathrm{ord}_{r+1,s}\rho_{I_0} \leq \mathrm{ord}_{r+1,s}\rho$. Put $\rho' = \rho_{I_0}^{1/p}$. Now

$$0 < \mathrm{ord}_{r+1,s}(\rho') \leq \left(\frac{1}{p}\right)\mathrm{ord}_{r+1,s}\rho, \quad \deg \rho' \leq \left(\frac{1}{p}\right)\deg \rho. \tag{38}$$

If $\mathrm{ord}_{r+1,s}(\rho') = 1$ this step is final. We replace ρ by ρ'. If $\mathrm{ord}_{r+1,s}(\rho') > 1$ we proceed to the next step of the recursion.

Assume that 2) holds. Then we put $F = \rho$ in the statement of Lemma 3. Applying this lemma we get a polynomial $\widetilde{F}$. Set $\rho' = \widetilde{F}$. Then

$$\mathrm{ord}_{1,s,\mathfrak{q}}\rho' > \mathrm{ord}_{1,s,\mathfrak{q}}\rho, \quad \mathrm{ord}_{r+1,s}\rho' = \mathrm{ord}_{r+1,s}\rho \tag{39}$$

and by (25) and (26) the inequality

$$\deg \rho' \leq \deg(F) + \mathrm{ord}_{1,s,\mathfrak{q}}(\rho)(-r + \deg \psi_1 + \ldots + \deg \psi_r) \tag{40}$$

holds. We replace ρ by ρ' and proceed to the next step of the recursion.

Assume that 3) holds. Then we put $F = \rho$ in the statement of Lemma 4. Applying this lemma we get an index $1 \leq j \leq r$ such that (33) holds. Set $\rho' = \partial F / \partial Z_j$. Then by (33)

$$\deg \rho' \leq -1 + \deg \rho, \quad \mathrm{ord}_{1,s,\mathfrak{q}}\rho' = -1 + \mathrm{ord}_{1,s,\mathfrak{q}}\rho, \tag{41}$$

$$\mathrm{ord}_{1,s,\mathfrak{q}}(\rho') = \mathrm{ord}_{1,s,\Omega+\mathfrak{q}}(\rho'). \tag{42}$$

If $\mathrm{ord}_{r+1,s}(\rho') = 1$ this step is final. We replace ρ by ρ'. If $\mathrm{ord}_{r+1,s}(\rho') > 1$ we proceed to the next step of the recursion. Notice that now at the next step 3) or 4) holds.

Assume that 4) holds. Then we put $F = \rho$ in the statement of Lemma 5. Applying this lemma we get an index $1 \leq i \leq r$ such that (37) holds. Set $\rho' = \mathcal{D}_i(F)$. Then by (33)

$$\mathrm{ord}_{r+1,s,\mathfrak{q}}(\rho') = \mathrm{ord}_{r+1,s,\mathfrak{q}}(\rho') - 1, \tag{43}$$

$$\deg(\rho') \leq \deg(F) + \deg(\psi_1) + \ldots + \deg(\psi_r) - r - 1. \tag{44}$$

If $\mathrm{ord}_{r+1,s}(\rho') = 1$ this step is final. We replace ρ by ρ'. If $\mathrm{ord}_{r+1,s}(\rho') > 1$ we proceed to the next step of the recursion. Notice that now at the next step again 4) holds.

The recursion is described completely. In the next lemma we show that it terminates after a finite number of steps. Notice that for every step of the recursion if $\rho \in k[X_1/X_0, \ldots, X_n/X_0]$ at the beginning of the step then obviously $\rho' \in k[X_1/X_0, \ldots, X_n/X_0]$ at the end of this step (for the step of type 1) this follows from the fact that the field k is perfect). We have $\rho_{r+1} \in k[X_1/X_0, \ldots, X_n/X_0]$. Hence at the end of the recursion the element $\rho \in k[X_1/X_0, \ldots, X_n/X_0]$.

