Double-Exponential Lower Bound for the Degree of Any System of Generators of a Polynomial Prime Ideal

Alexander L. Chistov

St. Petersburg Department of Steklov Mathematical Institute
of the Academy of Sciences of Russia
Fontanka 27, St. Petersburg 191023, Russia,
e-mail: alch@pdmi.ras.ru

2008

Abstract

Consider a polynomial ring A in $n+1$ variables over an arbitrary infinite field k. We prove that for all sufficiently big n and d there is a homogeneous prime ideal $\mathfrak{p} \subset A$ satisfying the following conditions. The ideal $\mathfrak{p}$ corresponds to a defined over k and irreducible over $\overline{k}$ component of a projective algebraic variety given by a system of homogeneous polynomial equations with polynomials from A of degrees less than d. Any system of generators of $\mathfrak{p}$ contains a polynomial of degree at least $d^{2^{cn}}$ for an absolute constant $c > 0$ which can be computed efficiently. This solves an important old problem in effective algebraic geometry. For the case of finite fields we obtain a slightly less strong result.

Introduction

In the classical paper [7] D. Hilbert proved that any polynomial ideal is generated by a finite number of polynomials. Hence it is true for a prime polynomial ideal $\mathfrak{p}$ of an irreducible component of an algebraic variety given by a system of polynomial equations in n unknowns of degrees less than d. The problem arose to give upper and lower bounds for degrees of the generators of $\mathfrak{p}$ as functions of d and n. Notice that the degree of the ideal $\mathfrak{p}$ itself (see the definition of the degree of an ideal below) is bounded from above by d^n by the Bézout theorem. It is known that there is a system of generators of $\mathfrak{p}$ with degrees $d^{2^{O(n)}}$, see Remark 2 below (the case of nonhomogeneous prime ideal is easily reduced to the one of the homogeneous prime ideal). One of the most important open problem in effective algebraic geometry has been to obtain the similar lower bound for degrees of any system of generators of an ideal $\mathfrak{p}$. In this paper we solve this old problem over an arbitrary infinite field, see Theorem 1 below. This implies also the same lower bound for the stabilization of the characteristic function of a homogeneous $\mathfrak{p}$, see Theorem 1 and Remark 1.

So far double–exponential lower bounds have been known for binomial ideals, see Section 1 for more detail. These ideals are far from being prime: they have many primary components. All the attempts to reduce the case of a prime ideal to the known one of binomial ideals failed. Our construction is simple but ingenious in this sense. We managed to fulfill this reduction! The key to all is Lemma 2. But how did we make this discovery? Not occasionally. We investigated the problem of effective normalization of algebraic varieties. It turns out that the construction of the normalization of an algebraic variety is reduced to solving a linear equation $aX + bY + cZ = 0$ over a polynomial ring. Simultaneously as one of the consequence of our results we got Lemma 2. We hope to return to the normalization of an algebraic variety from algorithmic point of view in one of the next papers. Notice that the problem of solving the equality $aX+bY+cZ = 0$ over a polynomial ring is close to the one formulated at the end of the Introduction.

Let k be a field with algebraic closure $\overline{k}$. Let $n \geqslant 0$ and $X_0, \dots, X_n$ be variables. Let $\mathfrak{a} \subset k[X_0, \dots, X_n] = A$ be a homogeneous ideal Denote by $h(\mathfrak{p}, m) = \dim_k (A/\mathfrak{a})_m$ the characteristic function of the ideal $\mathfrak{a}$, where $(A/\mathfrak{a})_m$ is the vector space of the homogeneous elements of degree $m \geqslant 0$ of the ring $A/\mathfrak{a}$. Recall that there is a polynomial $P = \sum_{0 \leqslant i \leqslant n-s} p_i Z^i$, all $p_i \in \mathbb{Q}$, of degree $\deg P = n - s$ such that $h(\mathfrak{p}, m) = p(m)$ for all sufficiently big $m > 0$. By definition P is the Hilbert polynomial $A/\mathfrak{a}$. The degree of the ideal $\mathfrak{a}$ can be defined by the formula $\deg \mathfrak{a} = (n-s)! p_{n-s}$. Denote by $\mathcal{Z}(\mathfrak{a}) \subset \mathbb{P}^n(\overline{k})$ the set of all common zeroes of the polynomials from $\mathfrak{a}$ in $\mathbb{P}^n(\overline{k})$ (the similar notations will be used below with other ideals or family of polynomials and other projective or affine spaces).

Below in the statements of the theorem, the proposition, lemmas and the corollary the existence of constants c, n_0, d_0, c_0, c_1 and so on is claimed. All these constants can be computed efficiently. We prove the following result.

THEOREM 1 *There are constants $c > 0$, $n_0 > 0$, $d_0 > 0$ such that for every infinite field k for all integers $n > n_0$ and $d > d_0$ there are homogeneous polynomials $f_1, \dots, f_\nu \in A$, $\nu \leqslant n$, with all degrees $\deg f_i < d$, $1 \leqslant i \leqslant \nu$, and a homogeneous prime ideal $\mathfrak{p} \subset A$ satisfying the following conditions.*

(a) *The set of zeroes* $\mathcal{Z}(\mathfrak{p}) \subset \mathbb{P}^n(\overline{k})$ *of the ideal* $\mathfrak{p}$ *coincides with a defined over* k *and irreducible over* $\overline{k}$ *component of the projective algebraic variety* $\mathcal{Z}(f_1, \ldots, f_\nu) \subset \mathbb{P}^n(\overline{k})$ *of all common zeroes of the polynomials* $f_1, \ldots, f_\nu$. *Hence the ideal* $\overline{k} \otimes_k \mathfrak{p} \subset \overline{k} \otimes_k A$ *is prime. Moreover,* $\mathfrak{p}$ *is a primary component of the ideal* $(f_1, \ldots, f_\nu) \subset A$*, the height* $\mathrm{ht}(\mathfrak{p}) = \nu$ *and the projective algebraic variety* $\mathcal{Z}(f_1, \ldots, f_\nu)$ *has exactly two irreducible over* $\overline{k}$ *components:* $\mathcal{Z}(\mathfrak{p})$ *and some linear subspace* $\mathcal{L} \subset \mathbb{P}^n(\overline{k})$ *defined over* k.

(b) *Suppose that the characteristic function* $h(\mathfrak{p}, m)$ *is stable for* $m \geqslant m_0$*, i.e., coincides with the Hilbert polynomial of* $A/\mathfrak{p}$ *for these* m. *Then* $m_0 \geqslant d^{2^{cn}}$.

(c) *Let* $a_1, \ldots, a_m$ *be an arbitrary system of generators of the ideal* $\mathfrak{p}$. *Then the maximal degree* $\max_{1 \leqslant i \leqslant m} \deg_{X_0, \ldots, X_n} a_i \geqslant d^{2^{cn}}$.

It is quite probable that one can remove the word "infinite" in the statement of the theorem and obtain the result for an arbitrary field, see Remark 5 at the end of Section 4. Also here Remark 4 at the beginning of Section 3 may be useful. But in this paper we prove only the following result.

PROPOSITION 1 *Let us replace in the statement of Theorem 1 the words "infinite field" by "finite field" and* $d^{2^{cn}}$ *by* $d^{2^{c\sqrt{n}}}$ *in conditions (b) and (c). Then this new statement of theorem holds for finite fields.*

REMARK 1 *It is known, see [5] Sections 6 and 7, that for any homogeneous ideal* $\mathfrak{a} \subset A$ *the following assertion is satisfied. If the characteristic function* $h(\mathfrak{a}, m)$ *is stable for* $m \geqslant m_0$ *where* $m_0 \geqslant 0$ *then for any admissible ordering of monomials the reduced Gröbner basis of* $\mathfrak{a}$ *with respect to this ordering of monomials consists of homogeneous polynomials of degrees at most* $m_0 + 1$. *Hence there is a system of generators of* $\mathfrak{a}$ *with degrees at most* $m_0 + 1$.

Here probably one needs to give some details related to the last remark. We shall use the notation from [5] (but replace n by $n+1$). In [5] the constant $b_0 \geqslant b_1 \geqslant \ldots \geqslant b_{n+2} = 0$ corresponding to the ideal $I = \mathfrak{a}$ are considered. Let the integer $m_0 \geqslant 0$ be the least possible such that the characteristic function $h(\mathfrak{a}, m)$ is stable for $m \geqslant m_0$. Then either $m_0 = b_0$, or $m_0 = b_1 - 1$. More precisely, if $m_0 = b_1 - 1$ then $b_0 = b_1$ and there is no pair $\langle h, u \rangle$ in a 0-standard exact cone decomposition of N_I with $|u| = 0$ and $\deg h = b_1 - 1$. On the other hand, by Lemma 7.2 [5] the degrees of polynomials in the considered reduced Gröbner basis are bounded from above by b_0. The assertion of Remark 1 follows from here.

Notice also that before Lemma 7.2 [5] there is the following formula: $b_0 = \min\{d \geqslant b_1 : \forall_{z \geqslant d}\, \overline{\varphi}(z) = \varphi(z)\}$. Here we have corrected the misprint (which may mislead the reader now) and replaced $z > d$ by $z \geqslant d$. Otherwise, this formula contradicts to the definition of b_i on p.765 of [5].

REMARK 2 *Let* $\mathfrak{P} \subset A$ *be an arbitrary homogeneous prime ideal of height* $\mathrm{ht}(\mathfrak{P}) = s$, $0 \leqslant s \leqslant n$, *and of degree* d. *We shall suppose additionally that the ideal* $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ *is radical or which is equivalent the variety* $\mathcal{Z}(\mathfrak{P})$ *is defined over* k. *Then by Lemma 9 and Corollary 1 the characteristic function* $h(\mathfrak{P}, m)$ *of this ideal is stable for* $m \geqslant \min\{(sd)^{O(n-s+1)^{n-s}}, d^{2^{O(n)}}\}$ *and hence* $\mathfrak{P}$ *has a system of generators with degrees at most* $\min\{(sd)^{O(n-s+1)^{n-s}}, d^{2^{O(n)}}\}$.

PROBLEM *Are there constants $c > 0$, $n_0 > 0$, $d_0 > 0$ satisfying the following property? For all integers $n > n_0$, $d > d_0$ for every field k there is a homogeneous prime ideal $\mathfrak{p} \subset k[X_0, \ldots, X_n]$ with the degree* $\deg \mathfrak{p} = d$ *and the height* $\mathrm{ht}(\mathfrak{p}) = 2$ *such that for this ideal $\mathfrak{p}$ assertion (c) of Theorem 1 holds.*

1 Lower bounds for the stabilization of the characteristic function of a binomial ideal in arbitrary characteristic

A power product in the ring $k[X_1, \ldots, X_{n-1}]$ is a monomial $X_1^{i_1} \cdot \ldots \cdot X_{n-1}^{i_{n-1}}$ for some integers $i_j \geqslant 0$. By definition a binomial from $k[X_1, \ldots, X_{n-1}]$ is a difference of two distinct power products. A polynomial ideal $\mathfrak{g} \subset k[X_1, \ldots, X_{n-1}]$ is called binomial if and only if it has a system of generators $q_1, \ldots, q_v$ consisting of binomials. In the similar way binomials and binomial ideals are defined for the ring $A^{(0)} = k[X_0, \ldots, X_{n-1}]$ and other polynomial rings.

LEMMA 1 *There are constants $c_1 > 0$, $n_0 > 0$ and $d_0 > 0$ such that for any field k (of arbitrary characteristic and not necessarily infinite) for all integers $n > n_0$, $d > d_0$ there is a homogeneous ideal $\mathfrak{b} \subset k[X_0, \ldots, X_{n-1}] = A^{(0)}$ satisfying the following condition. The ideal $\mathfrak{b}$ is generated by a system of homogeneous binomials $b_1, \ldots, b_\mu$ of degrees* $\deg b_i = m_i < d$ *and $\mu = O(n)$. Suppose that the characteristic function $h(\mathfrak{b}, m)$ is stable for $m \geqslant m_0$, i.e., coincides with the Hilbert polynomial of $A^{(0)}/\mathfrak{b}$ for these m. Then $m_0 \geqslant d^{2^{c_1 n}}$.*

PROOF Let us show, cf. [11], that the reduced Gröbner basis of any binomial ideal with respect to any admissible ordering of monomials consists of binomials. Indeed, one can construct this Gröbner basis by the Buchberger algorithm. Each new polynomial in the Buchberger algorithm comes from either (i) the reduction of a binomial by another binomial, or (ii) by the S-polynomial of two binomials. In both (i) and (ii) the result is again a binomial. This proves the required assertion.

