AAECC 8, 125–134 (1997)

AAECC
Applicable Algebra in Engineering, Communication and Computing

On Intrinsic Bounds in the Nullstellensatz

T. Krick[1], **J. Sabia**[1], **P. Solernó**[2]

[1] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, -1428- Buenos Aires, Argentina (e-mail: krick@dm.uba.ar/jsabia@dm.uba.ar)
[2] Departamento de Economía y Matemática, Universidad de San Andrés, Vito Dumas 284, -1644- Victoria, Buenos Aires, Argentina (e-mail: psolerno@udesa.edu.ar)

Received November 24, 1995, revised version January 19, 1996

Abstract. Let k be a field and $f_1, \ldots, f_s$ be non constant polynomials in $k[X_1, \ldots, X_n]$ which generate the trivial ideal. In this paper we define an invariant associated to the sequence $f_1, \ldots, f_s$: the geometric degree of the system. With this notion we can show the following effective Nullstellensatz: if δ denotes the geometric degree of the trivial system $f_1, \ldots, f_s$ and $d := \max_j \deg(f_j)$, then there exist polynomials $p_1, \ldots, p_s \in k[X_1, \ldots, X_n]$ such that $1 = \sum_j p_j f_j$ and $\deg p_j f_j \leqq 3n^2 \delta d$. Since the number δ is always bounded by $(d+1)^{n-1}$, one deduces a classical single exponential upper bound in terms of d and n, but in some cases our new bound improves the known ones.

Keywords: complete intersection polynomial ideals, trace theory, effective Nullstellensatz, geometric degree.

1 Introduction

Let k be a field, $\bar{k}$ its algebraic closure and let $X_1, \ldots, X_n$ be indeterminates over k; for any finite polynomial sequence $f_1, \ldots, f_s$ in $k[X_1, \ldots, X_n]$ such that 1 belongs to the ideal $(f_1, \ldots, f_s)$ we define $D(f_1, \ldots, f_s)$ in the following way:

$$D(f_1, \ldots, f_s) := \min\{\max\{\deg p_j f_j;\ 1 = \sum p_j f_j\}\}.$$

An *effective Hilbert Nullstellensatz* means to provide an explicit function which is an upper bound for D.

During the last years, many efforts have been made in order to improve the effective double exponential version of Hilbert Nullstellensatz due to G. Hermann [15]. The first single exponential bound for D was obtained by D. Brownawell [5] for $k = \mathbb{C}$ in 1986. Later, L. Caniglia, A. Galligo and J. Heintz [6] extended this

Partially supported by UBACYT and CONICET

result for any field and finally, J. Kollár [16] showed that $D \leqq (\max\{d, 3\})^n$, where d is the maximum of the total degrees of the polynomials $f_1, \ldots, f_s$ (see also [10] and [19]). This is the best bound known up to now for $d \geqq 3$ (for $d = 2$ the more precise bound $n2^{n+2}$ can be obtained; see [20, 22]) and, in fact, a well known example shows that it is asymptotically optimal (see Example 1 below). Related results can be found also in the research papers [21, 4, 19, 7, 12, 11, 1, 17, 13] and in the surveys [3, 23].

In this paper we exhibit a new effective Nullstellensatz which doesn't depend so much on the degree of the involved polynomials as the ones mentioned above, but on a more intrinsic invariant: the *geometric degree of a trivial polynomial system.*

First, following [14], we define the *geometric* (or *set-theoretical*) *degree* of an algebraic affine variety $V \subset \mathbb{A}^n_{\bar{k}}$ as the sum of the degrees of its irreducible components (where, as usual, the degree of an irreducible variety is the cardinal of its intersection with a generic linear variety of complementary dimension).

If $V, W \subset \mathbb{A}^n_{\bar{k}}$ are affine varieties, Bezout Inequality states the inequality $\deg(V \cap W) \leqq \deg(V)\deg(W)$ (see for instance [14, Theorem 1] for an elementary proof).

Let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be non constant polynomials such that $1 \in (f_1, \ldots, f_s)$. First let us suppose that the characteristic of k is zero; from Bertini's Theorem and suitable arguments of genericity (cf. [12, Section 3.2], [20, Section 5.2] and [17, Section 6.1]), it is possible to show that there exist an integer t, $2 \leqq t \leqq n + 1$, and t $\bar{k}$-linear combinations $g_1, \ldots, g_t$ of the polynomials f_j such that:

- $1 \in (g_1, \ldots, g_t)$,
- $g_1, \ldots, g_{t-1}$ is a regular sequence,
- $(g_1, \ldots, g_j)$ is a radical ideal, for all $j = 1, \ldots, t$.