REMARK 2 *The analog of condition 4) for zero–characteristic is* $\mathrm{ord}_{r+1,s}\rho < +\infty$. *Only this case is used in the construction of [2] Section 10. Thus, in* *comparison with zero–characteristic we need to consider three more cases in the recursion.*

LEMMA 7 *The described recursion terminates after a finite number of steps. At the end of the recursion* $\mathrm{ord}_{1,s}(\rho) = \mathrm{ord}_{r+1,s}(\rho) = 1$, *and if* $\delta < p$ *then*

$$\deg \rho \le \deg(\rho_{r+1}) + (\delta - 1)(-r - 1 + \deg \psi_1 + \ldots + \deg \psi_r), \tag{45}$$

and for an arbitrary δ

$$\deg \rho \le \frac{\deg(\rho_{r+1})}{p^{\mu_1}} + \Big((s-r)(p-1) + \frac{1-p^{1-\mu}}{1-p^{-1}}\lambda \Big)(-r + \deg \psi_1 + \ldots + \deg \psi_r), \tag{46}$$

where μ, μ_1 *are integers such that*

$$1 \le \mu \le 1 + (\log \delta / \log p), \tag{47}$$

$$\mu_1 = \max\{\mu - 2, 0\}, \tag{48}$$

and

$$\lambda = 1 + 2 + \ldots + s(p-1) = s(p-1)(s(p-1)+1)/2 \le s^2p^2/2.$$

PROOF Let us show that there exist an integer $\mu \ge 1$, two finite sequences of integers $a_{2,i}, a_{1,i}$, $1 \le i \le \mu - 1$ (these sequences are empty if $\mu = 1$), and integers $a_{3,\mu}, a_{4,\mu+1}$ satisfying the following properties:

(i) $a_{2,i} > 0$, for all $2 \le i \le \mu - 1$, and if $\mu \ge 2$ then $a_{2,1} \ge 0$,

(ii) $a_{1,i} > 0$ for all $1 \le i \le \mu - 2$, and if $\mu \ge 2$ then $a_{1,\mu-1} \ge 0$,

(iii) $a_{3,\mu} \ge 0$,

(iv) $a_{4,\mu+1} \ge 0$,

(v) in the described recursion step j (recall that $j \ge 1$) is of type 2) if and only if there is $0 \le \nu \le \mu - 2$ such that

$$\sum_{1 \le i \le \nu} (a_{2,i} + a_{1,i}) < j \le a_{2,\nu+1} + \sum_{1 \le i \le \nu} (a_{2,i} + a_{1,i}),$$

(vi) in the described recursion step j is of type 1) if and only if there is $0 \le \nu \le \mu - 2$ such that

$$a_{2,\nu+1} + \sum_{1 \le i \le \nu} (a_{2,i} + a_{1,i}) < j \le \sum_{1 \le i \le \nu+1} (a_{2,i} + a_{1,i}),$$

(vii) in the described recursion step j is of type 3) if and only if

$$\sum_{1 \le i \le \mu-1} (a_{2,i} + a_{1,i}) < j \le a_{3,\mu} + \sum_{1 \le i \le \mu-1} (a_{2,i} + a_{1,i}),$$

(viii) finally, in the described recursion step j is of type 4) if and only if

$$a_{3,\mu} + \sum_{1 \le i \le \mu-1} (a_{2,i} + a_{1,i}) < j \le a_{4,\mu+1} + a_{3,\mu} + \sum_{1 \le i \le \mu-1} (a_{2,i} + a_{1,i}).$$

Indeed, assume that a step of type 3) (respectively 4)) is not final. Then, as we have noticed above, the following step is of type 3) or 4) (respectively 4)). Hence by (20) and (41) (respectively (18) and (43)) there might be only a finite number of steps of type 3) (respectively 4)). So now, saying less formally, we need to prove that in the described recursion after a nonnegative finite number of iterations with steps of type 1) and 2) we shall come to a step of type 3) or 4), or to the end of the recursion.

By (19) and (39) there might be only a finite number of subsequent steps of type 2). After any step of type 2) (respectively 1)) we have $\mathrm{ord}_{r+1,s}(\rho') \le \mathrm{ord}_{r+1,s}(\rho)$ (respectively $\mathrm{ord}_{r+1,s}(\rho') \le p^{-1}\mathrm{ord}_{r+1,s}(\rho)$) by (39) (respectively (23)). The integer $\mathrm{ord}_{r+1,s}(\rho) \ge 1$ at the beginning of each step. Hence in the described recursion there might be only a finite number of subsequent steps of types 2) or 1). Thus, the existence of an integer $\mu \ge 1$, two finite sequences of integers $a_{2,i}, a_{1,i}$, $1 \le i \le \mu-1$, and integers $a_{3,\mu}, a_{4,\mu+1}$ satisfying properties (i)–(viii) is proved. By (38)–(44) if $\delta < p$ then only the steps of type 4) occur in the recursion, i.e., in this case $\mu = 1$ and $a_{3,\mu} = 0$.