Besides that, if $e_1, \ldots, e_\alpha$ is the reduced Gröbner basis of the binomial ideal $(q_1, \ldots, q_v) \subset \mathbb{Q}[X_1, \ldots, X_{n-1}]$ with respect to an admissible ordering of monomials for any fixed field k of zero–characteristic (say, for the field of rational numbers $k = \mathbb{Q}$) then by the same argument $e_1 \bmod p, \ldots, e_\alpha \bmod p$ is the reduced Gröbner basis of the ideal $(q_1 \bmod p, \ldots, q_v \bmod p) \subset k_p[X_1, \ldots, X_{n-1}]$ with respect to the same ordering of monomials over any field k_p of characteristic p for every prime integer p. Hence the number of elements α and the maximal degree $\max_{1 \leqslant i \leqslant \alpha} e_i$ of the reduced Gröbner basis does not depend on the choice of the field k, in particular of the characteristic of the field k.

In [11] the following assertion is proved (actually with $\mathbb{Q}[X_1, \ldots, X_n]$ in place of $\mathbb{Q}[X_1, \ldots, X_{n-1}]$ but for us it is convenient to formulate it for $\mathbb{Q}[X_1, \ldots, X_{n-1}]$). There are constants $c_0 > 0$, $n_0 > 0$ and $d_0 > 0$ such that for all integers $n > n_0$, $d > d_0$ there are an integer $\mu = O(n)$ and binomials $g_1, \ldots, g_\mu \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$ (they are constructed explicitly) of degrees $\deg g_i < d$, $1 \leqslant i \leqslant \mu$, satisfying the following condition. Put the ideal $\mathfrak{g} = (g_1, \ldots, g_\mu) \subset \mathbb{Q}[X_1, \ldots, X_{n-1}]$. Let $e_1, \ldots, e_\alpha$ is the reduced Gröbner basis of $\mathfrak{g}$ with respect to some admissible ordering $<$ of monomials (this ordering can be chosen arbitrary). Then $\max_{1 \leqslant i \leqslant \alpha} \deg e_i \geqslant d^{2^{c_0 n}}$. By the previous arguments the same assertion holds with an arbitrary field k in place of $\mathbb{Q}$. In what follows we shall denote by $e_1, \ldots, e_\alpha$ the reduced Gröbner basis of the ideal $(g_1, \ldots, g_\mu) \subset k[X_1, \ldots, X_{n-1}]$ with respect to the ordering of monomials $<$.

For every $1 \leqslant i \leqslant \mu$ put $b_i = X_0^{\deg g_i} g_i(X_1/X_0, \ldots, X_{n-1}/X_0) \in A^{(0)}$ to be the homogenization of g_i. Hence b_i is a homogeneous binomial from $k[X_0, \ldots, X_{n-1}]$. By definition put $\mathfrak{b} = (b_1, \ldots, b_\mu) \subset k[X_0, \ldots, X_{n-1}]$ to be the homogeneous ideal. We shall assume without loss of generality that the ordering of monomials $<$ is degree-compatible, i.e., for all monomial $v_1, v_2 \in A$ the condition $\deg v_1 < \deg v_2$ implies $v_1 < v_2$. Further, consider the admissible ordering of monomials from $A^{(0)}$ which extends the ordering $<$ on the monomials from $k[X_1, \ldots, X_{n-1}]$ and such that $X_0^i < X_j$ for all $1 \leqslant j \leqslant n$ and $i \geqslant 0$. Let $e'_1, \ldots, e'_\lambda$ be the reduced Gröbner basis of the ideal $\mathfrak{b}$ with respect to the considered ordering of the monomials. Then from the definition of the Gröbner basis we get immediately that $e'_1(1, X_1, \ldots, X_{n-1}), \ldots, e'_\lambda(1, X_1, \ldots,\ X_{n-1})$ is a Gröbner basis with respect to ordering $<$ of the ideal $(g_1, \ldots, g_\mu)$. Since the ordering $<$ on the monomials from $k[X_1, \ldots, X_{n-1}]$ is degree-compatible we have

$$\max_{1 \leqslant i \leqslant \lambda} \deg e'_i(1, X_1, \ldots, X_{n-1}) \geqslant \max \deg_{1 \leqslant i \leqslant \alpha} e_i \geqslant d^{2^{c_0 n}}.$$

Therefore, $\max_{1 \leqslant i \leqslant \lambda} \deg e'_i \geqslant d^{2^{c_0 n}}$. Now by Remark 1 the assertion of the lemma holds. The lemma is proved.

In [11] one can find also a survey of the results on this subject. All the works here are based on the initial ideas from [9] where zero–characteristic fields are considered (or, more precisely, the field of rational numbers). The proof of Lemma 2 [9] about all possible binomials from a binomial ideal is given for zero–characteristic. D. Yu. Grigoriev (a private communication) noticed that there is another simple proof of this lemma in arbitrary characteristic. It seems that there are no other obstacles to extend these results for the case of nonzero characteristic. Hence all the lower bounds for binomial ideals are valid in arbitrary characteristic. In our proof of Lemma 1 we even don't use Lemma 2 from [9] in nonzero characteristic.

2 Proof of Theorem 1: conditions (a) and (b)

The ring of polynomials $A = k[X_0, \ldots, X_n]$ is graded by the degree with respect to all the variables $X_0, \ldots, X_n$. For a graded A-module M and an integer ν denote by $M(\nu)$ the graded A-module with the shifted graduation. Namely, one can identify the homogeneous components $M(\nu)_m = M_{\nu+m}$ for every m and this identification induces the isomorphism of A-modules $M(\nu) \simeq M$. The last isomorphism is an isomorphism degree ν of graded A-modules $M(\nu)$ and M.

Let X_{n+1}, $Z_1, \ldots, Z_\mu$ be new variables. Let

$$\Phi = X_0 X_n X_{n+1} + X_n^3 + X_{n+1}^3.$$

Set the rings of polynomials $A^{(1)} = A[X_{n+1}]$. Put the ring $B_\Phi = A^{(1)}/(\Phi)$. Now A, $A^{(1)}$, $A^{(1)}[Z_1, \ldots, Z_\mu]$ are graded rings by the total degree with respect to all the variables $X_0, \ldots, X_{n+1}, Z_1, \ldots, Z_\mu$, i.e., the homogeneous elements of degree m these rings are homogeneous polynomials of degree m with respect to all these variables. The polynomial Φ is homogeneous. Hence B_Φ and $B_\Phi[Z_1, \ldots, Z_\mu]$ are also a graded rings.

Denote by $K^{(1)}$ and K' the fields of fractions of $A^{(1)}$ and B_Φ respectively. For an arbitrary rational function $P/Q \in K^{(1)}$ such that $P, Q \in A^{(1)}$ and Φ does not divide Q we shall denote by $(P/Q) \bmod \Phi$ the image of this rational function in K'.

LEMMA 2 *Let k be an arbitrary field. Let $\mathfrak{a} \subset A$ be a homogeneous ideal such that $X_n \in \mathfrak{a}$ or $\mathfrak{a} = A$. Put*

$$B_{\mathfrak{a}} = \left\{ \left(z_0 + z_1 X_{n+1} + z_2 \frac{X_{n+1}^2}{X_n} \right) \bmod \Phi \,:\, z_0, z_1 \in A \,\&\, z_2 \in \mathfrak{a} \right\} \subset K'.$$

Then $B_{\mathfrak{a}}$ is a graded ring and a finitely generated A-module. Further, the A-module $B_{\mathfrak{a}} \simeq A \oplus A(-1) \oplus \mathfrak{a}(-1)$. The ring $\overline{k} \otimes_k B_{\mathfrak{a}}$ is integral. The field of fractions of $B_{\mathfrak{a}}$ is K', the tensor product $\overline{k} \otimes_k K'$ is a field, and the extension of fields $\overline{k} \otimes_k K' \supset \overline{k}(X_0, \ldots, X_n)$ is finite separable.

PROOF The element $X_{n+1}^2 \bmod \Phi \in B_{\mathfrak{a}}$ since $X_n \in \mathfrak{a}$. For all $x_1, x_2 \in \mathfrak{a}$ we have

$$x_1 X_{n+1}^3 / X_n \bmod \Phi = (-x_1 X_n^2 - x_1 X_0 X_{n+1}) \bmod \Phi \in B_{\mathfrak{a}},$$
$$x_1 x_2 X_{n+1}^4 / X_n^2 \bmod \Phi = (-x_1 x_2 X_n X_{n+1} - x_1 x_2 X_0 X_{n+1}^2 / X_n) \bmod \Phi \in B_{\mathfrak{a}}$$

and $B_{\mathfrak{a}}$ is an A-module. Hence $B_{\mathfrak{a}}$ is a ring. Other assertions are also straightforward. The lemma is proved.

Let $\mathfrak{b} \subset A^{(0)}$ be the ideal from Lemma 1. We shall suppose without loss of generality that $n_0 > 1$ in Lemma 1 and hence $n \geqslant 2$. Set $\mathfrak{b}' = \mathfrak{b}A + (X_n)$ to be the homogeneous ideal of A. Set $\mathfrak{a} = \mathfrak{b}'$ in Lemma 2 and $B' = B_{\mathfrak{b}'}$. We have $A/\mathfrak{b}' = A^{(0)}/\mathfrak{b}$. Hence if $\dim(B')_m$ is stable for $m \geqslant m_0$ (i.e., coincides with the Hilbert polynomial of $A^{(0)}/\mathfrak{b}$ for these m) then $m_0 \geqslant d^{2^{c_1 n}} + 1$ by Lemma 1.

We shall construct recursively the graded ring $B^{(0)} = B'$, $B^{(1)}, \ldots, B^{(\mu)}$ satisfying for all i the following properties.

(i) The ring $\overline{k} \otimes_k B^{(i)}$ is integral

(ii) The extension of rings $B^{(i)} \supset A$ is integral.

(iii) Denote by $K^{(i)}$ the field of fractions of $B^{(i)}$. Then the extension of fields $\overline{k} \otimes_k K^{(i)} \supset \overline{k}(X_0, \ldots, X_n)$ is finite separable.

(iv) For $i \geqslant 1$ there are nonzero $\lambda_{i,1}, \lambda_{i,2}, \lambda_{i,3}, \lambda_{i,4} \in k$ such that the polynomial

$$\varphi_i = Z_i^{m_i+1} + \lambda_{i,1} X_0^{m_i} Z_i + \lambda_{i,2} X_0^{m_i} X_1 + \lambda_{i,3} X_0^{m_i} X_2 +$$
$$\lambda_{i,4} (b_i X_{n+1}^2 / X_n) \bmod \Phi \in B^{(i-1)}[Z_i]$$

is an irreducible element of the ring $\overline{k} \otimes_k K^{(i)}[Z_i]$, and by definition the ring $B^{(i)} = B^{(i-1)}[Z_i]/(\varphi_i)$.

For $i = 0$ these properties follow from the definition of the ring B'. Let $1 \leqslant i \leqslant \mu$ and $B^{(i-1)}$ is constructed. Let us construct $B^{(i)}$. Obviously (i)–(iii) follow from (iv). So it is sufficient to construct the polynomial φ_i from (iv).

Denote by $E^{(i-1)}$ the integral closure of the ring $\overline{k} \otimes_k B^{(i-1)}$ in its field of fractions $\overline{k} \otimes_k K^{(i-1)}$. Notice that $E^{(i-1)}[Z_i] \supset \overline{k} \otimes_k B^{(i-1)}[Z_i]$. Denote by $V^{(i-1)}$ the normal affine algebraic variety with the ring of regular functions $E^{(i-1)}[Z_i]$.