If the characteristic of k is positive, a similar result holds for $\bar{k}$-linear combinations of the polynomials f_j and $X_i f_j$, $j = 1, \ldots, s$, $i = 1, \ldots, n$ (see [12, Section 3.2] or [20, Section 5.2]).

In both cases denote by $\mathscr{G}$ the set of all sequences $g_1, \ldots, g_t$ for all possible t, $2 \leqq t \leqq n + 1$, which verify the three conditions.

Definition 1 Under these assumptions we define the *geometric degree of the trivial system* $f_1, \ldots, f_s$ as the quantity

$$\min_{\mathscr{G}} \left\{ \max_{1 \leqq j \leqq \min\{t-1, n-1\}} \{\deg V(g_1, \ldots, g_j)\} \right\},$$

where $V(g_1, \ldots, g_j) \subset \mathbb{A}^n_{\bar{k}}$ denotes the variety of common zeros of the polynomials $g_1, \ldots, g_j$.

With this notion our main result is the following (see Theorem 7 below):

Theorem *Let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be polynomials which generate the trivial ideal, $d := \max_j \deg f_j$ and δ be the associated geometric degree. Then $D(f_1, \ldots, f_s) \leqq 3n^2\delta d$.*

Let us observe that the geometric degree of a system is always bounded by its algebraic-combinatoric "Bezout number" which is given by the Hilbert function of a suitable homogeneous ideal. Moreover, from Bezout inequality, this number is bounded by d^{n-1} (in characteristic zero) or by $(d + 1)^{n-1}$ (in any characteristic), and then, from our result a single exponential bound for $D(f_1, \ldots, f_s)$ can be reobtained. However, in many cases, the value of the geometric degree of the system is much smaller than its Bezout number since this geometric degree does not take into account multiplicities or degrees of certain components at infinity. In this sense, our effective Nullstellensatz can be considered more intrinsic and improves the known ones (see Example 3 of Section 4).

As an intermediate step in the proof of the Nullstellensatz, we also obtain similar bounds for the membership problem in a complete intersection case (see Lemma 5 below).

The techniques used here are exactly the same ones that in [20], which rely on elementary duality theory for Gorenstein algebras applied as a tool for algebraic complexity questions (method introduced in [11]). In fact, this paper may be considered as another way (more intrinsic) of applying the trace inequalities of [20] and [11] to effective Nullstellensätze.

Similar results can be obtained by means of algorithmic tools (see [13]) or combinatoric methods (see [22]).

We thank Joos Heintz and Marc Giusti for pointing out this problem to us.

2 Preliminaries

We denote by k an arbitrary field; since our statements of effective Nullstellensätze don't depend on algebraic extensions of k, we may suppose in the sequel that k is algebraically closed.

Let $X_1, \ldots, X_n$ be indeterminates over k and $k[X_1, \ldots, X_n]$ be the polynomial ring with coefficients from k. For each polynomial $f \in k[X_1, \ldots, X_n]$ we write $\deg f$ for its total degree (by convention $\deg 0 := -1$).

Let $0 \leqq r < n$ be a non-negative integer, $f_1, \ldots, f_{n-r} \in k[X_1, \ldots, X_n]$ a regular sequence, $A := k[X_1, \ldots, X_r]$, $B := k[X_1, \ldots, X_n]/(f_1, \ldots, f_{n-r})$ and suppose that the canonical morphism $A \to B$ is an integral monomorphism (Noether position). In this case, it is well known that B is a free A-module. For any polynomial $f \in k[X_1, \ldots, X_n]$ we denote by $\bar{f}$ its class in B. Δ denotes the determinant of the Jacobian matrix $\left(\dfrac{\partial f_i}{\partial X_{r+j}}\right)_{1 \leqq i, j \leqq n-r}$ and we assume that $\bar{\Delta}$ is not a zero divisor in B (therefore the Jacobian criterion implies that B is reduced).

The set of common zeros of the regular sequence $f_1, \ldots, f_{n-r}$ in $\mathbb{A}_k^n$ is denoted by V.

The following definitions and statements of basic trace theory for Gorenstein algebras can be found in [18, Appendix F] (see also [20, Sect. 4.2]). This is a useful tool in Effective Algebra and several applications of duality theory in this field can be found for instance in [4, 9, 24, 11, 8, 2, 17].

Consider the ring B as an A-algebra and denote by B^* its dual space $\mathrm{Hom}_A(B, A)$. Our assumptions guarantee that B^* admits a natural structure of cyclic B-module (any generator of B^* is called a *trace* of B over A).