Let δ be arbitrary. Recall that $\mathrm{ord}_{r+1,s}\rho_{r+1} \le \delta$ by Lemma 6. Therefore, by (39) and (23) the inequality $\delta/p^{\mu-1} \ge 1$ holds. Hence (47) is satisfied. Further, by (19) and (39) we have $a_{2,i} \le s(p-1)$ for every $1 \le i \le \mu-1$. Recall that $a_{1,i} \ge 1$ for $1 \le i \le \mu-2$. Hence by (38), (39), (40) after the first $\sum_{1\le i\le \mu-1}(a_{2,i}+a_{1,i})$ steps of the recursion for the obtained element ρ we have the estimation

$$\deg\rho \le \frac{\deg(\rho_{r+1})}{p^{\mu_1}} + \Big(\frac{1-p^{1-\mu}}{1-p^{-1}}\Big)\lambda(-r+\deg\psi_1+\ldots+\deg\psi_r). \qquad (49)$$

By (21) the same bound (49) is satisfied after the first $a_{3,\mu}+\sum_{1\le i\le\mu-1}(a_{2,i}+a_{1,i})$ steps. By (18) we have $a_{4,\mu+1} \le (s-r)p$. Finally, by (43), (44) and (49) at the end of the recursion estimation (46) holds.

Assume that $\delta < p$. Then the recursion consists only of steps of type 4), see above. Hence by (43), (44) at the end of the recursion (45) is fulfilled. The lemma is proved.

Let $\rho \in \overline{k}[Z_1,\ldots,Z_n]$ be the polynomial obtained at the end of the described recursion. Now our aim is to construct g_{r+1} and polynomials $f_{r+1,r+2},\ldots,f_{r+1,s}$, i.e., to describe the recursion from Section 1. As we have seen $\rho \in k[X_1/X_0,\ldots, X_n/X_0] \cap \widetilde{\mathfrak{P}}$. Hence by (17) the element ρ vanishes on $W \setminus \mathcal{Z}(X_0)$. We have $\mathrm{ord}_{r+1,s}\rho = 1$. Therefore, by Lemma 5 there is $1 \le i \le r$ such that

$$\mathrm{ord}_{r+1,s}\mathcal{D}_i(\rho) = 0. \qquad (50)$$

Now (17) implies that $\mathcal{D}_i(\rho)$ does not vanish on $W \setminus \mathcal{Z}(X_0)$. Therefore, by (50) there is a non–empty open in the Zariski topology subset $S \subset W$ such that every point $y \in S$ is a smooth point of W and the differentials at the point y

$$d_y\psi_1,\ldots,d_y\psi_r,d_y\rho$$

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

Set $d_{r+1} = \deg(\rho)$ and

$$g_{r+1} = \rho X_0^{d_{r+1}}. \qquad (51)$$

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 $\dim_y \mathcal{Z}(g_1,\ldots,g_{r+1}) = n-r-1$.

Recall the definition from [2], Section 2.

DEFINITION 4 *Let $0 < j \le s$ be an integer. Consider a sequence of homogeneous polynomials $\theta_i \in \mathfrak{P}$, $1 \le i \le j$. Let $0 \le u < j$ be an integer. Denote by $\mathcal{W} = \mathcal{W}(\mathfrak{P}, u)$ the set of all irreducible components E defined over k of the algebraic variety $\mathcal{Z}(\theta_1, \ldots, \theta_u)$ such that $E \supset W$. Suppose that for every integer $0 \le u < j$ the polynomial $\theta_{u+1} \in \mathfrak{P}$ is such that for every irreducible component $E \in \mathcal{W}$ the algebraic variety*

$$E \not\subset \mathcal{Z}(\theta_{u+1})$$

and if $u \ge 1$ then $\deg \theta_{u+1} \ge \deg \theta_u$. Then any such sequence $\theta_1, \ldots, \theta_j$ will be called weak $\mathfrak{P}$–sequence (of length j).

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

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 $\theta_{2,i} = \eta f_i$, $1 \le i \le s$, for a homogeneous polynomial η which is not vanishing on W,
- $\deg \theta_{1,i} \le \deg \eta$ for all $1 \le i \le r+1$,
- $\deg \theta_{1,i} > \deg \theta_{2,s}$ for all $r+2 \le i \le s$.

Let us apply Lemma 1 [2] to these $\mathfrak{P}$-sequences. We get the third $\mathfrak{P}$-sequence $\theta_{3,1}, \ldots, \theta_{3,s}$. Recall that by Lemma 1 [2] for every $1 \le j \le s$ the element $\theta_{3,j}$ belongs to the union of the ideals $(\theta_{1,1}, \ldots, \theta_{1,s}) \cup (\theta_{2,1}, \ldots, \theta_{2,s}) \subset k[X_0, \ldots, X_n]$, and the degree $\deg \theta_{3,j} = \min\{\deg \theta_{1,j}, \deg \theta_{2,j}\}$. Hence $\theta_{3,j} \in (\theta_{2,1}, \ldots, \theta_{2,s})$, and η divides $\theta_{3,j}$ for every $r+1 \le j \le s$.

