Алгебра и анализ
Том 20 (2008), № 6

St. Petersburg Math. J.
Vol. 20 (2009), No. 6, Pages 983–1001
S 1061-0022(09)01081-4
Article electronically published on October 2, 2009

DOUBLE-EXPONENTIAL LOWER BOUND FOR THE DEGREE OF ANY SYSTEM OF GENERATORS OF A POLYNOMIAL PRIME IDEAL

A. L. CHISTOV

Abstract. Let A be a polynomial ring in $n+1$ variables over an arbitrary infinite field k. It is proved that for all sufficiently large n and d there is a homogeneous prime ideal $\mathfrak{p} \subset A$ satisfying the following conditions. The ideal $\mathfrak{p}$ corresponds to a component, defined over k and irreducible over $\bar{k}$, of a projective algebraic variety given by a system of homogeneous polynomial equations with polynomials in 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 a slightly less strong result is obtained.

Introduction

In the classical paper [7], Hilbert proved that any polynomial ideal is generated by a finite number of polynomials. Hence, this 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 the 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 a nonhomogeneous prime ideal reduces easily to that of a homogeneous prime ideal). One of the most important open problems in effective algebraic geometry has been to obtain a similar lower bound for the 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 §1 for more details. These ideals are far from being prime: they have many primary components. All attempts to reduce the case of a prime ideal to the known case 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? We did not just stumble upon it. We investigated the problem of effective normalization of algebraic varieties. It turned out that the construction of a normalization of an algebraic variety reduces to solving a linear equation $aX + bY + cZ = 0$ over a polynomial ring. Simultaneously, as a consequence of our results, we got Lemma 2. We hope to return to the normalization of an algebraic variety from an algorithmic point of view in one of our

2000 *Mathematics Subject Classification.* Primary 13P10, 14Q20.

Key words and phrases. Polynomial ideal, projective algebraic variety, Gröbner basis, effective algebraic geometry.

next papers. Notice that the problem of solving the equation $aX + bY + cZ = 0$ over a polynomial ring is close to that formulated at the end of the Introduction.

Let k be a field with algebraic closure $\bar{k}$. Let $n \geq 0$, and let $X_0, \ldots, X_n$ be variables. Let $\mathfrak{a} \subset k[X_0, \ldots, X_n] = A$ be a homogeneous ideal that is not an $(X_0, \ldots, X_n)$-primary 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 homogeneous elements of degree $m \geq 0$ in the ring $A/\mathfrak{a}$. Recall that there is a polynomial $P = \sum_{0 \leq i \leq n-s} p_i Z^i$ (all $p_i \in \mathbb{Q}$) of degree $\deg P = n - s$ such that $h(\mathfrak{p}, m) = P(m)$ for all sufficiently large $m > 0$. By definition, P is the Hilbert polynomial of $A/\mathfrak{a}$. The degree of the ideal $\mathfrak{a}$ can be defined by the formula $\deg \mathfrak{a} = (n - s)! p_{n-s}$. Denote by $\mathcal{Z}(\mathfrak{a}) \subset \mathbb{P}^n(\bar{k})$ the set of all common zeros of the polynomials from $\mathfrak{a}$ in $\mathbb{P}^n(\bar{k})$ (similar notation will be used below with other ideals or families of polynomials and other projective or affine spaces).

Below, in the statements of the theorem, the proposition, the 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 $c > 0$, $n_0 > 0$, and $d_0 > 0$ such that, for every infinite field k, for all integers $n > n_0$ and $d > d_0$ there are homogeneous polynomials $f_1, \ldots, f_\nu \in A$, $\nu \leq n$, such that $\deg f_i < d$, $1 \leq i \leq \nu$, and a homogeneous prime ideal $\mathfrak{p} \subset A$ satisfying the following conditions.*

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

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

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

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

Proposition 1. *In the statement of Theorem 1, let us replace the words "infinite field" by the words "finite field" and $d^{2^{cn}}$ by $d^{2^{c\sqrt{n}}}$ in conditions* (b) *and* (c). *Further, in condition* (a) *let us delete the phrase "and the projective algebraic variety $\mathcal{Z}(f_1, \ldots, f_\nu)$ has exactly two irreducible over $\bar{k}$ components: $\mathcal{Z}(\mathfrak{p})$ and some linear subspace $\mathcal{L} \subset \mathbb{P}^n(\bar{k})$ defined over k". Then the resulting statement holds true for finite fields.*

Remark 1. It is known, see [5, §§6 and 7], that for any homogeneous ideal $\mathfrak{a} \subset A$ the following assertion is valid. If the characteristic function $h(\mathfrak{a}, m)$ is stable for $m \geq m_0$, where $m_0 \geq 0$, 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, some details related to the last remark are needed. We shall use the notation of [5] (but replace n by $n + 1$). In [5], the constants $b_0 \geq b_1 \geq \cdots \geq b_{n+2} = 0$ corresponding to the ideal $I = \mathfrak{a}$ are considered. Let the integer $m_0 \geq 0$ be the smallest

possible such that the characteristic function $h(\mathfrak{a}, m)$ is stable for $m \geq m_0$. 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 [5, Lemma 7.2], the degrees of the polynomials in the reduced Gröbner basis under consideration are bounded from above by b_0. The assertion of Remark 1 follows from this.

Note also the correct version of a formula before Lemma 7.2 in [5]: $b_0 = \min\{d \geq b_1 : \forall_{z \geq d}\, \bar{\varphi}(z) = \varphi(z)\}$. In [5], $z > d$ occurred in place of $z \geq d$, which might mislead the reader. The original version contradicts 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 $\operatorname{ht}(\mathfrak{P}) = s$, $0 \leq s \leq n$, and of degree d. We shall suppose additionally that the ideal $\bar{k} \otimes_k \mathfrak{P} \subset \bar{k} \otimes_k A$ is radical, or equivalently, 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 $m \geq \min\{(sd)^{O(n-s+1)^{n-s}}, d^{2^{O(n)}}\}$, and $\mathfrak{P}$ 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 $c > 0$, $n_0 > 0$, $d_0 > 0$ with the following property: for all integers $n > n_0$, $d > d_0$ and every field k, there is a homogeneous prime ideal $\mathfrak{p} \subset k[X_0, \ldots, X_n]$ with $\deg \mathfrak{p} = d$ and $\operatorname{ht}(\mathfrak{p}) = 2$ such that assertion (c) of Theorem 1 holds true for $\mathfrak{p}$.

§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 $X_1^{i_1} \cdots X_{n-1}^{i_{n-1}}$ for some integers $i_j \geq 0$. By definition, a binomial in $k[X_1, \ldots, X_{n-1}]$ is a difference of two distinct power products. A polynomial ideal $\mathfrak{g} \subset k[X_1, \ldots, X_{n-1}]$ is said to be binomial if and only if it has a system of generators $q_1, \ldots, q_v$ consisting of binomials. In a similar way, the 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) and for all integers $n > n_0$, $d > d_0$, there is a homogeneous ideal $\mathfrak{b} \subset k[X_0, \ldots, X_{n-1}] = A^{(0)}$ such that $\mathfrak{b}$ 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 $m \geq m_0$, i.e., it coincides with the Hilbert polynomial of $A^{(0)}/\mathfrak{b}$ for these m. Then $m_0 \geq d^{2^{c_1 n}}$.*

Proof. We 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 the two cases (i) and (ii), the result is again a binomial. This proves the claim.