Let $\mu : B \otimes_A B \to B$ be the multiplication morphism $\mu(b \otimes b') := bb'$ and denote by $\mathscr{K}$ its kernel. The annihilator $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ is a cyclic B-module. Moreover, for each generator $\sum_m b_m \otimes b'_m$, there exists a uniquely determinated trace $\sigma \in B^*$ such that for all $b \in B$ the so-called *trace formula* holds:

$$b = \sum_{1 \leqq m \leqq M} \sigma(bb'_m) b_m. \tag{1}$$

In particular we observe that $b_1, \ldots, b_M$ is a system of generators of the A-module B.

Let $Y_{r+1}, \ldots, Y_n$ be new indeterminates over k; for each polynomial $f \in k[X_1, \ldots, X_n]$ we denote by $f^{(Y)}$ the element of the polynomial ring $k[X_1, \ldots, X_r, Y_{r+1}, \ldots, Y_n]$ defined by $f^{(Y)} := f(X_1, \ldots, X_r, Y_{r+1}, \ldots, Y_n)$. Hence we have the canonical isomorphism of A-algebras:

$$B \otimes_A B \cong A[X_{r+1}, \ldots, X_n, Y_{r+1}, \ldots, Y_n]/(f_1, \ldots, f_{n-r}, f_1^{(Y)}, \ldots, f_{n-r}^{(Y)}). \quad (2)$$

If one considers each polynomial $f_i^{(Y)} - f_i$ as a polynomial in the variables $Y_{r+1}, \ldots, Y_n$ with coefficients in $k[X_1, \ldots, X_n]$ $(1 \leqq i \leqq n-r)$, its Taylor expansion around the point $(X_{r+1}, \ldots, X_n)$ gives the relation:

$$f_i^{(Y)} - f_i = \sum_{1 \leqq j \leqq n-r} a_{ij}(Y_{r+j} - X_{r+j})$$

where $a_{ij} \in k[X_1, \ldots, X_n, Y_{r+1}, \ldots, Y_n] = A[X_{r+1}, \ldots, X_n, Y_{r+1}, \ldots, Y_n]$ are polynomials of total degree bounded by $d-1$. Following [18, Corollary E.19 and Example F.19] the class of $\det(a_{ij})$ modulo the ideal $(f_1, \ldots, f_{n-r}, f_1^{(Y)}, \ldots, f_{n-r}^{(Y)})$ gives a generator of $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ by means of the identification (2). Developing this determinant we obtain (see [11, §3.4]):

Proposition 2 *There exists polynomials* a_m, c_m *in* $k[X_1, \ldots, X_n]$ *satisfying* $\deg(a_m) + \deg(c_m) \leqq (n-r)(d-1)$ $(1 \leqq m \leqq M)$ *such that* $\sum_m \bar{a}_m \otimes \bar{c}_m$ *is a generator of* $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$. ∎

Definition 3 The trace associated to the generator of $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ introduced in Proposition 2 will be called *the trace associated to the regular sequence* $f_1, \ldots, f_{n-r}$ and we will denote it by σ_Δ. In particular we have $\bar{f} = \sum_m \sigma_\Delta(\bar{f}\,\bar{c}_m)\bar{a}_m$, for all $f \in k[X_1, \ldots, X_n]$.

For any polynomial $g \in k[X_1, \ldots, X_n]$ such that its class $\bar{g} \in B$ is not a zero divisor, let $\mathscr{X}_g = T^s + \alpha_{s-1}T^{s-1} + \cdots + \alpha_0 \in A[T]$ be the characteristic polynomial of the endomorphism of B consisting in multiplication by $\bar{g}$. We define a new polynomial $g^* \in k[X_1, \ldots, X_n]$ which depends on g in the following way:

$$g^* := g^{s-1} + \alpha_{s-1}g^{s-2} + \cdots + \alpha_2 g + \alpha_1. \quad (3)$$

Observe that $gg^* + \alpha_0 = \mathscr{X}_g(g)$ is an element of the ideal $(f_1, \ldots, f_{n-r})$ (Hamilton-Cayley) and $\alpha_0 \neq 0$ since multiplication by $\bar{g}$ is injective.

Under these hypothesis we have:

Theorem 4 ([20, Theorem 10]) *Let* $\sigma_\Delta \in B^*$ *be the trace associated to* $f_1, \ldots, f_{n-r}$; *let* g *and* f *be polynomials in* $k[X_1, \ldots, X_n]$ *such that* $\bar{g} \in B$ *is not a zero divisor. Then the following inequality holds*:

$$\deg \sigma_\Delta(\overline{g^*}\,\bar{f}) \leqq \deg(V)(1 + \max\{\deg f, \deg g + (n-r)d\}). \quad ∎$$

3 A Division Lemma for Complete Intersections and Nullstellensatz

Let r be an integer, $0 \leqq r \leqq n-1$. We assume that $f_1, \ldots, f_{n-r}$ is a regular sequence contained in $k[X_1, \ldots, X_n]$. Let d be an upper bound for the degrees of all polynomials f_j, $1 \leqq j \leqq n-r$.