Let $\alpha \in k$ be a nonzero element. Let us define the elements of the ring $\overline{k} \otimes_k B^{(i-1)}[Z_i]$

$$\begin{array}{ll} \psi_1 = X_0^{m_i} X_2, & \psi_2 = X_0^{m_i} Z_i, \quad \psi_3 = X_0^{m_i} X_1, \\ \widetilde{\psi}_1 = \alpha Z_i^{m_i+1} + X_0^{m_i} X_2, & \widetilde{\psi}_2 = X_0^{m_i} Z_i, \\ \widetilde{\psi}_3 = X_0^{m_i} X_1 + \alpha(b_i X_{n+1}^2 / X_n) \bmod \Phi. & \end{array}$$

Then

$$V^{(i-1)} \cap \mathcal{Z}(\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3) \subset V^{(i-1)} \cap \mathcal{Z}(Z_i, X_0 X_2).$$

Hence by (ii) for $i-1$

$$\dim(V^{(i-1)} \cap \mathcal{Z}(\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3)) \leqslant \dim(V^{(i-1)}) - 2. \tag{1}$$

Further, by (iii) for $i-1$ the family $X_0, X_0^{m_i} X_1, X_0^{m_i} X_2, X_3, X_4, \ldots, X_n, X_0^{m_i} Z_i$ is a separable basis of transcendency of the field $\overline{k} \otimes_k K^{(i-1)}(Z_i)$ over $\overline{k}$. Therefore, the morphism

$$V^{(i-1)} \to \mathbb{A}^3(\overline{k}), \quad z \mapsto (\psi_1(z), \psi_2(z), \psi_3(z)) \tag{2}$$

is separable dominant, or which equivalent the differential of this morphism at some smooth point ξ is an epimorphism

Let us show that there is a nonempty open in the Zariski topology subset $\mathcal{U}'' \subset \overline{k}$ (obviously the number of elements $\#(\overline{k} \setminus \mathcal{U}'') < +\infty$) such that for all $\alpha \in \mathcal{U}''$ the rational morphism

$$V^{(i-1)} \to \mathbb{P}^2(\overline{k}), \quad z \mapsto (\widetilde{\psi}_1(z) : \widetilde{\psi}_2(z) : \widetilde{\psi}_3(z)) \tag{3}$$

is separable dominant. Indeed, consider the morphism

$$\widetilde{\psi} : V^{(i-1)} \to \mathbb{A}^3(\overline{k}), \quad z \mapsto (\widetilde{\psi}_1(z), \widetilde{\psi}_2(z), \widetilde{\psi}_3(z)).$$

Let $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\overline{k})$, $n_1 \geqslant n+1$, and $\mathbb{A}^{n_1+2}(\overline{k})$ has coordinate functions $Z_i, X_0, \ldots, X_{n_1}$. Let $h_1, \ldots, h_s \in \overline{k}[Z_i, X_0, \ldots, X_{n_1}]$ be a system of local parameters of the algebraic variety $V^{(i-1)}$ at the point ξ. Then the differential of morphism (2) at the point ξ is an epimorphism if and only if the differentials $d_\xi h_1, \ldots, d_\xi h_s, d_\xi \psi_1, d_\xi \psi_2, d_\xi \psi_3$ are linearly independent over $\overline{k}$. Therefore, the differentials $d_\xi h_1, \ldots, d_\xi h_s$, $d_\xi \widetilde{\psi}_1, d_\xi \widetilde{\psi}_2, d_\xi \widetilde{\psi}_3$ are linearly independent over $\overline{k}$ for all α from a nonempty open in the Zariski topology subset of $\mathcal{U}'' \subset \overline{k}$. Hence morphism $\widetilde{\psi}$ is dominant and separable for all $\alpha \in \mathcal{U}''$. The natural morphism $\pi : \mathbb{A}^3(\overline{k}) \setminus \{0\} \to \mathbb{P}^2(\overline{k})$ is dominant separable. Morphism (3) is equal to $\pi \circ \widetilde{\psi}$. Hence the last morphism is also separable dominant for all $\alpha \in \mathcal{U}''$. This proves the required assertion.

Let $V', V'' \subset \mathbb{A}^n(\overline{k})$ be arbitrary affine algebraic varieties. Recall that by definition the intersection of V' and V'' is transversal if and only if for every irreducible over $\overline{k}$ component W of the intersection $V' \cap V''$ there is a smooth point $z \in W$ such that z is a smooth point of V' and V'' simultaneously, and the intersection of tangent spaces of the algebraic varieties V' and V'' at the point z is transversal where the tangent spaces are considered as subspaces of $\mathbb{A}^n(\overline{k})$.

In what follows unless it is not stated otherwise we shall suppose that the field k is infinite. Let us choose and fix $\alpha \in \mathcal{U}'' \cap k$. Recall that $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\overline{k})$. The morphism (3) is separable dominant, (1) holds and $n \geqslant 2$. Hence one can apply the first Bertini theorem, see [12], [1], cf. [4], to morphism (3). By this theorem there is a polynomial φ which is a linear combination of $\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3$ with coefficients from k in general position such that the intersection $\widetilde{V}^{(i-1)}$ and $\mathcal{Z}(\varphi)$ is transversal in $\mathbb{A}^{n_1+2}(\overline{k})$ and irreducible over $\overline{k}$.

Since $E^{(i-1)}[Z_i]$ is integrally closed for any nonzero element $\varphi' \in E^{(i-1)}[Z_i]$ the ideal $(\varphi') \subset E^{(i-1)}[Z]$ is unmixed, i.e., all the associated prime ideals of (φ') have the same height 1.

In our situation this implies that the ideal $(\varphi) \subset E^{(i-1)}[Z_i]$ is prime. Hence the polynomial $\varphi \in \overline{k} \otimes_k K^{(i-1)}[Z_i]$ is irreducible since $E^{(i-1)}$ is integrally closed. Multiplying φ by a nonzero factor from k we shall suppose without loss of generality that the leading coefficient with respect to Z_i of the polynomial φ is 1. Now put $\varphi_i = \varphi$. Hence condition (iv) is satisfied. We get also $\lambda_{i,3} = \alpha^{-1}$, $\lambda_{i,4} = \alpha\lambda_{i,2}$ and hence $\lambda_{i,2} = \lambda_{i,3}\lambda_{i,4}$.

Put $B = B^{(\mu)}$. Denote by K the field of fractions of B. Hence $\overline{k} \otimes_k K$ is the field of fractions of $\overline{k} \otimes_k B$. By (iii) the extension of fields $\overline{k} \otimes_k K \supset \overline{k}(X_0, \ldots, X_n)$ is finite separable.

By (iv) the isomorphism of graded A-modules $B \simeq \oplus_{i \in I} B'(-\alpha_i)$ holds, where the number of elements $\#I = (m_1 + 1) \cdot \ldots \cdot (m_\mu + 1) \leqslant d^\mu = d^{O(n)}$ and $0 \leqslant \alpha_i \leqslant (m_1 + \ldots + m_\mu) \leqslant (d-1)\mu = O(nd)$.

By (iv) the ring B is generated over k by its homogeneous component B_1 and $\dim_k B_1 \leqslant N + 1$ where $N = n + 1 + \mu = O(n)$. Put $X_{n+1+i} = Z_i$, $1 \leqslant i \leqslant \mu$. Let $\mathbb{P}^N(\overline{k})$ has the homogeneous coordinate functions $X_0, \ldots, X_N$. Then by our construction $\overline{k} \otimes_k B$ is a homogeneous ring of a projective algebraic variety $V' \subset \mathbb{P}^N(\overline{k})$ defined over k and irreducible over $\overline{k}$. Set $\mathfrak{P}'$ to be the homogeneous ideal of the projective algebraic variety V'. Put $f_1 = \Phi$ and

$$\begin{aligned} f_{i+1} = X_n X_{n+1+i}^{m_i+1} + \lambda_{i,1} X_0^{m_i} X_n X_{n+1+i} + \lambda_{i,2} X_0^{m_i} X_1 X_n + \\ \lambda_{i,3} X_0^{m_i} X_2 X_n + \lambda_{i,4} b_i X_{n+1}^2 \in k[X_0, \ldots, X_N], \quad 1 \leqslant i \leqslant \mu, \end{aligned}$$

cf. the formulas for φ_i above. Now $B = k[X_0, \ldots, X_N]/\mathfrak{P}'$,

$$f_1, \ldots, f_{\mu+1} \in k[X_0, \ldots, X_N], \quad \deg f_i < d' = O(d), \ 1 \leqslant i \leqslant \mu+1, \quad N = O(n). \tag{4}$$

Further, $\mathcal{Z}(\mathfrak{P}')$ is a defined over k and irreducible over $\overline{k}$ component of $\mathcal{Z}(f_1, \ldots, f_{\mu+1})$. More precisely, we have the decomposition into the union of two irreducible over $\overline{k}$ components: $\mathcal{Z}(f_1, \ldots, f_{\mu+1}) = \mathcal{Z}(\mathfrak{P}') \cup \mathcal{Z}(X_n, X_{n+1})$. Finally, by our construction $\mathfrak{P}'$ is a primary component of the ideal $(f_1, \ldots, f_{\mu+1}) \subset k[X_0, \ldots, X_N]$, the height $\mathrm{ht}(\mathfrak{P}') = \mu + 1$ and the dimension $\dim \mathcal{Z}(\mathfrak{P}') = n$. Hence assertion (a) of the theorem holds for N, $(f_1, \ldots, f_{\mu+1})$, $\mathfrak{P}'$ (in place of n, $(f_1, \ldots, f_\nu)$, $\mathfrak{p}$).

Let $\alpha = \max_{i \in I} \alpha_i$. Then $\dim_k B_m$ is stable for $m \geqslant m_0$ if and only if $\dim_k B'(-\alpha)_m$ is stable for $m \geqslant m_0$. We have $B' \simeq A \oplus A(-1) \oplus \mathfrak{b}'(-1)$ and $\mathfrak{b}' = A\mathfrak{b} + (X_n)$ where $\mathfrak{b}$ is the ideal from Lemma 1. Hence if $\dim_k B_m$ is stable for $m \geqslant m_0$ then $\dim_k((A^{(0)}/\mathfrak{b})(-\alpha - 1))_m$ is stable for $m \geqslant m_0$. Therefore, $m_0 \geqslant d^{2^{c_1 n}} + \alpha + 1$ by Lemma 1.

REMARK 3 *Let $\mathfrak{P} \subset A$ be a homogeneous prime ideal. Let $A' = A[X_{n+1}, \ldots, X_{n'}]$ for $n' \geqslant n$. Consider the homogeneous prime ideal $\mathfrak{P}' = \mathfrak{P}A' + (X_{n+1}, \ldots, X_{n'}) \subset A'$. Then the Hilbert function of $A/\mathfrak{P}$ is stable for $m \geqslant m_0$ if and only if the Hilbert function of $A'/\mathfrak{P}'$ is stable for $m \geqslant m_0$. Further, the ideal $\mathfrak{P}$ has a system of generators $b_1, \ldots, b_w$ with all $\deg b_i \leqslant v$ if and only if the ideal $\mathfrak{P}'$ has a system of generators $b'_1, \ldots, b'_{w'}$ with all $\deg b'_i \leqslant v$.*

Now one can consider the prime ideal $\mathfrak{P}'' = \mathfrak{P}A'$. The Hilbert function of $A'/\mathfrak{P}''$ is stable for $m \geqslant m_0$ if and only if the Hilbert function of $A'/\mathfrak{P}'$ is stable for $m \geqslant m_0 + n' - n$ (this is proved using the induction on $n' - n$; here m_0 or $m_0 + n' - n$ may be negative).

The integers n, d are arbitrary sufficiently big. Hence from our construction and (4) using Remark 3 and changing the notations (N, $\mathfrak{P}'$, d' by n, $\mathfrak{P}^{(0)}$, d respectively; we leave the details to the reader) we get the following assertion.

(*) *there are constants $c_2 > 0$, $n_0 > 0$, $d_0 > 0$ (they may be distinct from the ones from Lemma 1) such that for all integers $n > n_0$, $d > d_0$ for every infinite field k there are homogeneous polynomials $f_1, \ldots, f_{\mu+1} \in k[X_0, \ldots, X_n]$, $\mu < n$, with all $\deg f_i < d$, and a homogeneous prime ideal $\mathfrak{P}^{(0)} \subset k[X_0, \ldots, X_n]$ satisfying conditions (a) and (b) of Theorem 1 (in place of the polynomials $f_1, \ldots, f_\nu$ and the prime ideal $\mathfrak{p}$) with c_2 in place of c. Besides that, according to our construction the height $\mathrm{ht}(\mathfrak{P}^{(0)}) = \mu + 1 \leqslant n - 1$. The polynomials $f_1, \ldots, f_{\mu+1}$ depend on the choice of the family of elements $\lambda_{i,j}$, $1 \leqslant i \leqslant \mu$, $1 \leqslant j \leqslant 3$, see above. Finally, $\mathfrak{P}^{(0)}$ is a primary component of the ideal $(f_1, \ldots, f_{\mu+1}) \subset k[X_0, \ldots, X_n]$, and the projective algebraic variety $\mathcal{Z}(f_1, \ldots, f_{\mu+1})$ has exactly two irreducible over $\overline{k}$ components: $\mathcal{Z}(\mathfrak{P}^{(0)})$ and some linear subspace $\mathcal{L}^{(0)} \subset \mathbb{P}^n(\overline{k})$ defined over k.*

3 Proof of Theorem 1: condition (c)

Now our aim is to consider (a), (b) and (c) together.

REMARK 4 *It would be interesting to ascertain that $\mathfrak{P}^{(0)}$ also satisfies (c) with a constant $c_3 > 0$ in place of c, and after that take $c = \min\{c_2, c_3\}$ (actually $c_2 \geqslant c_3$). Since $3\mu = O(n)$ from here one could deduce similarly to the proof of Proposition 1, see below at the end of the section, that Theorem 1 is true also for any finite field k, i.e., without any restrictions on the field k.*

But we shall obtain another result which is sufficient to prove the theorem.

