JOURNAL OF
PURE AND
APPLIED ALGEBRA

ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 565–599

Bounds for the Hilbert function of polynomial ideals and for the degrees in the Nullstellensatz

Martín Sombra[1]

Departamento de Matemática, Universidad de Buenos Aires, 1428 Buenos Aires, Argentina

Abstract

We present a new effective Nullstellensatz with bounds for the degrees which depend not only on the number of variables and on the degrees of the input polynomials but also on an additional parameter called the *geometric degree of the system of equations*. The obtained bound is polynomial in these parameters. It is essentially optimal in the general case, and it substantially improves the existent bounds in some special cases.

The proof of this result is combinatorial, and relies on global estimates for the Hilbert function of homogeneous polynomial ideals.

In this direction, we obtain a lower bound for the Hilbert function of an arbitrary homogeneous polynomial ideal, and an upper bound for the Hilbert function of a generic hypersurface section of an unmixed radical polynomial ideal. © 1997 Elsevier Science B.V.

1991 Math. Subj. Class.: Primary 13P10; Secondary 13D40

Introduction

Let k be a field with an algebraic closure denoted by $\bar{k}$, and let $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ be polynomials which have no common zero in $\bar{k}^n$. Classical Hilbert's Nullstellensatz ensures then that there exist polynomials $a_1,\ldots,a_s \in k[x_1,\ldots,x_n]$ such that

$$1 = a_1 f_1 + \cdots + a_s f_s.$$

[1] Partially supported by CONICET PID 3949/92 and UBA CYT EX. 001.

PII S0022-4049(97)00028-5

An *effective Nullstellensatz* amounts to estimate the degrees of the polynomials $a_1,\dots,a_s$ in one such a representation. An explicit bound for the degrees reduces the problem of effectively finding the polynomials $a_1,\dots,a_s$ to the solving of a system of linear equations.

The effective Nullstellensatz has been the object of much research during the last ten years because of both its theoretical and practical interest. The most precise bound obtained up to now for this problem in terms of the number of variables n and the maximum degree d of the polynomials $f_1,\dots,f_s$ is

$$\deg a_i \le \max\{3,d\}^n, \quad 1 \le i \le s.$$

This bound is due to Kollár [22], and it is essentially optimal for $d \ge 3$; in the case when $d=2$ a sharper estimate can be given [30].

Related results can be found in the research papers [2, 4, 7, 8, 12, 23, 29, 31], also there are extensive discussions and bibliography about the effective Nullstellensatz in the surveys [3, 33].

Because of its exponential nature, this bound is hopeless for most practical applications. This behavior is, in general, unavoidable for polynomial elimination problems when only the number of variables and the degrees of the input polynomials are considered.

However, it has been observed that there are many particular instances in which this bound can be notably improved. This fact has motivated the introduction of new parameters which enable to differentiate special families of systems of polynomial equations whose behavior for the problem in question is polynomial instead of exponential [14, 15].

In this spirit, we consider an additional parameter associated to the input polynomials $f_1,\dots,f_s$, called the *geometric degree of the system of equations*, which is defined as follows.

Suppose that k is a zero characteristic field and let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials such that $1 \in (f_1,\dots,f_s)$. Then there exist $g_1,\dots,g_s$ $\bar{k}$-linear combinations of $f_1,\dots,f_s$ and an integer $t \le s$ such that $1 \in (g_1,\dots,g_t)$, $g_1,\dots,g_{t-1}$ is a regular sequence, and $(g_1,\dots,g_{t-1})$ is a radical ideal for $1 \le i \le t-1$. Let $V_i \subseteq \mathbb{A}^n(\bar{k})$ be the affine variety defined by $g_1,\dots,g_i$ for $1 \le i \le s$, and set

$$\delta_{g_1,\dots,g_s} := \max_{1 \le i \le \min\{t,n\}-1} \deg V_i,$$

where $\deg V_i$ stands for the degree of the affine variety V_i. Then the geometric degree of the system of equations $\delta(f_1,\dots,f_s)$ is defined as the minimum of the $\delta_{g_1,\dots,g_s}$ over all linear combinations of $f_1,\dots,f_s$ satisfying the stated conditions.

In the case when k is a field of positive characteristic, the degree of the system of equations $f_1,\dots,f_s$ is defined in an analogous way, by considering $\bar{k}$-linear combinations of the polynomials $\{f_i, x_j f_i \mid 1 \le i \le s, 1 \le j \le n\}$.

In both cases, the existence of $g_1,\dots,g_s$ satisfying these properties is a consequence of Bertini's theorem.

We obtain (Theorem 37):

Theorem. *Let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials such that $1 \in (f_1,\dots,f_s)$. Let $d := \max_{1\le i\le s} \deg f_i$, and let δ be the geometric degree of the system of equations $f_1,\dots,f_s$. Then there exist polynomials $a_1,\dots,a_s \in k[x_1,\dots,x_n]$ such that*

$$1 = a_1 f_1 + \cdots + a_s f_s$$

with $\deg a_i f_i \le \min\{n,s\}^2(d+3n)\delta$ for $i = 1,\dots,s$.

We also obtain a similar bound for the representation problem in complete intersections (Theorem 36).

Let $d := \max_{1\le i\le s} \deg f_i$. Then we have that

$$\delta(f_1,\dots,f_s) \le (d+1)^{\min\{s,n\}-1}$$

holds and so our bounds for the effective Nullstellensatz and for the representation problem in complete intersections are essentially sharp in the general case. We remark however that they can substantially improve the usual estimates in some special cases (see Example 39).

Similar bounds for the effective Nullstellensatz have also been recently obtained by algorithmic tools [15, Theorem 19], [14, Section 4.2] and by duality methods [24].

The proofs of these bounds are combinatorial, and they rely on *global* estimates for the Hilbert function of certain polynomials ideals.

The study of the global behavior of the Hilbert function of homogeneous ideals is of independent interest. It is related to several questions of effective commutative algebra, mainly in connection with the construction of regular sequences of maximal length with polynomials of controlled degree lying in a given ideal [10], and to transcendental number theory, in the context of the so-called zero lemmas [5].

Let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous ideal. We understand by the dimension of I the dimension of the projective variety that it defines, and we denote by h_I its Hilbert function and by $\deg I$ the degree of the ideal I.

The problem of estimating h_I was first considered by Nesterenko [28], who proved that for a zero characteristic field k and a homogeneous prime ideal $P \subseteq k[x_0,\dots,x_n]$ of dimension $d \ge 0$ the following holds:

$$\binom{m+d+1}{d+1} - \binom{m-\deg P+d+1}{d+1} \le h_P(m) \le \deg P\,(4m)^d, \quad m \ge 1.$$

Later on, Chardin [10] improved Nesterenko's upper bound by simplifying his proof, and obtained that for a perfect field k and a homogeneous unmixed radical ideal

$I \subseteq k[x_0, \dots, x_n]$ of dimension $d \geq 0$ the following inequality holds:

$$h_I(m) \leq \deg I \binom{m+d}{d}, \quad m \geq 1.$$

This estimate has also been obtained by Kollár, by using cohomological arguments [10].

In this direction, we obtain a lower bound for the Hilbert function of an arbitrary homogeneous polynomial ideal of dimension $d \geq 0$ (Theorem 4). We have that

$$h_I(m) \geq \binom{m+d+1}{d+1} - \binom{m - \deg I + d + 1}{d+1}, \quad m \geq 1$$

holds. This result generalizes the bound of Nesterenko for the case of a homogeneous prime ideal $P \subseteq k[x_0, \dots, x_n]$. It is optimal in terms of the dimension and the degree of the ideal I.

We present also an upper bound for the Hilbert function of a generic hypersurface section f of a homogeneous unmixed radical ideal $I \subseteq k[x_0, \dots, x_n]$ of dimension $d \geq 1$ (Theorem 22). We have the inequality

$$h_{(I,f)}(m) \leq 3 \deg f \deg I \binom{m+d-1}{d-1}, \quad m \geq 5d \deg I.$$

Our approach to the Hilbert function is elementary, and yields a new point of view into the subject which is clearer than that of the previous works. We hope that our techniques would also be useful for treating arithmetic Hilbert functions (see [28]).

We shall briefly sketch the relationship between these bounds for the Hilbert function, and the effective Nullstellensatz and the representation problem in complete intersections.

Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be a regular sequence. There are several effectiveness questions about this set of polynomials which can be easily solved in the case when the homogenization of these polynomials $\tilde{f}_1, \dots, \tilde{f}_s \in k[x_0, \dots, x_n]$ is again a regular sequence. An example of this situation is the effective Nullstellensatz, for which there exists a simple and well-known proof in this condition (see, for instance, [26]).

The central point in our proof of the effective Nullstellensatz consists then in showing that the regular sequence $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ can, in fact, be replaced by polynomials $p_1, \dots, p_s \in k[x_1, \dots, x_n]$ of controlled degrees such that $(f_1, \dots, f_i) = (p_1, \dots, p_i)$ for $1 \leq i \leq s$, and such that the homogenizated polynomials $\tilde{p}_1, \dots, \tilde{p}_s$ define a regular sequence in $k[x_0, \dots, x_n]$. The proof of this result proceeds by induction, and the bounds for the Hilbert function allows us to control at each step $1 \leq i \leq s$ the degree of the polynomial p_i.

The spirit of our proof follows Dubé's paper on the classical effective Nullstellensatz [11]. We remark here that there are many errors in Dubé's argument, and a serious gap, for it relies on an assumption on the Hilbert function of certain class of homogeneous polynomial ideals [11, Section 2.1] which is unproved in his paper and which is neither in the literature, as it was noted by Almeida [1, Section 3.1], and so his proof should be considered incomplete as it stands.

Our approach allows us not only to avoid Dubé's assumption and to prove the results stated in his paper, but also to obtain our more refined bounds.

Finally, we remark that our exposition is elementary and essentially self-contained.

The exposition is divided in four parts. In Section 1 we state some well-known features of degree of projective varieties and Hilbert function that will be needed in the subsequent parts, and we prove some of them when suitable reference is lacking. In Section 2 we prove the lower and upper bounds for the Hilbert function and analyze the extremal cases. In Section 3, we apply the obtained results to the construction of regular sequences. In Section 4 we consider the consequences for the effective Nullstellensatz and for the representation problem in complete intersections.

0. Notations and conventions

We work over an arbitrary field k with algebraic closure $\bar{k}$. As usual, $\mathbb{P}^n$ and $\mathbb{A}^n$ denote the projective space and the affine space of dimension n over $\bar{k}$. A variety is not necessarily irreducible.

The ring $k[x_0,\dots,x_n]$ will be denoted alternatively by R or R_k.

Let $I \subsetneq k[x_0,\dots,x_n]$ be a homogeneous ideal. We understand by the dimension of I the dimension of the projective variety that it defines and we shall denote it by $\dim I$, so that $\dim I = \dim_{\mathrm{krull}} I - 1$.

Let $J \subsetneq k[x_1,\dots,x_n]$ be an affine ideal. We shall understand by the dimension of J its Krull dimension. At each appearance, it will be clear from the context to which notion we are referring to.

An ideal $I \subsetneq k[x_0,\dots,x_n]$ is *unmixed* if its associated prime ideals have all the same dimension. In particular, I has not imbedded associated primes and its primary decomposition is unique.

Given an ideal $I \subseteq k[x_0,\dots,x_n]$, then $I^e := \bar{k} \otimes_k I \subseteq \bar{k}[x_0,\dots,x_n]$ is the extended ideal of I in $\bar{k}[x_0,\dots,x_n]$.

Given $I \subseteq R_k$ a homogeneous ideal, then $V(I) := \{x \in \mathbb{P}^n \mid f(x) = 0 \ \forall f \in I\} \subseteq \mathbb{P}^n$ denotes the projective variety defined by I. Conversely, given a projective variety $V \subseteq \mathbb{P}^n$ we define the ideal $I_k(V) := \{f \in R_k \mid f|_V \equiv 0\} \subseteq R_k$, and we denote by $I(V) := I_{\bar{k}}(V) \subseteq \bar{k}[x_0,\dots,x_n]$ the defining ideal of V.

Given a graded R-module M and $m \in \mathbb{Z}$, M_m denotes the homogeneous part of degree m.

Let be given a homogeneous ideal $I \subseteq k[x_0,\dots,x_n]$. The *Hilbert function* or *characteristic function* h_I of the ideal I is defined as

$$m \mapsto \dim_k(k[x_0,\dots,x_n]/I)_m.$$

Given a projective variety $V \subseteq \mathbb{P}^n, h_V$ is the Hilbert function of $I(V)$.

Given $f \in k[x_0,\dots,x_n]$ a homogeneous polynomial, $f^a \in k[x_1,\dots,x_n]$ is its affinization and given $I \subseteq k[x_0,\dots,x_n]$ a homogeneous ideal, $I^a \subseteq k[x_1,\dots,x_n]$ is its affinization.

Conversely, given a polynomial $g \in k[x_1,\dots,x_n]$, $\tilde{g} \in k[x_0,\dots,x_n]$ is its homogenization, and given an ideal $J \subseteq k[x_1,\dots,x_n]$, we denote by $\tilde{J} \subseteq k[x_0,\dots,x_n]$ its homogenization.

1. Preliminaries on degree and Hilbert function

In this section we state some well-known properties concerning the degree of a variety and the Hilbert function of a homogeneous polynomial ideal which will be needed in the sequel. Also we shall prove some of them when suitable reference is lacking.

Let $V \subseteq \mathbb{P}^n$ be an irreducible projective variety of dimension d. The *degree* of V is defined as

$$\deg V := \sup\{\#(V \cap H_1 \cap \cdots \cap H_d) \mid H_1,\dots,H_d \subseteq \mathbb{P}^n \text{ hyperplanes} \\ \text{and } \dim(V \cap H_1 \cap \cdots \cap H_d) = 0\}.$$

This number is finite, and it realizes generically, if we think the set $\{(H_1,\dots,H_d) \mid H_1,\dots,H_d \subseteq \mathbb{P}^n \text{ hyperplanes}\}$ as parameterized by a nonempty set of $\mathbb{A}^{(n+1)d}$ [17, Lecture 18]. We agree that $\deg \emptyset = 1$.

The notion of degree can be extended to possible reducible projective varieties following [19]. Let $V \subseteq \mathbb{P}^n$, and let $V = \bigcup_C C$ be the minimal decomposition of V in irreducible varieties. Then the (*geometric*) *degree* of V is defined as

$$\deg V := \sum_C \deg C$$

For this notion of degree the following Bézout's inequality without multiplicities for the degree of the intersection of two varieties holds. Let $V, W \subseteq \mathbb{P}^n$ be varieties. Then

$$\deg(V \cap W) \le \deg V \deg W.$$

This is a consequence of Bézout's inequality for affine varieties [19, Theorem 1]. The details can be found in [9]. This result can also be deduced from the Bézout's theorems [13, Theorem 12.3], [34, Theorem 2.1].

We turn our attention to the Hilbert function of a homogeneous ideal. Let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous ideal of dimension d. There exists a polynomial $p_I \in \mathbb{Q}[t]$ of degree d, and $m_0 \in \mathbb{Z}$ such that

$$h_I(m) = p_I(m)$$

for $m \ge m_0$. The polynomial p_I is called the *Hilbert polynomial* of the ideal I.

The degree of a homogeneous ideal $I \subseteq k[x_0,\dots,x_n]$ can be defined through its Hilbert polynomial.

Let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous ideal of dimension d, with $d \geq 0$. Let $p_I = a_d t^d + \cdots + a_0 \in \mathbb{Q}[t]$ be its Hilbert polynomial. Then the (*algebraic*) *degree* of the ideal I is defined as

$$\deg I := d! a_d \in \mathbb{N}$$

If $I \subseteq k[x_0,\dots,x_n]$ is a homogeneous ideal of dimension -1, then I is a $(x_0,\dots,x_n)$-primary ideal, and the *degree* of I is defined as the length of the k-module $k[x_0,\dots,x_n]/I$, which equals its dimension as a k-linear space. We also agree that $\deg k[x_0,\dots,x_n] = 0$.

Given $I \subseteq k[x_0,\dots,x_n]$ a homogeneous ideal, we denote by $\operatorname{irr} I$ the number of irreducible components of $V(I) \subseteq \mathbb{P}^n$.

Let I, $J \subseteq k[x_0,\dots,x_n]$ be homogeneous ideals. Then we have the following exact sequence of graded k-algebras:

$$0 \to R/(I \cap J) \to R/I \oplus R/J \to R/(I+J) \to 0$$

$$(f,g) \mapsto f - g$$

from where we get that

$$h_{I\cap J}(m) = h_I(m) + h_J(m) - h_{I+J}(m), \quad m \geq 1$$

holds. In particular, if $\dim I > \dim J$, then $\deg(I \cap J) = \deg I$.

Let k be a perfect field, $I \subseteq k[x_0,\dots,x_n]$ an homogeneous radical ideal, and let $I = \bigcap_P P$ be the minimal primary decomposition of I. In this situation we have that

$$\deg I = \sum_{P\,:\,\dim P = \dim I} \deg V(P)$$

holds [34, Proposition 1.49], [17, Proposition 13.6], and thus the degree of the ideal I may be calculated from the degrees of the varieties defined by its associated prime ideals of maximal dimension.

Let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous radical ideal, and $I = \bigcap_P P$ the minimal primary decomposition of I. From the canonical inclusion of graded modules $R/I \hookrightarrow \bigoplus_P R/P$, we deduce that

$$h_I(m) \leq \sum_P h_P(m), \quad m \geq 1.$$

Let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous ideal, and $I^e \subseteq \bar{k}[x_0,\dots,x_n]$ be the extended ideal. Let $R/I = \bigoplus_m (R/I)_m$ be the decomposition of $k[x_0,\dots,x_n]/I$ into homogeneous parts. Then we have that $(R_{\bar{k}}/I^e)_m = \bar{k} \otimes_k (R/I)_m$ holds and so $h_{I^e}(m) = h_I(m)$, i.e. the Hilbert function is invariant under change of the base field. In particular $\deg I^e = \deg I$.

We have also that there exist $y_0,\dots,y_d \in \bar{k}[x_0,\dots,x_n]$ algebraically independent linear forms such that $\bar{k}[y_0,\dots,y_d] \hookrightarrow \bar{k}[x_0,\dots,x_n]/I^e$ is an inclusion of $\bar{k}$-algebras, and so

$$h_I(m) = h_{I^e}(m) \geq \dim_{\bar{k}}(\bar{k}[y_0,\dots,y_d])_m = \binom{m+d}{d}.$$

We shall need the following identity for the combinatorial numbers.

Lemma 1. *Let $d \geq 0$, $D \geq 1$, $m \in \mathbb{Z}$. Then*

$$\binom{m+d+1+D}{d+1} - \binom{m+d+1}{d+1} = \sum_{i=1}^{D} \binom{m+d+i}{d}.$$

Proof. The case $D = 1$ is easy. In the case when $D > 1$, we have that

$$\binom{m+d+1+D}{d+1} - \binom{m+d+1}{d+1}$$
$$= \sum_{i=1}^{D} \left\{ \binom{m+d+1+i}{d+1} - \binom{m+d+i}{i} \right\} = \sum_{i=1}^{D} \binom{m+d+i}{d}. \qquad \square$$

We shall also make appeal to Macaulay's characterization of the Hilbert function of a homogeneous polynomial ideal.

Given positive integers i, c, the *i-binomial expansion* of c is the unique expression

$$c = \binom{c(i)}{i} + \cdots + \binom{c(j)}{j}$$

with $c(i) > \cdots > c(j) \geq j \geq 1$.

Let $c = \binom{c(i)}{i} + \cdots + \binom{c(j)}{j}$ be the i-binomial expansion of c. Then we set

$$c^{\langle i \rangle} := \binom{c(i)+1}{i+1} + \cdots + \binom{c(j)+1}{j+1}.$$

We note that this expression is the $(i+1)$-binomial expansion of $c^{\langle i \rangle}$.

Remark 2. Let b, c, $i \in \mathbb{Z}_{>0}$. Then it is easily seen that $b \geq c$ if and only if $(b(i),\dots,b(j))$ is greater or equal that $(c(i),\dots,c(j))$ in the lexicographic order, and thus $b \geq c$ if and only if $b^{\langle i \rangle} \geq c^{\langle i \rangle}$.

We recall that a sequence of nonnegative integers $(c_i)_{i \in \mathbb{Z}_{\geq 0}}$ is called an *O-sequence* if

$$c_0 = 1, \qquad c_{i+1} \leq c_i^{\langle i \rangle}, \quad i \geq 1$$

We then have:

Theorem (Macaulay, [16]). *Let $h : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$. Then h is the Hilbert function of a homogeneous polynomial ideal if and only if*

$$(h(i))_{i \in \mathbb{Z}_{\geq 0}}$$

is an O-sequence.

2. Bounds for the Hilbert function

In this section we shall derive both lower and upper bounds for the Hilbert function of homogeneous polynomial ideals. These estimates depend on the dimension and on the degree of the ideal in question, and eventually on its length.

We derive first a lower bound for the Hilbert function of an arbitrary homogeneous polynomial ideal.

We consider separately the case when $\dim I = 0$.

Lemma 3. *Let $I \subseteq k[x_0, \ldots, x_n]$ be a homogeneous unmixed ideal of dimension zero. Then*

$$h_I(m) \geq m + 1, \qquad \deg I - 2 \geq m \geq 0,$$

$$h_I(m) = \deg I, \qquad m \geq \deg I - 1.$$

Proof. We have that $I^e \subseteq \bar{k}[x_0, \ldots, x_n]$ is an unmixed ideal of dimension zero [35, Ch. VII, Theorem 36, Corollary 1]. As $\bar{k}$ is an infinite field, there exists a linear form $u \in \bar{k}[x_0, \ldots, x_n]$ which is a nonzero divisor modulo I^e. Then

$$h_I(m) - h_I(m-1) = h_{I^e}(m) - h_{I^e}(m-1) = h_{(I^e,u)}(m).$$

Let m_0 be minimum such that $h_{I^e}(m) = \deg I^e = \deg I$ for $m \geq m_0$. Then $h_{(I^e,u)}(m) \geq 1$ for $0 \leq m \leq m_0 - 1$ and $h_{(I^e,u)}(m) = 0$ for $m \geq m_0$, and thus we have that

$$h_I(m) = h_{I^e}(m) \geq m + 1, \qquad \deg I - 2 \geq m \geq 0$$

holds, and also $h_I(m) = h_{I^e}(m) = \deg I$ for $m \geq \deg I - 1$.

Theorem 4. *Let $I \subseteq k[x_0, \ldots, x_n]$ be a homogeneous ideal of dimension d, with $d \geq 0$. Then*

$$h_I(m) \geq \binom{m + d + 1}{d + 1} - \binom{m - \deg I + d + 1}{d + 1}, \quad m \geq 1$$

Proof. Let $I^e = \bigcap_P Q_P$ be a minimal primary decomposition of I^e, and let

$$I^* = \bigcap_{P : \dim P = \dim I^e} Q_P$$

be the intersection of the primary components of I^e of maximal dimension, which is an unmixed ideal of dimension d. Then $h_I(m) = h_{I^e}(m) \geq h_{I^*}(m)$ for $m \geq 1$, and we have that $\deg I = \deg I^*$. We shall proceed by induction on d. Consider first the case $d = 0$. We then have that

$$h_I(m) = h_{I^e}(m) \geq h_{I^*}(m) \geq \binom{m+1}{1} - \binom{m - \deg I + 1}{1}, \quad m \geq 1$$

holds, by Lemma 3 applied to I^*.

Now let $d \geq 1$. Let $u \in \bar{k}[x_0, \dots, x_n]$ be a linear form which is not a zero-divisor modulo I^*. Then we have that

$$h_{I^*}(m) - h_{I^*}(m-1) = h_{(I^*,u)}(m).$$

Then $\dim(I,u) = d - 1$ and $\deg(I^*, u) = \deg I^* = \deg I$. By the inductive hypothesis we have that

$$h_{I^*}(m) - h_{I^*}(m-1) = h_{(I^*,u)}(m) \geq \binom{m+d}{d} - \binom{m - \deg I + d}{d}, \quad m \geq 1$$

holds. Then

$$h_I(m) \geq h_{I^*}(m) = \sum_{j=0}^{m} h_{(I^*,u)}(j) \geq \sum_{j=0}^{m} \left\{ \binom{j+d}{d} - \binom{j - \deg I + d}{d} \right\}$$

$$= \binom{m+d+1}{d+1} - \binom{m - \deg I + d + 1}{d+1}, \quad m \geq 1$$

by Lemma 1. $\square$

This inequality extends Nesterenko's estimate for the case of a prime ideal [28, Section 6, Proposition 1] to the case of an arbitrary ideal.

Remark 5. By Gotzmann's persistence theorem [16] we have that for a homogeneous ideal $I \subseteq k[x_0, \dots, x_n]$ of dimension d there exists $m_0 \in \mathbb{Z}$ such that

$$h_I(m) \geq \binom{m+d+1}{d+1} - \binom{m - \deg I + d + 1}{d+1}, \quad m \geq m_0$$

as it is noted in [6, Remark 0.6]. Our theorem shows that this inequality holds globally, not only for big values of m.

Given $I \subseteq k[x_0, \dots, x_n]$ an homogeneous ideal of dimension $d \geq 0$, let $H_I(t) := \sum_{m=0}^{\infty} h_I(m)\, t^m$ denote its Hilbert–Poincaré series. Then the previous result states that

$$H_I(t) \geq \frac{1 - t^{\deg I}}{(1-t)^{d+2}}$$

in the sense that the inequality holds at each term of the power series.

This estimate is optimal in terms of the dimension and the degree of the ideal I. The extremal cases correspond to hypersurfaces of linear subspaces of $\mathbb{P}^n$. This can be deduced from [6, Corollary 2.8], which in turn depends on Gotzmann's theorem, but it can also be proved in an elementary way [32, Proposition 2.34].

We devote now to the upper bounds. In this respect we have two different estimates. The first bound is sharp for small values and the second for big ones.

The first upper bound will be deduced from a series of results and observations.

Definition 6. Let $V \subseteq \mathbb{P}^n$ be a variety. Then the *linear closure* of V is the smallest linear subspace of $\mathbb{P}^n$ which contains V, and it is denoted by $L(V)$.

Remark 7. Let $E \subseteq \mathbb{P}^n$ be a linear space. Then its defining ideal $I(E) \subseteq R_{\bar{k}}$ is generated by linear forms, and it is easy to see that

$$\dim E = n - \dim_{\bar{k}} I(E)_1.$$

Let $V \subseteq \mathbb{P}^n$ be a variety, and let $L \in R_{\bar{k}}$ be a linear form. Then $L|_V \equiv 0$ if and only if $L|_{L(V)} \equiv 0$, and thus $I(L(V)) = (I(V)_1)$. In particular, we have that

$$h_V(1) = n + 1 - \dim_{\bar{k}} I(V)_1 = \dim L(V) + 1.$$

The following proposition shows that the dimension of the linear closure is bounded in terms of the dimension and the degree of the variety. It is a consequence of Bertini's theorem [21, Theorem 6.3]. A proof can be found in [17, Corollary 18.12].

Proposition 8. *Let $V \subseteq \mathbb{P}^n$ be an irreducible variety. Then*

$$\dim L(V) + 1 \leq \deg V + \dim V.$$

The following is an estimate for the degree of the image of a variety under a regular map. It is a variant of [20, Lemma 1] and [30, Proposition 1].

Proposition 9. *Let $V \subseteq \mathbb{P}^n$ be a variety and $f_0, \ldots, f_N \in \bar{k}[x_0, \ldots, x_n]$ homogeneous polynomials of degree D which define a regular map*

$$\varphi : \mathbb{P}^n \longrightarrow \mathbb{P}^N,$$

$$x := (x_0 : \ldots : x_n) \mapsto (f_0(x) : \ldots : f_N(x)).$$

Then $\deg \varphi(V) \leq \deg V \, D^{\dim V}$.

Proof. We can suppose, without loss of generality, that V is irreducible. Let $d := \dim \varphi(V)$, and let $H_1, \dots, H_d \subseteq \mathbb{P}^n$ be hyperplanes such that

$$\#(\varphi(V) \cap H_1 \cap \cdots \cap H_d) = \deg \varphi(V).$$

For each $i = 1, \dots, d$, let $L_i \in R_{\bar{k}}$ be a linear form such that $H_i = \{L_i = 0\}$. Then $\#(\varphi(V) \cap H_1 \cap \cdots \cap H_d)$ is bounded by the number of irreducible components of $\varphi^{-1}(\varphi(V) \cap H_1 \cap \cdots \cap H_d)$ and so we have that

$$\begin{aligned} \#(\varphi(V) \cap H_1 \cap \cdots \cap H_d) &\leq \deg \varphi^{-1}(\varphi(V) \cap H_1 \cap \cdots \cap H_d) \\ &= \deg\left(V \cap \bigcap_{i=1}^{d} V(L_i(f_0, \dots, f_N)) \right) \leq \deg V\, D^d \end{aligned}$$

holds, by Bézout's inequality. We then have that $\deg \varphi(V) \leq \deg V\, D^{\dim V}$ holds, as $\dim \varphi(V) \leq \dim V$. $\square$

Now it follows easily the desired inequality for the case of an irreducible variety.

Proposition 10. *Let $V \subseteq \mathbb{P}^n$ be an irreducible variety of dimension d, with $d \geq 0$. Then*

$$h_V(m) \leq \deg V\, m^d + d, \quad m \geq 1$$

Proof. For $n, m \in \mathbb{N}$, let

$$v_m : \mathbb{P}^n \to \mathbb{P}^{\binom{n+m}{n}}, \qquad (x_0 : \dots : x_n) \mapsto (x^{(i)})_{|i|=m}$$

be the Veronese map of degree m. Then $v_m|_V : V \mapsto v_m(V)$ is a birregular morphism of degree m, and so we have that

$$h_{v_m(V)}(k) = h_V(mk), \quad k \geq 1$$

In particular, we have that

$$h_V(m) = h_{v_m(V)}(1) = \dim L(V) + 1$$

holds, by Remark 7, and so

$$h_V(m) \leq \deg v_m(V) + \dim v_m(V) \leq \deg V\, m^d + d$$

by application of Propositions 8 and 9. $\square$

We can extend this bound to the more general case of an unmixed radical ideal in $k[x_0, \dots, x_n]$.

Theorem 11. *Let k be a perfect field, and let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous unmixed radical ideal of dimension d, with $d \geq 0$. Then*

$$h_I(m) \leq \deg I\, m^d + \operatorname{irr} I\, d, \quad m \geq 1.$$

Proof. Let $I^e \subseteq R_{\bar{k}}$ be the extended ideal of I in $R_{\bar{k}}$. Then I^e is an unmixed radical ideal of dimension d [35, Ch. VII, Theorem 36, Corollary 1], [27, Theorem 26.3]. Let $I^e = \bigcap_P P$ be the minimal primary decomposition of I^e. Then we have that

$$h_I(m) \leq \sum_P h_P(m)$$

holds, from where

$$h_I(m) \leq \sum_P (\deg V(P)\, m^d + d) = \deg I\, m^d + \operatorname{irr} I\, d, \quad m \geq 1$$

by Proposition 10. □

This inequality has the same order of growth of h_I. We see also that it does not improve the estimate

$$h_I(m) \leq \deg I \binom{m+d-1}{d} + \operatorname{irr} I \binom{m+d-1}{d-1}, \quad m \geq 1,$$

which follows from Chardin's arguments [10].

From the asymptotic behavior $h_I(m) \sim (\deg I/d!) m^d$ we see that this inequality is sharp for big values of m only when $d=1$. In this case, the inequality is optimal in terms of the degree and the length of the ideal, and we determine the extremal cases.

Definition 12. Let $V, W \subseteq \mathbb{P}^n$ be varieties. Then V, W are *projectively equivalent* if there exists an automorphism $A \in PGL_{n+1}(\bar{k})$ such that $W = A(V)$ [17, p. 22].

Remark 13. Let $V, W \subseteq \mathbb{P}^n$ be varieties. Then V, W are projectively equivalent if and only if its coordinated rings $\bar{k}[V]$, $\bar{k}[W]$ are isomorphic as graded $\bar{k}$-algebras. In particular, their Hilbert function coincide.

A curve $C \subseteq \mathbb{P}^n$ is called a *rational normal curve* if it is projectively equivalent to $v_n(\mathbb{P}^1)$. Then C is nondegenerated, i.e. $L(C) = \mathbb{P}^n$ [17, Example 1.14], and its degree is n. By Proposition 8 the degree of C is minimum with the condition of being nondegenerated. In fact, rational normal curves are characterized by this property [17, Proposition 18.9].

Now let $l, n \in \mathbb{N}$, $\delta = (\delta_1,\dots,\delta_l) \in \mathbb{N}^l$ such that $|\delta| := \delta_1 + \cdots + \delta_l \leq n+1-l$. For $1 \leq j \leq l$, let $n_j := \delta_1 + \cdots + \delta_j + j$, and consider the inclusion of linear spaces given by

$$i_j : \mathbb{P}^{\delta_j} \hookrightarrow \mathbb{P}^n, \qquad (x_0 : \ldots : x_{\delta_j}) \mapsto (\overbrace{0 : \ldots : 0}^{n_{j-1}} : x_0 : \ldots : x_{\delta_j} : 0 : \ldots : 0).$$

The linear subspaces $i_j(\mathbb{P}^{\delta_j}) \subseteq \mathbb{P}^n$ are disjoint one from each other. Let

$$C(n,\delta) := \bigcup_{j=1}^{l} i_j(v_{\delta_j}(\mathbb{P}^1)) \subseteq \mathbb{P}^n.$$

A curve $C \subseteq \mathbb{P}^n$ is projectively equivalent to $C(n,\delta)$ if and only if there exist disjoint linear subspaces $E_1,\ldots,E_l \subseteq \mathbb{P}^n$ such that $\dim E_j = \delta_j$, $C \subseteq \bigcup_j E_j$, and

$$C_j := C \cap E_j \subseteq E_j$$

is a rational normal curve for $1 \le j \le l$.

Definition 14. Let $V \subseteq \mathbb{P}^n$ be a variety. Then V is *defined over* k if $I_{\bar{k}}(V) = \bar{k} \otimes_k I_k(V) \subseteq \bar{k}[x_0,\ldots,x_n]$, i.e. if its defining ideal is generated over k.

The following lemma is well known; we prove it here for lack of suitable reference.

Lemma 15. *Let $\varphi : \mathbb{P}^n \to \mathbb{P}^N$ be a regular map defined over k, $V \subseteq \mathbb{P}^n$ be a variety defined over k. Then $\varphi(V) \subseteq \mathbb{P}^N$ is defined over k.*

Proof. We have the following commutative diagram:

$$\begin{array}{ccc} k[x_0,\ldots,x_N] & \xrightarrow{\varphi_k^*} & k[V] \\ \big\downarrow & & \big\downarrow \\ \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\varphi_{\bar{k}}^*} & \bar{k}[V] \end{array}$$

with $\ker \varphi_k^* = I_k(W)$ and $\ker \varphi_{\bar{k}}^* = I_{\bar{k}}(W)$. We have that $\bar{k} \otimes_k k[V] \cong \bar{k}[V]$, as V is defined over k, and tensoring with $\bar{k}$ we get

$$\begin{array}{ccc} \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\bar{k} \otimes_k \varphi_k^*} & \bar{k} \otimes_k k[V] \\ \Big\| & & \Big\| \\ \bar{k}[x_0,\ldots,x_N] & \xrightarrow{\varphi_{\bar{k}}^*} & \bar{k}[V] \end{array}$$

with $\ker \bar{k} \otimes_k \varphi_k^* = \bar{k} \otimes_k I_k(W)$, from where we deduce that $I_{\bar{k}}(W) = \bar{k} \otimes_k I_k(W)$ holds, i.e. $I_{\bar{k}}(W)$ is defined over k. □

The Veronese map $v_n : \mathbb{P}^1 \to \mathbb{P}^n$ is defined over k. Then $v_n(\mathbb{P}^1)$ is defined over k, by the preceding lemma. We have that

$$C(n,\delta) = \bigcup_{j=1}^{l} i_j(v_{\delta_j}(\mathbb{P}^1))$$

is the minimal decomposition of $C(n,\delta)$ in irreducible curves. Thus, $C(n,\delta)$ is also defined over k, and so

$$\operatorname{irr} I_k(C(n,\delta)) = l, \qquad \deg I_k(C(n,\delta)) = |\delta|.$$

Lemma 16. *Let V, $W \subseteq \mathbb{P}^n$ be varieties. Then*

$$I(V) + I(W) = (x_0, \dots, x_n)$$

if and only if V, W lie in disjoint linear subspaces of $\mathbb{P}^n$.

Proof. Given V, $W \subseteq \mathbb{P}^n$ varieties, they lie in disjoint linear subspaces if and only if

$$L(V) \cap L(W) = \emptyset.$$

Let $L_V := I(L(V))$, $L_W := I(L(W))$. By Remark 7 we have that $L_V = (I(V)_1) \subseteq I(V)$ and $L_W = (I(W)_1) \subseteq I(W)$ holds. In particular, L_V, L_W are generated by linear forms, and so

$$L_V + L_W = I(L(V) \cap L(W)).$$

Let be given varieties $V, W \subseteq \mathbb{P}^n$ such that $L(V) \cap L(W) = \emptyset$. Then

$$L_V + L_W = (x_0, \dots, x_n)$$

and so $I(V) + I(W) = (x_0, \dots, x_n)$. Conversely, suppose that $I(V) + I(W) = (x_0, \dots, x_n)$. Then

$$x_0, \dots, x_n \in I(V)_1 + I(W)_1.$$

Thus, $L_V + L_W = (x_0, \dots, x_n)$ and so $L(V) \cap L(W) = \emptyset$. □

Proposition 17. *Let k be a perfect field, and let $I \subseteq k[x_0, \dots, x_n]$ be a homogeneous unmixed radical ideal of dimension one. Then*

$$h_I(m) = \deg\ I\, m + \operatorname{irr} I, \quad m \geq 1$$

if and only if there exists $\delta \in \mathbb{N}^l$ with $l := \operatorname{irr} I$, such that $|\delta| = \deg I$, and a curve $C \subseteq \mathbb{P}^n$ defined over k projectively equivalent to $C(n,\delta)$ such that $I = I_k(C)$.

Proof. Let $C \subseteq \mathbb{P}^n$ be a curve defined over k, projectively equivalent to $C(n,\delta)$ for some $\delta \in \mathbb{N}^l$ and $l = \operatorname{irr} I$. Then $\bar{k} \otimes_k I_k(C) = I_{\bar{k}}(C)$, and so

$$\operatorname{irr} I_k(C) = \operatorname{irr} I(C(n,\delta)) = l, \qquad \deg I_k(C) = \deg I(C(n,\delta)) = |\delta|.$$

We aim at proving that

$$h_{I_k(C)}(m) = |\delta| m + l, \quad m \geq 1$$

We have that $h_{I_k(C)}(m) = h_C(m) = h_{C(n,\delta)}(m)$ and so it suffices to prove that

$$h_{C(n,\delta)}(m) = |\delta| m + l, \quad m \geq 1.$$

We shall proceed by induction on l. Let $C_d := v_d(\mathbb{P}^1)$. We have the inclusion of graded $\bar{k}$-algebras

$$\bar{k}[C_d] = \bar{k}[x_0, \dots, x_d]/I(C_d) \overset{v_d^*}{\hookrightarrow} \bar{k}[x,y], \qquad x_i \mapsto x^i y^{d-i}.$$

We then have that $\bar{k}[C_d] \cong \bigoplus_{j=0}^{\infty} \bar{k}[x,y]_{dj}$ holds, from where $h_{C_d}(m) = dm+1$ for $m \geq 1$, and so the assertion is true for $l = 1$. Let $l > 1$, and let $C(n,\delta) = \bigcup_j C_j$ be the minimal decomposition of $C(n,\delta)$ in irreducible curves. Then $C_1 \cup \cdots \cup C_{l-1}$, and C_l lie in disjoint linear spaces, and so

$$I(C_1 \cup \cdots \cup C_{l-1}) + I(C_l) = (x_0, \dots, x_n)$$

by Lemma 16. We then have that

$$h_C(m) = h_{C_1 \cup \cdots \cup C_{l-1}}(m) + h_{C_l}(m), \quad m \geq 1$$

holds, and from the inductive hypothesis we get

$$h_C(m) = \{(\delta_1 + \cdots + \delta_{l-1})m + (l-1)\} + \{\delta_l m + 1\} = |\delta| m + l, \quad m \geq 1.$$

Now we shall prove the converse. We have that I^e is a radical ideal, and so I^e is the ideal of some curve $C \subseteq \mathbb{P}^n$ defined over k.

We shall proceed by induction on $l := \operatorname{irr} I$. Let $l = 1$, i.e. $C \subseteq \mathbb{P}^n$ irreducible. Then

$$\dim L(C) = h_C(1) - 1 = \deg C$$

and so $C \subseteq L(C)$ is a nondegenerated irreducible curve of minimal degree. We then have that $C \subseteq L(C)$ is a rational normal curve [17, Proposition 18.9].

Let $l > 1$, and suppose that the assertion is proved for $l(I) \leq l-1$ and K an arbitrary field. In particular, it is proved for $\bar{k}$, the algebraic closure of k. Let $C = C_1 \cup \cdots \cup C_l$ be the minimal decomposition of C in irreducible curves. Then

$$h_C(m) = h_{C_1 \cup \cdots \cup C_{l-1}}(m) + h_{C_l}(m) - h_{I(C_1 \cup \cdots \cup C_{l-1}) + I(C_l)}(m), \quad m \geq 1$$

We deduce from Theorem 11 that

$$h_{C_l}(m) = \delta_l m + 1,$$
$$h_{C_1 \cup \cdots \cup C_{l-1}}(m) = (\delta_1 + \cdots + \delta_{l-1})m + (l-1)$$

and so $C_l \subseteq L(C_l)$ is a rational normal curve, and by the inductive hypothesis $C_1 \cup \cdots \cup C_{l-1}$ is projectively equivalent to $C(n, (\deg C_1, \dots, \deg C_{l-1}))$. Thus,

$$h_C(m) = |\delta| m + l - h_{I(C_1 \cup \cdots \cup C_{l-1}) + I(C_l)}(m), \quad m \geq 1$$

from where

$$I(C_1 \cup \cdots \cup C_{l-1}) + I(C_l) = (x_0, \dots, x_n)$$

Then $C_1 \cup \cdots \cup C_{l-1}$, and C_l lie in disjoint linear spaces, by Lemma 16, and so C is projectively equivalent to $C(n, (\deg C_1, \dots, \deg C_l))$. □

Now, we shall derive another upper bound for the Hilbert function of an unmixed radical ideal. The following lemma is well known; we prove it here for lack of suitable reference.

Lemma 18. *Let A be an integrally closed domain, K its quotient field, L a finite separable extension of K, B the integral closure of A in L. Let $\eta \in B$ such that $L = K[\eta]$, and let $f \in A[t]$ be its minimal polynomial. Then*

$$f'(\eta) B \subseteq A[\eta]$$

Proof. Let $M \subseteq L$ be an A-module. Then

$$M' := \{x \in L \mid \mathrm{Tr}_K^L(xM) \subseteq A\}$$

is called the *complementary module* (relative to the trace) of M [25, Ch. III, Section 1].

It is straightforward that if $M \subseteq B$ then $M' \supseteq B$. We have that

$$A[\eta]' = \frac{A[\eta]}{f'(\eta)}$$

holds [25, Ch. III, Proposition 2, Corollary], and so $B \subseteq A[\eta]' = A[\eta]/f'(\eta)$. □

In the language of integral dependence theory, the last assertion says that $f'(\eta)$ lies in the conductor of B in $A[\eta]$. □

Theorem 19. *Let k be a perfect field, and let $I \subseteq k[x_0, \dots, x_n]$ be a homogeneous unmixed radical ideal of dimension d, with $d \geq 0$. Then*

$$h_I(m) \leq \binom{m + \deg I + d}{d+1} - \binom{m+d}{d+1}, \quad m \geq 1$$

Proof. We shall consider first the case when $P \subseteq \bar{k}[x_0, \dots, x_n]$ is a homogeneous prime ideal.

The field $\bar{k}$ is algebraically closed, and so it is both infinite and perfect. Let $y_0,\dots,y_d$, $\eta \in \bar{k}[x_0,\dots,x_n]$ be linear forms such that

$$\bar{k}[y_0,\dots,y_d] \hookrightarrow \bar{k}[x_0,\dots,x_n]/P$$

is an integral inclusion of graded $\bar{k}$-algebras, and such that if K, L are the quotient fields of $\bar{k}[y_0,\dots,y_d]$, $\bar{k}[x_0,\dots,x_n]/P$, respectively, then $K \hookrightarrow L$ is separable algebraic and $L = K[\eta]$.

Let $A := \bar{k}[y_0,\dots,y_d]$, $B := \bar{k}[x_0,\dots,x_n]/P$. As a consequence of Krull's Hauptidealsatz we have that

$$A[\eta] \cong A[t]/(F),$$

where $F \in \bar{k}[y_0,\dots,y_d][t]$ is a nonzero homogeneous polynomial. We then have that

$$\dim_{\bar{k}}(A[\eta])_m = h_{(F)}(m) = \binom{m+d+1}{d+1} - \binom{m-\deg F+d+1}{d+1}.$$

We also have that $A[\eta] \hookrightarrow B \hookrightarrow A[\eta]/F'(\eta)$ holds, by Lemma 18, and thus

$$\binom{m+d+1}{d+1} - \binom{m-\deg F+d+1}{d+1} \le$$

$$\le h_p(m) \le \binom{m+\deg F+d}{d+1} - \binom{m+d}{d+1}, \quad m \ge 1.$$

We deduce that $\deg F = \deg P$, and so

$$h_P(m) \le \binom{m+\deg P+d}{d+1} - \binom{m+d}{d+1}, \quad m \ge 1.$$

Now we extend this bound to the case of an unmixed ideal. We have that I^e is and unmixed radical ideal. Let $I^e = \bigcap_P P$ be the primary decomposition of I^e. We have that

$$h_I(m) \le \sum_P \left\{ \binom{m+\deg P+d}{d+1} - \binom{m+d}{d+1} \right\}, \quad m \ge 1$$

Then, we have that

$$h_I(m) \le \sum_P \sum_{i=0}^{\deg P-1} \binom{m+d+i}{d} \le \sum_{i=0}^{\deg I-1} \binom{m+d+i}{d}$$

$$= \binom{m+\deg I+d}{d+1} - \binom{m+d}{d+1}. \qquad \square$$

Remark 20. This inequality is sharp for big values of m, as it is seen by comparing it with the principal term of the Hilbert polynomial of I.

From the expression

$$h_I(m) \leq \binom{m+\deg I+i}{d+1} - \binom{m+d}{d+1} = \sum_{i=0}^{\deg I-1} \binom{m+d+i}{d},$$

we see that it does not improve Chardin's estimate [10]

$$h_I(m) \leq \deg I \binom{m+d}{d} = \sum_{i=0}^{\deg I-1} \binom{m+d}{d}$$

in any case. However, we remark that the proof is simpler and that we can use it in our applications instead of Chardin's estimate obtaining very similar results.

Let k be a perfect field, $I \subseteq k[x_0,\dots,x_n]$ an homogeneous unmixed radical ideal of dimension $d \geq 0$, and let H_I denote its Hilbert–Poincaré series. Then the previous result states that

$$t^{\deg I-1} H_I(t) \leq \frac{1-t^{\deg I}}{(1-t)^{d+2}}$$

in the sense that this inequality holds at each term of the power series.

We derive an upper bound for the Hilbert function of a generic hypersurface section of an unmixed radical ideal, which need not be unmixed nor radical. This result is an application of both our upper and lower bounds for the Hilbert function. The use of our upper bound (Theorem 19) can be replaced by Chardin's estimate [10] but the bound so obtained is essentially the same. In this way we keep our exposition self-contained.

Lemma 21. *Let k be a perfect field, and let $I \subseteq k[x_0,\dots,x_n]$ be a homogeneous unmixed radical ideal of dimension d, with $d \geq 1$. Let $\eta \in k[x_0,\dots,x_n]$ be a linear form which is not a zero-divisor modulo I. Then there exists m_0 such that*

$$h_{(I,\eta)}(m_0) \leq \binom{m_0+d}{d} - \binom{m_0+d-3\deg I}{d}$$

and $3\deg I \leq m_0 \leq 5d \deg I$.

Proof. Let $\delta := \deg I$, $k := 3\delta$, $l := 2\delta$, $m := 5d\delta$. We aim at proving that

$$\sum_{j=0}^{l-1} \left\{ \binom{m-j+d}{d} - \binom{m-j+d-k}{d} \right\} \geq \sum_{j=0}^{l-1} h_{(I,\eta)}(m-j).$$

We have that

$$\sum_{j=0}^{l-1} \left\{ \binom{m+d-j}{d} - \binom{m+d-k-j}{d} \right\} = \left\{ \binom{m+d+1}{d+1} - \binom{m+d+1-l}{d+1} \right\}$$

$$- \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\}$$

holds. We also have that

$$\sum_{j=0}^{l-1} h_{(I,\eta)}(m-j) = h_{(I,\eta^l)}(m) \le \left\{ \binom{m+d+\delta}{d+1} - \binom{m+d}{d+1} \right\}$$

$$- \left\{ \binom{m+d+1-l}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\}$$

holds, by application of Theorems 19 and 4. Then, it suffices to prove that

$$\left\{ \binom{m+d+1-\delta}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\}$$

$$- \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\}$$

$$\ge \left\{ \binom{m+d+\delta}{d+1} - \binom{m+d}{d+1} \right\} - \left\{ \binom{m+d+1}{d+1} - \binom{m+d+1-\delta}{d+1} \right\}.$$

We have that

$$\left\{ \binom{m+d+1-\delta}{d+1} - \binom{m+d+1-\delta-l}{d+1} \right\}$$

$$- \left\{ \binom{m+d+1-k}{d+1} - \binom{m+d+1-k-l}{d+1} \right\}$$

$$= \sum_{i=1}^{l} \left\{ \binom{m+d+1-\delta-i}{d} - \binom{m+d+1-k-i}{d} \right\}$$

$$= \sum_{i=1}^{l} \sum_{j=1}^{k-\delta} \binom{m+d+1-\delta-i-j}{d-1} \ge l(k-\delta) \binom{m+d-1-k-l}{d-1}$$

and

$$\left\{ \binom{m+d+\delta}{d+1} - \binom{m+d}{d+1} \right\} - \left\{ \binom{m+d+1}{d+1} - \binom{m+d+1-\delta}{d+1} \right\}$$

$$= \sum_{i=1}^{\delta} \left\{ \binom{m+d+\delta-i}{d} - \binom{m+d+1-i}{d} \right\}$$

$$= \sum_{i=1}^{\delta} \sum_{j=1}^{\delta} \binom{m+d+\delta-i-j}{d-1} \le \delta^2 \binom{m+d-1+\delta}{d-1}$$

hold, and thus it suffices to prove that

$$4=\frac{l(k-\delta)}{\delta^2}\geq\frac{\binom{m+d-1+\delta}{d-1}}{\binom{m+d-1-k-l}{d-1}}.$$

This is clear when $d=1$, as in this case, the right-hand side of this expression equals 1. When $d\geq 2$ we have that

$$\frac{\binom{m+d-1+\delta}{d-1}}{\binom{m+d-1-k-l}{d-1}}=\prod_{j=1}^{d-1}\frac{m+\delta+j}{m-k-l+j}\leq\left(1+\frac{6/5}{d-1}\right)^{d-1}\leq e^{6/5}$$

and so our claim follows, and we conclude that

$$h_{(I,\eta)}(m_0)\leq\binom{m_0+d}{d}-\binom{m_0+d-3\deg I}{d}$$

for some m_0 such that $5d\delta-2\delta+1\leq m_0\leq 5d\delta$. □

Theorem 22. *Let k be a perfect field, and let $I\subseteq k[x_0,\dots,x_n]$ be an homogeneous unmixed radical ideal of dimension d, with $d\geq 0$. Let $f\in k[x_0,\dots,x_n]$ be a polynomial which is not a zero-divisor modulo I. Then*

$$\begin{aligned}h_{(I,f)}(m)&\leq\deg I, & m&\geq 1,\\ h_{(I,f)}(m)&=0, & m&\geq\deg I+\deg f-1\end{aligned}$$

if $d=0$, and

$$h_{(I,f)}(m)\leq 3\deg f\deg I\binom{m+d-1}{d-1}$$

if $d\geq 1$ and $m\geq 5d\deg I$.

Proof. Let $\delta:=\deg I$, $d_0:=\deg f$. We have that $h_{(I,f)}(m)=h_I(m)-h_I(m-d_0)$. Consider first the case $d=0$. Then $h_I(m)\leq\delta$ for $m\geq 1$ and $h_I(m)=\delta$ for $m\geq\delta-1$ by Lemma 3, and thus

$$h_{(I,f)}(m)=0,\quad m\geq\delta+d_0-1.$$

Now let $d\geq 1$. We have that I^e is an unmixed radical ideal, and so there exists a linear form $\eta\in k[x_0,\dots,x_n]$ which is not a zero-divisor modulo I^e. By Lemma 21

$$h_{(I^e,\eta)}(m_0)\leq\binom{m+d}{d}-\binom{m+d-3\deg I}{d}$$

for some $3\deg I\leq m_0\leq 5d\deg I$.

Let $m \geq 3\delta$. We then have that

$$\binom{m+d}{d}-\binom{m+d-3\deg I}{d}=\sum_{j=1}^{3\delta}\binom{m+d-j}{m-j+1}$$

is the m-binomial expansion of

$$\binom{m+d}{d}-\binom{m+d-3\deg I}{d},$$

and so

$$h_{(I,\eta)}(m) \leq \binom{m+d}{d}-\binom{m+d-3\delta}{d}$$

for $m \geq m_0$ by Macaulay's theorem and Remark 2. We then have that

$$h_{(I,f)}(m)=h_{(I^e,f)}(m)=\sum_{j=0}^{d_0-1} h_{(I^e,\eta)}(m-j) \leq 3d_0\delta\binom{m+d-1}{d-1}$$

for $m \geq 5d\delta$. □

3. Construction of regular sequences

In this section we devote to the construction of regular sequences with polynomials of controlled degrees satisfying different conditions. Throughout this section k will denote an infinite perfect field.

Let be given a homogeneous unmixed radical ideal $I \subseteq k[x_0,\dots,x_n]$ of dimension $d \geq 0$, and a homogeneous polynomial $F \in k[x_0,\dots,x_n]$ which is not a zero-divisor modulo I. We shall show first that there exist homogeneous polynomials of controlled degrees $f_1,\dots,f_{n-d} \in I$ which form a regular sequence which avoids the hypersurface $\{F=0\}$, i.e. such that no associated prime ideal of $(f_1,\dots,f_i)$ lies in $\{F=0\}$ for $1 \leq i \leq n-d$. This result is an application of our bound for the Hilbert function of a generic hypersurface section of an unmixed radical ideal (Theorem 22).

Lemma 23. *Let $I,P \subseteq k[x_0,\dots,x_n]$ be homogeneous ideals, I unmixed radical of dimension d, with $d \geq 0$, P prime of dimension e, with $e \geq d$. Let $F \in k[x_0,\dots,x_n]$ be a homogeneous polynomial which is not a zero-divisor modulo I. Then there exists $g \in (I,F)-P$ such that*

$$\deg g \leq \begin{cases} \deg I + \deg F - 1 & \text{if } d=0,\\ 5d \deg F \deg I & \text{if } d \geq 1.\end{cases}$$

Proof. Let $\delta := \deg I$, $d_0 := \deg F$, $J := (I, F)$. Consider first the case $d = 0$. Then

$$h_J(m) = 0, \quad m \geq \delta + d_0 - 1$$

by Theorem 22, and so there exists $g \in J - P$ with $\deg g \leq \delta + d_0 - 1$.

Now let $d \geq 1$. We have that $P \subseteq k[x_0, \dots, x_n]$ is a homogeneous prime ideal of dimension $e \geq d$, and so

$$h_P(m) \geq \binom{m+e}{e} \geq \binom{m+d}{d}.$$

Let $m_0 := 5 d d_0 \delta$. We then have that

$$h_{(I,f)}(m_0) \leq 3 d_0 \delta \binom{m_0 + d - 1}{d - 1} < \binom{m_0 + d}{d} \leq h_P(m)$$

holds, by Theorem 22, and so there exists $g \in J - P$ such that $\deg g \leq m_0$. $\square$

Theorem 24. *Let $I \subseteq k[x_0, \dots, x_n]$ be an unmixed radical ideal of dimension d, with $d \geq 0$, and let $F \in k[x_0, \dots, x_n]$ be a homogeneous polynomial which is not a zero-divisor modulo I. Then there exist homogeneous polynomials $f_1, \dots, f_{n-d} \in I$ such that $F, f_1, \dots, f_{n-d} \in k[x_0, \dots, x_n]$ is a regular sequence and*

$$\deg f_i \leq \begin{cases} \deg I + \deg F - 1 & \textit{if } d = 0, \\ 5d \deg F \deg I & \textit{if } d \geq 1. \end{cases}$$

Proof. We show first that there exist homogeneous polynomials $g_1, \dots, g_{n-d} \in (I, F)$ such that $F, g_1, \dots, g_{n-d}$ is a regular sequence and

$$\deg g_i \leq \begin{cases} \deg I + \deg F - 1 & \text{if } d = 0, \\ 5d \deg F \deg I & \text{if } d \geq 1. \end{cases}$$

We proceed by induction. By Lemma 23 there exists $g \in (I, F)$, $g \neq 0$ which satisfies the stated bound.

Now let $1 \leq j \leq n - d - 1$, and let $g_1, \dots, g_j \in (I, F)$ be homogeneous polynomials satisfying the stated bound on the degrees and such that $F, g_1, \dots, g_j$ is a regular sequence. Let

$$J_j := (F, g_1, \dots, g_j) \subseteq k[x_0, \dots, x_n]$$

and let P be an associated prime ideal of J_j. The ideal J_j is unmixed, and so $\dim P = n - j - 1 \leq d$. Then there exists $g_P \in (I, F) - P$ which satisfies the stated bound on the degrees by Lemma 23. By eventually multiplying each g_P by a linear form which is not a zero-divisor modulo P we can suppose that

$$\deg g_P = \begin{cases} \deg I + \deg F - 1 & \text{if } d = 0, \\ 5d \deg F \deg I & \text{if } d \geq 1. \end{cases}$$

As the field is infinite, there exists a k-linear combination $g := \sum_P \lambda_P g_P$ such that $g \in (I,F) - P$ for every associated prime ideal of J_j, so that g is a homogeneous polynomial and $F, g_1, \ldots, g_j$, g is a regular sequence of polynomials satisfying the stated bounds on the degrees.

Let $g_i = f_i + F h_i$ with $f_i \in I$ for $1 \leq i \leq n - d$. Then $\deg f_i = \deg g_i$, and $g_i \equiv f_i \bmod (F)$, and so $F, f_1, \ldots, f_{n-d}$ is also a regular sequence for which it holds the announced bounds on the degrees. □

We observe that in the case when $\deg F = 1$, Lemma 23 can be deduced from Lemma 21, and so Theorem 24 does not depend on Macaulay's theorem. It can also be shown in the case when $\deg F \geq 2$ that it does not depend on Macaulay's theorem altogether [32, Theorem 3.40].

Definition 25. Let A be a ring. Then $f_1, \ldots, f_s \in A$ is a weak regular sequence if $\bar{f_i}$ is a nonzero divisor in $A/(f_1, \ldots, f_{i-1})$ for $1 \leq i \leq s$.

This definition differs from the usual definition of regular sequence only in one point, namely in that we allow $\bar{f_s} \in A/(f_1, \ldots, f_{s-1})$ to be a unit.

Let $F, f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials such that $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]_F$ is a weak regular sequence. It is not always the case that $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ is a regular sequence, as some components of high dimension may appear in the hypersurface $\{F = 0\}$. Consider the following example.

Example 26. Let $d \geq 1$, and let

$$f_1 := x_1, \qquad f_2 := x_1^{d+1} + x_2 x_0^d, \qquad f_3 := x_1^{d+1} + x_3 x_0^d \in k[x_0, x_1, x_2, x_3].$$

Then $f_2 \equiv x_2 x_0^d$, $f_3 \equiv x_3 x_0^d \bmod (f_1)$, and so they form a regular sequence in $k[x_0, x_1, x_2, x_3]_F$. We have that

$$\{(x_0 : \ldots : x_4) \in \mathbb{P}^3 \mid x_0 = 0,\ x_1 = 0\} \subseteq V(f_1, f_2, f_3) \subseteq \mathbb{P}^3$$

and so f_1, f_2, f_3 cannot be a regular sequence in $k[x_0, \ldots, x_3]$.

We shall show that the weak regular sequence $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]_F$ can, in fact, be replaced by polynomials $p_1, \ldots, p_s \in k[x_0, \ldots, x_n]$ of controlled degrees such that $(f_1, \ldots, f_i) = (p_1, \ldots, p_i) \subseteq k[x_0, \ldots, x_n]_F$ for $1 \leq i \leq s$ and such that $p_1, \ldots, p_s \in k[x_0, \ldots, x_n]$ is a regular sequence. Our proof follows Dubé's arguments, who gave an incomplete proof of a similar statement [11, Lemma 4.1] under an unproved assumption on the Hilbert function of a certain class of ideals [11, Section 2.1].

Proposition 27. *Let $s \le n+1$, and let $F, f_1, \dots, f_s \in k[x_0, \dots, x_n]$ be homogeneous polynomials, with $\deg F \ge 1$, such that $f_1, \dots, f_s \in k[x_0, \dots, x_n]_F$ is a weak regular sequence and such that $(f_1, \dots, f_i) \in k[x_0, \dots, x_n]_F$ is a radical ideal for $1 \le i \le s-1$. Let $I_i := (f_1, \dots, f_i) \subseteq k[x_0, \dots, x_n]_F$ and let $I_i^c := I_i \cap k[x_0, \dots, x_n]$ for $1 \le i \le s$. Then there exist homogeneous polynomials $p_1, \dots, p_s \in k[x_0, \dots, x_n]$ which satisfy the following conditions:*

(i) $p_1 = F^{c_1} f_1$, $p_2 = F^{c_2} f_2$, $p_i \equiv F^{c_i} f_i \bmod I_{i-1}^c$ *for some* $c_i \in \mathbb{Z}$, *for* $i = 3, \dots, s$.

(ii) $p_1, \dots, p_s \in k[x_0, \dots, x_n]$ *is a regular sequence.*

(iii) $\deg p_i \le \max\{\deg f_i, 5(n+1-i) \deg F \deg I_{i-1}^c\}$ *if* $i \le n$, *and* $\deg p_{n+1} \le \max\{\deg f_{n+1}, \deg I_n^c + \deg F - 1\}$.

Proof. We shall proceed by induction. Let $f_1 = F^{e_1} a_1$, $f_2 = F^{e_2} a_2$, with $F \nmid a_1$, $F \nmid a_2$. Then f_1, f_2 is a weak regular sequence in $k[x_0, \dots, x_n]_F$ if and only if $a_1 \ne 0$ and $(a_1 : a_2) = 1$, and thus

$$p_1 := F^{-e_1} f_1, \qquad p_2 := F^{-e_2} f_2$$

is a regular sequence in $k[x_0, \dots, x_n]$. Now let $i \ge 3$, and suppose that $p_1, \dots, p_{i-1}$ are already constructed with the stated properties. Let

$$L_{i-1} := (p_1, \dots, p_{i-1}) \subseteq k[x_0, \dots, x_n]$$

and let $L_{i-1} = \bigcap_{j=1}^t Q_j$ be an irredundant primary decomposition of L_{i-1} such that

$$F \notin \sqrt{Q_j} \quad \text{for } 1 \le j \le r,$$
$$F \in \sqrt{Q_j} \quad \text{for } r+1 \le j \le t.$$

Let (L_{i-1}) denote the extension of L_{i-1} to the ring $k[x_0, \dots, x_n]_F$. Then $(L_{i-1}) = I_{i-1}$ and so

$$I_{i-1}^c = \bigcap_{j=1}^r Q_j$$

is a primary decomposition of I_{i-1}^c. We have $I_{i-1}^c = (1)$ or $\dim I_{i-1}^c = n - i + 1$. In any case, there exist $b_1, \dots, b_{i-1} \in I_{i-1}^c$ homogeneous polynomials such that $F, b_1, \dots, b_{i-1}$ is a regular sequence and such that

$$\deg b_j = \max\{\deg f_i, 5\ (n+1-i) \deg F \deg I_{i-1}^c\}, \quad 1 \le j \le i-1$$

if $i \le n$ and

$$\deg b_j = \max\{\deg f_{n+1}, \deg I_n^c + \deg F - 1\}, \quad 1 \le j \le n$$

if $i=n+1$, by application of Theorem 24 and by eventually multiplying each b_j by an appropriate linear form. Let

$$u_i := \sum_{j=1}^{i-1} \lambda_j b_j \in I_{i-1}^c$$

be a k-linear combination of the b_j. We shall prove that a generic choice of $\lambda_1, \dots, \lambda_{i-1}$ makes $p_i := F^{c_i} f_i + u_i$ with $c_i := \deg u_i - \deg f_i \geq 0$ satisfy the stated conditions. We have that

$$\deg p_i = \max\{\deg f_i, 5(n+1-i)\deg F \deg I_{i-1}^c\} \quad \text{if } i \leq n$$

and

$$\deg p_{n+1} = \max\{\deg f_{n+1}, \deg I_n^c + \deg F - 1\}.$$

hold. We aim at proving that p_i does not belong to any of the associated prime ideals of L_{i-1}.

Consider first $1 \leq j \leq r$. Then $f_i \notin \sqrt{Q_j}$ as f_i is a nonzero divisor modulo I_{i-1}. We have that $u_i \in I_{i-1}^c$, and so $p_i = F^{c_i} f_i + u_i \notin \sqrt{Q_j}$.

Now let $r+1 \leq j \leq t$. Then $\dim Q_j = n - i + 1$ as L_{i-1} is an unmixed ideal of dimension $n-i+1$, and we have also that $F \in \sqrt{Q}_j$. Thus there exists $1 \leq l \leq i-1$ such that $b_l \notin \sqrt{Q}_j$, and so $p_i \notin \sqrt{Q}_j$ for a generic choice of the $\lambda_1, \dots, \lambda_{i-1}$. □

As a corollary, we deduce that if we have a weak regular sequence $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ of affine polynomials, we can replace it by another weak regular sequence $p_1, \dots, p_s \in k[x_1, \dots, x_n]$ with polynomials of controlled degrees such that $(f_1, \dots, f_i) = (p_1, \dots, p_i)$ for $1 \leq i \leq s$ and such that the homogenizated polynomials $\tilde{p}_1, \dots, \tilde{p}_s \in k[x_0, \dots, x_n]$ form a regular sequence.

Corollary 28. *Let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be a weak regular sequence of affine polynomials such that $(f_1, \dots, f_i) \subseteq k[x_1, \dots, x_n]$ is a radical ideal for $1 \leq i \leq s-1$. Let $I_i := (f_1, \dots, f_i) \subseteq k[x_1, \dots, x_n]$ for $1 \leq i \leq s$. Then there exist polynomials $p_1, \dots, p_s \in k[x_1, \dots, x_n]$ which satisfy the following conditions:*

(i) $p_1 = f_1$, $p_2 = f_2$, $p_i \equiv f_i \bmod I_{i-1}$ *for* $i = 3, \dots, s$.

(ii) $\tilde{p}_1, \dots, \tilde{p}_s \in k[x_0, \dots, x_n]$ *is a regular sequence.*

(iii) $\deg p_i \leq \max\{\deg f_i, 5(n+1-i)\deg \tilde{I}_{i-1}\}$ *if* $i \leq n$ *and* $\deg p_{n+1} = \max\{\deg f_{n+1}, \deg \tilde{I}_n\}$.

Proof. We have that $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ is a weak regular sequence, and so $\tilde{f}_1, \dots, \tilde{f}_s \in k[x_0, \dots, x_n]_{x_0}$ is also a weak regular sequence. We have also that $(\tilde{f}_1, \dots, \tilde{f}_i) \subseteq k[x_0, \dots, x_n]_{x_0}$ is a radical ideal for $1 \leq i \leq s-1$. Let $r_1, \dots, r_s \in k[x_0, \dots, x_n]$ be the homogeneous polynomials we obtain by applying Proposition 27 to $\tilde{f}_1, \ldots, \tilde{f}_s$. Let

$$p_i := r_i^a, \quad 1 \le i \le s$$

Thus, $\deg p_i \le \deg r_i$, and $x_0^{e_i} \tilde{p}_i = r_i$ for some $e_i \ge 0$. Then $\tilde{p}_1, \ldots, \tilde{p}_s \in k[x_0, \ldots, x_n]$ is a regular sequence, and so $p_1, \ldots, p_s$ satisfy the stated conditions. □

Our bounds for the degrees in the preceding propositions depend on the degree of certain ideals associated to $f_1, \ldots, f_s$. The following is a Bézout-type lemma which shows that these bounds can also be expressed in terms of the degrees of the polynomials $f_1, \ldots, f_s$.

Lemma 29. *Let $s \le n$, and let $F, f_1, \ldots, f_s \in k[x_0, \ldots, x_n]$ be homogeneous polynomials, with $\deg F \ge 1$, such that $f_1, \ldots, f_s \in k[x_0, \ldots, x_n]_F$ is a weak regular sequence. Let $I := (f_1, \ldots, f_s) \subseteq k[x_0, \ldots, x_n]_F$, and let $I^c := I \cap k[x_0, \ldots, x_n]$. Then*

$$\deg I^c \le \prod_{i=1}^{s} \deg f_i.$$

Proof. If $I^c = (1)$ there is nothing to prove. Otherwise we have that $\dim I^c \ge 0$.

Let $I_i := (f_1, \ldots, f_i) \subseteq k[x_0, \ldots, x_n]_F$, $J_i := (I_{i-1}^c, f_i) \subseteq k[x_0, \ldots, x_n]$ for $1 \le i \le s$. Then $\dim I_i^c = \dim J_i = n - i$ and $J_i \subseteq I_i^c$, and so $\deg I_i^c \le \deg J_i$.

We shall proceed by induction on i. For $i = 1$ we have that $\deg I_1^c \le \deg J_1 = \deg f_1$ holds.

Let $i \ge 2$. Then f_i is a nonzero divisor modulo I_{i-1}^c and so

$$\deg I_i^c \le \deg J_i = \deg f_i \, \deg I_{i-1}^c \le \prod_{j=1}^{s} \deg f_j$$

by the inductive hypothesis. □

4. The effective Nullstellensatz and the representation problem in complete intersections

In this section we consider the problem of bounding the degrees of the polynomials in the Nullstellensatz and in the representation problem in complete intersections.

As a consequence of the results of the previous section we obtain bounds for these two problems which depend not only on the number of variables and on the degrees of the input polynomials but also on an additional parameter called the geometric degree of the system of equations. The bounds so obtained are more intrinsic and refined than the usual estimates, and we show that they are sharper in some special cases.

Our arguments at this point are essentially the same of Dubé [11].

The bound we obtain for the effective Nulltellensatz is similar to that announced in [15, Theorem 19] and proved in [14] by algorithmic methods and to that obtained in [24] by duality methods.

Let $g, f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be polynomials such that $g \in (f_1, \dots, f_s)$. Let $D \geq 0$. Then there exist polynomials $a_1, \dots, a_s \in k[x_1, \dots, x_n]$ such that

$$g = a_1 f_1 + \cdots + a_s f_s$$

with $\deg a_i f_i \leq \deg g + D$ for $i = 1, \dots, s$ if and only if

$$x_0^D \tilde{g} \in (\tilde{f}_1, \dots, \tilde{f}_s) \subseteq k[x_0, \dots, x_n]$$

and so in this situation we aim at bounding D such that $x_0^D \tilde{g} \in (\tilde{f}_1, \dots, \tilde{f}_s)$.

We shall suppose $n, s \geq 2$, as the cases $n = 1$ or $s = 1$ are well known. Also we shall suppose, without loss of generality, that k is algebraically closed, and in particular infinite and perfect.

Let $h_1, \dots, h_s \in k[x_1, \dots, x_n]$ be a weak regular sequence such that $(h_1, \dots, h_i)$ is radical for $1 \leq i \leq s-1$. In particular, we have that $s \leq n+1$. We fix the following notation:

$$I_i := (h_1, \dots, h_i) \subseteq k[x_1, \dots, x_n],$$

$$J_i := (\tilde{I}_{i-1}, \tilde{h}_i) \subseteq k[x_0, \dots, x_n],$$

$$H_i := (\tilde{h}_1, \dots, \tilde{h}_i) \subseteq k[x_0, \dots, x_n],$$

for $1 \leq i \leq s$. Let $J_i = \bigcap_P Q_P$ be a primary decomposition of J_i, and let

$$J_i^* = \bigcap_{P : \dim P = \dim I} Q_P$$

be the intersection of the primary components of maximal dimension of J_i, which is well defined as the isolated components of J_i are unique.We have that $J_i \subseteq J_i^* \subseteq \tilde{I}_i$.

Let

$$\gamma_1 := 0,$$

$$\gamma_i := \deg h_i \deg \tilde{I}_{i-1} - \deg \tilde{I}_i, \quad 2 \leq i \leq n,$$

$$\gamma_{n+1} := \deg h_{n+1} + \deg \tilde{I}_n - 1,$$

Lemma 30. *Let $g \in \tilde{I}_i$ for some $1 \leq i \leq s$. Then we have that $x_0^{\gamma_i} g \in J_i^*$ holds.*

Proof. The case $1 \leq i \leq n$ is [11, Lemma 5.5].

We consider the case $i = n+1$. We have that $\tilde{I}_n \subseteq k[x_0, \dots, x_n]$ is an unmixed radical ideal of dimension zero and we have that h_{n+1} is not a zero-divisor modulo I_n, and so by Theorem 22, $h_{J_{n+1}}(m)=0$ for $m \geq \deg \tilde{I}_n + \deg h_{n+1} - 1$. Then $x_0^{\gamma_{n+1}} \in J_{n+1} \subseteq J_{n+1}^*$ and thus $x_0^{\gamma_{n+1}} g \in J_{n+1}^*$. $\square$

Then we apply Corollary 28 to the sequence $h_1, \ldots, h_s$, to obtain polynomials $p_1, \ldots, p_s \in k[x_1, \ldots, x_n]$ such that

(i) $p_1 = h_1$, $p_2 = h_2$, and $p_i = h_i + u_i$ for some $u_i \in I_{i-1}$, for $3 \leq i \leq s$.

(ii) $\tilde{p}_1, \ldots, \tilde{p}_s \in k[x_0, \ldots, x_n]$ is a regular sequence.

(iii) $\deg p_i \leq \max\{\deg h_i, 5(n+1-i) \deg \tilde{I}_{i-1}\}$ for $1 \leq i \leq n$ and $\deg p_{n+1} \leq \max\{\deg h_{n+1}, \deg \tilde{I}_n\}$.

Then $\tilde{p}_i = x_0^{c_i} \tilde{h}_i + \tilde{u}_i$, with $c_1 = 0$ $c_2 = 0$ and $c_i = \max\{0, 5(n+1-i) \deg \tilde{I}_{i-1} - \deg h_i\}$ for $3 \leq i \leq n$, and $c_{n+1} = \max\{0, \deg \tilde{I}_n - \deg h_{n+1}\}$. Let

$$D_i := \sum_{j=2}^{i} (i+1-j)\gamma_j + \sum_{j=3}^{i-1} (i-j) c_j$$

for $1 \leq i \leq s$.

Lemma 31. *Let $g \in \tilde{I}_i$ for some $1 \leq i \leq s$. Then we have that $x_0^{D_i} g \in H_i$ holds.*

Proof. This proposition follows from the proof of [11, Lemma 6.1] and [11, Lemma 6.2], applying Lemma 30 for the case $i = n+1$. $\square$

Now the task consists in bounding D_s. Our bound will depend not only on the number of variables and on the degrees of the polynomials $h_1, \ldots, h_s$, but also on the degrees of some homogeneous ideals associated to them.

Lemma 32. *Let $d := \max_{1 \leq i \leq s} \deg h_i$ and $\delta_i := \deg \tilde{I}_i$ for $1 \leq i \leq s$. We then have that*

$$D_s \leq \min\{s,n\}^2 (d + 3n) \max_{1 \leq i \leq \min\{s,n\}-1} \delta_i$$

holds.

Proof. Let $d_i := \deg h_i$ for $1 \leq i \leq s$. We have that

$$\begin{aligned}\sum_{j=3}^{s-1} (s-j) c_j &= \sum_{j=3}^{s-1} (s-j) \max\{0, 5(n+1-j)\delta_{j-1} - d_j\} \\ &\leq 5(n-2) \left(\sum_{j=3}^{s-1} (s-j) \right) \max_{1 \leq i \leq s-2} \delta_i \\ &\leq 3(n-2)(s-2)^2 \max_{1 \leq i \leq s-2} \delta_i.\end{aligned}$$

holds. Let $s \leq n$. We then have

$$\sum_{j=2}^{s} (s+1-j)\gamma_j = \sum_{j=2}^{s} (s+1-j)(d_j\delta_{j-1} - \delta_j)$$

$$\leq \sum_{j=1}^{s-1} jd \max_{1 \leq i \leq s-1} \delta_i \leq s^2 d \max_{1 \leq i \leq s-1} \delta_i.$$

Thus,

$$D_s \leq s^2 d \max_{1 \leq i \leq s-1} \delta_i + 3(n-2)(s-2)^2 \max_{1 \leq i \leq s-2} \delta_i$$

$$\leq s^2 (d+3n) \max_{1 \leq i \leq s-1} \delta_i.$$

Also, we have that

$$\sum_{j=2}^{n+1} (n+2-j)\gamma_j = \sum_{j=2}^{n} (n+2-j)(d_j\delta_{j-1} - \delta_j) + d_{n+1} + \delta_n - 1$$

$$\leq \sum_{j=1}^{n} jd \max_{1 \leq i \leq n-1} \delta_i \leq n^2 d \max_{1 \leq i \leq n-1} \delta_i$$

holds, and, thus,

$$D_{n+1} \leq n^2 d \max_{1 \leq i \leq n-1} \delta_i + 3(n-2)(n-1)^2 \max_{1 \leq i \leq n-1} \delta_i$$

$$\leq n^2(d+3n) \max_{1 \leq i \leq n-1} \delta_i. \qquad \square$$

Let k be an arbitrary field, and let be given $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ polynomials which define a proper ideal $(f_1,\dots,f_s) \subseteq k[x_1,\dots,x_n]$ of dimension $n-s$ or $1 \in (f_1,\dots,f_s)$. Then there exist $h_1,\dots,h_s$ $\bar{k}$-linear combinations of the polynomials $\{f_i, x_j f_i \mid 1 \leq i \leq s, 1 \leq j \leq n\}$, and an integer $t \leq s$ such that

(i) $(h_1,\dots,h_t) = (f_1,\dots,f_s)$.

(ii) $h_1,\dots,h_t$ is a weak regular sequence.

(iii) $(h_1,\dots,h_i)$ is a radical ideal for $1 \leq i \leq t-1$.

In the case when k is a zero characteristic field, we can take $h_1,\dots,h_t$ as $\bar{k}$-linear combinations of $f_1,\dots,f_s$. In fact, in both cases a generic linear combination will satisfy the stated conditions. This result is a consequence of Bertini's theorem [21, Corollary 6.7] (see, for instance [30, Section 5.2; 23, Proposition 37]), and allows us to reduce from the general situation to the previously considered one.

Let $d := \max_{1 \le i \le s} \deg f_i$, and suppose that $\deg f_i \ge \deg f_{i+1}$ for $1 \le i \le s-1$. Then in the case when k is a zero characteristic field we can take $h_1, \dots, h_t$ such that

$$\deg h_i \le \deg f_i, \quad 1 \le i \le t$$

and $\deg h_i \le d+1$ in the case when $\mathrm{char}(k) = p > 0$.

Definition 33. Let k be a zero characteristic field and let $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ be polynomials which define a proper ideal $(f_1, \dots, f_s) \subseteq k[x_1, \dots, x_n]$ of dimension $n - s$ or such that $1 \in (f_1, \dots, f_s)$. For $\lambda = (\lambda_{ij})_{ij} \in \bar{k}^{s \times s}$ and $1 \le i \le s$ let

$$g_i(\lambda) := \sum_j \lambda_{ij} f_j \in \bar{k}[x_1, \dots, x_n]$$

be $\bar{k}$-linear combinations of $f_1, \dots, f_s$. Consider the set of matrices $\Gamma \subseteq \bar{k}^{s \times s}$ such that for $\lambda \in \Gamma$ there exists $t = t(\lambda) \le s$ such that $(g_1, \dots, g_t) = (f_1, \dots, f_s)$, $g_1, \dots, g_t$ is a weak regular sequence and $(g_1, \dots, g_i) \subseteq \bar{k}[x_0, \dots, x_n]$ is a radical ideal for $1 \le i \le t-1$. Then $\Gamma \ne \emptyset$, and in fact Γ contains a nonempty open set $U \subseteq \bar{k}^{s \times s}$. Let $V_i(\lambda) := V(g_1, \dots, g_i) \subseteq \mathbb{A}^n$ be the affine variety defined by $g_1, \dots, g_i$ for $1 \le i \le s$, and define

$$\delta(\lambda) = \max_{1 \le i \le \min\{t(\lambda), n\} - 1} \deg V_i(\lambda).$$

Then the *geometric degree of the system of equations* $f_1, \dots, f_s$ is defined as

$$\delta(f_1, \dots, f_s) := \min_{\lambda \in \Gamma} \delta(\lambda)$$

In the case when $\mathrm{char}(k) = p > 0$ we define the degree of the system of equations $f_1, \dots, f_s$ in an analogous way by considering $\bar{k}$-linear combinations of the polynomials $f_1, \dots, f_s, x_1 f_1, \dots, x_n f_s$.

This definition extends [24, Definition 1] to the case of a complete intersection ideal. It is analogous to the definition of degree of a system of equations of [15], though this degree is not defined as a minimum over all the possible choices of $\lambda \in \Gamma$ but by a generic choice.

Remark 34. We see from the definition that the degree of a system of equations $f_1, \dots, f_s$ does not depend on invertible linear combinations, i.e. if $\mu = (\mu_{ij})_{ij} \in GL_s(k)$ and

$$g_i := \sum_j \mu_{ij} f_j$$

for $1 \le i \le s$, then $\delta(f_1, \dots, f_s) = \delta(g_1, \dots, g_s)$, and so this parameter is in some sense an invariant of the system.

The following lemma shows that $\delta(f_1,\dots,f_s)$ can be bounded in terms of the degrees of the polynomials $f_1,\dots,f_s$.

Lemma 35. *Let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials which define a proper ideal $(f_1,\dots,f_s) \subseteq k[x_1,\dots,x_n]$ of dimension $n-s$, or $1 \in (f_1,\dots,f_s)$. Let $d_i := \deg f_i$ and $d := \max_{1\le i\le s} d_i$, and suppose that $d_i \ge d_{i+2}$ for $1 \le i \le s-2$. Then*

$$\delta(f_1,\dots,f_s) \le \prod_{i=1}^{\min\{s,n\}-1} d_i$$

in the case when k is a zero characteristic field, and

$$\delta(f_1,\dots,f_s) \le (d+1)^{\min\{s,n\}-1}$$

in the case when $char(k) = p > 0$.

Proof. This follows at once from Lemma 29. □

We have the following bounds for the representation problem in complete intersections and for the effective Nullstellensatz in terms of this parameter.

Theorem 36 (Representation problem in complete intersections). *Let $s \le n$, and let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials which define a proper ideal $(f_1,\dots,f_s) \subseteq k[x_1,\dots,x_n]$ of dimension $n-s$. Let $d := \max_{1\le i\le s} \deg f_i$, and let δ be the geometric degree of the system of equations $f_1,\dots,f_s$. Let $g \in (f_1,\dots,f_s)$. Then there exist polynomials $a_1,\dots,a_s \in k[x_1,\dots,x_n]$ such that*

$$g = a_1 f_1 + \cdots + a_s f_s$$

with $\deg a_i f_i \le \deg g + s^2(d+3n)\delta$ for $i = 1,\dots,s$.

Proof. This follows from Lemmas 31 and 32. □

Theorem 37 (Effective Nullstellensatz). *Let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials such that $1 \in (f_1,\dots,f_s)$. Let $d := \max_{1\le i\le s} \deg f_i$, and let δ be the geometric degree of the system of equations $f_1,\dots,f_s$. Then there exist polynomials $a_1,\dots,a_s \in k[x_1,\dots,x_n]$ such that*

$$1 = a_1 f_1 + \cdots + a_s f_s$$

with $\deg a_i f_i \le \min\{n,s\}^2 (d+3n)\delta$ for $i = 1,\dots,s$.

Proof. This follows from Lemmas 31 and 32. □

We can essentially recover from Theorems 36 and 37 the usual bounds for the representation problem in complete intersections and the effective Nullstellensatz. We have for instance:

Corollary 38. *Let k be a zero characteristic field and let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ be polynomials such that $1 \in (f_1,\dots,f_s)$. Let $d_i = \deg f_i$ and $d := \max_{1\le i\le s} d_i$, and suppose that $d_i \ge d_{i+2}$ for $1 \le i \le s$. Then there exist polynomials $a_1,\dots,a_s \in k[x_1,\dots,x_n]$ such that*

$$1 = a_1 f_1 + \cdots + a_s f_s$$

with $\deg a_i f_i \le \min\{n,s\}^2 (d+3n) \prod_{j=1}^{\min\{n,s\}-1} d_j$ *for* $i = 1,\dots,s$.

We remark that our bounds for these two problems are much sharper than this estimate in some particular cases. Consider, for instance, the following example.

Example 39. Let k be a zero characteristic field and let $h_1,\dots,h_s \in k[x_1,\dots,x_n]$ be a weak regular sequence of polynomials such that $1 \in (h_1,\dots,h_s)$. Let $d := \max_{1\le i\le s} \deg h_i$, and let $f_1,\dots,f_s \in k[x_1,\dots,x_n]$ such that

$$f_i = h_i + u_i$$

with $u_i \in (h_1,\dots,h_{i-1})$ for $1 \le i \le s$. Then

$$\delta := \delta(f_1,\dots,f_s) = \delta(h_1,\dots,h_s) \le d^{\min\{n,s\}-1}$$

Let $D := \max_{1\le i\le s} \deg f_i$. By Theorem 37 there exist polynomials $a_1,\dots,a_s \in k[x_1,\dots,x_n]$ such that

$$1 = a_1 f_1 + \cdots, a_s f_s$$

with $\deg a_i f_i \le \min\{n,s\}^2\,(D+3n) d^{\min\{n,s\}-1}$ for $i = 1,\dots,s$. This estimate is sharper for big values of D than the bound

$$\deg a_i f_i \le D^{\min\{n,s\}}, \quad i = 1,\dots,s$$

for $D \ge 3$, which results from application of the bound of [22].

Acknowledgements

I am specially grateful to P. Solernó for many discussions and suggestions which substantially improved the paper. I also want to acknowledge J. Heintz for many helpful suggestions and encouragement, T. Krick for her assistance during the redaction of the paper, L.M. Pardo and G. Valla for their comments on both the contents and the presentation of the paper, P. Philippon for pointing me out an error in a previous version of this paper, and M. Almeida, who turned my attention to Dubé's work on the effective Nullstellensatz.

References

[1] M. Almeida, Función de Hilbert de álgebras graduadas y Nullstellensatz afín efectivo, Tesis de Licenciatura, Univ. Buenos Aires, 1995.

[2] F. Amoroso, On a conjecture of C. Berenstein and A. Yger, in: L. González-Vega and T. Recio, eds., Algorithms in Algebraic Geometry and Applications, Progress in Math., Vol. 143 (Birkhäuser, Basel, 1996) 17–28.

[3] C. Berenstein and D. Struppa, Recent improvements in the complexity of the effective Nullstellensatz, Linear Algebra Appl. 157 (1991) 203–215.

[4] C. Berenstein and A. Yger, Bounds for the degrees in the division problem, Mich. Math. J. 37 (1990) 25–43.

[5] D. Bertrand, Lemmes des zéros et nombres trascendants, Sém. Bourbaki 652, Astérisque 145–146, 21–44, Soc. Math. France, 1987.

[6] A. Bigatti, A. Geramita and J. Migliore, Geometric consequences of extremal behavior in a theorem of Macaulay, Trans. Amer. Math. Soc. 346 (1994) 203–235.

[7] D. Brownawell, Bounds for the degrees in the Nullstellensatz, Ann. Math. 126 (1987) 577–591.

[8] L. Caniglia, A. Galligo and J. Heintz, Some new effectivity bounds in computational geometry, T. Mora, ed., Proc. 6th Int. Conf. AAECC, Lect. Notes in Comput. Sci., Vol. 357 (Springer, Berlin, 1989) 131–151.

[9] L. Caniglia, A. Galligo and J. Heintz, Equations for the projective closure and effective Nullstellensatz, Discrete Appl. Math. 33 (1991) 11–23.

[10] M. Chardin, Une majoration pour la fonction de Hilbert et ses conséquences pour l'interpolation algébrique, Bull. Soc. Math. France 117 (1989) 305–318.

[11] T. Dubé, A combinatorial proof of the effective Nullestellensatz, J. Symbolic Comp. 15 (1993) 277–296.

[12] N. Fitchas and A. Galligo, Nullstellensatz effectif et conjecture de Sèrre (théorème de Quillen–Suslin) pour le Calcul Formel, Math. Nachr. 149 (1990) 231–253.

[13] W. Fulton, Intersection theory, Erg. Math.; 3. Folge., 2. Bd. (Springer, Berlin, 1984).

[14] M. Giusti, J. Heintz, K. Hägele, J. Montaña, J. Morais and L. Pardo, Lower bounds for diophantine approximation, J. Pure Appl. Algebra 117&118 (1997) 277–317, this volume.

[15] M. Giusti, J. Heintz, J. Morais, J. Morgenstern and L. Pardo, Straight-line programs in geometric elimination theory, to appear in: J. Pure Appl. Algebra.

[16] M. Green, Restrictions of linear series to hyperplanes, and some results of Macaulay and Gotzmann, in: E. Ballico and C. Ciliberto, eds., Algebraic Curves and Projective Geometry, Proc. Trento, 1988, Lect. Notes in Math., Vol. 1389 (Springer, Berlin, 1989) 76–86.

[17] J. Harris, Algebraic Geometry: a First Course, Graduate Texts in Math., Vol. 133 (Springer, Berlin, 1992).

[18] R. Hartshorne, Algebraic Geometry, Graduate Texts in Math., Vol. 52 (Springer, Berlin, 1977).

[19] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (1983) 239–277.

[20] J. Heintz and M. Sieveking, Lower bounds for polynomials with algebraic coefficients. Theoret. Comput. Sci. 11 (1980) 321–330.

[21] J.-P. Jouanolou, Théorèmes de Bertini et applications, Progress in Math., Vol. 42 (Birkhäuser, Basel, 1983).

[22] J. Kollár, Sharp effective Nullstellensatz, J. Amer. Math. Soc. 1 (1988) 963–975.

[23] T. Krick and L.M. Pardo, A computational method for diophantine approximation. in: L. González-Vega and T. Recio, eds., Algorithms in Algebraic Geometry and Applications, Progress in Math., Vol. 143 (Birkhäuser, Basel, 1996) 193–254.

[24] T. Krick, J. Sabia and P. Solernó, On intrinsic bounds in the Nullstellensatz, to appear in: AAECC J.

[25] S. Lang, Algebraic Number Theory (Addison-Wesley, Reading, MA, 1970).

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

[27] H. Matsumura, Commutative Ring Theory (Cambridge Univ. Press, Cambridge, 1986).

[28] Y. Nesterenko, Estimates for the characteristic function of a prime ideal, Math. URSS Sbornik 51 (1985) 9–32.

[29] P. Philippon, Dénominateurs dans le théorème des zeros de Hilbert, Acta Arith. 58 (1990) 1–25.
[30] J. Sabia and P. Solernó, Bounds for traces in complete intersections and degrees in the Nullstellensatz, AAECC J. 6 (1995) 353–376.
[31] B. Shiffman, Degree bounds for the division problem in polynomial ideals, Mich. Math. J. 36 (1989) 163–171.
[32] M. Sombra, Bounds for the Hilbert function of polynomial ideals, Impresiones Previas 91, Univ. Buenos Aires, 1996.
[33] B. Teissier, Résultats récents d'algèbre commutative effective, Sém. Bourbaki 718, Astérisque 189–190, 107–131, Soc. Math. France, 1991.
[34] W. Vogel, Lectures on Results on Bézout's Theorem, Tata Lecture Notes, Vol. 74 (Springer, Berlin, 1984).
[35] O. Zariski and P. Samuel, Commutative Algebra (Van Nostrand, New York, 1958).