For each $j, r \leqq j \leqq n-1$, let $\mathfrak{I}_j$ be the ideal generated by $f_1, \ldots, f_{n-j}$, and set $A_j := k[X_1, \ldots, X_j]$, $B_j := k[X_1, \ldots, X_n]/\mathfrak{I}_j$. Suppose that the canonical morphism $A_j \to B_j$ is an integral monomorphism and that the corresponding Jacobian Δ_j is not a zero divisor in B_j.

We write $\mathscr{K}_j$ for the kernel of the application $\mu_j : B_j \otimes_{A_j} B_j \to B_j$ introduced in Section 2 and $a_m^{(j)}, c_m^{(j)} \in k[X_1, \ldots, X_n]$ are such that $\sum_m \bar{a}_m^{(j)} \otimes \bar{c}_m^{(j)}$ is the generator of $\mathrm{Ann}_{B_j \otimes B_j}(\mathscr{K}_j)$ defined in Proposition 2. Its associated trace will be denoted by σ_j.

Let $V_j \subset \mathbb{A}_k^n$ be the algebraic variety defined by the ideal $\mathfrak{I}_j$ and let

$$\rho := \max\{\deg(V_j);\ r+1 \leqq j \leqq n-1\}.$$

Under the previous assumptions we have the following division lemma (see, for instance, [16, 4, 20, 17, 1] for similar results):

Lemma 5 *Let f be a polynomial in the ideal $\mathfrak{I}_r$. Then there exists polynomials $p_1, \ldots, p_{n-r}$ in $k[X_1, \ldots, X_n]$ such that*:

- $f = \sum_{i=1}^{n-r} p_i f_i$
- $\deg p_i f_i \leqq 2(n-r)^2 \rho d + \rho \max\{\deg f, d\} \quad (1 \leqq i \leqq n-r)$.

Proof. We shall construct recursively polynomials $p_{n-r}, p_{n-r-1}, \ldots, p_1 \in k[X_1, \ldots, X_n]$ such that for any index $j, r \leqq j \leqq n-1$, the following properties are verified:

(I) the polynomial $f - p_{n-r} f_{n-r} - \cdots - p_{n-j} f_{n-j}$ belongs to the ideal $\mathfrak{I}_{j+1}$ (where $\mathfrak{I}_n$ denotes the zero ideal)
(II) the polynomial p_{n-j} can be written in the form

$$p_{n-j} = \sum_m \alpha_m^{(j+1)} a_m^{(j+1)}$$

where $a_m^{(j+1)}$ are the polynomials which appear in Proposition 2 and $\alpha_m^{(j+1)}$ are polynomials in the ring A_{j+1} which degrees are uniformly bounded by a constant D_j defined recursively by:

$$D_r := \rho(1 + d(n-r-1) + \max\{\deg f, d\})$$

$$D_{j+1} := D_j + \rho(1 + 2d(n-j-1)) \tag{4}$$

for $r \leqq j \leqq n-2$. (Let us observe that, from these bounds, we have $\deg p_{n-j} < D_j + (n-j-1)d$ for all $j, r \leqq j \leqq n-1$.)

In order to show the fulfilment of statements (I) and (II) we start the recursive procedure at $j = r$.

Since the polynomial f belongs to the ideal $\mathfrak{I}_r$, there exists a polynomial $h \in k[X_1, \ldots, X_n]$ such that:

$$f \equiv h f_{n-r} \mod \mathfrak{I}_{r+1}. \tag{5}$$

We define $p_{n-r} := \sum_m \sigma_{r+1}(\bar{h}\bar{c}_m^{(r+1)}) a_m^{(r+1)}$.

First we observe that the trace formula (1) for the element $\sum_m \bar{a}_m^{(j+1)} \otimes \bar{c}_m^{(j+1)}$ implies that $p_{n-r} - h$ belongs to $\mathfrak{I}_{r+1}$. So p_{n-r} satisfies condition (I).

Since the element $\overline{f}_{n-r}$ is not a zero divisor in the ring B_{r+1} we can define, following (3), the polynomials $f^*_{n-r} \in k[X_1, \dots, X_n]$ and $\alpha \in A_{r+1}$ ($\alpha \neq 0$) in such a way that $f^*_{n-r} f_{n-r} - \alpha$ is an element of the ideal $\mathfrak{I}_{r+1}$. Multiplying the equality (5) by f^*_{n-r} we obtain:

$$f^*_{n-r} f \equiv \alpha h \mod \mathfrak{I}_{r+1}.$$

Thus the polynomial identity

$$\alpha p_{n-r} = \sum_m \sigma_{r+1}(\overline{f^*_{n-r}}\, \overline{f} \bar{c}_m^{(r+1)}) a_m^{(r+1)}$$

holds.