Moreover, 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 maximum degree $\max_{1 \leq i \leq \alpha} e_i$ of the reduced Gröbner basis do not depend on the choice of the field k, in particular, on the characteristic of the field k.

In [11], the following assertion was 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 $n > n_0$ and $d > d_0$ there is 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 $\deg g_i < d$, $1 \le i \le \mu$, satisfying the following condition. Let the ideal $\mathfrak{g} = (g_1, \ldots, g_\mu)$ be included in $\mathbb{Q}[X_1, \ldots, X_{n-1}]$, and let $e_1, \ldots, e_\alpha$ be the reduced Gröbner basis of $\mathfrak{g}$ with respect to some admissible ordering $<$ of monomials (this ordering can be chosen arbitrarily). Then $\max_{1 \le i \le \alpha} \deg e_i \ge d^{2^{c_0 n}}$. By the preceding arguments, the same is true 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 $1 \le i \le \mu$, we define $b_i = X_0^{\deg g_i} g_i(X_1/X_0, \ldots, X_{n-1}/X_0) \in A^{(0)}$ to be the homogenization of g_i. Hence b_i is a homogeneous binomial in $k[X_0, \ldots, X_{n-1}]$. By definition, let $\mathfrak{b} = (b_1, \ldots, b_\mu) \subset k[X_0, \ldots, X_{n-1}]$ be the corresponding homogeneous ideal. We shall assume without loss of generality that the ordering $<$ of monomials is degree-compatible, i.e., for all monomials $v_1, v_2 \in A$ the condition $\deg v_1 < \deg v_2$ implies $v_1 < v_2$. Next, consider the admissible ordering of monomials from $A^{(0)}$ that extends the ordering $<$ on the monomials from $k[X_1, \ldots, X_{n-1}]$ and is such that $X_0^i < X_j$ for all $1 \le j \le n$ and $i \ge 0$. Let $e'_1, \ldots, e'_\lambda$ be the reduced Gröbner basis of the ideal $\mathfrak{b}$ with respect to the above ordering of the monomials. Then the definition of the Gröbner basis implies 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 the ordering $<$ of the ideal $(g_1, \ldots, g_\mu)$. Since the ordering $<$ on the monomials in $k[X_1, \ldots, X_{n-1}]$ is degree-compatible, we have

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

Therefore, $\max_{1 \le i \le \lambda} \deg e'_i \ge d^{2^{c_0 n}}$. Now the assertion of the lemma follows from Remark 1. The lemma is proved. □

A survey of the results on this subject can be found in [11]. All the works here are based on the initial ideas from [9], where fields of zero characteristic were considered (or, more precisely, the field of rational numbers). In [9], the proof of Lemma 2 concerning all possible binomials in a binomial ideal was given for the case of zero characteristic. D. Yu. Grigoriev (private communication) noticed that there is another simple proof of that lemma in arbitrary characteristic. It seems that there are no other obstructions for extending these results to the case of nonzero characteristic. Hence, all lower bounds for binomial ideals are valid in arbitrary characteristic. In our proof of Lemma 1 we do not even use Lemma 2 of [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 grading. Namely, we can identify the homogeneous components $M(\nu)_m = M_{\nu+m}$ for every m and this identification induces an isomorphism of A-modules $M(\nu) \simeq M$. This isomorphism is an isomorphism of degree ν of graded A-modules $M(\nu)$ and M.

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

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

We introduce the rings of polynomials $A^{(1)} = A[X_{n+1}]$ and the ring $B_\Phi = A^{(1)}/(\Phi)$. Now A, $A^{(1)}$, $A^{(1)}[Z_1, \ldots, Z_\mu]$ are rings graded 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 in these rings are homogeneous polynomials of degree m with respect to all these variables. In what follows we shall view each graded $A^{(1)}$-module (respectively, each $A^{(1)}[Z_1, \ldots, Z_\mu]$-module) $M = \bigoplus_{m\in\mathbb{Z}} M_m$ as a graded A-module with the same grading $\{M_m\}_{m\in\mathbb{Z}}$. The polynomial Φ is homogeneous. Hence, B_Φ and $B_\Phi[Z_1, \ldots, Z_\mu]$ are also 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 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 ring graded in a natural way and a finitely generated A-module. Next, for the graded A-module $B_\mathfrak{a}$ we have $B_\mathfrak{a} \simeq A \oplus A(-1) \oplus \mathfrak{a}(-1)$. The ring $\bar{k} \otimes_k B_\mathfrak{a}$ is integral. The field of fractions of $B_\mathfrak{a}$ is K', the tensor product $\bar{k} \otimes_k K'$ is a field, and the extension of fields $\bar{k} \otimes_k K' \supset \bar{k}(X_0, \ldots, X_n)$ is finite separable.

Proof. The element $X_{n+1}^2 \bmod \Phi$ belongs to $B_\mathfrak{a}$ because $X_n \in \mathfrak{a}$. 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. We introduce the vector space $(B_\mathfrak{a})_m$, $m \geq 0$, of homogeneous elements of degree m of $B_\mathfrak{a}$ as $\{P/X_n \,:\, P \in (A^{(1)})_{m+1} \,\&\, P/X_n \bmod \Phi \in B_\mathfrak{a}\}$. Thus, $B_\mathfrak{a}$ is a graded ring. The remaining assertions are also straightforward. The lemma is proved. □

Let $\mathfrak{b} \subset A^{(0)}$ be the ideal as in Lemma 1. We shall suppose without loss of generality that $n_0 > 1$ in Lemma 1, so that $n \geq 2$. 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 $m \geq m_0$ (i.e., coincides with the Hilbert polynomial of $A^{(0)}/\mathfrak{b}$ for these m), then $m_0 \geq d^{2^{c_1 n}} + 1$ by Lemma 1.

We shall use recursion to construct graded rings $B^{(0)} = B'$, $B^{(1)}$, …, $B^{(\mu)}$ with the following properties for all i.

(i) The ring $\bar{k} \otimes_k B^{(i)}$ 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 $\bar{k} \otimes_k K^{(i)} \supset \bar{k}(X_0, \ldots, X_n)$ is finite separable.
(iv) For $i \geq 1$ 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 $\bar{k} \otimes_k K^{(i-1)}[Z_i]$. *By definition, put*

$$B^{(i)} = B^{(i-1)}[Z_i]/(\varphi_i).$$

Then $B^{(i)} \simeq B^{(i-1)} \oplus B^{(i-1)}(-1) \oplus \cdots \oplus B^{(i-1)}(-m_i)$. This is an isomorphism of graded A-modules.

For $i = 0$ these properties follow from the definition of the ring B'. Let $1 \le i \le \mu$ and suppose $B^{(i-1)}$ is constructed. We construct $B^{(i)}$. Obviously (i)–(iii) follow from (iv). So, it suffices to construct a polynomial φ_i as in (iv).