Let us identify the set of all $(n-s)$-tuples $(L_{s+1}, \ldots, L_n)$ of linear forms $L_j \in \overline{k}[X_0, \ldots, X_n]$, $s \leqslant j \leqslant n$, with $\mathbb{A}^{(n+1)(n-s)}(\overline{k})$.

Let $\mathfrak{P} \subset A$ be an arbitrary homogeneous prime ideal of height $s = \mathrm{ht}(\mathfrak{P})$, $0 \leqslant s \leqslant n-1$, and of degree $\deg \mathfrak{P} = d$. Let $V = \mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ be the projective algebraic variety of all common zeroes of the polynomials from $\mathfrak{P}$ in $\mathbb{P}^n(\overline{k})$. Hence $\dim V = n - s$. We shall suppose additionally that the ideal $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ is radical or which is equivalent the variety V is defined over k. Denote by $\mathfrak{M} = (X_0, \ldots, X_n)$ the maximal homogeneous prime ideal of A. The following lemma is known for the case when the algebraic variety $\mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ is irreducible over $\overline{k}$ (and actually this case is sufficient for our aims). Still we would like to prove it in the general case.

LEMMA 3 *There is a nonempty open in the Zariski topology subset* $\mathcal{U} \subset \mathbb{A}^{(n+1)(n-s)}(\overline{k})$ *satisfying the following properties. Let an* $(n-s)$*-tuple of linear forms* $(L_{s+1}, \dots, L_n) \in \mathcal{U}$ *and all* $L_j \in A$. *Then*

(i) *for every integer* $s \leqslant i \leqslant n$ *the intersection* V *and* $\mathcal{Z}(L_{s+1}, \dots, L_i)$ *is transversal or which is equivalent in the considered case the dimension* $\dim(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i)) = n - i$ *and the degree* $\deg V = \deg(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i))$;

(ii) *for every integer* $s \leqslant i < n$ *the number of irreducible over* $\overline{k}$ *components of* $V_i = V \cap \mathcal{Z}(L_{s+1}, \dots, L_i)$ *is equal to the number of irreducible over* $\overline{k}$ *components of* V;

(iii) *for every integer* $s \leqslant i \leqslant n$ *the algebraic variety* V_i *is defined over* k;

(iv) *for every integer* $s \leqslant i < n$ *the projective algebraic variety* V_i *is irreducible over* k *and corresponds to a homogeneous prime ideal* $\mathfrak{P}_{L_{s+1},\dots,L_i} \subset k[X_0, \dots, X_n]$ *of height* i;

(v) *for* $i = n$ *the projective algebraic variety* V_n *is a defined over* k *finite number of points in* $\mathbb{P}^n(\overline{k})$ *corresponding to a homogeneous radical ideal* $\mathfrak{P}_{L_{s+1},\dots,L_n} \subset k[X_0, \dots, X_n]$;

(vi) *hence the ideal* $\overline{k} \otimes_k \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \overline{k} \otimes_k A$ *is radical for all* $s+1 \leqslant i \leqslant n$;

(vii) *for every* $s+1 \leqslant i \leqslant n$

$$\mathfrak{P} + (L_{s+1}, \dots, L_i) = \mathfrak{P}_{L_{s+1},\dots,L_i} \cap \mathfrak{Q}_{L_{s+1},\dots,L_i},$$

where $\mathfrak{Q}_{L_{s+1},\dots,L_i}$ *is an* $\mathfrak{M}$*-primary ideal or* $\mathfrak{Q}_{L_{s+1},\dots,L_i} = A$;

(viii) *hence* $X_j^N \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \mathfrak{P} + (L_{s+1}, \dots, L_i)$ *for all* $0 \leqslant j \leqslant n$ *and all sufficiently big* $N \geqslant 0$.

PROOF There is a nonempty open in the Zariski topology subset $\mathcal{U}^{(0)} \subset \mathbb{A}^{(n-s)(n+1)}(\overline{k})$ such that for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}^{(0)}$ the intersection V and $\mathcal{Z}(L_{s+1}, \dots, L_n)$ is transversal, i.e., (i) holds (here we leave the details to the reader). Let $\overline{k} \otimes_k \mathfrak{P} = \bigcap_{j \in J} \mathfrak{p}_j$ be the irredundant primary decomposition of the ideal $\overline{k} \otimes_k \mathfrak{P}$, where all $\mathfrak{p}_j \subset \overline{k} \otimes_k A$, $j \in J$, are prime ideals. Then it is known (it is a corollary of the first Bertini theorem), see e.g., the Appendix of [4], that if one replaces $\mathcal{U}$, k, A, $\mathfrak{P}$ by $\mathcal{U}_j$, $\overline{k}$, $\overline{k}[X_0, \dots, X_n]$, $\mathfrak{p}_j$ (for an arbitrary but fixed $j \in J$) respectively then assertion (i)–(v), (vii), (viii) hold. Put $\mathcal{U} = \mathcal{U}^{(0)} \cap \bigcap_{j \in J} \mathcal{U}_j$.

Let $(L_{s+1}, \dots, L_n) \in \mathcal{U}$. Now (i) and (ii) are satisfied. The homogeneous ideal of the algebraic variety V_i is $\bigcap_{j \in J} \mathfrak{p}_{j, L_{s+1},\dots,L_i}$. We have $\overline{k} \otimes_k \mathfrak{P} + (L_{s+1}, \dots, L_n) \overline{k} \otimes_k A \subset \bigcap_{j \in J} (\mathfrak{p}_j + (L_{s+1}, \dots, L_n) \overline{k} \otimes_k A)$. Hence by (vii) for $\mathfrak{p}_j$ the equality

$$\overline{k} \otimes_k \mathfrak{P} + (L_{s+1}, \dots, L_n) \overline{k} \otimes_k A = \bigcap_{j \in J} \mathfrak{p}_j \cap \mathfrak{Q}' \qquad (5)$$

holds, where $\mathfrak{Q}'$ is an $\overline{k} \otimes_k \mathfrak{M}$-primary ideal or $\mathfrak{Q}' = \overline{k} \otimes_k A$.

Let us prove (iii). There is a nonzero linear form $L_0 \in A$ such that $V_i \setminus \mathcal{Z}(L_0)$ is a dense open in the Zariski topology subset in V_i. By (5) the ring of defined over $\overline{k}$ regular functions on $V_i \setminus \mathcal{Z}(L_0)$ is $\overline{k}[V \setminus \mathcal{Z}(L_0)]/(L_{s+1}/L_0, \dots, L_i/L_0)$.

Hence $V_i \setminus \mathcal{Z}(L_0)$ is defined over k. Denote by k_s the separable closure of k. Therefore, the set of points $(V_i \setminus \mathcal{Z}(L_0))(k_s)$ is a dense with respect to the Zariski topology and invariant with respect to the action of the Galois group $\mathrm{Gal}(\overline{k}/k)$ subset of V_i. Hence by the known criterion V_i is defined over k. Assertion (iii) is proved. Now also (v) holds.

Let us prove (iv). The Galois group $\mathrm{Gal}(\overline{k}/k)$ acts transitively on the irreducible over $\overline{k}$ components $\mathcal{Z}(\mathfrak{p}_{j,L_{s+1},\ldots,L_i})$ of the algebraic variety V_i. Hence V_i is irreducible over k and (iv) is proved. Now also (vi) is proved.

Let us prove (viii). By (5) we have

$$X_j^N \mathfrak{P}_{L_{s+1},\ldots,L_i} \subset (\overline{k} \otimes_k \mathfrak{P} + (L_{s+1},\ldots,L_i)\overline{k} \otimes_k A) \cap A = \mathfrak{P} + (L_{s+1},\ldots,L_i)$$

and (viii) is proved. Obviously (viii) implies (vii). The lemma is proved.

Let $u = \{u_{i,j}\}$, $i \in \{0, s+1, s+2, \ldots, n+1\}$, $0 \leqslant j \leqslant n$, be a family of algebraically independent elements over the field k, i.e., the transcendency degree of this family over k is $(n-s+2)(n+1)$. Denote by $k_u = k(u)$ the extension of the field k by the elements of the family u. Put $U_i = \sum_{0 \leqslant j \leqslant n} u_{i,j} X_j \in k_u[X_0,\ldots,X_n]$, $s+1 \leqslant i \leqslant n$, to be the family of generic linear forms over k. Then the $(n-s)$-tuple $(U_{s+1},\ldots,U_n)$ is a generic point of $\mathcal{U}$, see Lemma 3, and $(U_{n+1},\ldots,U_n) \in \mathcal{U}(\overline{k_u})$. Let us extend the ground field k till k_u. We shall denote again by $\mathfrak{P}$ the ideal of $k_u \otimes_k \mathfrak{P} \subset k_u \otimes_k A$ (this will not lead to an ambiguity). Now the ideals $\mathfrak{P}_{U_{s+1},\ldots,U_i}$ are defined for all $s \leqslant i \leqslant n$.

Denote by $k[u]$ the polynomial ring with coefficients from k and variables from the family u. Denote by $k[u, X_0, \ldots, X_n]$ the polynomial ring coefficients from k and variables from the families u and $X_0, \ldots, X_n$ (the similar notation will be used with other variables). Let $s+1 \leqslant i \leqslant n$ be an integer. Denote for brevity $\mathfrak{P}_{i-1} = \mathfrak{P}_{U_{s+1},\ldots,U_{i-1}}$, $\mathfrak{P}_i = \mathfrak{P}_{U_{s+1},\ldots,U_i}$. Put

$$k_u'' = \left\{ P/Q \in k_u \,:\, P, Q \in k[u] \,\&\, \deg_{u_{i,n}} P \leqslant 0,\, \deg_{u_{i,n}} Q = 0 \right\},$$

i.e., k_u'' is the subfield of k_u of all the elements which do not depend on $u_{i,n}$. Notice that the ideal $\mathfrak{P}_{i-1}$ has a system of generators $p_1, \ldots, p_\gamma \in k_u''[X_0, \ldots, X_n]$ (actually one can choose all $p_j \in k[u, X_0, \ldots, X_n]$ with $\deg_{u_{i_1,j_1}} p_j = 0$ for all $i_1 \in \{0, i, \ldots, n+1\}$, $0 \leqslant j_1 \leqslant n$). Let us define the multiplicatively closed sets

$$\begin{aligned}
&S_{\mathfrak{P}_{i-1}} = k_u''[X_0,\ldots,X_n] \setminus (p_1,\ldots,p_\gamma) \subset k_u''[X_0,\ldots,X_n],\\
&S_{i,n} = k[u, X_0,\ldots,X_n] \setminus U_i k[u, X_0,\ldots,X_n] \subset k[u, X_0,\ldots,X_n],\\
&S = \{X_n^i \,:\, 0 \leqslant i \in \mathbb{Z}\} \subset k[X_0,\ldots,X_n].
\end{aligned}$$

The localization $S_{i,n}^{-1} k[u, X_0, \ldots, X_n] \supset k_u[X_0, \ldots, X_n]$. If $z \in S_{i,n}^{-1} k[u, X_0, \ldots, X_n]$ then one can substitute $u_{i,n} = (-\sum_{0 \leqslant i \leqslant n-1} u_{i,j} X_j)/X_n$ in z. Denote by $\pi(z)$ the result of this substitution. Then obviously $\pi(z) \in k_u''(X_0, \ldots, X_n)$ and the mapping $z \mapsto \pi(z)$ is the homomorphism k_u''-algebras $\pi : S_{i,n}^{-1} k[u, X_0, \ldots, X_n] \to k_u''(X_0, \ldots, X_n)$. If $z \in k_u''(X_0, \ldots, X_n)$ then $\pi(z) = z$. Obviously the kernel $\mathrm{Ker}(\pi) = U_i S_{i,n}^{-1} k[X_0, \ldots, X_n]$.

LEMMA 4 *Under previous conditions suppose that $X_n \notin \mathfrak{P}$. Then for every $z \in k_u[X_0, \ldots, X_n]$ the element $\pi(z) \in S_{\mathfrak{P}_{i-1}}^{-1} k_u''[X_0, \ldots, X_n]$. Further, if $z \in \mathfrak{P}_i$ then $\pi(z) \in S_{\mathfrak{P}_{i-1}}^{-1}(k_u''[X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1})$. Finally, if $z \in k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_i$ then $\pi(z) \in S^{-1}(k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1})$.*

PROOF Let $z \in k_u[X_0, \dots, X_n]$. Then $z = P/Q$ where $0 \neq Q \in k[u]$, $P \in k[u, X_0, \dots, X_n]$. We have $\pi(P) \in S^{-1}k''_u[X_0, \dots, X_n] \subset S^{-1}_{\mathfrak{P}_{i-1}}k''_u[X_0, \dots, X_n]$. Let $\deg_{u_{i,n}} Q = r$. Then $X_n^r\pi(Q) \in k''_u[X_0, \dots, X_n]$. Hence it is sufficient to prove that $X_n^r\pi(Q) \in S_{\mathfrak{P}_{i-1}}$. The definition of the homomorphism π implies $\pi(Q) = q((-\sum_{0\leqslant j\leqslant n-1} X_j u_{i,j})/X_n)$ for a polynomial $0 \neq q \in k''_u[Z]$. Denote by $k_u(\mathcal{Z}(\mathfrak{P}_{i-1}))$ the field of defined over k_u rational functions on the variety $\mathcal{Z}(\mathfrak{P}_{i-1}) \subset \mathbb{P}^n(\overline{k_u})$. We have $X_n \notin \mathfrak{P}$ and $U_{s+1}, \dots, U_{i-1}$ are generic linear forms. Hence X_n does not vanish at the generic point of the algebraic variety $\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(U_{s+1}, \dots, U_{i-1}) \subset \mathbb{P}^n(\overline{k_u})$. Therefore, $X_n \notin \mathfrak{P}_{i-1}$ and obviously $i - 1 < n$. Let

$$k'''_u = \left\{ P/Q \in k_u \,:\, P, Q \in k[u] \,\&\, \deg_{u_{i,j}} P \leqslant 0,\, \deg_{u_{i,j}} Q = 0,\, 0 \leqslant j \leqslant n \right\},$$

i.e., k'''_u is the subfield of k_u of all the elements which do not depend on all $u_{i,j}$, $0 \leqslant j \leqslant n$. The algebraic variety $\mathcal{Z}(\mathfrak{P}_{i-1})$ is defined over k'''_u by Lemma 3 with the ground field k'''_u in place of k. Hence

$$-\sum_{0\leqslant j\leqslant n-1} u_{i,j}(X_j/X_n) \in k_u(\mathcal{Z}(\mathfrak{P}_{i-1}))$$

is a transcendental element over the field k_u. Therefore, $X_n^r\pi(Q) \notin \mathfrak{P}_{i-1}$. The required assertion is proved.

Let $z \in \mathfrak{P}_i$. Then $z \in S^{-1}(\mathfrak{P}_{i-1} + (U_i))$ by Lemma 3 (viii) with the ground field k_u in place of k. Hence one can represent $z = \sum_{1\leqslant j\leqslant\gamma} p_j q_j + U_i q$ where p_j are introduced above, all $q_j, q \in S^{-1}k_u[X_0, \dots, X_n]$. Therefore,

$$\pi(z) = \sum_{1\leqslant j\leqslant\gamma} p_j \pi(q_j) \in S^{-1}_{\mathfrak{P}_{i-1}}(k''_u[X_0, \dots, X_n] \cap \mathfrak{P}_{i-1}).$$

Let $z \in k[u, X_0, \dots, X_n] \cap \mathfrak{P}_{i-1}$. Then by the proved

$$\pi(z) \in S^{-1}k[u, X_0, \dots, X_n] \cap S^{-1}_{\mathfrak{P}_{i-1}}\mathfrak{P}_{i-1} = S^{-1}(k[u, X_0, \dots, X_n] \cap \mathfrak{P}_{i-1}).$$

The last assertion and all the lemma are proved.

LEMMA 5 *Under previous notation suppose that for some $s+1 \leqslant i \leqslant n-1$ the ideal $\mathfrak{P}_{U_{s+1},\dots,U_i}$ has a system of generators of degrees with respect to $X_0, \dots, X_n$ at most D where $D \geqslant 2$. Then the following assertions hold.*

- *(i) There is a system of generators $q_1, \dots, q_\beta \in k[u, X_0, \dots, X_n]$ of the ideal $\mathfrak{P}_{U_{s+1},\dots,U_i}$ such that $\deg_{X_0,\dots,X_n} q_j \leqslant D$ and $\deg_{u_{v,w}} q_j = (Dd)^{O(n-i)}$ for all v, w (here and below $\deg_{u_{w,v}}$ is the degree with respect to the variable $u_{w,v}$) with an universal constant in $O(n-i)$.*
- *(ii) There is a nonempty open in the Zariski topology subset $\mathcal{U}'_i \subset \mathcal{U}$ satisfying the following properties. There is an absolute constant $c'_4 > 0$ such that for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}'_i$ the ideal*

  $$X_j^N \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i) \qquad (6)$$

  for an integer $N \leqslant (Dd)^{c'_4(n-i)}$. Hence there is an absolute constant $c_4 > 0$ such that for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}'_i$ for all $m \geqslant (Dd)^{c_4(n-i)}$ the homogeneous components $(\mathfrak{P}_{L_{s+1},\dots,L_i})_m$ and $(\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i))_m$ (of the ideals $\mathfrak{P}_{L_{s+1},\dots,L_i}$ and $\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i)$) coincide.

PROOF Let us prove (i). Consider the morphism $\pi_U : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \ldots : X_n) \mapsto (U_0 : U_{s+1} : \ldots : U_{n+1})$ of projective algebraic varieties. Then, cf. [3], the image $\pi_U(\mathcal{Z}(\mathfrak{P}))$ is closed in $\mathbb{P}^{n-s+1}(\overline{k_u})$ and defined over k_u, $\deg \pi_U(\mathcal{Z}(\mathfrak{P})) = d$. Further, $\pi_U(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_{\mathfrak{P}})$ where $F_{\mathfrak{P}} \in k[u, Z_0, Z_{s+1}, \ldots, Z_n]$ is a homogeneous polynomial with respect to $Z_0, Z_{s+1}, \ldots, Z_n$ such that $F_{\mathfrak{P}}(U_0, U_{s+1}, \ldots, U_{n+1})$ vanishes on $\mathcal{Z}(\mathfrak{P})$ in $\mathbb{P}^n(\overline{k_u})$, the degree $\deg F_{\mathfrak{P}} = d$ and the leading coefficient $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P}} \in k[u]$ (here we denote by $\mathrm{lc}_{Z_n} F_{\mathfrak{P}}$ the leading coefficient of $F_{\mathfrak{P}}$ with respect to Z_{n+1}). Since $\pi_U(\mathcal{Z}(\mathfrak{P}))$ is defined over k_u and irreducible over k_u the polynomial $F_{\mathfrak{P}}$ does not have multiple factors over $\overline{k_u}$ and is irreducible over k_u. Since $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P}} \in k[u]$ the polynomial $F_{\mathfrak{P}}$ is separable with respect to Z_{n+1}, i.e., $\partial F_{\mathfrak{P}}/\partial Z_{n+1} \neq 0$. Besides that, cf. [3], the morphism $\mathcal{Z}(\mathfrak{P}) \to \pi_U(\mathcal{Z}(\mathfrak{P}))$ induced by π_U is a finite separable and birational morphism of defined over k_u projective algebraic varieties.

The polynomial $F_{\mathfrak{P}}$ is uniquely defined up to factor from $k[u]$. In what follows we shall assume without loss of generality that GCD of all the coefficients from $k[u]$ at the monomials in $X_0, \ldots, X_n$ of the polynomial $F_{\mathfrak{P}}$ is 1. So we fix $F_{\mathfrak{P}}$ up to a nonzero factor from k. We have $\deg_{u_{i,0},\ldots,u_{i,n}} F_{\mathfrak{P}} = d$ for every $i \in \{0, s+1, s+2, \ldots, n+1\}$, see [3] Lemma 9.

Let $L_0, L_{s+1}, \ldots, L_{n+1} \in k[u, X_0, \ldots, X_n]$ be linear forms with respect to $X_0, \ldots, X_n$ in general position. Denote $L = (L_0, L_{s+1}, \ldots, L_{n+1})$. Let $L_i = \sum_{0 \leqslant j \leqslant n} l_{i,j} X_j$ where the coefficients $l_{i,j} \in k_u$ for all i, j. Let us substitute $u_{i,j} = l_{i,j}$ for all i, j in $F_{\mathfrak{P}}$. Denote the obtained polynomial by $F_{\mathfrak{P},L} \in k[u, X_0, \ldots, X_n]$. Since $L_0, L_{s+1}, \ldots, L_{n+1}$ are in general position the polynomial $F_{\mathfrak{P},L}$ is separable with respect to Z_{n+1}, $\deg F_{\mathfrak{P},L} = \deg_{Z_{n+1}} F_{\mathfrak{P},L} = d$, $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P},L} \in k[u]$ and the polynomial $F_{\mathfrak{P},L}(L_0, L_{s+1}, \ldots, L_{n+1})$ vanishes on $\mathcal{Z}(\mathfrak{P})$. Further, denote by $\pi_L : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+1} : \ldots : L_{n+1})$ the morphism of projective algebraic varieties. Then the image $\pi_L(\mathcal{Z}(\mathfrak{P}))$ is closed in $\mathbb{P}^{n-s+1}(\overline{k_u})$ and defined over k_u, $\deg \pi(\mathcal{Z}(\mathfrak{P})) = d$ and $\pi_L(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_{\mathfrak{P},L})$. Besides that, the morphism $\mathcal{Z}(\mathfrak{P}) \to \pi_L(\mathcal{Z}(\mathfrak{P}))$ induced by π_L is a finite separable and birational morphism of defined over k_u projective algebraic varieties. In particular the polynomial $F_{\mathfrak{P},L}$ is irreducible over k_u.

Let $s \leqslant i \leqslant n-1$. Put $L' = (L_0, U_{s+1}, \ldots, U_i, L_{i+1}, \ldots, L_{n+1})$ where all $L_i \in k[X_0, \ldots, X_n]$ are linear forms in general position. Recall the notation $\mathfrak{P}_i = \mathfrak{P}_{U_{s+1},\ldots,U_i}$. Since L_0 is in general position we shall suppose in what follows without loss of generality that L_0 does not vanish on any irreducible over $\overline{k}$ component of $\mathcal{Z}(\mathfrak{P}_i)$. The polynomial $F' = F_{\mathfrak{P},L'}(Z_0, 0, \ldots, 0, Z_{i+1}, \ldots, Z_{n+1}) \in k_u[Z_0, Z_{i+1}, \ldots, Z_{n+1}]$ (here we substitute 0 for U_j, $s+1 \leqslant j \leqslant i$) is nonzero of degree d since the leading coefficient of F' with respect to Z_{n+1} is a nonzero polynomial from $k[u]$. Obviously the polynomial F' vanishes on $\mathcal{Z}(\mathfrak{P}_i)$. Since linear forms L_i are in general position the polynomial $F_{\mathfrak{P}_i,(L_0,L_{i+1},\ldots,L_{n+1})}$ is defined and satisfies the properties analogous to the ones of the polynomial $F_{\mathfrak{P},L}$, see above. Now $F_{\mathfrak{P}_i,(L_0,L_{i+1},\ldots,L_{n+1})}$ coincides with F' up to a factor $f' \in k[u]$. In particular the polynomial F' is irreducible over k_u.

Let us replace F' by F'/f'. Denote by k'_u the subfield of k_u generated over k by the elements of the family $u' = \{u_{v,j}\}$, $s+1 \leqslant v \leqslant i$, $0 \leqslant j \leqslant n$. Now all the coefficients of F' belong to k'_u

Put $t_j = L_j/L_0$, $i+1 \leqslant j \leqslant n$, and $\Psi = F'(1, t_{i+1}, \ldots, t_n, Z) \in k[u, t_{i+1}, \ldots, t_n, Z]$. The polynomial $\Psi \in k_u(t_{i+1}, \ldots, t_n)[Z]$ is irreducible and separable with respect to Z, $\deg_Z \Psi = d$, $0 \neq \mathrm{lc}_Z \Psi \in k[u]$. Hence the field of defined over k_u rational functions $k_u(\mathcal{Z}(\mathfrak{P}_i)) \simeq k_u(t_{i+1}, \ldots, t_n)[Z]/(\Psi)$ according to the described construction. Put

$$\theta = Z \bmod \Psi \in k_u(t_{i+1}, \ldots, t_n)[Z]/(\Psi) \simeq k_u(\mathcal{Z}(\mathfrak{P}_i)). \tag{7}$$

Obviously the coefficients of Ψ belong to k'_u.

Put $L'' = (L_0, U_{s+1}, \ldots, U_i, L_{i+1}, \ldots, L_n, U_{n+1})$ where the linear forms $L_{i+1}, \ldots, L_n$ be the as above. Put $F'' = F_{\mathfrak{P}, L''}(Z_0, 0, \ldots, 0, Z_{i+1}, \ldots, Z_{n+1}) \in k_u[Z_0, Z_{i+1}, \ldots, L_n]$ (here we substitute 0 for U_j, $s+1 \leqslant j \leqslant i$). The rational function $F''(1, t_{i+1}, \ldots, t_n, U_{n+1}/L_0)$ vanishes on $\mathcal{Z}(\mathfrak{P}_i) \setminus \mathcal{Z}(L_0)$. Hence there is a root $Z = \xi_U$ of the polynomial $F''(1, t_{i+1}, \ldots, t_n, Z)$ in the field $k_u(t_{i+1}, \ldots, t_n)[\theta]$ of the form

$$\xi_U = \frac{1}{\xi^{(0)}} \sum_{0 \leqslant v \leqslant n} \left(\sum_{0 \leqslant j < \deg_Z \Psi} \xi_{v,j} \theta^j \right) u_{n+1,v},$$

where all $\xi^{(0)}, \xi_{v,j} \in k[u', t_{i+1}, \ldots, t_n]$, $0 \leqslant j \leqslant n$, $\xi^{(0)} \neq 0$, and the greatest common divisor $\mathrm{GCD}_{v,j}\{\xi^{(0)}, \xi_{v,j}\} = 1$ in the ring $k[u', t_{i+1}, \ldots, t_n]$.

Thus, there is a generic point of the algebraic variety $\mathcal{Z}(\mathfrak{P}_{U_{s+1}, \ldots, U_i}) \subset \mathbb{P}^n(\overline{k_u})$ of the form

$$\frac{X_v}{L_0} = \xi_v = \frac{1}{\xi^{(0)}} \sum_{0 \leqslant j < \deg_Z \Psi} \xi_{v,j} \theta^j \in k'_u(t_{i+1}, \ldots, t_n)[\theta], \quad 0 \leqslant v \leqslant n, \tag{8}$$

According to the algorithm for factoring polynomials, see [2]: $\deg_Z \Psi = d$, all the degrees

$$\deg_{t_j} \Psi,\ \deg_{u_{v,w}} \Psi,\ \deg_{t_j} \xi^{(0)},\ \deg_{t_j} \xi_{v,j},\ \deg_{u_{v,w}} \xi^{(0)},\ \deg_{u_{v,w}} \xi_{v,j}$$

are bounded from above by $(d+1)^{O(1)}$, with an absolute constant in $O(1)$ for all j v, w.

Denote by I_δ be the set of all $(i_0, \ldots, i_n)$ such that all $i_w \geqslant 0$ are integers and $i_0 + \ldots + i_n = \delta$. Let

$$F = \sum_{(i_0, \ldots, i_n) \in I_\delta} F_{i_0, \ldots, i_n} X_0^{i_0} \cdot \ldots \cdot X_n^{i_n}$$

be a homogeneous polynomial of degree $\delta \leqslant D$ with arbitrary coefficients $F_{i_0, \ldots, i_n}$ from the field k_u. Then the relation

$$F(\xi_0, \ldots, \xi_n) = 0 \tag{9}$$

holds if and only if F vanishes on $\mathcal{Z}(\mathfrak{P}_{U_{s+1}, \ldots, U_i})$. Denote by J_0 the set of all $j = (j_{i+1}, \ldots, j_n, j_0)$ such that all $j_w \geqslant 0$ are integers and $0 \leqslant j_0 < \deg \Psi$. Then by (8), (7) equality (9) is equivalent to

$$\sum_{j \in J_0} \left(\sum_{(i_0, \ldots, i_n) \in I_\delta} a_{j, i_0, \ldots, i_n} F_{i_0, \ldots, i_n} \right) t_{i+1}^{j_{i+1}} \cdot \ldots \cdot t_n^{j_n} \theta^{j_0} = 0, \tag{10}$$

where all $a_{j, i_0, \ldots, i_n} \in k[u]$ and the greatest common divisor $\mathrm{GCD}_{j, i_0, \ldots, i_n}\{a_{j, i_0, \ldots, i_n}\} = 1$ in $k[u]$. Further, the ascertained bounds for degrees of ξ_v and Ψ imply that for every nonzero $a_{j,i_0,\dots,i_n}$ each index $j_\alpha = (Dd)^{O(1)}$, $i+1 \leqslant \alpha \leqslant n$, and the degrees $\deg_{u_{v,w}} a_{j,i_0,\dots,i_n} = (Dd)^{O(1)}$ for all v, w. Hence there is a subset $J_1 \subset J_0$ such that the number of elements $\#J_1 = (Dd)^{O(n-i)}$ and if $a_{j,i_0,\dots,i_n} \neq 0$ then $j \in J_1$. Therefore, considering the coefficients $F_{i_0,\dots,i_n}$ as unknowns we get from (10) a linear system $\sum_{(i_0,\dots,i_n)\in I_\delta} a_{j,i_0,\dots,i_n} F_{i_0,\dots,i_n} = 0$, $j \in J_1$, with respect to $F_{i_0,\dots,i_n}$ with coefficients $a_{j,i_0,\dots,i_n} \in k_u$. Solving this linear system we find a basis $y_1, \dots, y_\gamma \in k[u, X_0, \dots, X_n]$ over the field k_u of the homogeneous component $(\mathfrak{P}_{U_{s+1},\dots,U_i})_\delta$ of degree δ of the ideal $\mathfrak{P}_{U_{s+1},\dots,U_i}$. According to the algorithm for solving linear systems we get $\deg_{u_{v,w}} y_j = (Dd)^{O(n-i)}$ for all v, w and $1 \leqslant j \leqslant \gamma$. Assertion (i) is proved.

Let us prove (ii). Let $y = y_j$ for some $1 \leqslant j \leqslant \gamma$, $\delta \leqslant D$. We shall suppose without loss of generality performing if necessarily a nondegenerate linear transformation of the coordinate functions $X_0, \dots, X_n$ over k that $X_i \notin \mathfrak{P}$ for every $0 \leqslant i \leqslant n$ (after this replacement the integer N for old coordinate functions will be $(n+1)N - n$). Then, see Lemma 4, $\pi(y) \in S^{-1}(\mathfrak{P}_{i-1} \cap k[u, X_0, \dots, X_n])$ and hence $y - \pi(y) \in U_i S^{-1} k[u, X_0, \dots, X_n]$. We have proved that $\deg_{u_{i,n}} y = (Dd)^{O(n-i)}$ with an absolute constant in $O(n-i)$. Therefore, $X_n^N \pi(y) \in \mathfrak{P}_{U_{s+1},\dots,U_{i-1}} \cap k[u, X_0, \dots, X_n]$ for an integer $N = (Dd)^{O(n-i)}$. Hence $X_n^N(y - \pi(y)) \in U_i k[u, X_0, \dots, X_n]$. Thus $X_n^N \mathfrak{P}_{U_{s+1},\dots,U_i} \subset \mathfrak{P}_{U_{s+1},\dots,U_{i-1}} + (U_i)$. Similarly we have $X_j^N \mathfrak{P}_{U_{s+1},\dots,U_i} \subset \mathfrak{P}_{U_{s+1},\dots,U_{i-1}} + (U_i)$ for every $0 \leqslant j \leqslant n$.

Let $\delta_1 = \delta + N$. We have constructed a basis $y_1, \dots, y_\gamma$ of the homogeneous component $(\mathfrak{P}_{U_{s+1},\dots,U_i})_\delta$ over the field k_u. In the similar way we can construct a basis $y'_1, \dots, y'_\sigma \in k[u, X_0, \dots, X_n]$ of the homogeneous component $(\mathfrak{P}_{U_{s+1},\dots,U_{i-1}})_{\delta_1}$. Now for all ρ, j one can represent

$$X_\rho^N y_j = \sum_{1\leqslant\alpha\leqslant\sigma} b_{\rho,j,\alpha} y'_\alpha, \quad b_{\rho,j,\alpha} \in k_u. \tag{11}$$

To complete the proof we use "the specialization of parameters" $u_{v,j}$. We leave to the reader to check that the described explicit construction admits "the specialization of parameters", i.e., if $(l_{v,j})$ belong to a nonempty open in the Zariski topology subset of $\mathbb{A}^{(n-s+2)(n+1)}(\overline{k})$ then one can substitute $u_{v,j} = l_{v,j} \in k$ in (7), (8) and get a generic point of the variety $\mathcal{Z}(\mathfrak{P}_{L_{s+1},\dots,L_i})$ with all $L_v = \sum_{0\leqslant j\leqslant n} l_{v,j} X_j$. Here Lemma 3 is also used. Further, again for a nonempty open in the Zariski topology subset one can substitute $u_{v,j} = l_{v,j}$ in $y_1, \dots, y_\gamma$ and get the basis over the field k of the homogeneous component $(\mathfrak{P}_{L_{s+1},\dots,L_i})_\delta$ of degree δ of the ideal $\mathfrak{P}_{L_{s+1},\dots,L_i}$. This follows from the algorithm for solving linear systems. The similar assertion is fulfilled for the basis $y'_1, \dots, y'_\sigma$ of the homogeneous component $(\mathfrak{P}_{L_{s+1},\dots,L_{i-1}})_{\delta_1}$ of the ideal $\mathfrak{P}_{L_{s+1},\dots,L_{i-1}}$. For all $0 \leqslant \delta \leqslant D$ formulas (11) related to generic point $(u_{v,i})$ also admit "the specialization of parameters". Finally, notice that we have the natural linear projection

$$\begin{aligned} \varepsilon \,:\, \mathbb{A}^{(n-s+2)(n+1)}(\overline{k}) &\to \mathbb{A}^{(n-s)(n+1)}(\overline{k}), \\ (L_0, L_{s+1}, \dots, L_{n+1}) &\mapsto (L_{s+1}, \dots, L_n), \end{aligned}$$

and for every open in the Zariski topology subset of $\mathcal{W}$ of the affine space $\mathbb{A}^{(n-s+2)(n+1)}(\overline{k})$ its image $\varepsilon(\mathcal{W})$ is open in the Zariski topology in the affine space $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$. So now using this projection ε we get the required subset $\mathcal{U}'_i$. Thus, assertion (ii) and all the lemma are proved.

LEMMA 6 *Under previous notation let $s = \mathrm{ht}(\mathfrak{P}) = n - 1$. Let $\mathcal{U} \subset \mathbb{A}^n(\overline{k})$ be the open in the Zariski topology subset of linear forms corresponding to the* *prime ideal $\mathfrak{P}$, see above. Then for every $L_n \in \mathcal{U}$ the characteristic function $h(\mathfrak{P}_{L_n}, m) = \dim_k (A/\mathfrak{P}_{L_n})_m$ is stable for $m \geqslant (n-1)d - n + 2$. Further, for all $m \geqslant (n-1)d - n + 2$ we have the equality*

$$(\mathfrak{P}_{L_n})_m = (\mathfrak{P} + (L_n))_m \tag{12}$$

of homogeneous components of the degree m of the ideals $\mathfrak{P}_{L_n}$ and $\mathfrak{P} + (L_n)$.

PROOF There are homogeneous polynomials $F_1, \ldots, F_m \in k[X_0, \ldots, X_n]$ of the same degree d such that $\mathcal{Z}(\mathfrak{P}) = \mathcal{Z}(F_1, \ldots, F_m)$ in $\mathbb{P}^n(\overline{k})$ and $\mathfrak{P}$ is a $\mathfrak{P}$-primary component of the ideal $(F_1, \ldots, F_m) \subset k[X_0, \ldots, X_n]$, cf. [2], [3]. Then for a linear form $L_n \in \mathcal{U}$ the ideal $\mathfrak{P} + (L_n) \supset (F_1, \ldots, F_m, L_n) = \mathfrak{P}_{L_n} \cap \mathfrak{Q}$ where $\mathfrak{Q}$ is an $\mathfrak{M}$-primary ideal or $\mathfrak{Q} = k[X_0, \ldots, X_n]$. Hence, see [8], the homogeneous components $(F_1, \ldots, F_m, L_n)_m = (\mathfrak{P}_{L_n})_m$ of the ideals $(F_1, \ldots, F_m, L_n)$ and $\mathfrak{P}_{L_n}$ coincide for $m \geqslant (n-1)d - n + 2$ and (12) holds. Therefore, see [8], the characteristic function $h(\mathfrak{P}_{L_n}, m)$ is stable for $m \geqslant (n-1)d - n + 2$, cf. also Lemma 8 below. The lemma is proved.

LEMMA 7 *Suppose that the conditions of Lemma 5 hold for all $s+1 \leqslant i \leqslant n-1$ with the same D. Put $\mathcal{U}' = \bigcap_{s+1 \leqslant i \leqslant n-1} \mathcal{U}'_i$, see Lemma 5 (ii) and*

$$D_1 = \max\{(Dd)^{c_4(n-s-1)}, sd - s\}.$$

Then for every $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$ for every $s \leqslant i \leqslant n-1$ the characteristic function

$$h(\mathfrak{P}_{L_{s+1}, \ldots, L_i}, m) = \dim_k (A/\mathfrak{P}_{L_{s+1}, \ldots, L_i})_m \tag{13}$$

is stable for $m \geqslant D_1$.

PROOF Let $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$. Notice that $k[X_0, \ldots, X_n]/(L_{s+1}, \ldots, L_{n-1})$ is isomorphic to the ring of polynomials over k in $s+2$ variables and $\mathcal{U}' \subset \mathcal{U}$ where $\mathcal{U}$ is an open set from Lemma 3. Let us apply Lemma 6 to the ideal

$$\mathfrak{P}_{L_{s+1}, \ldots, L_{n-1}}/(L_{s+1}, \ldots, L_{n-1}) \subset k[X_0, \ldots, X_n]/(L_{s+1}, \ldots, L_{n-1})$$

in place of $\mathfrak{P} \subset k[X_0, \ldots, X_n]$. We get that for $i = n$ characteristic function (13) is stable for $m \geqslant sd - s + 1$. Now (12) and the exact sequence (14) with $i = n$, see below, imply that for $i = n-1$ characteristic function (13) is stable for $m \geqslant sd - s$. This proves the required assertion for $i = n-1$.

We shall use the decreasing induction on i. Suppose that this characteristic function is stable for $m \geqslant D_1$ for some $s+1 \leqslant i \leqslant n-1$. Let us prove that it is stable for $m \geqslant D_1$ also for $i-1$ (in place of i). We have exact sequence

$$\begin{array}{l} 0 \to (A/\mathfrak{P}_{L_{s+1}, \ldots, L_{i-1}})_{m-1} \to (A/\mathfrak{P}_{L_{s+1}, \ldots, L_{i-1}})_m \to \\ (A/(\mathfrak{P}_{L_{s+1}, \ldots, L_{i-1}} + (L_i)))_m \to 0 \end{array} \tag{14}$$

of vector spaces and $(A/(\mathfrak{P}_{L_{s+1}, \ldots, L_{i-1}} + (L_i)))_m = (A/\mathfrak{P}_{L_{s+1}, \ldots, L_i})_m$ for $m \geqslant (Dd)^{c_4(n-s-1)}$ by Lemma 5. Hence (13) is stable for $m \geqslant D_1$ by the inductive assumption. The lemma is proved.

CONCLUSION OF THE PROOF OF THEOREM 1 Put $\mathfrak{P} = \mathfrak{P}_0$, see (*). Hence now by (*) the height $\mathrm{ht}(\mathfrak{P}) = s = \mu + 1$ and by the Bézout theorem $\deg \mathfrak{P} = \deg \mathfrak{P}_0 = d_1 \leqslant d^s$ in place of $\deg \mathfrak{P} = d$. We have $s \leqslant n-1$ since $\mathrm{ht}(\mathfrak{P}^{(0)}) \leqslant n-1$. Let D be the least integer such that the conditions of Lemma 5 hold for all $s+1 \leqslant i \leqslant n-1$ for $\mathfrak{P} = \mathfrak{P}_0$ with d_1 in place of d. Let $\mathcal{U}'_i$, $s+1 \leqslant i \leqslant n-1$, be the sets from Lemma 5 (ii) and $\mathcal{U}' = \bigcap_{s+1 \leqslant i \leqslant n-1} \mathcal{U}'_i$. Let us apply Lemma 7 with d_1 in place of d. So now $D_1 = \max\{(Dd_1)^{c_4(n-s-1)}, sd_1 - s\}$. For $i = s$ by (*) we get $D_1 \geqslant d^{2^{c_2 n}}$. Therefore, for all sufficiently big n and d the number $D \geqslant d^{2^{c' n}} + 1$ for an absolute constant $c' > 0$. Hence for every $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$ there is $s+1 \leqslant i_0 \leqslant n-1$ such that any system of generators of the prime ideal $\mathfrak{P}_{L_{s+1},\ldots,L_{i_0}}$ contains a polynomial of degree at least $d^{2^{c'n}} + 1$ (the integer i_0 may depend on $(L_{s+1}, \ldots, L_n)$). Let us choose and fix $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$. Now we set $\mathfrak{p} = \mathfrak{P}_{L_{s+1},\ldots,L_{i_0}}$ and $c = c'$. Hence $\mathcal{Z}(\mathfrak{p})$ is a defined over k and irreducible over $\overline{k}$ component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_{\mu+1}, L_{s+1}, \ldots, L_{i_0})$ by Lemma 3. Put $f_j = L_j$ for all $\mu + 2 \leqslant j \leqslant i_0$, and $\nu = i_0$. Now all the polynomials $f_1, \ldots, f_\nu$ are defined, and assertion (a) of the theorem is satisfied. Obviously assertion (c) holds. By Remark 1 also assertion (b) is satisfied. Theorem 1 is proved.

PROOF OF PROPOSITION 1 Let $\mathfrak{p}$ be the ideal constructed in the proof of Theorem 1. Recall that in the proof we use the first Bertini theorem several times and obtain elements from k in place of transcendental elements. Now we would like to avoid applying the first Bertini theorem. Namely, let us replace the family of elements $\lambda_{v,w}$, $1 \leqslant v \leqslant \mu$, $1 \leqslant w \leqslant 3$ (recall that $\lambda_{v,4} = \lambda_{v,2}\lambda_{v,3}^{-1}$) by the family λ of transcendental over k elements. We shall denote them again by $\lambda_{v,w}$. Denote by k_λ the extension of the field k by the all elements from the family λ. So now the transcendency degree of the field k_λ over k is 3μ. Further, let us replace the family of coefficients of $l_{i,j}$, $i \in \{0, s+1, \ldots, n+1\}$, $0 \leqslant j \leqslant n$ of linear forms $L_{s+1}, \ldots, L_{n+1}$ by the family u of transcendental over k_λ elements $u_{i,j}$ with transcendency degree $(n-s+2)(n+1)$ over k_λ. Denote by $k_{\lambda,u}$ the extension of the field k_λ by the all elements from the family $u_{i,j}$. So the transcendency degree of the field $k_{\lambda,u}$ over k is $3\mu + (n-s+2)(n+1) = O(n^2)$. Let k be a finite field. After this replacement by the construction from the proof of Theorem 1 we get a family of polynomials $f_1, \ldots, f_\nu \in k_{\lambda,u}[X_0, \ldots, X_n]$ (we use for them the same notation) and a prime ideal $\mathfrak{p}' \subset k_{\lambda,u}[X_0, \ldots, X_n]$ in place of $\mathfrak{p} \subset k[X_0, \ldots, X_n]$.

Denote by $k[\lambda, u, X_0, \ldots, X_n]$ the polynomial ring over k with the variables from the families λ, u, $X_0, \ldots, X_n$. Put $\mathfrak{p}'' = \mathfrak{p}' \cap k[\lambda, u, X_0, \ldots, X_n]$. By the described construction all $f_1, \ldots, f_\nu \in k[\lambda, u, X_0, \ldots, X_n]$ and all the degrees $\deg_{\lambda,u,X_0,\ldots,X_n} f_i < d+1$.

The ideal $\mathfrak{p}''$ is not necessarily homogeneous with respect to all the variables. To simplify the notation denote all the variables from the families λ, u, $X_0, \ldots, X_n$ by $Y_1, \ldots, Y_m$. Denote by $\mathbb{A}^m(\overline{k})$ the affine space with the coordinate functions $Y_1, \ldots, Y_m$. The field k is perfect since it is finite. Hence $\mathcal{Z}(\mathfrak{p}'') \subset \mathbb{A}^m(\overline{k})$ is a defined over k component of the algebraic variety $\mathcal{Z}(f_1, \ldots, f_\nu) \subset \mathbb{A}^m(\overline{k})$. The variety $\mathcal{Z}(\mathfrak{p}'') \subset \mathbb{A}^m(\overline{k})$ is irreducible over $\overline{k}$ since the variety $\mathcal{Z}(\mathfrak{p}') \subset \mathbb{P}^n(\overline{k_{\lambda,v}})$ is irreducible over $\overline{k_{\lambda,v}}$ by the condition (a) of the theorem.

Let Y_0 be a new variable. The homogenization of a polynomial $a \in k[Y_1, \ldots, Y_m]$ is the polynomial $\overline{a} = Y_0^{\deg a} a(Y_1/Y_0, \ldots, Y_m/Y_0) \in k[Y_0, \ldots, Y_m]$. Let $\mathfrak{p}''' \subset k[Y_0, \ldots, Y_m]$ be the homogeneous prime ideal generated by all the elements $\overline{a}$, $a \in \mathfrak{p}''$. Let $\mathbb{P}^m(\overline{k})$ be the projective space with the homogeneous coordinate functions $Y_0, \ldots, Y_m$. The projective algebraic varieties $\mathcal{Z}(\mathfrak{p}''') \subset \mathbb{P}^m(\overline{k})$ and $\mathcal{Z}(\overline{f_1}, \ldots, \overline{f_\nu}) \subset \mathbb{P}^m(\overline{k})$ are closure with respect to Zariski topology of the affine algebraic varieties $\mathcal{Z}(\mathfrak{p}'')$ and $\mathcal{Z}(f_1, \dots, f_\nu)$ respectively. Therefore, $\mathcal{Z}(\mathfrak{p}''') \subset \mathbb{P}^m(\overline{k})$ is a defined over k and irreducible over $\overline{k}$ component of the algebraic variety $\mathcal{Z}(\overline{f_1}, \dots, \overline{f_\nu}) \subset \mathbb{P}^m(\overline{k})$. By (*) $\mathfrak{p}$ is primary component of the ideal $f_1, \dots, f_\nu$ and the height $\mathrm{ht}(\mathfrak{p}) = \nu$. Hence $\mathfrak{p}'''$ is primary component of the ideal $(\overline{f_1}, \dots, \overline{f_\nu})$ and the height $\mathrm{ht}(\mathfrak{p}''') = \nu$. Thus, over the finite field k assertion (a) of Theorem 1 holds for m, $\overline{f_1}, \dots, \overline{f_\nu}$ and $\mathfrak{p}'''$ in place of n, $f_1, \dots, f_\nu$ and $\mathfrak{p}$ respectively. Obviously all the degrees $\deg_{Y_0,\dots,Y_m} \overline{f_i} < d+1$. For the proof of the new versions of assertions (b) and (c), see the statement of the proposition, we shall consider also $\overline{f_1}, \dots, \overline{f_\nu}$ and $\mathfrak{p}'''$.

Assertion (c) of Theorem 1 holds for $\mathfrak{p}'$ over the field $k_{\lambda,u}$ (in place of $\mathfrak{p}$ over the field k). Any system of generators of the ideal $\mathfrak{p}''$ is a system of generators of the ideal $\mathfrak{p}'$. Hence for any system of generators $a_1, \dots, a_m$ of the ideal $\mathfrak{p}''$ the maximal degree

$$\max_{1 \leqslant i \leqslant m} \deg_{Y_1,\dots,Y_m} a_i \geqslant \max_{1 \leqslant i \leqslant m} \deg_{X_0,\dots,X_n} a_i \geqslant \deg d^{2^{cn}}$$

Therefore, for any system of generators $a'_1, \dots, a'_{m'}$ of the ideal $\mathfrak{p}'''$

$$\max_{1 \leqslant i \leqslant m'} \deg_{Y_0,\dots,Y_m} a'_i \geqslant d^{2^{cn}}.$$

This implies the assertion (c) of the new version of the theorem, see the statement of the proposition, since $n > n_0$, $d > d_0$ are arbitrary, $m = O(n^2)$, all $\deg \overline{f_i} < d+1$, see Remark 3. Moreover, obviously here in (c) one can replace $d^{2^{c\sqrt{n}}}$ by $d^{2^{c\sqrt{n}}} + 1$ (and get a slightly more strong assertion). Then the new version of assertion (b) follows from Remark 1. The proposition is proved.

REMARK 5 *Let k be a finite field and t be a transcendental element over k. Let $\mathfrak{p} \subset k(t)[X_0, \dots, X_n]$ be the ideal constructed in the proof of Theorem 1 over an infinite field $k(t)$. By the proof of Proposition 1 to prove Theorem 1 for the finite field k it is sufficient to ascertain the following. Applying the first Bertini theorem one can choose all the coefficients $\lambda_{v,w} \in k[t]$ of the polynomials f_{v+1}, and the coefficients $l_{i,j} \in k[t]$ of linear forms L_i with degrees $\deg_t \lambda_{v,w}$, $\deg_t l_{i,j}$ bounded from above by $d^{n^{O(1)}}$.*

REMARK 6 *There is the similar problem also for an infinite field k. Let the $\lambda_{v,w} \in k$ and $l_{i,j} \in k$, see the proof of Theorem 1, correspond to the ideal $\mathfrak{p}$. One needs to prove that the lengths of $\lambda_{v,w} \in k$ and $l_{i,j} \in k$ are bounded from above by $d^{n^{O(1)}}$.*

One of the difficulties related to the assertions of Remark 5 and Remark 6 is to estimate the size of the normalization of an algebraic variety. I could not find an explicit estimation of the normalization in literature. But we see that one can give it. We hope to return to this question in one of the next papers. It seems that there are no other principal difficulties, cf. the Appendix from [4].

4 Upper bounds

We are able to give also upper bounds for the stabilization of the characteristic function of a homogeneous polynomial prime ideal and for a system of generators of this ideal. Let $\mathfrak{P}$ be the prime ideal from Section 3 but now we assume that the height $\mathrm{ht}(\mathfrak{P}) = s$, $0 \leqslant s \leqslant n$. So the degree $\deg \mathfrak{P} = d$ and the ideal $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ is radical.

LEMMA 8 *Let $\mathfrak{Q} \subset A$ be a homogeneous ideal such that the ideal $\overline{k} \otimes_k \mathfrak{Q} \subset \overline{k} \otimes_k A$ is radical, the dimension of the variety of zeroes $\dim \mathcal{Z}(\mathfrak{q}) = 0$ in $\mathbb{P}^n(\overline{k})$ and the degree $\deg \mathfrak{Q} = d$. Then the characteristic function $h(\mathfrak{Q}, m)$ is stable for all $m \geqslant d-1$. In particular, this is true for a homogeneous prime ideal $\mathfrak{P} \subset A$ (in place of $\mathfrak{Q}$) with $s = \mathrm{ht}(\mathfrak{P}) = n$ such that the algebraic variety $\mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ is defined over k.*

PROOF Denote for brevity $\overline{A} = \overline{k} \otimes_k A$. We have $h(\mathfrak{Q}, m) = h(\overline{k} \otimes_k \mathfrak{Q}, m)$. Let $\overline{k} \otimes_k \mathfrak{Q} = \cap_{1 \leqslant j \leqslant d} \mathfrak{m}_j$ be the irredundant primary decomposition of the ideal $\overline{k} \otimes_k \mathfrak{Q}$. Hence all $\mathfrak{m}_j \subset \overline{A}$, $1 \leqslant j \leqslant d$, are homogeneous prime ideals of degree one and height n. Hence it is sufficient to prove that the characteristic function $h(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j, m)$ is stable for $m \geqslant \delta - 1$. We use the induction on δ. The base $\delta = 1$ is obvious. There is the exact sequence of homogeneous components of degree m induced by the exact sequence of the homomorphisms of graded $\overline{A}$-modules

$$\begin{aligned} &0 \to (\overline{A}/(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j))_m \to (\overline{A}/(\cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m \times (\overline{A}/(\mathfrak{m}_\delta))_m \to \\ &(\overline{A}/(\mathfrak{m}_\delta + \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m \to 0. \end{aligned} \tag{15}$$

There is a homogeneous polynomial $\varphi \in \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j \setminus \mathfrak{m}_\delta$ such that $\deg \varphi = \delta - 1$. Therefore, $(\overline{A}/(\mathfrak{m}_\delta + \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m = \{0\}$ for $m \geqslant \delta - 1$. Hence by the inductive assumption and (15) the characteristic function $h(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j, m)$ is stable for $m \geqslant \delta - 1$. The lemma is proved.

LEMMA 9 *Under the notation from the beginning of the section suppose that $1 \leqslant s \leqslant n-1$. Then the characteristic function $h(\mathfrak{P}, m) = \dim_k (A/\mathfrak{P})_m$ is stable for all integers $m \geqslant (sd)^{(c_5(n-s))^{n-s-1}}$ for an absolute constant $c_5 > 0$. Therefore, by Remark 1 the ideal $\mathfrak{P}$ has a system of generators consisting of homogeneous polynomials of degrees at most $1 + (sd)^{(c_5(n-s))^{n-s-1}}$. Finally, Lemma 8 now implies that for all $0 \leqslant s \leqslant n$ the characteristic function $h(\mathfrak{P}, m)$ is stable for $m \geqslant (sd)^{(c_5(n-s+1))^{n-s}}$ and the ideal $\mathfrak{P}$ has a system of generators consisting of homogeneous polynomials of degrees at most $1 + (sd)^{(c_5(n-s+1))^{n-s}}$.*

PROOF We shall suppose without loss of generality that $1 < s < n$, Hence $sd \geqslant 2$. Let us show that for all $(L_{s+1}, \ldots, L_n)$ from a nonempty open in the Zariski topology subset of $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$ for every $s \leqslant i \leqslant n-1$ the characteristic function (13) is stable for $m \geqslant (sd)^{(c_5(n-s))^{n-i-1}}$, and hence by Remark 1 the ideal $\mathfrak{P}_{L_{s+1},\ldots,L_i}$ has a system of homogeneous generators of degrees at most $1 + (sd)^{(c_5(n-s))^{n-i-1}}$ for an absolute constant $c_5 > 0$. Indeed, this is true for $i = n-1$ by Lemma 6. We shall use the decreasing induction on i. Suppose that our assertion is proved for some $s+1 \leqslant i \leqslant n-1$. Let us prove that it is true also for $i-1$ (in place of i). We have the exact sequence (14) of vector spaces. Hence by the inductive assumption and Lemma 5 with $D = (sd)^{(c_5(n-s))^{n-i-1}}$ for all $(L_{s+1}, \ldots, L_n) \in \bigcap_{i \leqslant j \leqslant n-1} \mathcal{U}'_j$ (the set $\mathcal{U}'_i$ is defined at this step of the induction in Lemma 5 (ii), and similarly the sets $\mathcal{U}'_j$, $i+1 \leqslant j \leqslant n-1$, are defined at the previous steps of the induction) the equality $(A/(\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}} + (L_i)))_m = (A/\mathfrak{P}_{L_{s+1},\ldots,L_i})_m$ holds for

$$m \geqslant (sd)^{(c_5(n-s))^{n-i}} \geqslant ((sd)^{(c_5(n-s))^{n-i-1}} d)^{c_4(n-i)}$$

for an appropriate constant c_5. Therefore, characteristic function (13) with $i-1$ in place of i is stable for $m \geqslant (sd)^{(c_5(n-s))^{n-i}}$ by the inductive assumption. The required assertion is proved. The lemma is proved.

LEMMA 10 *Under the notation from the beginning of the section there is an absolute constant $c_6 > 0$ such that the prime ideal $\mathfrak{P}$ has a system generators $q_1, \ldots, q_w \in k[X_0, \ldots, X_n]$ with $\deg q_i \leqslant d^{2^{c_6 n}}$ for all $1 \leqslant i \leqslant w$.*

PROOF We can suppose without loss of generality that $1 < s < n$, see Lemma 8, and $d > 1$. There are homogeneous polynomials $F_1, \ldots, F_m \in k[X_0, \ldots, X_n]$ of the same degree d such that $\mathcal{Z}(\mathfrak{P}) = \mathcal{Z}(F_1, \ldots, F_m)$ in $\mathbb{P}^n(\overline{k})$ and $\mathfrak{P}$ is a $\mathfrak{P}$-primary component of the ideal $(F_1, \ldots, F_m) \subset k[X_0, \ldots, X_n]$, cf. [2], [3]. Let $\widetilde{F}_1, \ldots, \widetilde{F}_s$ be linear combinations of $F_1, \ldots, F_m$ with coefficients from $\overline{k}$ in general position. Then by the first Bertini theorem, see [12], [1], cf. [4], the ideal of the ring $\overline{k}[X_0, \ldots, X_n]$

$$(\widetilde{F}_1, \ldots, \widetilde{F}_s) = (\overline{k} \otimes_k \mathfrak{P}) \cap \widetilde{\mathfrak{P}},$$

where $\widetilde{\mathfrak{P}}$ is a homogeneous prime ideal of the ring $\overline{k}[X_0, \ldots, X_n]$ with the height $\mathrm{ht}(\widetilde{\mathfrak{P}}) = s$, the degree $\deg(\widetilde{\mathfrak{P}}) = d^s - d > 0$ and such that $\widetilde{\mathfrak{P}}$ is not a primary component of the ideal $\overline{k} \otimes_k \mathfrak{P}$. Let $\overline{k} \otimes_k \mathfrak{P} = \bigcap_{j \in J} \mathfrak{p}_j$ be the irredundant primary decomposition of the radical ideal $\overline{k} \otimes_k \mathfrak{P}$. There is a homogeneous polynomial $F \in \widetilde{\mathfrak{P}} \setminus \bigcup_{j \in J} \mathfrak{p}_j$ such that $\deg F \leqslant d^s - d$. Now $\overline{k} \otimes_k \mathfrak{P} = \{z \in \overline{k}[X_0, \ldots, X_n] : zF \in (F_1, \ldots, F_m)\}$. Consider the linear equation

$$ZF = \sum_{1 \leqslant i \leqslant s} Z_i F_i \tag{16}$$

over the ring of polynomials $\overline{k}[X_0, \ldots, X_n]$. By [6], [10] the submodule of $(\overline{k} \otimes_k A)^{s+1}$ of solutions $(Z, Z_1, \ldots, Z_s)$ of equality (16) has a system of generators $z_i, z_{i,1}, \ldots, z_{i,s}$, $i \in I$, consisting of polynomials from $\overline{k} \otimes_k A$ of degrees $\deg z_i$, $\deg z_{i,j}$ bounded from above by $d^{2^{c_6 n}}$ for an appropriate universal constant $c_6 > 0$. Now $z_i \in \overline{k} \otimes_k A$, $i \in I$, is the system of generators of $\overline{k} \otimes_k \mathfrak{P}$ of the required degrees. Since the variety $\mathcal{Z}(\mathfrak{P})$ is defined over k there is also a system of generators $q_1, \ldots, q_w \in k[X_0, \ldots, X_n]$ of the ideal $\mathfrak{P}$ with $\deg q_i \leqslant d^{2^{c_6 n}}$ for all $1 \leqslant i \leqslant w$. The lemma is proved.

COROLLARY 1 *Under the notation from the beginning of the section there is an absolute constant $c_7 > 0$ such that the characteristic function $h(\mathfrak{P}, m)$ of the prime ideal $\mathfrak{P}$ is stable for $m \geqslant d^{2^{c_7 n}}$.*

PROOF Indeed, by Lemma 8 and [8] we can suppose without loss of generality that $\mathrm{ht}(\mathfrak{P}) = s \leqslant n-1$. By Lemma 10 with the ground field k_u (in place of k) the conditions of Lemma 5 hold for all $s+1 \leqslant i \leqslant n-1$ for $D = d^{2^{c_6 n}} + 1$. Let $(L_{s+1}, \ldots, L_n) \in \mathcal{U}' = \bigcap_{s+1 \leqslant i \leqslant n-1} \mathcal{U}'_i$, see Lemma 5 (ii). Now the required assertion follows from Lemma 7. The corollary is proved.

References

[1] **Baldassarry M.:** *"Algebraic varieties"*, Springer–Verlag, Berlin–Göttingen–Heidelberg, 1956.

[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.:** *"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].

[4] **Chistov A. L.:** *"A deterministic polynomial–time algorithm for the first Bertini theorem"*, Preprint of St.Petersburg Mathematical Society (2004), http://www.mathsoc.spb.ru/preprint/

[5] **Dubé T. W.:** *"The structure of polynomial ideals and Gröbner bases"*, SIAM J. Comput. 19 (1990), 750–775.

[6] **Hermann G.:** *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95**, (1926), 736-788.

[7] **Hilbert D.:** *"Über die Teorie der algebraischen Formen"*, Math. Ann. 36 (1890), 473–534.

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

[9] **Mayr E.W., Meyer A.R.:** *"The complexity of the word problems for commutative semigroups and polynomial ideals"*, Adv. Math. 46 (1982), 305-329.

[10] **Seidenberg A.:** *"Constructions in algebra"*, Trans. Amer. Math. Soc. 97 (1974), 273–313.

[11] **Yap Chee K.:** *"A new lower bound construction for commutative Thue systems, with applications"*, J. Symb. Comput., 12 (1991), 1–28.

[12] **Zariski O.:** *"Pencils on an algebraic variety and a new proof of a theorem of Bertini"*, Trans. Amer. Math. Soc., v. 50 (1941) p. 48–70.