Since $\alpha \in A_{r+1}$ and σ_{r+1} is A_{r+1}-linear, α divides the polynomials $\sigma_{r+1}(\overline{f^*_{n-r}}\, \overline{f} \bar{c}_m^{(r+1)})$, whose degrees are uniformly bounded by $\rho\ (1 + d(n-r-1) + \max\{\deg f, d\}) = D_r$ (see Theorem 4). Therefore defining

$$\alpha_m^{(r+1)} := \frac{1}{\alpha} \sigma_{r+1}(\overline{f^*_{n-r}}\, \overline{f} \bar{c}_m^{(r+1)})$$

property (II) holds.

Let now $j, r \leqq j \leqq n-2$ and suppose that there exist polynomials $p_{n-r}, \dots, p_{n-j}$ satisfying conditions (I) and (II). We are going to repeat *mutatis mutandis* the same procedure used in the case $j = r$ in order to prove conditions (I) and (II) for $j+1$.

Since the polynomial $g := f - p_{n-r} f_{n-r} - \dots - p_{n-j} f_{n-j}$ belongs to the ideal $\mathfrak{I}_{j+1}$ (condition (I) for j) there exists a polynomial $h \in k[X_1, \dots, X_n]$ such that:

$$g \equiv h f_{n-j-1} \mod \mathfrak{I}_{j+2}. \tag{6}$$

The polynomial p_{n-j-1} is defined by:

$$p_{n-j-1} := \sum_m \sigma_{j+2}(\bar{h} \bar{c}_m^{(j+2)}) a_m^{(j+2)}.$$

The trace formula (1) implies that $p_{n-j-1} - h$ belongs to $\mathfrak{I}_{j+2}$. So condition (I) is verified for $j+1$.

Following (3) let us consider the polynomials $f^*_{n-j-1} \in k[X_1, \dots, X_n]$ and $\alpha \in A_{j+2}$ such that $f^*_{n-j-1} f_{n-j-1} - \alpha \in \mathfrak{I}_{j+2}$.

From (6) we obtain:

$$f^*_{n-j-1} g \equiv \alpha h \mod \mathfrak{I}_{j+2}.$$

Therefore

$$\alpha p_{n-j-1} = \sum_m \sigma_{j+2}(\overline{f^*_{n-j-1}}\, \bar{g} \bar{c}_m^{(j+2)}) a_m^{(j+2)}$$

holds in the polynomial ring $k[X_1, \dots, X_n]$. Taking into account that α divides the polynomials $\sigma_{j+2}(\overline{f^*_{n-j-1}}\, \bar{g} \bar{c}_m^{(j+2)})$ we define

$$\alpha_m^{(j+2)} := \frac{1}{\alpha} \sigma_{j+2}(\overline{f^*_{n-j-1}}\, \bar{g} \bar{c}_m^{(j+2)}).$$

In order to show that p_{n-j-1} satisfies condition (II) it suffices to prove that the degrees of the polynomials $\alpha_m^{(j+2)}$ are bounded by D_{j+1}.

First we observe that $\deg \alpha_m^{(j+2)}$ is bounded by $\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\, \bar{g} \bar{c}_m^{(j+2)})$ for each index m.

From the definition of the polynomial g we have:

$$\begin{aligned}
&\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\bar{g}\bar{c}_m^{(j+2)}) \\
&= \deg \sigma_{j+2}\left(\overline{f^*_{n-j-1}}\,\bar{f}\bar{c}_m^{(j+2)} - \sum_{l=r}^{j} \overline{f^*_{n-j-1}}\bar{p}_{n-l}\bar{f}_{n-l}\bar{c}_m^{(j+2)}\right) \\
&\leqq \max\left\{\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\,\bar{f}\bar{c}_m^{(j+2)}),\ \deg \sigma_{j+2}\right. \\
&\quad \left.\times\left(\sum_{l=r}^{j} \overline{f^*_{n-j-1}}\bar{p}_{n-l}\bar{f}_{n-l}\bar{c}_m^{(j+2)}\right)\right\} \qquad (7)
\end{aligned}$$

Theorem 4 implies:

$$\begin{aligned}
&\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\,\bar{f}\bar{c}_m^{(j+2)}) \leqq \\
&\leqq \rho(1 + \max\{\deg f + \deg c_m^{(j+2)}, \deg f_{n-j-1} + (n-j-2)d\}) \leqq \\
&\leqq \rho(1 + (n-j-2)d + \max\{d, \deg f\}).
\end{aligned}$$