Set $f_{r+1,j} = \theta_{3,j}/\eta$, $r+2 \le j \le s$. Let us replace in conditions (a)–(d) r by $r+1$ and the point x by a point y. Then by Lemma 1 [2] there is a point $y \in S$ such that (a)–(d) are satisfied for the constructed homogeneous polynomials $g_1, \ldots, g_{r+1}, f_{r+1,r+2}, \ldots, f_{r+1,s}$ at the point y. This finishes the description of the recursion step and all the recursion from Section 1.

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

LEMMA 8 *There is a constant $0 \le C \in \mathbb{R}$ and there are $e_j \in \mathbb{R}$, $1 \le j \le s$ such that the inequalities*

$$\deg g_j \le e_j \deg f_j, \quad 1 \le j \le s, \tag{52}$$

$$e_j \le n^{2^{s^C}}, \quad 1 \le j \le s \tag{53}$$

hold

PROOF Suppose that inequalities (52) hold for all $1 \le j \le r$ where $0 \le r < s$. Then by Theorem 1 from [2] and Lemma 6 we have

$$\mathrm{ord}_{r+1,s}(\rho_{r+1}) \le \delta \le 1 + e_1 \cdot \ldots \cdot e_r \delta_1 \cdot \ldots \cdot \delta_s / \deg W \le 1 + a_s e_1 \cdot \ldots \cdot e_r,$$

where

$$a_s < n^{2^{s^{C_1}}} \tag{54}$$

for an absolute constant $0 < C_1 \in \mathbb{R}$, see Theorem 1 from [2]. The inequalities (45) for $\delta < p$ and (46) for $\delta \geq p$ imply

$$\deg \rho \leq \deg(\rho_{r+1}) + (n\delta + 1)^2(-r + \deg \psi_1 + \ldots + \deg \psi_r) \tag{55}$$

(for both cases $\delta < p$ and $\delta \geq p$). Recall that $\deg \rho_{r+1} = \delta_{r+1}$. Hence from (55) we get

$$\deg g_{r+1} \leq \delta_{r+1} + (n(1 + a_s e_1 \cdot \ldots \cdot e_r) + 1)^2 \Big(-r + \sum_{1 \leq j \leq r} e_j \delta_j \Big).$$

Put

$$e_{r+1} = 1 + (n(1 + a_s e_1 \cdot \ldots \cdot e_r) + 1)^2 (e_1 + \ldots + e_r).$$

Then (52) holds for $j = r + 1$. Now the existence of the constant C such that inequalities (52) and (53) hold for all $1 \leq j \leq s$ follows from (54) (the cases when $n = 1$ or $s = 1$ are trivial). The lemma and Theorem 1 are proved.

References

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

[2] **Chistov A. L.:** *"Efficient Construction of Local Parameters of Irreducible Components of an Algebraic Variety"*, Proc. of the St.–Petersburg Mathematical Society, 1999, v. 7, p. 230–266 (in Russian). [English transl. in: Proceedings of the St.Petersburg Mathematical Society, American Math. Soc. Publisher v. VII, 2001].

[3] **Chistov A. L.:** *"Efficient Smooth Stratification of an Algebraic Variety in Zero–Characteristic and its Applications"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 266 (2000) p.254–311 (in Russian) [English transl.: Journal of Mathematical Sciences v. 113 (5), (2003), p 689–717].

[4] **Chistov A. L.:** *"A correction in the statement of my theorem on the efficient smooth cover and smooth stratification of an algebraic variety."*, Preprint of the St.–Petersburg Mathematical Society, 2004, #13, http://www.mathsoc.spb.ru/preprint/2004/index.html#13

[5] **Chistov A. L.:** *"Polynomial–time computation of the degrees of algebraic varieties in zero–characteristic and its applications"*, Zap. Nauchn. Semin. St-Petersburg. Otdel. Mat. Inst. Steklov (POMI) v. 258 (1999), p. 7–59 (in Russian) [English transl.: Journal of Mathematical Sciences 108 (6), (2002) p. 897–933].

[6] **Shafarevich I. R.** *Basic Algebraic Geometry*, Springer–Verlag New–York, 1972.