Denote by $E^{(i-1)}$ the integral closure of the ring $\bar{k} \otimes_k B^{(i-1)}$ in its field of fractions $\bar{k} \otimes_k K^{(i-1)}$. Notice that $E^{(i-1)}[Z_i] \supset \bar{k} \otimes_k B^{(i-1)}[Z_i]$. 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. We introduce the following elements of the ring $\bar{k} \otimes_k B^{(i-1)}[Z_i]$:

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

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 $i - 1$,

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

Next, 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 $\bar{k} \otimes_k K^{(i-1)}(Z_i)$ over $\bar{k}$. Therefore, the morphism

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

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

We show that there is a nonempty Zariski open subset $\mathcal{U}'' \subset \bar{k}$ (obviously, the number of elements $\#(\bar{k} \setminus \mathcal{U}'')$ is finite) such that for all $\alpha \in \mathcal{U}''$ the rational morphism

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

is separable dominant. Indeed, consider the morphism

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

Suppose $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\bar{k})$, $n_1 \ge n + 1$, and $\mathbb{A}^{n_1+2}(\bar{k})$ has coordinate functions $Z_i, X_0, \ldots, X_{n_1}$. Let $h_1, \ldots, h_s \in \bar{k}[Z_i, X_0, \ldots, X_{n_1}]$ be a system of local parameters of the algebraic variety $V^{(i-1)}$ at the point ξ. Then the differential of the 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 $\bar{k}$. 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 $\bar{k}$ for all α in a nonempty Zariski open subset of $\mathcal{U}'' \subset \bar{k}$. Hence, the morphism $\widetilde{\psi}$ is dominant and separable for all $\alpha \in \mathcal{U}''$. The natural morphism $\pi : \mathbb{A}^3(\bar{k}) \setminus \{0\} \to \mathbb{P}^2(\bar{k})$ is dominant separable. The morphism (3) is equal to $\pi \circ \widetilde{\psi}$. Hence, this morphism is also separable dominant for all $\alpha \in \mathcal{U}''$. This proves the claim.

Let $V', V'' \subset \mathbb{A}^n(\bar{k})$ 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 $\bar{k}$) 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 the tangent spaces of the algebraic varieties V' and V'' at the point z is transversal, where the tangent spaces are viewed as subspaces of $\mathbb{A}^n(\bar{k})$.

In what follows, unless it is not stated otherwise, we assume that the field k is infinite. We choose and fix $\alpha \in \mathcal{U}'' \cap k$. Recall that $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\bar{k})$. The morphism (3) is separable dominant, (1) is fulfilled, and $n \ge 2$. Hence, we can apply the first Bertini theorem (see [12, 1], cf. [4]), to the morphism (3). By that theorem, there is a polynomial

φ that is a linear combination of $\widetilde{\psi}_1$, $\widetilde{\psi}_2$, $\widetilde{\psi}_3$ with coefficients from k in general position and is such that the intersection of $\widetilde{V}^{(i-1)}$ and $\mathcal{Z}(\varphi)$ is transversal in $\mathbb{A}^{n_1+2}(\bar{k})$ and irreducible over $\bar{k}$.

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 $\varphi \in \bar{k} \otimes_k K^{(i-1)}[Z_i]$ is irreducible, because $E^{(i-1)}$ is integrally closed. Multiplying φ by a nonzero factor from k, we shall assume without loss of generality that the leading coefficient with respect to Z_i of the polynomial φ is 1. Now we put $\varphi_i = \varphi$. Hence, condition (iv) is satisfied. Also, we get $\lambda_{i,3} = \alpha^{-1}$ and $\lambda_{i,4} = \alpha\lambda_{i,2}$, whence $\lambda_{i,2} = \lambda_{i,3}\lambda_{i,4}$.

We put $B = B^{(\mu)}$ and denote by K the field of fractions of B. Then $\bar{k} \otimes_k K$ is the field of fractions of $\bar{k} \otimes_k B$. By (iii), the extension of fields $\bar{k} \otimes_k K \supset \bar{k}(X_0, \dots, X_n)$ is finite separable.

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

$$f_{i+1} = X_n X_{n+1+i}^{m_i+1} + \lambda_{i,1} X_0^{m_i} X_n X_{n+1+i} + \lambda_{i,2} X_0^{m_i} X_1 X_n + \lambda_{i,3} X_0^{m_i} X_2 X_n + \lambda_{i,4} b_i X_{n+1}^2 \in k[X_0, \dots, X_N], \quad 1 \le i \le \mu;$$

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

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

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

By (iv), we have an isomorphism of graded A-modules $B \simeq \bigoplus_{i \in I} B'(-\alpha_i)$, where the number of elements $\#I = (m_1+1)\cdots(m_\mu+1)$ is not greater than $d^\mu = d^{O(n)}$ and $0 \le \alpha_i \le (m_1 + \cdots + m_\mu) \le (d-1)\mu = O(nd)$.

Let $\alpha' = \max_{i \in I} \alpha_i$. We show that $\dim_k B_m$ is stable for all $m \ge m_0$ if and only if $\dim_k B'(-\alpha')_m$ is stable for all $m \ge m_0$. Indeed, let $m_0' \ge 0$ be the smallest integer such that $\dim_k B'_m$ is stable for all $m \ge m_0'$. Observe that $m_0' > 0$ by Lemma 1. Then $\dim_k B'(-\alpha_i)_m$ is stable for all $m \ge m_0$ if and only if $m_0 \ge m_0' + \alpha_i$. Hence, $\dim_k B_m$ is stable for all $m \ge m_0' + \alpha'$. Put $I' = \{i \in I : \alpha_i = \alpha'\}$. Now, if $i \in I \setminus I'$, then $\dim_k B'(-\alpha_i)_m$ is stable for all $m \ge m_0' + \alpha' - 1$. Suppose that $\dim_k B_m$ is stable for all $m \ge m_0' + \alpha' - 1$. We have an isomorphism of graded modules

$$B \simeq \Big(\bigoplus_{i \in I \setminus I'} B'(-\alpha_i) \Big) \oplus \Big(\bigoplus_{i \in I'} B'(-\alpha') \Big).$$

Therefore, $\dim_k B'(-\alpha')_m$ is stable for all $m \ge m_0' + \alpha' - 1$, a contradiction. The claim is proved.

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 occurring in Lemma 1. Hence, if $\dim_k B_m$ is stable for $m \geq m_0$, then $\dim_k((A^{(0)}/\mathfrak{b})(-\alpha'-1))_m$ is stable for $m \geq m_0$. Therefore, $m_0 \geq d^{2^{c_1 n}} + \alpha' + 1$ 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 $n' \geq n$. 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 $m \geq m_0$ if and only if the Hilbert function of $A'/\mathfrak{P}'$ is stable for $m \geq m_0$. Next, the ideal $\mathfrak{P}$ has a system of generators $b_1, \ldots, b_w$ with $\deg b_i \leq v$ for all i if and only if the ideal $\mathfrak{P}'$ has a system of generators $b'_1, \ldots, b'_{w'}$ with $\deg b'_i \leq v$ for all i.

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

The quantities n, d are arbitrary sufficiently large integers. Hence, using our construction, (4), and Remark 3, and changing the notation (replacing 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 differ from those in Lemma 1) such that, for all integers $n > n_0$, $d > d_0$ and every infinite field k, there are homogeneous polynomials $f_1, \ldots, f_{\mu+1} \in k[X_0, \ldots, X_n]$, $\mu < n$, with $\deg f_i < d$ and a homogeneous prime ideal $\mathfrak{P}^{(0)} \subset k[X_0, \ldots, X_n]$ satisfying conditions (a) and (b) of Theorem 1 (in which now ν should be replaced by $\mu+1$ and $\mathfrak{p}$ by $\mathfrak{P}^{(0)}$) with c_2 in place of c. Moreover, in accordance with our construction, $\mathrm{ht}(\mathfrak{P}^{(0)}) = \mu+1 \leq n-1$. The polynomials $f_1, \ldots, f_{\mu+1}$ depend on the choice of the family of the elements α and the elements $\lambda_{i,j}$, $1 \leq i \leq \mu$, $1 \leq j \leq 3$; 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 components irreducible over $\bar{k}$: $\mathcal{Z}(\mathfrak{P}^{(0)})$ and some linear subspace $\mathcal{L}^{(0)} \subset \mathbb{P}^n(\bar{k})$ 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 of interest 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 $c_2 \geq c_3$). Since $2\mu+1 = O(n)$, this would imply, as in the proof of Proposition 1 (see below at the end of this section) that the following is true. Let us delete from condition (a) the phrase "and the projective algebraic variety $\mathcal{Z}(f_1, \ldots, f_\nu)$ has exactly two components irreducible over $\bar{k}$: $\mathcal{Z}(\mathfrak{p})$ and some linear subspace $\mathcal{L} \subset \mathbb{P}^n(\bar{k})$ defined over k". Then this new statement of Theorem 1 is also true for any finite field k, i.e., without any restrictions on the field k.

However, we shall obtain another result, which suffices to prove the theorem.

The set of all $(n-s)$-tuples $(L_{s+1}, \ldots, L_n)$ of linear forms $L_j \in \bar{k}[X_0, \ldots, X_n]$, $s+1 \leq j \leq n$, will be identified with $\mathbb{A}^{(n+1)(n-s)}(\bar{k})$.

Let $\mathfrak{P} \subset A$ be an arbitrary homogeneous prime ideal of height $s = \mathrm{ht}(\mathfrak{P})$, $0 \leq s \leq n-1$, and of degree $\deg \mathfrak{P} = d$. Let $V = \mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\bar{k})$ be the projective algebraic variety of all common zeros of the polynomials from $\mathfrak{P}$ in $\mathbb{P}^n(\bar{k})$. Then $\dim V = n - s$. We shall suppose additionally that the ideal $\bar{k} \otimes_k \mathfrak{P} \subset \bar{k} \otimes_k A$ is radical, or equivalently, 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 where the algebraic variety $\mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\bar{k})$ is irreducible over $\bar{k}$ (and actually this case suffices for our purposes). Still, we would like to prove the lemma in the general case.

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

(i) *for every integer $s \le i \le n$ the intersection of V and $\mathcal{Z}(L_{s+1}, \dots, L_i)$ is transversal or, which is equivalent in the case under consideration, we have $\dim(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i)) = n - i$ and $\deg V = \deg(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i))$;*

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

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

(iv) *for every integer $s \le i < n$ 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 finite set of points in $\mathbb{P}^n(\bar{k})$ defined over k; this finite set corresponds to a homogeneous radical ideal $\mathfrak{P}_{L_{s+1},\dots,L_n} \subset k[X_0, \dots, X_n]$;*

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

(vii) *for every $s+1 \le i \le n$ the ideal $\mathfrak{P} + (L_{s+1}, \dots, L_i)$ of the ring A is equal to $\mathfrak{P}_{L_{s+1},\dots,L_i} \cap \mathfrak{Q}_{L_{s+1},\dots,L_i}$, where $\mathfrak{Q}_{L_{s+1},\dots,L_i}$ is an $\mathfrak{M}$-primary ideal or $\mathfrak{Q}_{L_{s+1},\dots,L_i} = A$ (we use the same notation $(L_{s+1}, \dots, L_i)$ for the ideal and the $(n-s)$-tuple of linear forms, but its meaning is always seen from the context);*

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

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

Let $(L_{s+1}, \dots, L_n) \in \mathcal{U} \cap A^{n-s}$. Now (i) and (ii) are fulfilled. 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 $\bar{k} \otimes_k \mathfrak{P} + (L_{s+1}, \dots, L_n)\bar{k} \otimes_k A \subset \bigcap_{j \in J} (\mathfrak{p}_j + (L_{s+1}, \dots, L_n)\bar{k} \otimes_k A)$. Hence, by (vii) for $\mathfrak{p}_j$, we have

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

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

We prove (iii). There is a nonzero linear form $L_0 \in A$ such that $V_i \setminus \mathcal{Z}(L_0)$ is a dense subset in V_i open in the Zariski topology. By (5), the ring of regular functions on $V_i \setminus \mathcal{Z}(L_0)$ defined over $\bar{k}$ is $\bar{k}[V \setminus \mathcal{Z}(L_0)]/(L_{s+1}/L_0, \dots, L_i/L_0)$. Hence, $V_i \setminus \mathcal{Z}(L_0)$ is defined over k. Denote by k_s the separable closure of k. Therefore, the subset $(V_i \setminus \mathcal{Z}(L_0))(k_s)$ of V_i is dense with respect to the Zariski topology and is invariant under the action of the Galois group $\mathrm{Gal}(\bar{k}/k)$. Hence, by a well-known criterion, V_i is defined over k. Assertion (iii) is proved, together with (v).

To prove (iv), we note that the Galois group $\mathrm{Gal}(\bar{k}/k)$ acts transitively on the irreducible over $\bar{k}$ components $\mathcal{Z}(\mathfrak{p}_{j,L_{s+1},\dots,L_i})$ of the algebraic variety V_i. Hence, V_i is irreducible over k and (iv) is proved together with (vi).

We prove (viii). By (5), we have

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

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

Let $u = \{u_{i,j}\}$, $i \in \{0, s+1, s+2, \ldots, n+1\}$, $0 \le j \le n$, 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 $U_i = \sum_{0 \le j \le n} u_{i,j} X_j \in k_u[X_0, \ldots, X_n]$, $s+1 \le i \le n$, 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 $(U_{s+1}, \ldots, U_n) \in \mathcal{U}(\overline{k_u})$. We extend the ground field k up to k_u and, again, denote by $\mathfrak{P}$ the ideal of $k_u \otimes_k \mathfrak{P} \subset k_u \otimes_k A$ (this will lead to no ambiguity). Now the ideals $\mathfrak{P}_{U_{s+1},\ldots,U_i}$ are defined for all $s \le i \le n$.

We denote by $k[u]$ the polynomial ring with coefficients in k and variables in the family u, and by $k[u, X_0, \ldots, X_n]$ the polynomial ring with coefficients in k and with variables belonging either to u, or to the family $X_0, \ldots, X_n$ (similar notation will be used with other variables). Let $s+1 \le i \le n$ 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

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

i.e., k''_u is the subfield of k_u formed by all elements that 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 $i_1 \in \{0, i, \ldots, n+1\}$, $0 \le j_1 \le n$). We introduce the multiplicatively closed sets

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

The localization $S_{i,n}^{-1} k[u, X_0, \ldots, X_n]$ includes $k_u[X_0, \ldots, X_n]$. If z is an element of $S_{i,n}^{-1} k[u, X_0, \ldots, X_n]$, then we can substitute $u_{i,n} = (-\sum_{0 \le i \le n-1} u_{i,j} X_j)/X_n$ 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 a homomorphism

$$\pi \,:\, S_{i,n}^{-1} k[u, X_0, \ldots, X_n] \to k''_u(X_0, \ldots, X_n)$$

of k''_u-algebras. If $z \in k''_u(X_0, \ldots, X_n)$, then $\pi(z) = z$. Obviously,

$$\operatorname{Ker}(\pi) = U_i S_{i,n}^{-1} k[X_0, \ldots, X_n].$$

Lemma 4. *In the above notation, suppose that $X_n \notin \mathfrak{P}$. Then for all $z \in k_u[X_0, \ldots, X_n]$ we have $\pi(z) \in S_{\mathfrak{P}_{i-1}}^{-1} k''_u[X_0, \ldots, X_n]$. Next, 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 $z \in k_u[X_0, \ldots, X_n]$. Then $z = P/Q$, where $0 \ne Q \in k[u]$ and $P \in k[u, X_0, \ldots, X_n]$. We have $\pi(P) \in S^{-1} k''_u[X_0, \ldots, X_n] \subset S_{\mathfrak{P}_{i-1}}^{-1} k''_u[X_0, \ldots, X_n]$. Let $\deg_{u_{i,n}} Q = r$. Then $X_n^r \pi(Q) \in k''_u[X_0, \ldots, X_n]$. Hence, it suffices to prove that $X_n^r \pi(Q) \in S_{\mathfrak{P}_{i-1}}$. The definition of the homomorphism π implies the formula $\pi(Q) = q((-\sum_{0 \le j \le n-1} X_j u_{i,j})/X_n)$ for a polynomial $0 \ne q \in k''_u[Z]$. Denote by $k_u(\mathcal{Z}(\mathfrak{P}_{i-1}))$ the field of rational functions on the variety $\mathcal{Z}(\mathfrak{P}_{i-1}) \subset \mathbb{P}^n(\overline{k_u})$, defined over k_u. We have $X_n \notin \mathfrak{P}$, and $U_{s+1}, \ldots, U_{i-1}$ 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

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

i.e., k_u''' is the subfield of k_u formed by all elements that do not depend on all $u_{i,j}$, $0 \le j \le n$. 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,

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

is a transcendental element over the field k_u. Therefore, $X_n^r \pi(Q) \notin \mathfrak{P}_{i-1}$. The claim 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 we can write $z = \sum_{1 \le j \le \gamma} p_j q_j + U_i q$, where the p_j are introduced above and all q_j, q belong to $S^{-1}k_u[X_0, \dots, X_n]$. Therefore,

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

Let $z \in k[u, X_0, \dots, X_n] \cap \mathfrak{P}_{i-1}$. Then, by what has been proven above,

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

This proves the last assertion and all of the lemma. □

Lemma 5. *In the above notation, suppose that for some $s + 1 \le i \le n - 1$ the ideal $\mathfrak{P}_{U_{s+1},\dots,U_i}$ has a system of generators of degrees at most D with respect to $X_0, \dots, X_n$, where $D \ge 2$. Then the following is true.*

(i) *There exists 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 $\deg_{X_0,\dots,X_n} q_j \le D$ 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 a universal constant in $O(n - i)$.*

(ii) *There is a nonempty subset $\mathcal{U}_i' \subset \mathcal{U}$ open in the Zariski topology and enjoying the following properties. There is an absolute constant $c_4' > 0$ such that for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}_i' \cap A^{n-s}$ and every $0 \le j \le n$ we have*

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

for some integer $N \le n(Dd)^{c_4'(n-i)}$. Next, there is an absolute constant $c_4 > 0$ such that for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}_i'$ and for all $m \ge n(Dd)^{c_4(n-i)}$ 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. We prove (i). Consider the morphism $\pi_U : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \dots : X_n) \mapsto (U_0 : U_{s+1} : \dots : U_{n+1})$ 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, $\deg \pi_U(\mathcal{Z}(\mathfrak{P})) = d$. Also, $\pi_U(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_\mathfrak{P})$, where $F_\mathfrak{P} \in k[u, Z_0, Z_{s+1}, \dots, Z_n]$ is a homogeneous polynomial with respect to $Z_0, Z_{s+1}, \dots, Z_n$ such that $F_\mathfrak{P}(U_0, U_{s+1}, \dots, U_{n+1})$ vanishes on $\mathcal{Z}(\mathfrak{P})$ in $\mathbb{P}^n(\overline{k_u})$, the degree $\deg F_\mathfrak{P}$ is d, and $0 \ne \mathrm{lc}_{Z_{n+1}} F_\mathfrak{P} \in k[u]$ (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 $0 \ne \mathrm{lc}_{Z_{n+1}} F_\mathfrak{P} \in k[u]$, the polynomial $F_\mathfrak{P}$ is separable with respect to Z_{n+1}, i.e., $\partial F_\mathfrak{P}/\partial Z_{n+1} \ne 0$. Moreover, cf. [3], the morphism $\mathcal{Z}(\mathfrak{P}) \to \pi_U(\mathcal{Z}(\mathfrak{P}))$

induced by π_U is a finite birational isomorphism of projective algebraic varieties defined over k_u.

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

Let $L_0, L_{s+1}, \dots, L_{n+1} \in k[u, X_0, \dots, X_n]$ be linear forms with respect to $X_0, \dots, X_n$ in general position. Denote $L = (L_0, L_{s+1}, \dots, L_{n+1})$. Let $L_i = \sum_{0 \le j \le n} l_{i,j} X_j$, where $l_{i,j} \in k_u$ for all i, j. We substitute $u_{i,j} = l_{i,j}$ for all i, j in $F_{\mathfrak{P}}$ and denote the resulting polynomial by $F_{\mathfrak{P},L} \in k[u, X_0, \dots, X_n]$. Since $L_0, L_{s+1}, \dots, L_{n+1}$ are in general position, the polynomial $F_{\mathfrak{P},L}$ is separable with respect to Z_{n+1}, $\deg F_{\mathfrak{P},L} = \deg_{Z_{n+1}} F_{\mathfrak{P},L} = d$, $0 \ne \operatorname{lc}_{Z_{n+1}} F_{\mathfrak{P},L} \in k[u]$, and the polynomial $F_{\mathfrak{P},L}(L_0, L_{s+1}, \dots, L_{n+1})$ vanishes on $\mathcal{Z}(\mathfrak{P})$. Next, denote by $\pi_L : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \dots : X_n) \mapsto (L_0 : L_{s+1} : \dots : L_{n+1})$, 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 $\pi_L(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_{\mathfrak{P},L})$. Moreover, the morphism $\mathcal{Z}(\mathfrak{P}) \to \pi_L(\mathcal{Z}(\mathfrak{P}))$ induced by π_L is a finite birational isomorphism of projective algebraic varieties defined over k_u. In particular, the polynomial $F_{\mathfrak{P},L}$ is irreducible over k_u.

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

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

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

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

Obviously, the coefficients of Ψ belong to k'_u.

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

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

where all $\xi^{(0)}, \xi_{v,j}$ are in $k[u', t_{i+1}, \dots, t_n]$, $0 \le j \le n$, $\xi^{(0)} \ne 0$, and the greatest common divisor $\mathrm{G\,C\,D}_{v,j}\{\xi^{(0)}, \xi_{v,j}\}$ is equal to 1 in the ring $k[u', t_{i+1}, \dots, t_n]$.

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

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

Next we use estimates for degrees of factors from the algorithm for factoring polynomials; see [2, Chapter 1, §2, Lemma 1.3]. That lemma is deduced as a direct consequence of the construction in Theorem 1.1 of [2, Chapter 1, §1]. We apply that lemma to the following data: the variable Z; the field k; the field $k_u(t_{i+1}, \dots, t_n)[\theta]$; the element θ; the polynomial Ψ; the polynomial $F''(1, t_{i+1}, \dots, t_n, Z)$; the numbers $d+1$, $d+1$, and $d+1$; the family consisting of all elements $u_{v,w}$, t_j, respectively, in place of the variables $X_0, \dots, X_n$; the field H; the field F; the element η; the polynomial φ; the polynomial f; the numbers r, r_1, and r_2; the family $T_1, \dots, T_l$; see the notation in the Introduction in [2]. As a result, we get: $\deg_Z \Psi = d$, and 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.

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

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

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

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

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

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

where all $a_{j,i_0,\dots,i_n}$ are in $k[u]$ and the greatest common divisor $\mathrm{GCD}_{j,i_0,\dots,i_n}\{a_{j,i_0,\dots,i_n}\}$ is equal to 1 in $k[u]$. Next, the bounds established for the degrees of ξ_v and Ψ imply that for every nonzero $a_{j,i_0,\dots,i_n}$ each index j_α is dominated by $(Dd)^{O(1)}$, $i+1 \le \alpha \le n$, and $\deg_{u_{v,w}} a_{j,i_0,\dots,i_n} = (Dd)^{O(1)}$ for all v, w. Hence, there is a subset $J_1 \subset J_0$ such that the number of elements $\#J_1$ is $(Dd)^{O(n-i)}$ and if $a_{j,i_0,\dots,i_n} \ne 0$, then $j \in J_1$. Therefore, viewing the coefficients $F_{i_0,\dots,i_n}$ as unknowns, from (10) we get 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 $\mathfrak{P}_{U_{s+1},\dots,U_i}$. In accordance with the algorithm for solving linear systems, we get $\deg_{u_{v,w}} y_j = (Dd)^{O(n-i)}$ for all v, w and $1 \le j \le \gamma$. Assertion (i) is proved.

Now we prove (ii). Performing if necessary a nondegenerate linear transformation of the coordinate functions $X_0, \dots, X_n$ over k, we may assume that $X_i \notin \mathfrak{P}$ for every $0 \le i \le n$. Now, it suffices to prove only the first assertion in (ii) with $N' = (Dd)^{O(n-i)}$ in place of $N = n(Dd)^{O(n-i)}$: the entire assertion (ii) for old coordinate functions will follow immediately (we can take $N = (n+1)N' - n$).

Let $y = y_j$ for some $1 \le j \le \gamma$, and let $\delta \le D$. Then, see Lemma 4, we have $\pi(y) \in S^{-1}(\mathfrak{P}_{i-1} \cap k[u, X_0, \dots, X_n])$, whence $y - \pi(y) \in U_i S^{-1} k[u, X_0, \dots, X_n]$. 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, $X_j^{N'} \mathfrak{P}_{U_{s+1},\dots,U_i} \subset \mathfrak{P}_{U_{s+1},\dots,U_{i-1}} + (U_i)$ for every $0 \le j \le n$.

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 a 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 we can write

$$X_\rho^{N'} y_j = \sum_{1 \le \alpha \le \sigma} b_{\rho,j,\alpha} y'_\alpha + b_{\rho,j} U_i, \quad b_{\rho,j,\alpha} \in k_u,\ b_{\rho,j} \in k_u[X_0, \dots, X_n]. \tag{11}$$

To complete the proof, we use "specialization of the parameters" $u_{v,j}$. We leave to the reader to check that the explicit construction described above admits "specialization of parameters"; i.e., if $(l_{v,j})$ belong to a nonempty subset of $\mathbb{A}^{(n-s+2)(n+1)}(\bar{k})$ open in the Zariski topology, then the substitution $u_{v,j} = l_{v,j} \in k$ in (7), (8) results in a generic point of the variety $\mathcal{Z}(\mathfrak{P}_{L_{s+1},\dots,L_i})$ with all $L_v = \sum_{0 \le j \le n} l_{v,j} X_j$. Here Lemma 3 is also used. Next, again for a nonempty Zariski open subset, we can substitute $u_{v,j} = l_{v,j}$ in $y_1, \dots, y_\gamma$, obtaining a basis over the field k for 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. A similar assertion is valid 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 $0 \le \delta \le D$, formulas (11), related to a generic point $(u_{v,i})$, also admit "specialization of the parameters". Finally, note that we have a natural linear projection,

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

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

Lemma 6. *In the preceding notation, let $s = \mathrm{ht}(\mathfrak{P}) = n - 1$. Let $\mathcal{U} \subset \mathbb{A}^n(\bar{k})$ be the Zariski open subset of linear forms corresponding to the prime ideal $\mathfrak{P}$; see above. Then for every $L_n \in \mathcal{U} \cap A^{n-s}$ the characteristic function $h(\mathfrak{P}_{L_n}, m) = \dim_k(A/\mathfrak{P}_{L_n})_m$ is stable for $m \ge (n-1)d - n + 2$. Also, for all $m \ge (n-1)d - n + 2$ we have the coincidence*

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

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

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

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

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

Then, for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}' \cap A^{n-s}$ and every $s \le i \le n-1$, the characteristic function

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

is stable for $m \ge D_1$.

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

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

in place of $\mathfrak{P} \subset k[X_0, \dots, X_n]$. As a result, we see that for $i = n$ the characteristic function (13) is stable for $m \ge sd - s + 1$. Now (12) and the exact sequence (14) with $i = n$, see below, imply that for $i = n-1$ the characteristic function (13) is stable for $m \ge sd - s$. This proves the claim for $i = n-1$.

We shall use descending induction on i. Assuming that this characteristic function is stable for $m \ge D_1$ for some $s+1 \le i \le n-1$, we prove that it is stable for $m \ge D_1$ also for $i-1$ (in place of i). We have an exact sequence

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

of vector spaces, and

$$(A/(\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i)))_m = (A/\mathfrak{P}_{L_{s+1},\dots,L_i})_m \quad \text{for} \quad m \ge n(Dd)^{c_4(n-s-1)}$$

by Lemma 5. Hence, (13) is stable for $m \ge D_1$ by the inductive assumption. The lemma is proved. □

End of the proof of Theorem 1. Put $\mathfrak{P} = \mathfrak{P}^{(0)}$; see $(*)$. Hence, by $(*)$, now $\operatorname{ht}(\mathfrak{P}) = s = \mu + 1$ and, by the Bézout theorem, $\deg \mathfrak{P} = \deg \mathfrak{P}^{(0)} = d_1 \le d^s$, instead of $\deg \mathfrak{P} = d$. We have $s \le n-1$ because $\operatorname{ht}(\mathfrak{P}^{(0)}) \le n-1$. Let D be the smallest integer such that the conditions of Lemma 5 are fulfilled for all $s+1 \le i \le n-1$ for $\mathfrak{P} = \mathfrak{P}^{(0)}$, with d_1 in place of d. Let $\mathcal{U}_i'$, $s+1 \le i \le n-1$, be the sets occurring in Lemma 5 (ii) and let $\mathcal{U}' = \bigcap_{s+1\le i\le n-1} \mathcal{U}_i'$. We apply Lemma 7 with d_1 in place of d. So, now $D_1 = \max\{n(Dd_1)^{c_4(n-s-1)}, sd_1 - s\}$. For $i = s$, by $(*)$ we get $D_1 \ge d^{2^{c_2 n}}$. Therefore, for all sufficiently large n and d, we have $D \ge d^{2^{c' n}} + 1$ for an absolute constant $c' > 0$. Hence, for every $(L_{s+1}, \dots, L_n) \in \mathcal{U}' \cap A^{n-s}$, there is an i_0 with $s+1 \le i_0 \le n-1$ such that any system of generators of the prime ideal $\mathfrak{P}_{L_{s+1},\dots,L_{i_0}}$ contains a polynomial of degree at least $d^{2^{c' n}} + 1$ (the integer i_0 may depend on $(L_{s+1}, \dots, L_n)$). We choose and fix $(L_{s+1}, \dots, L_n) \in \mathcal{U}' \cap A^{n-s}$ such that $\mathcal{Z}(\mathfrak{P}^{(0)}) \cap \mathcal{Z}(L_{s+1}, \dots, L_n) \cap \mathcal{L}^{(0)} = \varnothing$ in $\mathbb{P}^n(\bar{k})$, where $\mathcal{L}^{(0)}$ is a linear subspace as in $(*)$. Now we set $\mathfrak{p} = \mathfrak{P}_{L_{s+1},\dots,L_{i_0}}$ and $c = c'$. Then $\mathcal{Z}(\mathfrak{p})$ is a component, defined over k and irreducible over $\bar{k}$, of the algebraic variety $\mathcal{Z}(f_1, \dots, f_{\mu+1}, L_{s+1}, \dots, L_{i_0})$; see Lemma 3. Put $f_j = L_j$ for all $\mu + 2 \le j \le i_0$, and let $\nu = i_0$. Now all the polynomials $f_1, \dots, f_\nu$ are well defined, and assertion (a) of the theorem is satisfied. Obviously assertion (c) is true. By Remark 1, assertion (b) is also true. Theorem 1 is proved. □

Proof of Proposition 1. Let $\mathfrak{p}$ be the ideal constructed in the proof of Theorem 1. Recall that in that proof we used the first Bertini theorem several times, obtaining elements of k instead of transcendental elements. Now we would like to avoid applying the first Bertini theorem. Namely, we replace the family of elements $\lambda_{v,w}$, $1 \le v \le \mu$, $1 \le w \le 4$ (recall that $\lambda_{i,4} = \lambda_{i,3}^{-1}\lambda_{i,2}$ and $\lambda_{i,3} = \lambda_{1,3}$ for all $1 \le i \le \mu$) by a family λ satisfying the same relations and such that λ has the maximal possible transcendency degree over k. We denote the elements of this family λ again by $\lambda_{v,w}$. Denote by k_λ the extension of the field k by all elements of λ. So, now the transcendency degree of the field k_λ over k is $2\mu+1$. Next, we replace the family of coefficients of $l_{i,j}$, $i \in \{0, s+1, \dots, n+1\}$, $0 \le j \le n$, of the linear forms $L_{s+1}, \dots, L_{n+1}$ by a family u of elements $u_{i,j}$ transcendental over k_λ with transcendency degree $(n-s+2)(n+1)$. Denote by $k_{\lambda,u}$ the extension of the field k_λ by all the elements of the family $u_{i,j}$. So, the transcendency degree of the field $k_{\lambda,u}$ over k is $2\mu+1+(n-s+2)(n+1) = O(n^2)$. Let k be a finite field. After the above replacement, by the construction in the proof of Theorem 1, we get a family of polynomials $f_1, \dots, f_\nu \in k_{\lambda,u}[X_0, \dots, X_n]$ (we keep the same notation for them) and a prime ideal $\mathfrak{p}' \subset k_{\lambda,u}[X_0, \dots, X_n]$ in place of $\mathfrak{p} \subset k[X_0, \dots, X_n]$.

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

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

Let Y_0 be a new variable. The homogenization of a polynomial $a \in k[Y_1, \dots, Y_m]$ is the polynomial $\bar{a} = Y_0^{\deg a} a(Y_1/Y_0, \dots, Y_m/Y_0) \in k[Y_0, \dots, Y_m]$. Let $\mathfrak{p}''' \subset k[Y_0, \dots, Y_m]$ be the homogeneous prime ideal generated by all the elements $\bar{a}$ with $a \in \mathfrak{p}''$. Let $\mathbb{P}^m(\bar{k})$ be the projective space with the homogeneous coordinate functions $Y_0, \dots, Y_m$. The projective algebraic variety $\mathcal{Z}(\mathfrak{p}''') \subset \mathbb{P}^m(\bar{k})$ is the closure with respect to the Zariski topology of the affine algebraic varieties $\mathcal{Z}(\mathfrak{p}'')$. Therefore, $\mathcal{Z}(\mathfrak{p}''') \subset \mathbb{P}^m(\bar{k})$ is a component, defined over k and irreducible over $\bar{k}$, of the algebraic variety $\mathcal{Z}(\bar{f}_1, \dots, \bar{f}_\nu) \subset \mathbb{P}^m(\bar{k})$. By $(*)$, $\mathfrak{p}$ is a primary component of the ideal $f_1, \dots, f_\nu$, and $\operatorname{ht}(\mathfrak{p}) = \nu$. Hence, $\mathfrak{p}'''$ is a primary component of the ideal $(\bar{f}_1, \dots, \bar{f}_\nu)$ and $\operatorname{ht}(\mathfrak{p}''') = \nu$. Thus, see the formulation of Proposition 1, over the finite field k the modified assertion (a) of Theorem 1 is valid for m, $\bar{f}_1, \dots, \bar{f}_\nu$, and $\mathfrak{p}'''$ in place of n, $f_1, \dots, f_\nu$, and $\mathfrak{p}$, respectively. Obviously, all the degrees satisfy $\deg_{Y_0,\dots,Y_m} \bar{f}_i < d+1$. For the proof of the new versions of assertions (b) and (c), see the formulation of the proposition, we shall consider also $\bar{f}_1, \dots, \bar{f}_\nu$ and $\mathfrak{p}'''$.

Assertion (c) of Theorem 1 holds true 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 $\mathfrak{p}''$,

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

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

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

This implies assertion (c) in the new version of the theorem, because $n > n_0$ and $d > d_0$ are arbitrary, $m = O(n^2)$, and $\deg \bar{f}_i < d+1$ for all i; see Remark 3. Moreover, obviously,

now in (c) we can replace $d^{2^{c\sqrt{n}}}$ by $d^{2^{c\sqrt{n}}}+1$, which yields a slightly stronger assertion. Then the new version of (b) follows from Remark 1. The proposition is proved. □

Remark 5. Let k be a finite field and t 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 k it suffices to verify that, by 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 the linear forms L_i with degrees $\deg_t \lambda_{v,w}$ and $\deg_t l_{i,j}$ bounded from above by $d^{n^{O(1)}}$.

Remark 6. There is a similar problem for an infinite field k. Let $\lambda_{v,w} \in k$ 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 $d^{n^{O(1)}}$.

A difficultly related to Remarks 5 and 6 is to estimate the size of the normalization of an algebraic variety. I could not find an explicit estimate for the normalization in the literature. However, we see that it can be given. We hope to return to this question in a forthcoming paper. It seems that there are no other principal difficulties (cf. the Appendix in [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 that ideal. Let $\mathfrak{P}$ be a prime ideal as in §3, but now we assume that $\operatorname{ht}(\mathfrak{P}) = s$, $0 \le s \le n$. Thus, $\deg \mathfrak{P} = d$ and the ideal $\bar{k} \otimes_k \mathfrak{P} \subset \bar{k} \otimes_k A$ is radical.

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

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

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

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

Lemma 9. *In the notation of the beginning of this section, suppose that $1 \le s \le n-1$. Then the characteristic function $h(\mathfrak{P}, m) = \dim_k (A/\mathfrak{P})_m$ is stable for all integers $m \ge (sd)^{(c_5(n-s))^{n-s-1}}$ with 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 $0 \le s \le n$ the characteristic function $h(\mathfrak{P}, m)$ is stable for $m \ge (sd)^{(c_5(n-s+1))^{n-s}}$ 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. Without loss of generality we may assume that $1 < s < n$, so that $sd \ge 2$. We show that for all $(L_{s+1}, \dots, L_n)$ in a nonempty Zariski open subset of $\mathbb{A}^{(n-s)(n+1)}(k)$ and for all $s \le i \le n-1$, the characteristic function (13) is stable for $m \ge (sd)^{(c_5(n-s))^{n-i-1}}$, and hence, by Remark 1, the ideal $\mathfrak{P}_{L_{s+1},\dots,L_i}$ has a system of homogeneous generators of degrees at most $1+(sd)^{(c_5(n-s))^{n-i-1}}$ with an absolute constant $c_5 > 0$. Indeed, this is true for $i = n-1$ by Lemma 6. We shall use descending induction on i. Assuming that our claim is proved for some $s+1 \le i \le n-1$, we check 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 hypothesis and Lemma 5 with $D = (sd)^{(c_5(n-s))^{n-i-1}}$, for all $(L_{s+1}, \dots, L_n) \in \bigcap_{i \le j \le n-1} \mathcal{U}'_j \cap A^{n-s}$ (the set $\mathcal{U}'_i$ is defined at this step of induction in Lemma 5 (ii), and similarly, the sets $\mathcal{U}'_j$, $i+1 \le j \le n-1$, are defined at the preceding steps of induction) we have $(A/(\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i)))_m = (A/\mathfrak{P}_{L_{s+1},\dots,L_i})_m$ with

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

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

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

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

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

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

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

over the ring of polynomials $\bar{k}[X_0, \dots, X_n]$. By [6, 10], in $(\bar{k} \otimes_k A)^{s+1}$ the submodule of solutions $(Z, Z_1, \dots, Z_s)$ of equation (16) has a system of generators $z_i, z_{i,1}, \dots, z_{i,s}$, $i \in I$, consisting of polynomials from $\bar{k} \otimes_k A$ 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, $z_i \in \bar{k} \otimes_k A$, $i \in I$, is a system of generators of $\bar{k} \otimes_k \mathfrak{P}$ of the required degrees. Since the variety $\mathcal{Z}(\mathfrak{P})$ is

defined over k, there is also a system of generators $q_1, \dots, q_w \in k[X_0, \dots, X_n]$ of the ideal $\mathfrak{P}$ with $\deg q_i \le d^{2^{c_6 n}}$ for all $1 \le i \le w$. The lemma is proved. □

Corollary 1. *In the notation of the beginning of this 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 $m \ge d^{2^{c_7 n}}$.*

Proof. Indeed, by Lemma 8 and [8], there is no loss of generality in assuming that $\operatorname{ht}(\mathfrak{P}) = s \le n-1$. By Lemma 10 with the ground field k_u in place of k, the conditions of Lemma 5 are fulfilled for all $s+1 \le i \le n-1$ for $D = d^{2^{c_6 n}} + 1$. Let $(L_{s+1}, \dots, L_n) \in \bigcap_{s+1 \le i \le n-1} \mathcal{U}_i' \cap A^{n-s}$; see Lemma 5 (ii). Now the claim follows from Lemma 7. The corollary is proved. □

References

[1] M. Baldassarri, *Algebraic varieties*, Ergeb. Math. Grenzgeb., Heft 12, Springer-Verlag, Berlin, 1956. MR0082172 (18:508f)

[2] A. L. Chistov, *An algorithm of polynomial complexity for factoring polynomials, and finding the components of varieties in subexponential time*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **137** (1984), 124–188; English transl., J. Soviet Math. **34** (1986), no. 4, 1838–1882. MR0762101 (86g:11077b)

[3] ———, *Efficient construction of local parameters of irreducible components of an algebraic variety*, Trudy S.-Peterburg. Mat. Obshch., vol. 7, Nauchn. Kniga, Novosibirsk, 1999, pp. 230–266; English transl. in Amer. Math. Soc. Transl. Ser. 2, vol. 203, Amer. Math. Soc., Providence, RI, 2001. MR1784700 (2002b:14081)

[4] ———, *A deterministic polynomial–time algorithm for the first Bertini theorem*, Preprint S.-Peterburg. Mat. Obshch. no. 9, 2004, http://www.mathsoc.spb.ru/preprint/.

[5] T. W. Dubé, *The structure of polynomial ideals and Gröbner bases*, SIAM J. Comput. **19** (1990), 750–775. MR1053942 (91h:13021)

[6] G. Hermann, *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95** (1926), 736–788. MR1512302

[7] D. Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534. MR1510634

[8] D. Lazard, *Algèbre linéaire sur $k[x_1, \dots, x_n]$ et élimination*, Bull. Soc. Math. France **105** (1977), 165–190. MR0491702 (58:10905)

[9] E. W. Mayr and A. R. Meyer, *The complexity of the word problems for commutative semigroups and polynomial ideals*, Adv. Math. **46** (1982), 305–329. MR0683204 (84g:20099)

[10] A. Seidenberg, *Constructions in algebra*, Trans. Amer. Math. Soc. **197** (1974), 273–313. MR0349648 (50:2141)

[11] Chee K. Yap, *A new lower bound construction for commutative Thue systems, with applications*, J. Symbolic Comput. **12** (1991), 1–27. MR1124303 (92i:03046)

[12] O. Zariski, *Pencils on an algebraic variety and a new proof of a theorem of Bertini*, Trans. Amer. Math. Soc. **50** (1941), 48–70. MR0004241 (2:345a)

St. Petersburg Branch, Steklov Mathematical Institute, Russian Academy of Sciences, Fontanka 27, 191023 St. Petersburg, Russia

E-mail address: alch@pdmi.ras.ru

Received 10/APR/2008

Translated by THE AUTHOR