In order to bound the remainder part of (7), we use condition (II) to replace each polynomial p_{n-l}, $r \leqq l \leqq j$:

$$\begin{aligned}
&\deg \sigma_{j+2}\left(\sum_{l=r}^{j} \overline{f^*_{n-j-1}}\left(\sum_{m'} \alpha_{m'}^{(l+1)}\bar{a}_{m'}^{(l+1)}\right)\bar{f}_{n-l}\bar{c}_m^{(j+2)}\right. \\
&\leqq \max_{l,m'}\{\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\alpha_{m'}^{(l+1)}\bar{a}_{m'}^{(l+1)}\bar{f}_{n-l}\bar{c}_m^{(j+2)})\}
\end{aligned}$$

Taking into account that the polynomials $\alpha_{m'}^{(l+1)}$ are elements of the ring A_{l+1} and therefore are in A_{j+2} we obtain:

$$\begin{aligned}
&\max_{l,m'}\{\deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\alpha_{m'}^{(l+1)}\bar{a}_{m'}^{(l+1)}\bar{f}_{n-l}\bar{c}_m^{(j+2)})\} = \\
&\qquad = \max_{l,m'}\{\deg \alpha_{m'}^{(l+1)} + \deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\bar{a}_{m'}^{(l+1)}\bar{f}_{n-l}\bar{c}_m^{(j+2)})\}
\end{aligned}$$

From Theorem 4 and condition (II) for l we deduce:

$$\deg \alpha_{m'}^{(l+1)} + \deg \sigma_{j+2}(\overline{f^*_{n-j-1}}\bar{a}_{m'}^{(l+1)}\bar{f}_{n-l}\bar{c}_m^{(j+2)}) \leqq D_l + \rho(1 + (2n-l-j-2)d)$$

Summarizing the inequalities above we have that $\deg \alpha_m^{(j+2)}$ is bounded by the expression:

$$\max\left\{\rho(1 + (n-j-2)d + \max\{d, \operatorname{def} f\}),\ \max_{r \leqq l \leqq j}\{D_l + \rho(1 + (2n-l-j-2)d)\}\right\}.$$

Since $D_{j+1} \geqq D_j$ for all index j one infers that $D_l \geqq \rho \max\{d, \deg f\}$ for all l and then

$$\deg \alpha_m^{(j+2)} \leqq \max_{r \leqq l \leqq j}\{D_l + \rho(1 + (2n-l-j-2)d)\}.$$

From the fact that $D_{j+1} \geqq D_j + \rho d$ a simple computation shows that:

$$\max_{r \leqq l \leqq j} \{D_l + \rho(1 + (2n - l - j - 2)d)\} = D_j + \rho(1 + 2d(n - j - 1)) = D_{j+1}.$$

Then we have:

$$\deg \alpha_m^{(j+2)} \leqq D_{j+1}$$

and so, condition (II) is verified for $j + 1$.

From the recursive definition of the integers D_j it is easy to prove the formula:

$$D_j = \rho(\max\{\deg f, d\} + 1 + d(n - r - 1) + (j - r)(1 + d(2n - r - j - 1))). \quad (8)$$

Summarizing, this recursive method produces polynomials $p_1, \ldots, p_{n-r}$ in $k[X_1, \ldots, X_n]$ such that $f = \sum_{1 \leqq i \leqq n-r} p_i f_i$ and $\deg p_i \leqq D_{n-i} + (i-1)d$, $1 \leqq i \leqq n - r$. From the definition of D_j and from (8) we have

$$D_{n-i} + (i - 1)d \leqq D_{n-1} = \rho d((n - r)^2 - 1) + \rho(\max\{\deg f, d\} + n - r - 1). \quad (9)$$

Therefore, $\deg p_i f_i \leqq D_{n-1} + d$ and, from (9), this quantity is obviously bounded by $2\rho d(n - r)^2 + \rho \max\{\deg f, d\}$ and the lemma follows. ■

Corollary 6 *Let $s \in \mathbb{N}$, $2 \leqq s \leqq n + 1$, $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$ such that $f_1, \ldots, f_{s-1}$ is a regular sequence verifying the previous assumptions for $r := n - s + 1$ and such that $1 \in (f_1, \ldots, f_s)$. Let d be an upper bound for the degrees of the polynomials f_j, $1 \leqq j \leqq s$. Then $D(f_1, \ldots, f_s) \leqq 2n^2 \rho d$. In particular, if δ is the geometric degree of the system $f_1, \ldots, f_s$, the inequality $D(f_1, \ldots, f_s) \leqq 2n^2 \delta d$ holds.*

Proof. First suppose $s < n + 1$. Taking into account that in the first step of the proof of Lemma 4 we didn't use the fact that the ideal is generated by a regular sequence (in fact, we only use that f_{n-r} is not a zero divisor modulo $\mathfrak{I}_{r+1}$) we obtain $1 = \sum_j p_j f_j$ where $\deg p_j f_j \leqq 2n^2 \rho d (1 \leqq j \leqq s)$.

Now assume $s = n + 1$. As $f_1, \ldots, f_n$ is a regular sequence these polynomials generate a 0-dimensional idea $\mathfrak{I}_0$ and the class of f_{n+1} is a unit in the factor ring $k[X_1, \ldots, X_n]/\mathfrak{I}_0$. In other words, there exists a polynomial $p_{n+1} \in k[X_1, \ldots, X_n]$ such that $1 - p_{n+1} f_{n+1} \in \mathfrak{I}_0$.

Formula (1) and Proposition 2 in the case $A = k$ and $B = k[X_1, \ldots, X_n]/\mathfrak{I}_0$ imply that there exists a k-system of generators of B consisting of polynomials $a_m \in k[X_1, \ldots, X_n]$ $(1 \leqq m \leqq M)$ with degrees bounded by $n(d - 1)$.

Therefore, without loss of generality, we can suppose that $\deg p_{n+1} \leqq n(d - 1)$.

Now, applying inequality (9) of Lemma 4 for $r = 0$ to the polynomial $f := 1 - p_{n+1} f_{n+1}$ which belongs to the ideal $\mathfrak{I}_0$ and has degree bounded by $n(d - 1) + d$, we obtain polynomials $p_1, \ldots, p_n$ such that:

$$- \sum_{i=1}^{n+1} p_i f_i = 1$$

$$- \deg p_i f_i \leqq \rho d(n^2 - 1) + \rho(n(d - 1) + d + n - 1) + d \leqq 2n^2 \rho d.$$

The stated last inequality is a direct consequence of the definition of the geometric degree of a trivial polynomial system (see Definition 1). ■

The general case can be deduced from this corollary by means of Bertini's Theorem:

Theorem 7 *Let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be polynomials which generate the trivial ideal, $d := \max_j \deg f_j$ and δ be the associated geometric degree (cf. Definition 1). Then $D(f_1, \ldots, f_s) \leqq 3n^2\delta d$.*

Proof. Without loss of generality we may suppose $d > 1$. Then the proof is an immediate consequence of [12, Section 3.2.] or [20, Section 5.2.] (see also [17]) which state the following: there exists a suitable number of generic linear combinations of the polynomials f_j (if $\mathrm{char}(k) = 0$) and eventually of the polynomials $X_i f_j$ (if $\mathrm{char}(k) > 0$), $j = 1, \ldots, s$ and $i = 1, \ldots, n$, say $g_1, \ldots, g_t$, which verify the conditions:

1. $1 \in (g_1, \ldots, g_t)$,
2. $g_1, \ldots, g_{t-1}$ is a regular sequence,
3. the ideal $(g_1, \ldots, g_j)$ is radical for $j = 1, \ldots, t$.

Therefore the result follows from Corollary 6 applied to the polynomials $g_1, \ldots, g_t$, after a suitable linear change of coordinates to put the variables into Noether position and taking into account that $\max_j \deg(g_j) \leqq d + 1$. ■

4 Examples

Example 1 The following example shows that in the definition of the geometric degree of a trivial polynomial system, the radical condition is unavoidable in order to obtain the stated bounds. Let us consider the classic example:

$$f_1 := X_1^d,\ f_2 := X_1 - X_2^d, \ldots, f_{n-1} := X_{n-2} - X_{n-1}^d, f_n = 1 - X_{n-1}X_n^{d-1}.$$

Clearly $f_1, \ldots, f_{n-1}$ is a regular sequence which is not reduced step-by-step, and $1 \in (f_1, \ldots, f_n)$. Specializing any equality $1 = p_1 f_1 + \cdots + p_n f_n$ on the curve parametrized by $(t^{(d-1)d^{n-2}}, \ldots, t^{(d-1)d}, t^{d-1}, t^{-1})$ one deduces that $\deg_{X_n} p_1 \geqq (d-1)d^{n-1}$ and therefore from Corollary 6 or Theorem 7 one has:

$$\delta \geqq \frac{(d-1)d^{n-2}}{2n^2}.$$

However in this case $\deg V(f_1, \ldots, f_j) = 1$, for all $1 \leqq j \leqq n-1$.

Example 2 In this simple example one easily sees that the maximum of the degrees of the involved polynomials must occur in the stated upper bounds:

$$f_1 := X_1,\ f_2 := X_2 - X_1, \ldots, f_n := X_n - X_1,\ f_{n+1} = 1 - X_1^d.$$

Here $f_1, \ldots, f_n$ is a step-by-step reduced regular sequence and $1 \in (f_1, \ldots, f_{n+1})$. Specializing again any representation $1 = p_1 f_1 + \cdots + p_{n+1} f_{n+1}$ on $(t, \ldots, t)$ it immediately follows that $\deg p_1 f_1 \geqq d$. On the other hand $\delta = 1$ and our bound is $2n^2$d (Corollary 6).

Example 3 The last example shows that our upper bound improves in some cases Kollár's:

$$f_1 := X_1,\ f_2 := X_2 - X_1^d, \ldots, f_n := X_n - X_{n-1}^d,\ f_{n+1} = 1 - X_n^d.$$

In this case Kollár's bound is d^{n-1} (see [16, 10, 19]) while ours is $2n^2 d$ since $\delta = 1$. Effectively we have the following representation:

$$1 = (X_1^{d-1} \dots X_n^{d-1}) f_1 + (X_2^{d-1} \dots X_n^{d-1}) f_2 + \dots + (X_n^{d-1}) f_n + f_{n+1}.$$

References

1. Amoroso, F.: On a conjecture of C. Berenstein and A. Yger. Proc. MEGA'94, Birkhäuser Progress in Math (to appear)
2. Alonso, M., Becker, E., Roy, M.-F., Wörmann, T.: Zeros, Multiplicities and Idempotents for Zerodimensional Systems. Proc. MEGA'94, Birkhäuser Progress in Math. (to appear)
3. Berenstein, C., Struppa, D.: Recent improvements in the Complexity of the Effective Nullstellensatz. Linear Algebra and Its Appl. **157**, 203–215 (1991)
4. Berenstein, C., Yger, A.: Bounds for the degrees in the division problem. Mich. Math. J. **37**, 25–43 (1990)
5. Brownawell, D.: Bounds for the degrees in the Nullstellensatz. Ann. Math. Second Series **126**(3), 577–591 (1987)
6. Caniglia, L., Galligo, A., Heintz, J.: Some new effectivity bounds in computational geometry. Proc. 6th Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC-6, Roma 1988. Lecture Notes Comput. Sci. Vol. 357, pp. 131–151. Berlin, Heidelberg, New York: Springer 1989
7. Caniglia, L., Guccione, J. A., Guccione, J. J.: Local membership problems for polynomial ideals. Effective Methods in Algebraic Geometry MEGA 90. Mora, T., Traverso, C. (eds). Progress in Mathematics Vol. 94, pp. 31–45, Birkhäuser 1991
8. Cardinal, J.-P.: Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux. Thesis, Université de Rennes (1993)
9. Dickenstein, A., Sessa, C.: An effective residual criterion for the membership problem in $\mathbb{C}[z_1, \dots, z_n]$. J. Pure and Appl. Algebra Vol. 74, pp. 149–158. Amsterdam: North-Holland 1991
10. Fitchas, N., Galligo, A.: Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le Calcul Formel. Math. Nachr. **149**, 231–253 (1990)
11. Fitchas, N., Giusti, M., Smietanski, F.: Sur la complexité du théorème des zéros. Approximation and Optimization Vol. 8, pp. 274–329, Verlag Peter Lang 1995
12. Giusti, M., Heintz, J., Sabia, J.: On the efficiency of effective Nullstellensätze. Comput. Complexity, Vol. 3, pp. 56–95, Basel: Birkhäuser 1993
13. Giusti, M., Heintz, J., Morais, J., Morgenstern, J., Pardo, L.: Straight-line Programs in Geometric Elimination Theory. J. Pure and Appl. Algebra (to appear)
14. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. **24**, 239–277 (1983)
15. Hermann, G.: Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. Math. Ann. **95**, 736–788 (1926)
16. Kollár, J.: Sharp effective Nullstellensatz. J. AMS **1**, 963–975 (1988)
17. Krick, T., Pardo, L.: A computational Method for Diophantine Approximation. Proc. MEGA '94, Birkhäuser Progress in Math (to appear)
18. Kunz, E.: Kähler Differentials. Adv. Lect. in Math. Vieweg Verlag 1986
19. Philippon, P.: Dénominateurs dans le théorème des zéros de Hilbert. Acta. Arith. **58**, 1–25 (1991)
20. Sabia, J., Solernó, P.: Bounds for Traces in Complete Intersections and Degrees in the Nullstellensatz. AAECC **6**(6), 353–376 (1995)
21. