INEQUALITIES FOR HILBERT FUNCTIONS
AND PRIMARY DECOMPOSITIONS

A. L. CHISTOV

Dedicated to the centenary of D. K. Faddeev’s birth

Abstract. Upper bounds are found for the characteristic function of a homogeneous
polynomial ideal \( I \); such estimates were previously known only for a radical ideal \( I \).
An analog of the first Bertini theorem for primary decompositions is formulated and
proved. Also, a new representation for primary ideals and modules is introduced and
used, which is convenient from an algorithmic point of view.

Introduction

Let \( k \) be a field with the characteristic exponent \( p \). Let \( I \subset k[X_0, \ldots, X_n] = A \) be a
homogeneous polynomial ideal, and let \((A/I)_m, m \geq 0\), be a homogeneous component
of degree \( m \) of \( A/I \) (see below for more details). Our aim in this paper is to get upper
bounds (1) and (5) for the characteristic function \( h(I, m) = \dim_k(A/I)_m \) of the ideal \( I \).
Earlier, similar bounds have been known only for the case of radical ideals over a perfect
ground field \( k \); see [2, 6] and a short survey of these results below. Such upper bounds
have important applications [2, 4, 5, 8, 11]. An inequality similar to (5) is obtained also
for primary modules; see Theorem 4. The main tool for the proof of (5) is a version of
the first Bertini theorem for primary decompositions; see Theorem 3. Besides that, in
this paper we introduce (and use) a new representation for primary ideals and modules,
which is convenient from an algorithmic point of view.

Important lower bounds for Hilbert functions can be found in the classical paper [10]
and also in [9]. For other interesting lower bounds, see [4], but we do not discuss them
in this paper.

Let \( \text{ass}(I) \) be the set of all associated prime ideals of the ideal \( I \) (it is well known
that they are homogeneous prime ideals), and let \( I = \bigcap_{p \in \text{ass}(I)} I(p) \) be an irredundant
primary decomposition of the ideal \( I \); here \( I(p) \) is a \( p \)-primary component of \( I \). Let
\( \text{ht}(p) = s(p), 0 \leq s(p) \leq n + 1 \), and let \( d(I(q)) \) be the degree of the \( p \)-primary ideal
\( I(p) \); see below for more details. By definition, put \( s(I(p)) = s(p) \) for every \( p \in \text{ass}(I) \)
and \( s(I) = \min\{s(p) : p \in \text{ass}(I)\} \). If \( s(p) = n + 1 \), then \( p = (X_0, \ldots, X_n) = \mathfrak{M} \) is the
maximal homogeneous ideal.

Let \( k^p \) be the perfect closure of the field \( k \). Let \( I \) be a primary ideal. Then the
ideal \( \bar{I} = I \otimes_k k^p \) is \( p \)-primary for a prime ideal \( \bar{p} \subset k^p \) \([X_0, \ldots, X_n]\). Let \( e \) be the
smallest integer such that \( (\bar{p})^e \subset \bar{I} \). By definition, we put \( e = e(I) = e(\bar{I}) \) to be the
exponent of \( I \) (actually it is the exponent of \( \bar{I} \) and not necessarily the exponent of \( I \) in
the sense generally accepted, but this definition is convenient for us and will not lead to
ambiguity in this paper).

2000 Mathematics Subject Classification. Primary 12F15, 12F20.

Key words and phrases. Characteristic function of an ideal, first Bertini theorem, Hilbert functions.

©2008 American Mathematical Society
Our first estimate for the characteristic function $h(I, m)$ of a $p$-primary ideal $I = I(p)$ is given in Theorem 1. For many primary ideals $I$, the bound obtained in Theorem 1 can be majorized by $C(n)d(I)m^{n-s(p)}$, $m \geq 1$, where $C(n)$ is a constant depending only on $n$. Hence, Theorem 1 for a primary ideal is similar to the initial result in [2], obtained for a prime ideal; see below for more details.

**Theorem 1.** Let $I$ be a homogeneous $p$-primary ideal, and let $d = d(p)$, $1 \leq s = s(p) \leq n$, $e = e(I)$; see the notation above. Then there is an absolute constant $C > 0$ (which can be computed explicitly) such that the characteristic function $h(I, m)$ of the ideal $I$ satisfies the inequality

$$h(I, m) \leq n^{2C}d e^s m^{n-s}, \quad m \geq 1. \quad (1)$$

The proof of this theorem involves the author’s results from [3, 4] and inequality (2), which is interesting by itself. Namely, for an ideal $I$, let $\text{ass}(I)$ denote the subset of $\text{ass}(I)$ consisting of all isolated associated prime ideals of $I$. Let $f_1, \ldots, f_s \in k[X_0, \ldots, X_n]$ be homogeneous polynomials such that $f_i \notin k$ for every $1 \leq i \leq s$. Put $I^{(s)} = \bigcap_{q \in \text{ass}(I), s(q) = s} I(q)$. Then for every $m \geq 0$ we have

$$h(I^{(s)}, m) \leq \left(\frac{m + n - s}{n - s}\right) \prod_{1 \leq i \leq s} \deg f_i; \quad (2)$$

see Lemma 1 for more details.

Consider the restrictions $m \geq \sum_{1 \leq i \leq s} \deg f_i$ and $\mathcal{Z}(I^{(s)}) \setminus \mathcal{Z}(X_n) = \mathcal{Z}(I) \setminus \mathcal{Z}(X_n)$ in $\mathbb{P}^n(k)$. Inequality (2) with such restrictions was formulated in Subsection 2.4 of [8] actually without proof (in my opinion, in the proof suggested in [8], there are inequalities of opposite directions in a chain, which gives nothing). This assertion is an essential part of [8]. In any case, [8] contains a very nice proof of the bounds for the Effective Nullstellensatz, and without using any duality. Thus, (2) and Lemma 1 are important for the Effective Nullstellensatz under this approach; cf. also [11]. In Lemma 2 we prove some additional interesting inequality. Although we do not use it in this paper.

We need some definitions. For $\mathfrak{m} \neq p \in \text{ass}(I)$, put $s = s(p)$. Let $U_i = \sum_{0 \leq j \leq n} u_{i,j} X_j$, $1 \leq i \leq n - s$, be generic linear forms; i.e., the transcendency degree of the family $u = \{u_{i,j}\}_{1 \leq i \leq n-s, 0 \leq j \leq n}$ over the field $k$ is $(n-s)(n+1)$. Denote by $k(u)$ the field generated over $k$ by all elements of the family $u$. We extend the ground field $k$ to $k(u)$. Let $0 \leq w \leq n - s - 1$ be an integer. We denote by $V_w = \text{Proj}(A/I(p) + (U_1, \ldots, U_w))$ the projective scheme over $k(u)$ and by $\Gamma(V_w, \mathcal{O}_{V_w}(\nu))$ the vector space of the global sections of the sheaf $\mathcal{O}_{V_w}(\nu)$, $\nu \in \mathbb{Z}$; see [3]. By definition, for every $0 \leq w \leq n - s - 1$ (if $s = n$, then $w$ does not exist), we set

$$\nu_w(A/I, p) = \inf\{\nu : \Gamma(V_w, \mathcal{O}_{V_w}(\nu)) \neq \{0\}\}$$

and

$$\nu(A/I, p) = \begin{cases} \nu_{n-s-1}(A/I, p) & \text{if } s = s(p) < n, \\ 0 & \text{if } s = s(p) = n. \end{cases}$$

Lemma 3 and Theorem 4 imply that if $s(p) < n$, then

$$-\infty < \nu_{n-s-1}(A/I, p) \leq \nu_{n-s-2}(A/I, p) \leq \cdots \leq \nu_0(A/I, p), \quad (3)$$

and hence, all $\nu_w(A/I, p)$ and $\nu(A/I, p)$ are integers. From Theorem 3 we get the upper bounds (9) and (10) for $-\nu(A/I, p)$.

Put $\gamma(I) = \sup_{m \geq 1} h(I(\mathfrak{m}), m)$ if $\mathfrak{m} \in \text{ass}(I)$ and $\gamma(I) = 0$ if $\mathfrak{m} \notin \text{ass}(I)$. 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
Now we can present our second upper bound. Namely, for an arbitrary ideal $I$ over $k$ dimension 1. Then the result is deduced from the Riemann–Roch theorem. Note that exact cohomological sequence obtained from the short exact sequence of sheaves that short proof of the result of [6] can be obtained as follows. One can consider the long proof in [6] is not easy.

In a letter to the author of [6], see the last section of [6], J. Kollar noticed that a short proof of the result of [6] can be obtained as follows. One can consider the long exact cohomological sequence obtained from the short exact sequence of sheaves that corresponds to the generic hyperplane section, and reduce the problem to the case of dimension 1. Then the result is deduced from the Riemann–Roch theorem. Note that
one more step can be performed in the last construction, which reduces everything to dimension 0 (although the resulting zero-dimensional variety is not necessarily irreducible) and avoids any reference to the Riemann–Roch theorem.

The same idea can be used with another functor; this leads to an estimate for the Hilbert function of the integral closure of a homogeneous ring for an irreducible projective algebraic variety (observe that this integral closure is not necessarily a homogeneous ring of a projective algebraic variety, because it may fail to be generated as a ring by its homogeneous component of degree 1). Namely, the following result is valid.

**Theorem 2.** Let $k$ be a perfect field, and let $p \subset k[X_0, \ldots, X_n]$ be a homogeneous prime ideal with $s = s(p) \leq n$, $d = d(p)$; see the notation above. Denote $B = A/p$. Let $\overline{B}$ be the integral closure of $B$ in its field of fractions; then $\overline{B}$ is a graded ring. Let $\overline{B}_m$, $m \geq 0$, denote the finite-dimensional $k$-vector space that is a homogeneous component of degree $m$ of $\overline{B}$. Then for the Hilbert function of $\overline{B}$ we have

$$H(\overline{B}, m) = \dim_k \overline{B}_m \leq \left(\frac{m + n - s}{n - s}\right) d, \quad m \geq 0.$$ 

In the paper [5], inequality (6) was proved for $B$ in place of $\overline{B}$. Thus, Theorem 2 also refines the main result of [5].

Let us return to inequality (5). We also use the functor of global sections of a sheaf in the proof of this inequality. However, the idea suggested by J. Kollar is not sufficient to get the required upper bound (5) in the case of a primary ideal. Additionally, we need an analog of the first Bertini theorem previously known for irreducible algebraic varieties; see [12]. This analog is of interest by itself. We prove it in a rather general situation: for reductions of finitely generated graded $A$-modules by linear forms; see Theorem 4. In brief, for the case of one linear form, this result is as follows. Assume (here only for simplicity) that the field $k$ is perfect and infinite. Let $M$ be a graded finitely generated $A$-module, let $\text{Ass}(M)$ be the set of all associated prime ideals of $M$, let $\{0\} = \bigcap_{p \in \text{Ass}(M)} M(p)$ be an irredundant primary decomposition of $\{0\}$ in $M$, let $p \in \text{Ass}(M)$ be a prime ideal with $s = s(p) \leq n - 2$, and let $L \in A$ be a linear form in general position. Then $p + LA = p_L \cap \Omega_L$, where $p_L$ is a prime ideal with $s(p_L) = s + 1$ and $\Omega_L$ is an $M$-primary ideal or $\Omega_L = A$ (this follows from the classical first Bertini theorem). Next, each $P \in \text{Ass}(M/LM)$ with $s(P) = s + 1 \leq n - 1$ has the form $P = p_L$ for a uniquely determined $p \in \text{Ass}(M)$ with $s(p) = s$. Finally, there is an irredundant primary decomposition $\{0\} = \bigcap_{p \in \text{Ass}(M/LM)} (M(P)/LM) \text{ of } \{0\} \text{ in } M/LM$ (here $M(P)$ is a submodule of $M$) such that for every $p \in \text{Ass}(M)$ with $s = s(p) \leq n - 2$ the module $LM + M(p)$ is equal to $M(p_L) \cap M'(p)$, where $M/M'(p)$ is an $M$-primary module or $M = M'(p)$. Theorem 4 is formulated over an arbitrary field and also gives information about the case of $s = n - 1$.

Of course, a $P$-primary ideal $I$ can be given by a system of generators (which are homogeneous polynomials), and $\nu(A/I, p)$ can be estimated by a function of an upper bound $d'$ for the degrees of these generators. Below we suggest another natural representation of a primary ideal, which depends on $d$, on the exponent $e$ of the ideal $I \otimes_k k^{p-\infty}$, and on some integer $\delta$ to be introduced below. Only homogeneous polynomials of degree $(e d \delta)^{O(1)}$ are used to give $I$. We get a smaller length of representation in comparison with that via a system of generators of $I$, because $d'$ is estimated from above by $(e d \delta)^{2^{2^e}}$ (only such bounds are known in the general case). Now we describe this new representation of a primary ideal explicitly, and give a bound for $\nu(A/I, p)$ in the case where $I = I(p)$, $p \in \text{ass}(I)$, $s(p) \leq n$.

First, we consider the case where the field $k$ is perfect and contains sufficiently many elements. Put $s = s(p)$, $d = d(p)$, and let $e = e(I(p))$ be the exponent of $I(p)$, i.e.,
the smallest integer such that \( p^e \subset I(p) \). Let \( E_0, E_{s+1}, \ldots, E_n \in k[X_0, \ldots, X_n] \) be linearly independent linear forms. Set \( A_0 = k[E_0, E_{s+1}, \ldots, E_n] \) (this ring \( A_0 \) should not be confused with the homogeneous component of degree 0 of \( A \); this notation will not cause any ambiguity), and let \( K_0 \) be the field of fractions of \( A_0 \). We denote by \( S_0 = A_0 \setminus \{0\} \) the multiplicatively closed set. Now \( K_0 = S_0^{-1}A_0 = k(E_0, E_{s+1}, \ldots, E_n) \) is the localization of \( A_0 \) with respect to \( S_0 \). Since the field \( k \) is perfect and contains sufficiently many elements, there are linear forms \( E_0, E_{s+1}, \ldots, E_n \in k[X_0, X_1, \ldots, X_n] \) such that \( A/p \) is a finitely generated \( k[E_0, E_{s+1}, \ldots, E_n]-\)module and \( S_0^{-1}(A/p) \supset S_0^{-1}A_0 = K_0 \) is a separable extension of \( K_0 \) of degree \( d \).

There exist homogeneous polynomials \( \eta_i, 0 \leq i \leq d-1 \), of degrees at most \( d-1 \) such that the elements \( \eta_i = \eta_i \mod p \), \( 0 \leq i \leq d-1 \), form a basis of the vector space \( S_0^{-1}(A/p) \) over \( K_0 \). Moreover, \( \sum_{0 \leq i \leq d-1} A_0 \eta_i \) is an \( A_0 \)-algebra, i.e., \( \sum_{0 \leq i \leq d-1} A_0 \eta_i \in \sum_{0 \leq i \leq d-1} A_0 \eta_i \) for all \( 0 \leq i \leq d-1 \). We can put, e.g., \( \eta_i = E_{n+i}^i \), where \( E_{n+i+1} \) is the linear form described in \( \S3 \); see (27). Let \( h_1, \ldots, h_s \in A \) be homogeneous polynomials such that \( (h_1, \ldots, h_s)(p) = p \); i.e., \( p \) is a \( p \)-primary component of the ideal generated by \( h_1, \ldots, h_s \). We choose \( h_1, \ldots, h_s \) with degrees at most \( d \) (it is well known that such \( h_1, \ldots, h_s \) exist).

Set \( p^{e}(s) = (h_1, \ldots, h_s)^e(p) \).

A primary ideal \( I(p) \) is uniquely determined by its localization \( S_0^{-1}I(p) \), and hence also by the \( K_0 \)-vector subspace \( W = S_0^{-1}I(p)/S_0^{-1}p^{e}(s) \subset S_0^{-1}(A/p^{e}(s)) \). Set

\[
J = \{(j_1, \ldots, j_s) \in \mathbb{Z}^s : j_1, \ldots, j_s \geq 0 \& j_1 + \cdots + j_s \leq e-1 \},
J_1 = \{(j_0, j_1, \ldots, j_s) \in \mathbb{Z}^{s+1} : 0 \leq j_0 \leq d-1 \& (j_1, \ldots, j_s) \in J \},
\]

and let \( \varepsilon = 1 \mod p^{e}(s) \), and \( e_j = \eta_j h_1^{j_1} \cdots h_s^{j_s} \in A \) for every \( j = (j_0, j_1, \ldots, j_s) \in J_1 \). The algebra \( S_0^{-1}(A/p^{e}(s)) \) has the basis \( e_j \varepsilon, j \in J_1 \), over the field \( K_0 \). Notice that for the number of elements of \( J_1 \) we have \( \#J_1 = d(\varepsilon^{s+1}) \).

Let \( \dim_{K_0} W = \mu \), and let \( w_i = \sum_{j \in J_1} w_{i,j} e_j \varepsilon, 1 \leq i \leq \mu \leq (\varepsilon^{s+1})d \), be a basis of \( W \) over \( K_0 \), where all \( w_{i,j} \) belong to \( A_0 \). We may assume without loss of generality that all \( w_{i,j} \) belong to \( A_0 \) (to ensure this, we multiply \( w_{i,j} \) by the least common denominator of all \( w_{i,j} \) in \( A_0 \)) and that all \( w_{i,j} \) are homogeneous. Thus, \( I(p) \) is determined by \( p, e, \eta_j, 0 \leq j \leq d-1, h_1, \ldots, h_s \), an integer \( \mu, 1 \leq \mu \leq \#J_1 \), and the matrix \( (w_{i,j})_{1 \leq i \leq \mu, j \in J_1} \) with entries in \( A_0 \).

Conversely, let \( \pi : S_0^{-1}A \to S_0^{-1}(A/p^{e}(s)) \) be the natural projection. Then any linear subspace \( W \subset S_0^{-1}(A/p^{e}(s)) \) that is an ideal of the \( K_0 \)-algebra \( S_0^{-1}(A/p^{e}(s)) \) (distinct from this algebra itself) corresponds to a \( p \)-primary ideal \( I = A \cap \pi^{-1}(W) \); see Lemma 6 in \( \S3 \). The \( W \mapsto I \) and \( I \mapsto W \) considered above are inverse to each other.

Set \( \delta = \max_{i,j} \deg_{E_0, E_{s+1}, \ldots, E_n} w_{i,j} \). Hence, \( \delta \) depends on all the objects in the above description. However, in what follows we write \( \delta = \delta(I) \). This will not lead to ambiguity.

Let \( t \) be a transcendental element over \( k \). To define \( \delta \) for an arbitrary field, we extend \( k \) up to the perfect closure \( k(t)^{p^{-\infty}} \) of the field \( k(t) \), where \( p \) is the characteristic exponent of the field \( k \). Denote \( k'(t) = k(t)^{p^{-\infty}} \). The ideal \( I \) is replaced by \( I' = I \otimes_k k' \subset k'[X_0, \ldots, X_n] \).

If \( I \) is a primary ideal and \( s(I) \leq n \), then \( I' \) is primary and \( s(I') = s(I) \leq n \). Hence an integer \( \delta(I') \) is defined. Put \( \delta = \delta(I) = \delta(I') \). So, actually, \( \delta(I) \) is not uniquely determined and depends on all the objects occurring in the construction of \( \delta(I') \).

If \( \text{char}(k) = p > 0 \), we put \( \alpha \) to be the integer such that \( p^\alpha > e \geq p^{\alpha-1} \). We shall consider two cases:

\[
(7) \quad \text{char}(k) = 0 \quad \text{or} \quad \text{char}(k) = p > 0 \& \alpha = 1,
(8) \quad \text{char}(k) = p > 0 \& \alpha > 1.
\]
In Theorem 3 we shall prove that

\begin{align}
0 & \leq -\nu(A/I,p) \leq \mu\delta + e(es - s + 2)d(d - 1)/2 \quad \text{if (7) is true,} \\
0 & \leq -\nu(A/I,p) < \mu\delta + (s + 1)e^{s+2}d^2 \quad \text{if (8) is true.}
\end{align}

Now we proceed to the details. We introduce a graduation on the ring \( A \), by representing \( A = \bigoplus_{i \geq 0} A_i \), where \( A_i \) is the set of homogeneous polynomials in \( A \) of degree \( i \).

Let \( \overline{k} \) be the algebraic closure of the field \( k \), and let \( \mathbb{P}^n(\overline{k}) \) be an \( n \)-dimensional projective space over \( \overline{k} \) with homogeneous coordinates \( X_0, \ldots, X_n \). For an ideal \( I \subseteq A \), denote by \( \mathcal{Z}(I) \subseteq \mathbb{P}^n(\overline{k}) \) the projective algebraic variety of all common zeros of the polynomials in \( I \).

Let \( M \) be a finitely generated graded \( A \)-module. Then \( M = \bigoplus_{i \in \mathbb{Z}} M_i = \{0\} \) is a direct sum of its homogeneous components \( M_i, i \in \mathbb{Z} \), each \( M_i \) is a finite-dimensional vector space over \( k \), and there is an integer \( N \) such that \( M_i = \{0\} \) for all \( i < N \). The set of all homogeneous prime ideals of height \( n \) in \( \text{Supp}(M) = \{p \in \text{Spec}(A) : M_p \neq \emptyset\} \) determines a projective algebraic variety \( V(M) \) in \( \mathbb{P}^n(\overline{k}) \). In what follows, unless we state otherwise, the homomorphisms of graded modules are of degree 0.

The Hilbert function of the module \( M \) is \( H(M,m) = \dim_k M_m, m \in \mathbb{Z} \). It is well known that there is a polynomial \( P(M,Z) \in \mathbb{Q}[Z] \) such that for all sufficiently large \( m \) the characteristic function satisfies \( H(M,m) = P(M,m) \). For the degree, we have \( \deg P(M,Z) = n - s = \dim V(M) \) (here we assume that the dimension of the empty set is \(-1\)), where \( 0 \leq s = s(M) \leq n + 1 \). Now the polynomial \((n - s)!P(M,Z)\) has integral coefficients. The degree \( D(M) \) of the module \( M \) is the coefficient of \( Z^{n-s} \) in the polynomial \((n - s)!P(M,Z)\) for \( 0 \leq s \leq n \), and \( D(M) = 0 \) if \( s = n + 1 \).

Let \( \text{Ass}(M) \) be the set of all associated prime ideals of the module \( M \) (in \( \text{Spec}(A) \)), and let

\begin{equation}
\{0\} = \bigcap_{p \in \text{Ass}(M)} M(p)
\end{equation}

be an irredundant primary decomposition of \( \{0\} \subset M \). Here \( M(p) \subset M \) is a graded submodule of \( M \), and \( M/M(p) \) is a \( p \)-primary module for every \( p \in \text{Ass}(M) \). Hence, we have an embedding \( M \rightarrow \prod_{p \in \text{Ass}(M)} (M/M(p)) \), and \( H(M,m) = \sum_{p \in \text{Ass}(M)} H(M/M(p),m) \) for all integers \( m \).

Let \( p \in \text{Ass}(M) \). Let \( S_p = A \setminus p \) be a multiplicatively closed set. For every \( A \)-module \( N \), denote by \( N_p = S_p^{-1}N \) the localization of \( N \). Hence, \( A_p \) is a local ring and \( (A/p)_p \) is a field. We denote the latter field by \( K_p \). Let \( l(M/M(p)) = \dim_{K_p} (M/M(p))_p \) be the dimension of the \( K_p \)-vector space \( (M/M(p))_p \). Then

\[ D(M/M(p)) = l(M/M(p))D(A/p) \]

by Lemma 3 (see below), and \( D(A/p) = d(p) = \deg \mathcal{Z}(p) \) is the degree of the projective algebraic variety \( \mathcal{Z}(p) \subseteq \mathbb{P}^n(\overline{k}) \). Note that if \( 0 \leq s(A/p) \leq n \), then \( \mathcal{Z}(p) \) is irreducible over \( k \). If \( s(A/p) = n + 1 \), then \( \mathcal{Z}(p) = \emptyset \) and \( d(p) = \deg \mathcal{Z}(p) = 0 \).

For a graded \( A \)-module \( M \) and an integer \( \nu \), we denote by \( M(\nu) \) the graded \( A \)-module with shifted graduation. 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 \( M(\nu) \cong M \). This isomorphism is an isomorphism of degree \( \nu \) of graded \( A \)-modules \( M(\nu) \) and \( M \).

Denote by \( X = \mathbb{P}^n_k = \text{Proj}(A) \) the scheme of the projective space and by \( \mathcal{O}_X \) the sheaf corresponding to \( \mathcal{O}_k^n \); see [3]. Let \( \mathcal{M} \) be the sheaf corresponding to the module \( M \); see [3]. Then \( \mathcal{M} \) is a sheaf of \( \mathcal{O}_X \)-modules. For every integer \( \nu \) the sheaf \( \mathcal{M}(\nu) \) is defined. We can identify \( M(\nu) \cong \mathcal{M}(\nu) \); see [3]. For every integer \( \nu \), let \( M_\nu^\circ = \Gamma(X, M(\nu) \cong M(\nu)) \) be
the finite-dimensional vector space of global sections of the sheaf $M(\nu)^\sim$. Put $M^\gamma = \bigoplus_{m \in \mathbb{Z}} \Gamma(X, M(m)^\sim)$. Then $M^\gamma$ is a graded $A$-module in a natural way; see [3]. The functor $N \mapsto N^\gamma$ is exact from the left; see [3].

If $p \subset A$ is a homogeneous prime ideal of height $\text{ht}(p) = n$, then $\dim_k(A/p)_m = d(p)$ for every integer $m$. This follows from the exact sequence of the hyperplane section; see below. If there exists $p \in \text{Ass}(M)$ with $\text{ht}(p) = n$, then there is a monomorphism $(A/p)(\nu) \rightarrow M$ for some integer $\nu$, and hence, by the exactness from the left of the functor $N \mapsto N^\gamma$, the vector space $M^\gamma_p$ is nonzero for every integer $m$. Therefore, in the case under consideration, the module $M^\gamma$ is not finitely generated. On the other hand, if $\text{ht}(p) \neq n$ for every $p \in \text{Ass}(M)$, then $M^\gamma$ is a finitely generated $A$-module. This follows from Lemma 3 in §2, the existence of the embedding $M \rightarrow \prod_{p \in \text{Ass}(M)} M/M(p)$, and again the exactness from the left of the functor $N \mapsto N^\gamma$.

Suppose $p \in \text{Ass}(M)$ and $\text{ht}(p) = s \leq n$. Let the linear forms $U_1, \ldots, U_{n-s}$, the family $u$, and the field $k(u)$ be as in the definition of $\nu_w(A/I, p)$; see above. We extend the ground field $k$ to $k(u)$. We denote by $X_{k(u)}$ the scheme of the projective space $\mathbb{P}^n_{k(u)} = \text{Proj}(A \otimes_k k(u))$. Let $0 \leq w \leq n-s-1$ be an integer, and let $Q_w = M/(M + U_1 M + \cdots + U_w M)$ be a graded $A \otimes_k k(u)$-module. The vector space of the global sections of the sheaf $Q_w(\nu)$, $\nu \in \mathbb{Z}$, will be denoted by $\Gamma(X_{k(u)}, \Omega_w(\nu))$ (see [3]). By definition, for every $0 \leq w \leq n-s-1$ (if $s = n$, then $w$ does not exist), we have

$$\nu_w(M, p) = \inf \{\nu : \Gamma(X_{k(u)}, \Omega_w(\nu)) \neq \{0\} \}$$

and

$$\nu(M, p) = \begin{cases} \nu_{n-s-1}(M, p) & \text{if } s = s(p) < n, \\ 0 & \text{if } s = s(p) = n. \end{cases}$$

Lemma 3 and Theorem 4 show that all $\nu_w(M, p)$ and $\nu(M/I, p)$ are integers.

Put $\gamma(M) = \sup_{m \in \mathbb{Z}} H(M/M(\mathfrak{M}), m)$ if $\mathfrak{M} \in \text{Ass}(M)$ and $\gamma(M) = 0$ if $\mathfrak{M} \notin \text{Ass}(M)$.

Now we consider the special case of $M = A/I$, where $I$ is a homogeneous ideal of $A$. We have $V(A/I) = \mathbb{Z}(I) \subset \mathbb{P}^n(k)$. The characteristic function $h(I, m)$ of the ideal $I$ is the Hilbert function of $A/I$. So, $h(I, m) = H(A/I, m)$. We denote $P(A/I, m) = p(I, m)$, $D(A/I) = d(I)$, $m \geq 0$, and $\text{Ass}(A/I) = \text{ass}(I)$. For every $p \in \text{ass}(I)$, we set $(A/I)(p) = A/I(p)$ for an ideal $I(p) \subset A$ (this notation $I(p)$ will not lead to ambiguity). Then $I(p)$ is a $p$-primary ideal of $A$, and

$$I = \bigcap_{p \in \text{ass}(I)} I(p)$$

is an irredundant primary decomposition of $I$.

Now we generalize the representation of primary ideals described above to the case of primary modules. Let $M$ be a finitely generated $p$-primary module. Let $s = s(p) \leq n$, $d = d(p)$. We have $s(M) = s(p)$; see above. First, suppose that the field $k$ is perfect and contains sufficiently many elements. The exponent $e = e(M)$ of the module $M$ is the smallest integer such that $p^e M = \{0\}$. Let the linear forms $E_0, E_{s+1}, \ldots, E_n$, the ring $A_0$, the field $K_0$, and the multiplicatively closed set $S_0$ be as above. We define the module $M$ as follows. Let $B = \bigoplus_{1 \leq i \leq n} A_0(a_i)$ for some integers $a_i$. We assume that for the module $M$ there is an exact sequence of homomorphisms (of degree 0) of graded modules

$$0 \rightarrow B' \xrightarrow{\varphi} B \rightarrow M \rightarrow 0$$

such that $\varphi(B') \supset p^{(e)}B$. Denote $W = S_0^{-1}B'/S_0^{-1}p^{(e)}B$. It is a $K_0$-vector subspace of the finite-dimensional vector space $S_0^{-1}(B/p^{(e)}B)$. Let $\pi : S_0^{-1}B \rightarrow S_0^{-1}(B/p^{(e)}B)$ denote the natural projection. We have $B' = B \cap \pi^{-1}(W)$. 
Set \( \mathcal{J} = \{1, \ldots, n_1\} \times J_1 \). For every \( \iota = (i, j) \in \mathcal{J} \) with \( i \in \mathbb{Z} \), \( j \in J_1 \), we let \( \varepsilon_{\iota} \in B \) be the canonical generator (corresponding to \( 1 \in A \)) of the direct summand \( A(a_{\iota})/p(\iota)A(a_{\iota}) \subset B \), and \( e_{\iota} = e_{\iota}\varepsilon_{\iota} \in B \), where \( e_j = \eta_\mu h_1^{i_1} \cdots h_2^{i_2} \). Hence \( e_{\iota}, \iota \in \mathcal{J} \), is a basis of the \( K_0 \)-vector space \( S^{-1}_0(B/p(\iota)B) \).

Let \( \dim_{K_0} W = \mu \), and let \( w_i = \sum_{\iota \in J} w_{i,\iota} e_{\iota}, 1 \leq i \leq \mu \leq (\nu - 1 + s)n_1d \), be a basis of \( W \) over \( K_0 \), where all \( w_{i,\iota} \) belong to \( K_0 \). We shall suppose without loss of generality that all \( w_{i,\iota} \) belong to \( A_0 \) (to ensure this, we multiply \( w_i \) by the least common denominator of all \( w_{i,\iota} \) in \( A_0 \)), and that all \( w_{i,\iota} \) are homogeneous (because \( S^{-1}_0(B/p(\iota)B) \) is a graded module). Thus, \( M \) is determined by \( p, e, \eta_j, 0 \leq j \leq d - 1, h_1, \ldots, h_s \), an integer \( \mu \), \( 1 \leq \mu < \#\mathcal{J} \), and the matrix \( (w_{i,\iota})_{1 \leq i \leq \mu, \iota \in \mathcal{J}} \) with entries in \( A_0 \).

Conversely, for an arbitrary \( K_0 \)-linear subspace \( W \subset S^{-1}(B/p(\iota)B) \) that is a graded \( S^{-1}_0(A/p(\iota)) \)-submodule of the vector space \( S^{-1}_0(B/p(\iota)B) \), we put \( B' = B \cap \pi^{-1}(W) \). Then \( B/B' = M \) is a \( p \)-primary graded \( A \)-module; see Lemma 6 in §3. The correspondences \( W \mapsto M \) and \( M \mapsto W \) considered above are inverse to each other.

Set \( \delta = \max_{\iota, \mu} \deg E_{\iota, E_{\iota + 1}, \ldots, E_n} w_{i,\iota} \). Then \( \delta \) depends on all the objects in the above description. In what follows we write \( \delta = \delta(M) \); this will not lead to any ambiguity.

To define \( \delta \) and \( \nu \) for an arbitrary field \( k \), we extend \( k \) up to the field \( k' = k(i)^{p - \infty} \); see above. The module \( M \) is replaced by \( M' = M \otimes_k k' \). If \( M \) is a \( p \)-primary module and \( s(p) \leq n \), then \( M' \) is primary and \( s(M') = s(M) \leq n \). Hence, an integer \( \delta(M') \) is defined. Put \( \delta(M) = \delta(M') \). So, actually, \( \delta(M) \) is not uniquely determined and depends on all the objects in the construction of \( \delta(M') \). By definition, we put \( \nu = \nu(M) = \nu(M') \).

One of our aims in this paper is to prove the following result.

**Theorem 3.** Let \( M \) be a finitely generated graded \( A \)-module. Under the previous notation, the following assertions are true.

(i) For all integers \( m \),
\[
H(M, m) \leq \gamma(M) + H(M', m)
\]
\[
\leq \gamma(M) + \sum_{m \neq p \in \text{Ass}(M)} \binom{m - \nu(M, p) + n - s(p)}{n - s(p)} D(M/M(p)),
\]
where \( \binom{n}{k} \) is the modified binomial coefficient defined by (4). Moreover, if \( \deg(p) = s \), then
\[
-\infty < \nu_{n-s-1}(M, p) \leq \nu_{n-s-2}(M, p) \leq \cdots \leq \nu_0(M, p).
\]
In particular, if \( M = A/I \) for a homogeneous polynomial ideal \( I \), then inequalities (5) and (3) are valid; see above.

(ii) Assume that \( M \) is a \( p \)-primary module, i.e., \( p \in \text{Ass}(M) \) and \( M(p) = 0 \). Suppose that \( 0 \leq s = s(p) < n \) and \( M \) is given as described above by the exact sequence (13); hence, the integers \( n_1, e, d, \delta, \mu, a_i, 1 \leq i \leq \mu \), are defined for \( M \); see above. Then:
\begin{enumerate}
  \item \( -\nu_{n-s-1}(M, p) \leq \mu \delta - \min_{1 \leq i \leq n_1} a_i + e(\xi s - s + 2)d(d - 1)/2 \) if (7) is fulfilled;
  \item \( -\nu_{n-s-1}(M, p) \leq \mu \delta - \min_{1 \leq i \leq n_1} a_i + d^2sp^2(p^2 - 1) + d(d - 1)p^3 \) if \( \text{char}(k) > 0 \);
  \item and hence \( -\nu_{n-s-1}(M, p) < \mu \delta - \min_{1 \leq i \leq n_1} a_i + (s + 1)e^{s+2}d^2 \) if (8) is fulfilled.
\end{enumerate}
In particular, if \( M = A/I \), then (9) and (10) are valid; see above.

Now our aim is to formulate an analog of the first Bertini theorem for primary decompositions. We identify the set of all \( v \)-tuples \( (L_1, \ldots, L_v) \) of linear forms \( L_j \in \mathbb{K}[X_0, \ldots, X_n] \) with the affine space \( \mathbb{A}^{n+1}v(\mathbb{K}) \). Hence, the \( v \)-tuples of linear forms from the ring \( A \) are identified with the elements of \( \mathbb{A}^{n+1}v(\mathbb{K}) \).
Suppose the graded $A$-module $M$ is as above and we have the primary decomposition (11). By the first Bertini theorem (see [12] and also, e.g., the Appendix in [7]: although the ground field $k$ is arbitrary, everything reduces to the case of a perfect field $k$, and for the perfect field $k$ the assertion formulated below follows immediately from the classical Bertini theorem), there is a nonempty Zariski open subset $U_0 \subset A^{(n+1)v}(\mathbb{K})$ with the following properties. For every $(L_1, \ldots, L_v) \in U_0(k)$ (this is the set of $k$-points of $U_0$; similar notation will be used also below; if the field $k$ is infinite, then $U_0(k) \neq \emptyset$) and every prime ideal $p \in \text{Ass}(M)$ of height $\text{ht}(p)$, we have

$$p + L_1A + \cdots + L_vA = \begin{cases} p'_{L_1, \ldots, L_v} \cap \Omega_{L_1, \ldots, L_v} & \text{if } v + \text{ht}(p) < n, \\ \bigcap_{j \in J} m'_j \cap \Omega_{L_1, \ldots, L_v} & \text{if } v + \text{ht}(p) = n, \\ \Omega_{L_1, \ldots, L_v} & \text{if } v + \text{ht}(p) > n, \end{cases}$$

where

(i) $p'_{L_1, \ldots, L_v}$ is an ideal, the radical $r(p'_{L_1, \ldots, L_v}) = p_{L_1, \ldots, L_v}$ is prime; for every $z \in p_{L_1, \ldots, L_v}$, the smallest integer $a \geq 0$ such that $z^a \in p'_{L_1, \ldots, L_v}$ has the form $a = p^b$ for an integer $b \geq 0$; and $\text{ht}(p_{L_1, \ldots, L_v}) = \text{ht}(p) + v$;

(ii) the ideal $p'_{L_1, \ldots, L_v}$ is $\mathfrak{m}$-primary;

(iii) the ideal $\Omega_{L_1, \ldots, L_v}$ is $\mathfrak{m}$-primary or $\Omega_{L_1, \ldots, L_v} = A$;

(iv) the set $J = J(p, L_1, \ldots, L_v)$ is finite, and the $m'_j$, $j \in J$, are pairwise distinct ideals;

(v) the radical $r(m'_j) = m_j$ is prime; for every $z \in m_j$, the smallest integer $a \geq 0$ such that $z^a \in m'_j$ has the form $a = p^b$ for an integer $b \geq 0$; next, $\text{ht}(m'_j) = n$;

(vi) for all $p, q \in \text{Ass}(M)$ with $p \neq q$ and $\text{ht}(p) = \text{ht}(q)$, the condition implies $v + \text{ht}(p) < n$, $p_{L_1, \ldots, L_v} \neq q_{L_1, \ldots, L_v}$; but if $v + \text{ht}(p) = n$, then $m_j \neq m'_j$ for all $j \in J(p, L_1, \ldots, L_v)$;

(vii) if the field $k$ is perfect, then $p_{L_1, \ldots, L_v} = p'_{L_1, \ldots, L_v}$ whenever $v + \text{ht}(p) < n$, and $m_j = m'_j$ for all $j \in J$ whenever $v + \text{ht}(p) = n$.

If $v + \text{ht}(p) = n$, we set $p_{L_1, \ldots, L_v} = \bigcap_{j \in J(p, L_1, \ldots, L_v)} m_j$. Then $p_{L_1, \ldots, L_v}$ is a radical ideal for $v + \text{ht}(p) \leq n$.

If $v + \text{ht}(p) > n$, it is convenient to set $p'_{L_1, \ldots, L_v} = p_{L_1, \ldots, L_v} = A$.

We have $d(p_{L_1, \ldots, L_v}) \leq d(p'_{L_1, \ldots, L_v}) = d(p)$ if $v + \text{ht}(p) \leq n$, and

$$\sum_{j \in J(p, L_1, \ldots, L_v)} d(m_j) + \sum_{j \in J(p, L_1, \ldots, L_v)} d(m'_j) = d(p)$$

if $v + \text{ht}(p) = n$.

In what follows we denote for brevity $L = (L_1, \ldots, L_v)$, $p'_L = p'_{L_1, \ldots, L_v}$, $p_L = p_{L_1, \ldots, L_v}$, $\Omega_L = \Omega_{L_1, \ldots, L_v}$, $J(p, L_1, \ldots, L_v) = J(p, L)$, $LA = L_1A + \cdots + L_vA \subset A$, and $LM = L_1M + \cdots + L_vM \subset M$.

**Remark 1.** Actually, there is a Zariski open set $U_0$ such that, for every $L = (L_1, \ldots, L_v) \in A^{(n+1)v}(\mathbb{K})$, properties (i)-(vii) occur if and only if $L \in U_0(k)$; cf. [7]. But we do not need this fact.

**Remark 2.** Let $0 \leq s \leq s(M) \leq n$, and let $E_0, E_{s+1}, \ldots, E_n \in k[X_0, \ldots, X_n]$ be linear forms such that $Z(p) \cap Z(E_0, E_{s+1}, \ldots, E_n) = \emptyset$ in $\mathbb{P}^n(\mathbb{K})$ for every $p \in \text{Ass}(M)$, $p \neq \mathfrak{m}$. We identify the set of all $v$-tuples $(L_1, \ldots, L_v)$ of linear forms $L_j \in k[E_0, E_{s+1}, \ldots, E_n]$ with the affine space $A^{(n+s+1)v}(\mathbb{K})$. Then the $v$-tuples of linear forms in the ring $A_0$ are identified with the elements in $A^{(n+s+1)v}(k)$. The above Zariski open set $U_0 \subset A^{(n+1)v}(\mathbb{K})$ can be replaced by the Zariski open set $U_0' \subset A^{(n-s+1)v}(\mathbb{K})$ of $v$-tuples of linear forms.
from $\mathbb{F}[E_0, E_{s+1}, \ldots, E_n]$. All the assertions above remain true after this replacement. This follows from [12] and also, e.g., from the Appendix in [7].

Consider an irredundant primary decomposition
\begin{equation}
\{0\} = \bigcap_{\mathfrak{P} \in \text{Ass}(M/\mathfrak{M})} (M/\mathfrak{M})(\mathfrak{P})
\end{equation}
of $\{0\}$ in $M/\mathfrak{M}$. Put $(M/\mathfrak{M})(\mathfrak{P}) = M(\mathfrak{P})/\mathfrak{M}$, where $M(\mathfrak{P}) \subset M$ is a submodule, $\mathfrak{P} \in \text{Ass}(M/\mathfrak{M})$.

**Theorem 4.** Let the graded module $M$ be as above. For each $\mathfrak{p} \in \text{Ass}(M)$, choose a sequence (21); see Lemma 3 in §2 below. There is a nonempty Zariski open subset $U_1 \subset U_0$ ($U_1$ depends on $M$, on the chosen sequences (21) for all $\mathfrak{M} \neq \mathfrak{p} \in \text{Ass}(M)$, and on the monomorphisms (23); see Lemma 5 below) with the following properties. For every $L \in U_1(k)$, the set of all associated prime ideals of heights at most $n$ of the module $M/\mathfrak{M}$ we have
\[
\text{Ass}(M/\mathfrak{M}) \setminus \{\mathfrak{M}\} = \{ \mathfrak{p}_L : \text{ht}(\mathfrak{p}) < n - v & \mathfrak{p} \in \text{Ass}(M) \} \\
\cup \{ \mathfrak{m}_j : j \in J(\mathfrak{p}, L) & \text{ht}(\mathfrak{p}) = n - v & \mathfrak{p} \in \text{Ass}(M) \}.
\]

Next, there exists a primary decomposition (16) such that, for every $\mathfrak{p} \in \text{Ass}(M)$,
\begin{equation}
M(\mathfrak{p}) + \mathfrak{M} = \left\{ \begin{array}{ll}
M(\mathfrak{p}_L) \cap M(\mathfrak{p}, L) & \text{if } v + \text{ht}(\mathfrak{p}) < n, \\
\bigcap_{j \in J(\mathfrak{p}, L)} M(\mathfrak{m}_j) \cap M(\mathfrak{p}, L) & \text{if } v + \text{ht}(\mathfrak{p}) = n, \\
M(\mathfrak{p}, L) & \text{if } v + \text{ht}(\mathfrak{p}) > n,
\end{array} \right.
\end{equation}
where $M(\mathfrak{p}, L) \subset M$ is a submodule, $M/\mathfrak{M}(\mathfrak{p}, L)$ is an $\mathfrak{M}$-primary module or $M = M(\mathfrak{p}, L)$. Finally, for every $\mathfrak{M} \neq \mathfrak{p} \in \text{Ass}(M)$ we have
\begin{equation}
\begin{array}{ll}
D(M/M(\mathfrak{p})) = D(M/M(\mathfrak{p}_L)) & \text{if } \text{ht}(\mathfrak{p}) + v < n, \\
D(M/M(\mathfrak{p})) = \sum_{j \in J(\mathfrak{p}, L)} D(M/M(\mathfrak{m}_j)) & \text{if } \text{ht}(\mathfrak{p}) + v = n.
\end{array}
\end{equation}

For $L \in U_1(k)$, it is convenient to denote
\[
M(\mathfrak{p}_L) = \left\{ \begin{array}{ll}
\bigcap_{j \in J(\mathfrak{p}, L)} M(\mathfrak{m}_j) & \text{if } \text{ht}(\mathfrak{p}) + v = n, \\
M & \text{if } \text{ht}(\mathfrak{p}) + v > n.
\end{array} \right.
\]

§1. Estimation of the characteristic function of an ideal by using a result on local parameters

We need some notation. Let $\varepsilon$ be a transcendental element over the field $k$. We can extend the ground field $k$ up to $k(\varepsilon)$. We identify $k[\varepsilon, X_0, \ldots, X_n] = A[\varepsilon] = A \otimes_k k[\varepsilon]$, $k(\varepsilon)[X_0, \ldots, X_n] = A \otimes_k k(\varepsilon)$. For an ideal $\mathfrak{a} \subset A$, let $\mathfrak{a} = (\mathfrak{a} + (\varepsilon)) \subset A[\varepsilon]$ be the ideal in $A[\varepsilon]$ generated by $\mathfrak{a}$ and $\varepsilon$. We identify $A/\mathfrak{a}$ with $A[\varepsilon]/\mathfrak{a}$. For an ideal $\mathfrak{b} \subset A[\varepsilon]$ we identify $\mathfrak{b} \otimes_{A[\varepsilon]} k(\varepsilon)$ with the ideal of $A \otimes_k k(\varepsilon)$. For every prime ideal $\mathfrak{P}$ of $A[\varepsilon]$ we define $s(\mathfrak{P}) = \text{ht}(\mathfrak{P})$, where $\text{ht}(\mathfrak{P})$ is the height of $\mathfrak{P}$ in $A[\varepsilon]$. Recall that for an ideal $I$ we denote by $\text{ass}(I)$ the set of all isolated associated prime ideals of $I$.

**Lemma 1.** In the previous notation, assume that there are homogeneous polynomials $f_1, \ldots, f_s \in A$, $1 \leq s \leq n$, such that $I = (f_1, \ldots, f_s) \subset A$ and $f_i \notin \mathfrak{M}$ for every $1 \leq i \leq s$. Let $\mathfrak{p} \in \text{ass}(I)$, and let $s(\mathfrak{p}) = s$. Put $I(\varepsilon) = \bigcap_{q \in \text{ass}(I), s(q) = s} I(q)$ to be the intersection of all isolated primary components of $I$ of codimension $s$. Let $\tilde{f}_1, \ldots, \tilde{f}_s \in A[\varepsilon]$ be homogeneous polynomials with respect to $X_0, \ldots, X_n$ such that $\dim(\tilde{f}_1, \ldots, \tilde{f}_s) = n - s$ in $\mathbb{P}^n(k(\varepsilon))$, $\deg \tilde{f}_i = \deg f_i$, and $\tilde{f}_i|_{\varepsilon = 0} = f_i$ for all $1 \leq i \leq s$ (for example, we can take
\( \bar{f}_i = f_i + \varepsilon X_i^{\deg f_i} \) for all \( i \). Denote by \( \bar{I} = (\bar{f}_1, \ldots, \bar{f}_s) \) the ideal generated by \( \bar{f}_1, \ldots, \bar{f}_s \) in \( A[\varepsilon] \). Put \( J = \{ \Omega \in \text{ass}(\bar{I}) : s(\Omega) = s \land k[\varepsilon] \cap \Omega = \{0\} \} \) and \( \bar{I}(s) = \bigcap_{\Omega \in J} \bar{I}(\Omega) \).

Then for every \( q \in \text{ass}(I) \) with \( s(q) = s \) we have \( q \in \text{ass}(\bar{I}(s)+(\varepsilon)) \subset \text{Spec}(A[\varepsilon]) \),

\[
(\bar{I}(s)+(\varepsilon))(q) = I(q),
\]

and

\[
h(I(p), m) \leq h(I(s), m) \leq h(\bar{I}(s) \otimes_{k[\varepsilon]} k(\varepsilon), m)
\]

\[
\leq h(\bar{I} \otimes_{k[\varepsilon]} k(\varepsilon), m) \leq \prod_{1 \leq i \leq s} \deg f_i
\]

for every \( m \geq 0 \) (obviously, the function \( h(\bar{I} \otimes_{k[\varepsilon]} k(\varepsilon), \ldots) \) depends only on \( \deg f_i, 1 \leq i \leq s \), and coincides with \( h((g_1, \ldots, g_s), \ldots) \), where \( g_1, \ldots, g_s \in A \) are arbitrary homogeneous polynomials such that \( \deg g_i = \deg f_i \) for every \( 1 \leq i \leq s \) and \( \dim Z(g_1, \ldots, g_s) = n - s \) in \( \mathbb{P}^n(k) \).

**Proof.** We check (19). We identify \( f \in k[\varepsilon] \) for every \( \varepsilon \) at the end of the statement of Lemma 3 (alternatively, here we may assume without loss of generality that the ground field \( k \) is perfect and observe that then the ideal \( (g_1, \ldots, g_s) \) is prime in general position for \( s < n \); hence, the inequality in question follows from [4] for \( s < n \) and from the Bézout theorem for \( s = n \)). The first and the third inequalities in (20) are obvious. It remains to prove that \( h(I(s), m) \leq h(\bar{I}(s) \otimes_{k[\varepsilon]} k(\varepsilon), m) \).

By (19), we have an epimorphism \( A[\varepsilon]/(\bar{I}(s)+(\varepsilon)) \to A/I(s) \) of graded modules. Hence, \( h(I(s), m) \leq \dim_k(A[\varepsilon]/(\bar{I}(s)+(\varepsilon)))m \). Next, \( (A[\varepsilon]/I(s))_m \) is a finitely generated \( k[\varepsilon] \)-module without torsion, because \( \Omega \cap k[\varepsilon] = \{0\} \) for every \( \Omega \in J \). Therefore, \( (A[\varepsilon]/\bar{I}(s))_m \) is
a free $k[\varepsilon]$-module. Consequently,
\[
\dim_k(A[\varepsilon]/(\overline{I}^{(s)} + (\varepsilon)))_m = \text{rank}_{k[\varepsilon]}(A[\varepsilon]/\overline{I}^{(s)})_m = \dim_k(A \otimes_k k(\varepsilon)/\overline{I}^{(s)} \otimes_{k[\varepsilon]} k(\varepsilon))_m = h(\overline{I}^{(s)} \otimes_{k[\varepsilon]} k(\varepsilon), m).
\]

The required inequality is proved. \qed

Although the next lemma will not be used in the present paper, it gives some additional information.

**Lemma 2.** Under the conditions of Lemma 1, for every $m \geq 0$ we have
\[
h(I \otimes_{k[\varepsilon]} k(\varepsilon), m) \leq h(I, m).
\]

**Proof.** Indeed, $h(I, m) = \dim_k(A[\varepsilon]/(\overline{I} + (\varepsilon)))_m = \text{rank}_{k[\varepsilon]}(A[\varepsilon]/\overline{I})_m$, where, by definition, the rank in the last term is the rank of any maximal free submodule of the finitely generated $k[\varepsilon]$-module $(A[\varepsilon]/\overline{I})_m$. But, obviously, $\text{rank}_{k[\varepsilon]}(A[\varepsilon]/\overline{I})_m = h(I \otimes_{k[\varepsilon]} k(\varepsilon), m)$. The lemma is proved. \qed

**Proof of Theorem 1.** We extend the ground field $k$ up to the field $k'$, see the Introduction, and replace $I$ by $I \otimes_k k'$. Then the ideal $I \otimes_k k'$ is primary and $h(I, m) = h(I \otimes_k k', m)$ for every $m$. This allows us to assume without loss of generality that in what follows the field $k$ is perfect and infinite. By \[4, 5\], there are homogeneous polynomials $h_1, \ldots, h_s$ such that $(h_1, \ldots, h_s)(p) = p$ and $\prod_{1 \leq i \leq s} \deg h_i \leq n^2 c_i^s d(p)$ for $n \geq s \geq 1$, with an absolute constant $C_1 > 0$ that can be computed explicitly. Moreover, if $s = 1$, then $\deg h_1 \leq d(p)$.

We have $(m + n - s) \leq n^2 m^{n-s}$ for all $n \geq s \geq 1, m \geq 1$. On the other hand, by Lemma 1 we have
\[
h((h_1^e, \ldots, h_s^e)(p), m) \leq e^s (m + n - s) \prod_{1 \leq i \leq s} \deg h_i.
\]

Therefore, $h(I, m) \leq e^s n^2 c^s d(p)m^{n-s}$ for all $n \geq s \geq 1$ and $m \geq 1$, with an appropriate constant $C > 0$. The theorem is proved. \qed

\

§2. A VERSION OF THE FIRST BERTINI THEOREM FOR PRIMARY DECOMPOSITIONS

**Lemma 3.** Let the graded module $M$ be as above, and let $\mathfrak{M} \neq p \in \text{Ass}(M)$. Then there exists a sequence
\[
M/M(p) = M^{(0)} \supset M^{(1)} \supset \cdots \supset M^{(\nu)} = \{0\}
\]
of graded $A$-modules such that $\nu = D(M/M(p))/d(p)$, and we have isomorphisms of graded $A$-modules $M^{(i)}/M^{(i+1)} \cong (a_i/p)(\mu_i), 0 \leq i \leq \nu - 1$, where $a_i$ is a homogeneous ideal of $A$ or $a_i = A$, $p \in a_i, a_i \neq a$, and the $\mu_i$ are integers. Hence, $\text{Ass}(M^{(i)}/M^{(i+1)}) = \{p\}$ and $D(M^{(i)}/M^{(i+1)}) = D(a_i/p) = d(p)$ for every $0 \leq i \leq \nu - 1$. Therefore,
\[
D(M/M(p)) = l(M/M(p))D(A/p).
\]

**Proof.** Replacing $M$ by $M/M(p)$, we may assume without loss of generality that $M(p) = \{0\}$, i.e., $M$ is $p$-primary. Let $a \subset A$ be a homogeneous ideal such that $a \supset p$ or $a = A$. Suppose $M \neq \{0\}$. It suffices to prove that there is an epimorphism of graded modules $M \rightarrow (a/p)(\mu)$ for such $a$ and an integer $\mu$. Let $S = A \setminus p$ be the multiplicatively closed set. Consider the homomorphism $M \rightarrow S^{-1}(M/pM)$. Let $M'' = \iota(M)$ and $M' = \text{Ker}(\iota)$. We show that $M'$ is a graded module. Indeed, let $z \in M'$. Then $zm \in pM$ for $s \in S$. There is no loss of generality in assuming that each nonzero homogeneous component of $s$ does not belong to $p$. Let $z'$ and $z''$ be the nonzero homogeneous components of


the smallest degrees of $z$ and $s$, respectively. Then, obviously, $s'z' \in pM$, i.e., $z' \in M'$. This implies the required assertion. Therefore, the module $M''$ is also graded. We have $Ass(M'') = \{p\}$ because $\{0\} \neq M'' \subset S^{-1}(M/pM)$. Also, $pM'' = \{0\}$. So, replacing $M$ by $M''$, we may assume without loss of generality that $pM = \{0\}$, i.e., $M$ is an $A/p$-module.

We shall use induction on $\nu = \dim KpS^{-1}M$. Let $z_0 \in M$ be a nonzero homogeneous element. Let the homogeneous degree of $z_0$ be $m$. Let $N = \{z \in M : \exists s \in S(sz \in Az_0)\}$. Then $N$ is a graded submodule of $M$ such that $\dim KpS^{-1}N = 1$. We choose a system of generators $z_0, \ldots, z_\alpha$ that are nonzero homogeneous elements of $N$. Then there are nonzero homogeneous elements $s_0, \ldots, s_\alpha \in S$ such that $s_0z_i = s_i z_0$ for all $1 \leq i \leq \alpha$. Put $a = (s_0, \ldots, s_\alpha) + p$. We have $N \cong (a/p)(\mu)$, where $\mu = m - \deg s_0$.

If $\nu = 1$, then $M = N$ and the lemma is proved. If $\nu > 1$, then $\dim KpS^{-1}(M/N) = \nu - 1$, and the definition of $N$ implies that $Ass(M/N) = \{p\}$. Thus, by the inductive assumption, there is an epimorphism of graded modules $M/N \to (a/p)(\mu)$ for some ideal $a$ and integer $\mu$. The lemma is proved. \hfill $\square$

For a finitely generated graded $A$-module $M$ as above, we put

$$M^p = M \left/ \left( \bigcap_{p \in Ass(M) \setminus \{0\}} M(p) \right) \right..$$

Observe that $\bigcap_{p \in Ass(M) \setminus \{0\}} M(p) = \{m \in M : \exists N \geq 1 (\mathfrak{M}^N m = \{0\}) \}$, because we have an embedding $M \to \prod_{p \in Ass(M)} M/M(p)$.

We shall prove Theorem 4 by using induction on $\nu$. For $\nu = 0$, Theorem 4 is trivial. Let $1 \leq \nu \leq n$. In what follows in this section we shall suppose that Theorem 4 is proved by induction for all graded $A$-modules $M$ and all $w$ in place of $v$ such that $0 \leq w < \nu$. Put $L' = (L_1, \ldots, L_{\nu - 1})$. We denote $U_0 = U_0(M, v)$ and $U_1 = U_1(M, v)$; see the statement of Theorem 4. Moreover, we assume that Lemmas 4 and 5, see below, are proved by induction for all $0 \leq w < \nu$.

**Lemma 4.** Let $1 \leq v \leq n$ be an integer. Let the graded module $M$ be as above, and let $\upsilon : Q \to M$ be a monomorphism of graded modules. Then there is a nonempty Zariski open subset $U(\upsilon, v) \subset U_0(M, v)$ such that for every $L = (L_1, \ldots, L_v) \in U(\upsilon, v)(k)$ one can embed $(Q/LQ)^p$ in $(M/LM)^p$ by using the natural homomorphism $Q/LQ \to M/LM$.

**Proof.** Let $L' \in U(\upsilon, v - 1)$ (recall that this set is defined inductively). Then we have the embedding $(Q/L'Q)^p \to (M/L'M)^p$. Put $R = (M/L'M)^p/((Q/L'Q)^p)$. We identify $R^p$ with $(M/(Q + L'M))^p$. We have a commutative diagram

\[\begin{array}{c}
0 \to (Q/L'Q)^p \to (M/L'M)^p \to R \to 0 \\
\downarrow L_v \quad \downarrow L_v \quad \downarrow L_v \\
0 \to (Q/L'Q)^p \to (M/L'M)^p \to R \to 0
\end{array}\]

with exact rows induced by the embedding $Q \to M$. The vertical arrows in this diagram are homomorphisms of multiplication by $L_v$. Let $L_v \notin p$ for every $\mathfrak{M} \neq p \in Ass(M/(Q + L'M))$. The Ker-Coker sequence corresponding to (22) implies that the homomorphism $\upsilon_v : (Q/LQ)^p \to (M/LM)^p$ is injective. By Theorem 4 for $v - 1$, if $L' \in U(\upsilon, v - 1) \cap U_1(M/Q, v - 1)$ and $L_v$ does not vanish on any irreducible component of $Z(p + L'A)$ for every $p \in Ass(M/Q)$ with $\text{ht}(p) + v - 1 \leq n$, then $\upsilon_v$ is injective. Hence, if $L' \in U(\upsilon, v - 1) \cap U_1(M/Q, v - 1)$ and $\dim Z(p + LA) = n - \text{ht}(p) - v$ for these $p$ (if the dimension is negative, then the variety is empty), then $\upsilon_v$ is injective. But for every $p$ under consideration the set of all $L \in \mathbb{A}^{v(n+1)}$ such that $\dim Z(p + LA) = n - \text{ht}(p) - v$
is a nonempty Zariski open subset of \( \mathbb{A}^{n+1} / (k) \). This can be proved, e.g., by considering
\( U \)-resultants. Thus, now we can define the set \( U(\ell, v) \). The lemma is proved. \( \square \)

Consider the sequence (21). For every \( 1 \leq i \leq \nu \), we choose a monomorphism of graded modules
\[
\kappa_i : (A/\mathfrak{p})(\mu_i' \to (a_i / \mathfrak{p})(\mu_i).
\]
Thus, here the integers \( \mu_i', \mu_i, \nu \) depend on \( \mathfrak{p} \in \text{Ass}(M) \setminus \{ \mathfrak{M} \} \) and the sequences (21) chosen in Lemma 3. Note that for every \( L \in U_0(k) \) we have isomorphisms of graded modules \((a_i + LA)/((\mathfrak{p} + LA))(\mu_i) \cong ((a_i + \mathfrak{p}_i')/\mathfrak{p}_i')(\mu_i) \) and \((A/(\mathfrak{p} + LA))(\mu_i') \cong (A/\mathfrak{p}_i')(\mu_i') \).

**Lemma 5.** Let the graded module \( M \) be as above. There is a nonempty Zariski open set \( U_2(M, v) \subset U_0(M, v) \) (depending actually also on the chosen exact sequences (21) for all \( \mathfrak{p} \) and on the monomorphisms \( \kappa_i, 1 \leq i \leq \nu - 1 \)) such that, for every prime ideal \( \mathfrak{M} \neq \mathfrak{p} \in \text{Ass}(M) \) and every \( L \in U_2(M, v)(k) \), the sequence (21) induces by Lemma 4 the following sequence of graded \( A \)-modules:
\[
(M/(M(p) + LM))^\rho = (M^{(0)}/LM^{(0)})^\rho \supset (M^{(1)}/LM^{(1)})^\rho \supset \cdots \supset (M^{(\nu)}/LM^{(\nu)})^\rho = \{0\},
\]
and (23) induces monomorphisms
\[
\kappa_{i, v} : (A/\mathfrak{p}_i')(\mu_i') \to ((\mathfrak{a}_i + \mathfrak{p}_i')/\mathfrak{p}_i')(\mu_i).
\]
Hence, \( \text{Ass}(A/\mathfrak{p}_i') = \text{Ass}((\mathfrak{a}_i + \mathfrak{p}_i')/\mathfrak{p}_i') \), and for the degree we have \( D(A/\mathfrak{p}_i') = D(\mathfrak{a}_i + \mathfrak{p}_i') \). In particular, for \( i = \nu - 1 \) we get \( \text{Ass}(A/\mathfrak{p}_i') \subset \text{Ass}(M^{(\nu-1)}) \subset \text{Ass}(M) \). Next, for every \( 0 \leq i \leq \nu - 1 \) we have an isomorphism of graded modules
\[
(M^{(i)}/LM^{(i)})^\rho / (M^{(i+1)}/LM^{(i+1)})^\rho \cong ((\mathfrak{a}_i + \mathfrak{p}_i')/\mathfrak{p}_i')(\mu_i).
\]
Therefore, \( (M/(M(p) + LM))^\rho = \{0\} \) whenever \( \text{ht}(\mathfrak{p}) + v > n \) and (17), (18) are fulfilled.

**Proof.** By Lemma 4 there is a nonempty Zariski open subset \( U'(M, v) \subset U_0 \) such that for every \( L \in U'(M, v)(k) \) there is sequence of modules (24) and all \( \kappa_{i, v} \) are monomorphisms. We have the isomorphisms
\[
(M^{(i)}/LM^{(i)})^\rho / (M^{(i+1)}/LM^{(i+1)})^\rho \cong (M^{(i)}/LM^{(i)})^\rho \
\cong ((\mathfrak{a}_i + \mathfrak{p}_i')/\mathfrak{p}_i')(\mu_i),
\]
so that we can take \( U_2(M, v) = U'(M, v) \). The lemma is proved. \( \square \)

**Proof of Theorem 4.** Consider the embedding
\[
\ell : M \to \prod_{\mathfrak{p} \in \text{Ass}(M)} (M/M(\mathfrak{p})).
\]
Put \( U_1(M, v) = U(\ell, v) \cap U_2(M, v) \), where \( U(\ell, v) \) and \( U_2(M, v) \) are Zariski open subsets from Lemmas 4 and 5, respectively. Now for \( L \in U_1(M, v) \) all the assertions of Theorem 4 follow from Lemmas 4 and 5. Thus, Theorem 4 is proved by induction on \( v \). \( \square \)
§3. Estimation of the Hilbert function of a primary module

Lemma 6. Suppose \( \mathfrak{M} \neq \mathfrak{p} \in \text{Ass}(M) \). Suppose that the field \( k \) is perfect and contains sufficiently many elements, \( s = s(p) \), the linear forms \( E_0, E_1, \ldots, E_n \) corresponding to \( p \) are as in the Introduction, \( A_0 = \{E_0, E_1, \ldots, E_n\} \), \( S_0 = A_0 \setminus \{0\} \), and the field \( K_0 \) is equal to \( S_0^{-1}A_0 \). Assume that \( p^nM = \{0\} \) for an integer \( n \). Then \( M \) is a \( p \)-primary \( A \)-module if and only if \( M \) is a \( \{0\} \)-primary \( A_0 \)-module.

Proof. Suppose that \( M \) is a \( p \)-primary \( A \)-module. Then \( S_0 \subset A \setminus p \). Hence, for every \( s \in S_0 \) the homomorphism \( M \to M \) of multiplication by \( s \) is injective. Thus, \( M \) is a \( \{0\} \)-primary \( A_0 \)-module. Conversely, suppose that \( M \) is a \( \{0\} \)-primary \( A_0 \)-module. We choose a basis \( z_1, \ldots, z_\nu \in M \) over the field \( K_0 \) of \( S_0^{-1}M \). Let \( s \in A \). We write \( sz_i = \sum_{1 \leq j \leq \nu} \lambda_{ij}z_j \in S_0^{-1}M \), \( 1 \leq i \leq \nu \), where all \( \lambda_{ij} \) belong to \( K_0 \). Let \( 0 \neq z \in M \) and \( sz = 0 \). Then \( sz = 0 \) in \( S_0^{-1}M \) and \( 0 \neq z = \sum_{1 \leq i \leq \nu} a_i z_i \in S_0^{-1}M \), \( a_i \in K_0 \). Hence, \( \sum_{1 \leq i \leq \nu} a_i \lambda_{ij} = 0 \) for every \( 1 \leq j \leq \nu \). This means that \( \det(\lambda_{ij}) = 0 \). Let \( K \) denote the field of fractions of \( A/p \). By the Wedderburn–Maltsev theorem, see [1], \( S_0^{-1}(A/p) \) is a \( K \)-algebra. Thus, \( S_0^{-1}M \) is a vector space over \( K \). Denoting \( l = \dim_K S_0^{-1}M \), we obtain \( \det(\lambda_{ij}) = (N_{K/K_0}(s \mod p))^l \), where \( N_{K/K_0}(s \mod p) \) is the norm of the element \( s \mod p \) of the field of fractions of \( A/p \) to \( K_0 \). Hence, \( N_{K/K_0}(s \mod p) = 0 \). Therefore, \( s \in p \), and \( M \) is a \( p \)-primary \( A \)-module. The lemma is proved.

Under the conditions of Lemma 6, we choose a linear form \( E_{n+1} \in k[X_0, \ldots, X_n] \) such that the field \( S_0^{-1}A \) coincides with \( K_0(E_{n+1} \mod p) \) and the extension of rings \( A_0(E_{n+1} \mod p) \supset A_0 \) is integral. Let \( \Phi \in A_0[Z] \) be the minimal polynomial of \( E_{n+1} \mod p \) over the field \( K_0 \) with the leading coefficient equal to 1, and let \( \Delta_0 \) be the discriminant with respect to \( Z \) of the separable polynomial \( \Phi \). It is well known that

\[
\Delta_0(A/p) \subset \sum_{0 \leq i \leq d-1} A_0(E_{n+1} \mod p)^i.
\]

We have \( \deg \Delta_0 \leq d(d-1) \).

We note that, under the conditions of Lemma 6, after an appropriate nondegenerate linear transformation of coordinates \( (X_0, \ldots, X_n) \mapsto (X'_0, \ldots, X'_n) \) with coefficients in \( k \), the Jacobian \( \delta_1 = \det(\partial h_i/\partial X'_j)_{1 \leq i, j \leq n} \) of \( A \) is nonzero. Let \( \Delta_1 = N_{K/K_0}\delta_1 \) be the norm of this Jacobian; see the notation in the proof of Lemma 6. In what follows, to simplify the notation, we assume that \( X_i = X'_i \) for all \( 0 \leq i \leq n \), performing if necessary a linear automorphism of coordinate functions. Observe that \( \deg \Delta_1 \leq sd(d-1) \).

Under the conditions of Lemma 6, we assume additionally that \( \text{char}(k) = p > 0 \).

Let \( \alpha \geq 1 \) be an integer such that \( p^\alpha > e \geq p^{\alpha-1} \); see the Introduction. We put \( \mathbb{Z}_+ = \{ z \in \mathbb{Z} : z \geq 0 \} \),

\[
T^{(\beta)} = \{ (i_1, \ldots, i_\alpha) \in \mathbb{Z}_+^\alpha : \forall w (0 \leq i_w < p^\beta) \}, \quad 1 \leq \beta \leq \alpha,
\]

and \( T = T^{(1)} \). Let \( 1 \leq \beta \leq \alpha \) be an integer. For \( i = (i_1, \ldots, i_\alpha) \in T \), we denote \( X_i^{p^\beta} = X_1^{p^\beta} \cdots X_n^{p^\beta} \), \( h^i = h_1^{i_1} \cdots h_n^{i_n} \). We can write \( h^{p^\beta-1} = \sum_{i \in T} h_i X_i^{p^\beta-1} \) for all \( i \in T \), where \( h_{i,j} \in k[X_0, X_1^{p^\beta}, \ldots, X_n^{p^\beta}, X_{n+1}, \ldots, X_n] = A^{(\beta)} \) (we shall use this notation for \( \beta \geq 0 \)). The extension of fields \( k(X_0, \ldots, X_n) \supset k(X_0, h_1, \ldots, h_n, X_{n+1}, \ldots, X_n) \) is finite separable, because \( \det(\partial h_i/\partial X_j)_{1 \leq i, j \leq n} \neq 0 \). Hence, the extension of fields

\[
k(X_0, X_1^{p^\beta-1}, \ldots, X_n^{p^\beta-1}, X_{n+1}, \ldots, X_n) \supset k(X_0, h_1^{p^\beta-1}, \ldots, h_n^{p^\beta-1}, X_{n+1}, \ldots, X_n)
\]

is also finite separable. Therefore, \( h^{p^\beta-1} \), \( i \in T \), is a basis of the field \( k(X_0, X_1^{p^\beta-1}, \ldots, X_n^{p^\beta-1}, X_{n+1}, \ldots, X_n) \) over \( k(X_0, X_1^{p^\beta}, \ldots, X_n^{p^\beta}, X_{n+1}, \ldots, X_n) \). Thus, the determinant

\[
d_{\beta} = \det(h_{i,j})_{i,j \in T}
\]

is nonzero. We denote by \( \Delta_{2,\beta} = N_{K/K_0}\det(h_{i,j})_{i,j \in T} \) the norm of this determinant, see the notation above, and put \( \Delta_2 = \prod_{1 \leq \beta \leq \alpha} \Delta_{2,\beta} \). Observe
that \( \deg h_{i,j} \leq \deg h^p - 1 \leq ds(p - 1)p^{\alpha - 1} \), whence \( \deg \Delta_{2,\beta} \leq d^2 sp^{\alpha}(p^\beta - p^{\beta - 1}) \) and \( \deg \Delta_2 \leq d^2 sp^{\alpha}(p^\alpha - 1) \). So, if \( \alpha > 1 \), then \( \deg \Delta_2 < se^{s+2}d^2 \).

**Lemma 7.** Under the conditions of Lemma 6, let \( z \in B/p^{(c)}B \) be an arbitrary element. Then:

(i) if \( \text{char}(k) = 0 \) or \( \text{char}(k) > 0 \) and \( \alpha = 1 \), then \( \Delta_0^t \Delta_1 \in \sum_{i \in I} A_0 e_i \);

(ii) if \( \text{char}(k) = p > 0 \), then \( \Delta_0^t \Delta_2 z \in \sum_{i \in I} A_0 e_i \).

Finally, \( \deg \Delta_0^t \Delta_1 \leq e(2s - 2)d/2 \) and \( \deg \Delta_0^t \Delta_2 \leq d^2 sp^{\alpha}(p^\alpha - 1) + d(d - 1)p^\alpha \). If \( \alpha > 1 \), then \( \deg \Delta_0^t \Delta_2 < d^2(s + 1)e^{s+2} \).

**Proof.** We prove (i). Let \( f \in A \). We use induction on \( r \geq 0 \) to show that for every \( r \leq e \) there is an element \( f_r \in \sum_{i \in I} A_0 e_i \) such that \( g_r = \Delta_0^t \Delta_1 \in S_0^{-1} p^r \).

The base of induction is trivial: \( f_0 = 0 \). Suppose that for \( r < e \) the claim is proved. We prove it for \( r + 1 \). Denote \( I_r = \{(i_1, \ldots, i_s) \in \mathbb{Z}_+^s : i_1 + \cdots + i_s = r \} \). We write \( g_r = \sum_{(i_1, \ldots, i_s) \in I_r} g_{i_1, \ldots, i_s} h_1^{i_1} \cdots h_s^{i_s} \), where all \( g_{i_1, \ldots, i_s} \) belong to \( S_0^{-1} A \).

Let \( 1 \leq w \leq s \) be an integer, and let \( f \in A \). Put \( \varphi_{w} = h_w \) for all \( 1 \leq v \neq w \leq s \) and \( \varphi_{w} = f \). Set \( D_w(f) = \text{det}(\partial_{x_1}/\partial y_1)_{1 \leq i,j \leq s} \). Now \( D_1^{i_1} \cdots D_s^{i_s} g_r = \lambda \delta_{1} g_{i_1, \ldots, i_s} + \bar{g}_{i_1, \ldots, i_s} \), where \( g_{i_1, \ldots, i_s} \in S_0^{-1} p^0 \) and \( \lambda \neq 0 \) in \( k \). Hence, \( \delta_{1}^{(r-i)} D_1^{i_1} \cdots D_s^{i_s} g_r = \lambda \delta_{1}^{(r-i)} g_{i_1, \ldots, i_s} + \bar{g}_{i_1, \ldots, i_s} \), where \( g_{i_1, \ldots, i_s} \in S_0^{-1} p^0 \) for every integer \( i > 0 \). Therefore, considering the minimal polynomial of \( \delta_{1} \) over \( K_0 \), we get \( g' = \lambda \Delta_{0}^{(r-i)} g_{i_1, \ldots, i_s} + \bar{g}_{i_1, \ldots, i_s} \), where \( g' \in A \) and \( \bar{g}_{i_1, \ldots, i_s} \in S_0^{-1} p^0 \). Next, there is an element \( f_{i_1, \ldots, i_s} \in \sum_{0 \leq j < d} A_0 e_{j} \) such that \( f_{i_1, \ldots, i_s} - \Delta_{0} g' \in p \). Now

\[
\Delta_0^t \Delta_1 g_r - \sum_{(i_1, \ldots, i_s) \in I_r} f_{i_1, \ldots, i_s} h_1^{i_1} \cdots h_s^{i_s} \in S_0^{-1} p^{r+1}.
\]

This implies the required assertion and (i).

Now we prove (ii). For every \( i \in I \), by the Cramer rule we have \( d_{\beta} X_i^{p^{\beta - 1}} = \sum_{j \in I} x_{i,j} h_i^{p^{\beta - 1}} \) with \( x_{i,j} \in A(\beta) \). Hence, for every \( f \in A(\beta - 1) \) the element \( d_{\beta} f \) can be written as \( \sum_{j \in I} f_{j} h_i^{p^{\beta - 1}} \) with \( f_{j} \in A(\beta) \). Therefore, for every integer \( w > 0 \) we have \( d_{\beta}^w f = \sum_{j \in I} f_{j} h_i^{p^{\beta - 1}} \) with \( f_{j} \in A(\beta) \). Considering the minimal polynomial of \( d_{\beta} \), we deduce that for every \( f \in A(\beta - 1) \) we can write \( \Delta_2, f = \sum_{j \in I} f_{j} h_i^{p^{\beta - 1}} \) with \( f_{j} \in A(\beta) \).

This implies that for every \( f \in A \) we have \( \Delta_2 f = \sum_{i \in I^{(s)}} f_i h_i^{p^\alpha} \) with \( f_i \in A^{(s)} \). For every \( i \in I^{(s)} \) there is an \( g_i \in \sum_{0 \leq j \leq d-1} A^{(s)} p^{\alpha} \) such that \( g_i - \Delta_2^{\alpha} f_i \in p^{(p^\alpha)} \subseteq p^{(e)} \). Thus, \( \Delta_0^t \Delta_2 f - \sum_{i \in I^{(s)}} g_i h_i^{p^\alpha} \in p^{(e)} \). This implies (ii). The lemma is proved.

Notice that \( M_f \) can be described explicitly as follows. Suppose that there are linear forms \( E_0, E_{s+1}, \ldots, E_n \in k[X_0, \ldots, X_n] \) satisfying

\[
V(M) \cap \mathbb{Z}(E_0, E_{s+1}, \ldots, E_n) = \emptyset
\]

in \( \mathbb{P}_n^d(\bar{k}) \), in the notation of the Introduction, i.e., \( \mathbb{Z}(p) \cap \mathbb{Z}(E_0, E_{s+1}, \ldots, E_n) = \emptyset \) for every isolated prime ideal \( p \in \text{Ass}(M) \), \( p \neq \mathfrak{m} \). Put \( J_0 = 0, s+1, \ldots, n \). For every nonzero homogeneous polynomial \( f \in A \), denote by \( S(f) = \{ f_i : i \geq 0 \} \) the multiplicatively closed set and by \( M(f) = S(f)^{-1} M \) the localization of \( M \) with respect to
\[ S_f. \text{ Then } M_f \text{ is a graded module: for the homogeneous component we have } (M_f)_m = \bigcup_{w \in \mathbb{Z}} \{ z/f^m \in M_f : z \in M_{m+w \cdot \deg f} \} \text{ for every integer } m, \text{ and} \]

\[ M^\nu_m = \left\{ (z_i)_{i \in J_0} \in \prod_{i \in J_0} (M(E_i)_m) : z_i = z_j \in (M(E_i,E_j)_m), \forall i,j \in J_0 \right\}. \]

Hence, \( M^\nu = M^p \nu \) in the notation of the Introduction. The natural homomorphism \( M^p \to M^\nu \) is a monomorphism. In particular, if \( M \) is a \( p \)-primary module with \( \mathfrak{M} \neq p \), then we have the natural embedding \( M \to M^\nu \).

**Proof of Theorem 3.** Let \( K \supset k \) be a separable extension such that \( K \) is a perfect field with transcendency degree over \( k \) at least \( 2(n-s+1)(n+1) \). We extend the ground field \( k \) up to \( K \), and change the notation: denote \( k, K, M, \) and \( M \otimes_k k' \) by \( k', k', M', \) and \( M \), respectively. Obviously, it suffices to prove the theorem for the new module \( M \) over the new ground field \( k \). Now, in particular, the field \( k \) is perfect infinite of transcendency degree over \( k' \) at least \( 2(n-s+1)(n+1) \), and \( M \cong M' \otimes_k k' \), i.e., \( M \) is defined over the field \( k' \). We define the objects \( A, A_0, S_0, K_0 \) as before, for the new ground field \( k \) (so that here we also change the notation).

We prove (i). We have the embedding (26). Hence, the inequality \( H(M^\nu, m) \leq \sum_{\mathfrak{M} \neq p \in \text{Ass}(M)} H(M/M(p), m) \) is true. If \( s(p) = n \), then (18) and Lemma 3 imply that \( H(M/M(p), m) = D(M/M(p)) \) for every \( m; \) cf. the end of the proof of (i), where the relation \( H(Q^\nu, m) = D(M) \) was established. Consequently, it suffices to prove (i) in the case where \( M \) is a \( p \)-primary module with \( p \neq \mathfrak{M} \) and \( s = s(p) < n \). We denote by \( \mathfrak{M}_0 = (E_0, E_{s+1}, \ldots , E_n) \) the maximal homogeneous ideal of \( A_0 \).

Let \( E_0, E_{s+1}, \ldots , E_n, A_0, S_0, K_0 \) be as in Lemma 6. Let \( e = e(M) \) be the exponent of \( M \); see the Introduction. Then \( p^e M = \{ 0 \} \) and \( M \) is a \( \{ 0 \} \)-primary \( A_0 \)-module by Lemma 6. We apply Lemma 5 to the module \( M \) over the ring \( A_0 \) in place of \( A \). Let \( \mathcal{U}_2(M, v) \subset k^{(n-s+1)v}(K', 1 \leq v \leq n-s, \) be the Zariski open subset given by Lemma 5 in our situation. We choose successively linear forms \( L_1, \ldots , L_{n-s+1} \) in \( E_0, E_{s+1}, \ldots , E_n \) with coefficients in \( k \) such that \( L^{(i)} = (L_1, \ldots , L_i) \in \mathcal{U}_2(M, i)(k) \) for every \( 1 \leq i \leq n-s \) and \( L_i \notin p \) for every \( \mathfrak{M}_0 \neq p \in \text{Ass}(M/L^{(i-1)} M) \subset \text{Spec}(A_0) \) and every \( 1 \leq i \leq n-s+1 \). This is possible because the field \( k \) is infinite and all the sets \( \mathcal{U}_2(M, i) \) are nonempty and open in the Zariski topology. Moreover, as \( E_0, E_{s+1}, \ldots , E_n \) we can take generic linear forms in \( X_0, \ldots , X_n \) over \( k' \) and after that \( L_1, \ldots , L_{n-s+1} \) can be taken to be generic linear forms in \( E_0, E_{s+1}, \ldots , E_n \) over \( k' \). Hence in this case \( L_1, \ldots , L_{n-s} \) are generic linear forms in \( X_0, \ldots , X_n; \) i.e., the transcendency degree of the field generated by the coefficients of \( L_1, \ldots , L_{n-s+1} \) over \( k' \) is \( (n-s+1)(n+1) \).

For brevity, we denote \( Q_i = (M/L^{(i)} M)^p, 0 \leq i \leq n-s \). Let \( w \) be an integer, and let \( 0 \leq i \leq n-s-1 \). Consider the exact sequence:

\[ 0 \to Q_i(w-1) \xrightarrow{L_{i+1}} Q_i(w) \to Q_i(w)/L_{i+1} Q_i(w) \to 0. \]

It induces the exact sequence:

\[ 0 \to (Q_i^{\nu})_{w-1} \xrightarrow{L_{i+1}} (Q_i^\nu)_w \to (Q_i^{\nu+1})_w \]

(we use the notation from the Introduction). Put \( \nu_i = \inf \{ w : (Q_i^\nu)_w \neq 0 \} \) for every \( 0 \leq i \leq n-s-1 \) and \( \nu = \nu_{n-s-1} \). In the case where \( L_1, \ldots , L_{n-s} \) are generic linear forms in \( X_0, \ldots , X_n; \) see above, \( \nu_i = \nu_i(M, p) \) and \( \nu = \nu(M, p) \).

Recall that the functor \( N \mapsto N^\nu \) is exact from the left. We have \( (A^\nu_0)_m = \{ 0 \} \) for every \( m < 0 \) because \( n-s+1 > 1 \). Next, \( M \) is a \( \{ 0 \} \)-primary \( A_0 \)-module. Hence, by Lemma 3, we have \( \nu_i > -\infty \) for every \( 0 \leq i \leq n-s-1 \). The sequence (30) implies that
\[ \nu_i \leq \nu_{i+1} \text{ for } 0 \leq i \leq n-s-2, \text{ and } H(Q_i, \nu_i) \leq H(Q_{i+1}, \nu_i) \text{ for } 0 \leq i \leq n-s-1. \text{ Thus, (15) is proved.} \]

Using induction on \( i \), from (30) we deduce successively the inequalities

\[ H(M^\gamma, m) \leq \sum_{0 \leq j \leq i-1} \left( \frac{m - \nu + j}{j} \right) (H(Q_j^\gamma, \nu) - H(Q_{j+1}^\gamma, \nu)) \]

\[ + \sum_{0 \leq \nu \leq m} \left( \frac{m - \nu + i - 1}{i - 1} \right) H(Q_i^\gamma, w), \quad m \geq \nu, \]

for \( i = 1, \ldots, n-s \). As we have seen, the first sum on the right-hand side in this inequality is at most 0.

We claim that \( H(Q_{n-s}^\gamma, w) = D(M) \) for every integer \( w \). Indeed, the sequences (30) with \( i = n-s \) imply \( H(Q_{n-s+1}^\gamma, w) = 0 \) and \( H(Q_{n-s}^\gamma, w - 1) = H(Q_{n-s}^\gamma, w) \) for every \( w \). Put \( L = L^{(n-s)} \). Now (18) with \( v = n-s \) and Lemma 3 applied to all modules \( M/M(\mathfrak{m})_j, j \in J(\{0\}, L) \), reduce our assertion to \( H((A_0/\mathfrak{m})^\gamma, w) = D(A_0/\mathfrak{m}) \) for all integers \( w \) and \( j \in J(\{0\}, L) \). But in our case the number of elements \( \# J(\{0\}, L) \) is equal to 1. Denote \( \mathfrak{m} = \mathfrak{m}_j \) for \( j \in J(\{0\}, L) \). Then, obviously, \( D(A_0/\mathfrak{m}) = 1 \) and \( H(A_0/\mathfrak{m}, w) = 1 \) for every \( w \geq 0 \). Therefore, \( H((A_0/\mathfrak{m})^\gamma, w) = 1 \) for all \( w \). The claim is proved.

Put \( i = n-s \) in (31). Substituting \( D(M) \) for \( H(Q_i^\gamma, w) \) and 0 for \( H(Q_{i+1}^\gamma, \nu) - H(Q_{i+1}^\gamma, \nu) \) in (31), we get

\[ H(M^\gamma, m) \leq H(M^\gamma, m) \leq \left( \frac{m - \nu + n-s}{n-s} \right) D(M). \]

Thus, (14) and (i) are proved.

Now we prove (ii). Let \( W \) be the \( K_0 \)-vector space occurring in the given representation of the module \( M \); see the Introduction. In what follows we use all the notation from the Introduction related to this representation of the module \( M \). Recall that \( \mu = \dim_{K_0} W \). We choose indices \( \nu_1, \ldots, \nu_\mu \in J \) such that \( \det(w_{i,i-j})_{1 \leq i,j \leq \mu} = \Delta \neq 0 \). Let \( L_1, \ldots, L_{n-1} \) be linear forms as in the proof of (i). Let \( S_i = A_0/L(i)A_0 \setminus \{0\} \) be the multiplicatively closed set, and \( K_i = S_i^{-1}(A_0/L(i)A_0) \) the field of fractions of \( A_0/L(i)A_0 \). The linear forms \( L_1, \ldots, L_{n-1} \) can be chosen so that, additionally, for every \( 0 \leq i \leq n-s-1 \),

1) the element \( \Delta \mod L(i)A \in A/L(i)A \) is nonzero;
2) the \( p_{L(i)} \)-primary component \( (h_1, \ldots, h_s) \in A/L(i)A \langle p_{L(i)} \rangle \) equals \( p_{L(i)} \);
3) \( \eta_j \mod p_{L(i)} \), \( 1 \leq j \leq d-1 \), is a basis of the \( K_i \)-vector space \( S_i^{-1}(A/p_{L(i)}) \)

(these are conditions of general position).

Now our aim is to prove inequalities (a)–(c) from statement (ii) of Theorem 3 for \( \nu_{n-s-1} \) in place of \( \nu_{n-s-1} \). In particular, if \( L_1, \ldots, L_{n-1} \) are generic linear forms over \( k' \), we shall obtain statement (ii) of the theorem.

For a polynomial \( a \in A \), denote \( \overline{a} = a \mod L^{(n-s-1)}A = A/L^{(n-s-1)}A \). Let \( \overline{\mathfrak{e}}_i \) be the canonical generator of the direct summand \( (A/L^{(n-s-1)}A)(\mu_i) \subset B/L^{(n-s-1)}B \). For \( \ell = (i,j) \in J \), we put \( \overline{\mathfrak{e}} = e_{\ell} \overline{\mathfrak{e}} \in B/L^{(n-s-1)}B \). We recall that \( Q_{n-s-1} = (M/L^{(n-s-1)}M)^{\rho} \) and denote \( R_{n-s-1} = (B/p^{(\rho)}B) \).

We show that the module \( Q_{n-s-1} \) is given by the vector subspace \( W_{n-s-1} \) with the \( K_{n-s-1} \)-basis \( \overline{w}_{i,j} = \sum_{i,j \in J} \overline{w}_{i,j} \). Indeed, the elements \( \overline{w}_{i,j} \) belong to \( A_0/L^{(n-s-1)}A_0 \). Therefore, \( \dim_{K_{n-s-1}} W_{n-s-1} = \mu \). Let \( \overline{W} \) denote the \( K_{n-s-1} \)-vector space that gives \( Q_{n-s-1} \) in accordance with the construction described in the Introduction. Recall that \( \delta \) corresponds to \( W \) by this construction. Similarly, let \( \tilde{\delta} \) correspond to \( \overline{W} \). Then, by Lemma 3, we have \( \dim_{K_{n-s-1}} W = D(B/p^{(\rho)}B) - D(M) \), where \( M \) and \( B/p^{(\rho)}B \) are viewed
as \( A_0 \)-modules, and similarly \( \dim_{K_{n-s-1}} \tilde{W} = D(R_{n-s-1}) - D(Q_{n-s-1}) \), where \( Q_{n-s-1} \) and \( R_{n-s-1} \) are viewed now as \( A_0 / L^{(n-s-1)} A_0 \)-modules. But \( D(M) = D(Q_{n-s-1}) \) and \( D(B/p^{(e)} B) = D(R_{n-s-1}) = n_1d\left( e - 1 + s \right) = \#J \)

by (18) and 2), 3). Hence, \( \mu = \dim_{K_0} W = \dim_{K_{n-s-1}} \tilde{W} \). Obviously, \( \tilde{W} \supset W_{n-s-1} \).

Thus, \( \tilde{W} = W_{n-s-1} \), and the required assertion is proved. We have \( \deg \pi_{i,t} \leq \deg w_{i,t} \) for all \( i, t \). Hence, \( \delta \leq \delta \).

Thus, in the proof we can replace \( A \) and \( M \) by \( A/L^{(n-s-1)} A \) and \( Q_{n-s-1} \), respectively, and assume in what follows that \( s = n - 1 \) without loss of generality. Now \( A_0 = k[E_0, E_n] \).

Note that condition (28) is fulfilled for the linear forms \( E_0, E_n \).

We choose a subset \( J(M) \subset J \) such that the collection of \( e_i, i \in J(M) \), and of \( w_1, \ldots, w_\mu \) is a basis of the \( K_0 \)-vector space \( S_0^{-1} B \) (hence, for the number of elements we have \( \#J = \mu = \#J(M) \)). Solving the appropriate linear systems by Cramer’s rule, we see that there is a nonzero homogeneous polynomial \( \Delta_3 \in A_0 \) of degree at most \( \mu \delta \) such that \( \Delta_3 e_v \in \sum_{w \in J(M)} A_0 w_\nu + \sum_{1 \leq j \leq \mu} A_0 w_\nu \) for every \( v \in J \).

Let \( a = \min_{1 \leq i \leq n} a_i \). Assume that \( M^{-}_n \neq 0 \) for an integer \( N \geq 0 \). By (29), this means that there are homogeneous elements \( b_0, b_n \in B/p^{(e)} B \) of homogeneous degree \( m + a, m \geq 0 \), such that \( E_0^{N+m} b_n - E_n^{N+m} b_0 \in B'/p^{(e)} B \subset W \), but \( b_0, b_n \notin W \).

Let \( \Delta_4 = \Delta_5^2 \Delta_3^2 \Delta_3 \) if char(\( k \)) = 0 or char(\( k \)) > 0 and \( \alpha = 1 \), or \( \Delta_4 = \Delta_0^\nu \Delta_3 \Delta_3 \) if char(\( k \)) = \( p > 0 \). By Lemma 7, we can write

\[
\Delta_4 b_i = \sum_{i \in J(M)} b_{i,i} e_i + \sum_{1 \leq j \leq \mu} b_{i,j} w_j, \quad i = 0, n,
\]

where all \( b_{i,i}, b_{i,j} \in A_0 \) are homogeneous elements and not all \( b_{i}, i \in J(M) \), are zeros. Consequently,

\[
\Delta_4 (E_0^{N+m} b_n - E_n^{N+m} b_0) = \sum_{i \in J(M)} (E_0^{N+m} b_{n,i} - E_n^{N+m} b_{0,i}) e_i + \sum_{1 \leq j \leq \mu} (E_0^{N+m} b_{n,j} - E_n^{N+m} b_{0,j}) w_j \in W.
\]

Therefore, \( E_0^{N+m} b_{n,i} - E_n^{N+m} b_{0,i} = 0 \) for every \( i \in J(M) \). Hence, the homogeneous degrees of all nonzero elements \( b_{i,i}, i = 0, n \), are at least \( N + m \). Now (32) implies that

\[
m + a + \deg(\Delta_4) \geq N + m + \min_{i \in J(M)} \deg e_i.
\]

But \( \min_{i \in J(M)} \deg e_i \geq \min_{1 \leq i \leq n} a_i = a \). Thus, \( N \leq \deg \Delta_4 \) and \( N - a \leq \deg(\Delta_4) - a \).

This implies (ii). The theorem is proved.

\[\square\]

§4. ESTIMATION OF THE HILBERT FUNCTION OF THE INTEGRAL CLOSURE

OF A GRADED RING

Now our aim is to prove Theorem 2. Extending \( k \) up to \( k(t)^{p-\infty} \), where \( t \) is a transcendental element over \( k \), we shall assume without loss of generality that \( k \) is infinite (it is well known that the ring \( B \otimes_k k(t)^{p-\infty} \) is integrally closed).

In (27) we can replace the ring \( A/p \) by \( B \). Hence, \( \deg B = \deg B \). The Hilbert function \( H(B, m) \) is monotone nondecreasing. This implies the assertion of the theorem for \( n = s \).

In what follows we assume that \( n > s \).

Suppose \( i + ht(p) < n \). Consider an \( i \)-tuple of \( (L_1, \ldots, L_i) = L^{(i)} \) of linear forms from \( k[E_0, E_{s+1}, \ldots, E_n] \) in general position. Then, by Remark 2, the ring \( (B/L^{(i)})^\rho \) is integral. Denote by \( (B/L^{(i)}) \) the integral closure of \( B/L^{(i)} \) in its field of
fractions. We have $D((B/L^{(i)}(B)^\nu)) = D((B/L^{(i)}(B)^\nu) = D(B)$ and $H((B/L^{(i)}(B)^\nu, m) = H((B/L^{(i)}(B)^\nu, m) = 0$ for every $m < 0$. Next, for every $1 \leq i \leq n - s$ there is an exact sequence of graded modules

$$0 \rightarrow (B/L^{(i-1)}(B)^\nu) \rightarrow (B/L^{(i-1)}(B)^\nu / L_i(B/L^{(i-1)}(B)^\nu) \rightarrow 0.$$  

If $1 \leq i < n - s$, then the ring $(B/L^{(i-1)}(B)^\nu / L_i(B/L^{(i-1)}(B)^\nu)$ is integral because $(B/L^{(i-1)}(B)^\nu)$ is integrally closed and $L_i$ is in general position; see, e.g., the Appendix in [7]. Hence in this case there is a monomorphism $(B/L^{(i-1)}(B)^\nu / L_i(B/L^{(i-1)}(B)^\nu) \rightarrow (B/L^{(i)}(B)^\nu).$ Considering the homogeneous components, for every $m \geq 0$ we get an exact sequence of linear spaces:

$$0 \rightarrow ((B/L^{(i-1)}(B)^\nu)_{m-1} \rightarrow ((B/L^{(i-1)}(B)^\nu)_{m} \rightarrow ((B/L^{(i)}(B)^\nu)_{m}.$$

The module $(B/L^{(n-s-1)}(B)^\nu / L_{n-s}(B/L^{(n-s-1)}(B)^\nu) = G$ contains no $\mathfrak{m}_0$-primary component, i.e., the maximal homogeneous ideal $\mathfrak{m}_0$ is not an associated prime ideal of the submodule $\{0\}$ of that module. Again, this is true because the ring $(B/L^{(n-s-1)}(B)^\nu)$ is integrally closed, so that the ideal $(L_{n-s}) \subset (B/L^{(n-s-1)}(B)^\nu)$ is unmixed. This implies that $D(G) = D(B)$ and the homomorphism of multiplication by $L_{n-s+1}$ of the module $G$ is injective. Therefore, the Hilbert function of $G$ is monotone nondecreasing. Hence, $H(G, m) \leq D(B)$ for every $m \geq 0$. Now, as in the proof of assertion (i) of Theorem 3, we can use the exact sequences (33) to get inequality (6). The theorem is proved.

References


ST. PETERSBURG BRANCH, STEKLOV MATHEMATICAL INSTITUTE, RUSSIAN ACADEMY OF SCIENCES, FONTANKA 27, ST. PETERSBURG 191023, RUSSIA

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

Received 10/MAY/2007

Translated by THE AUTHOR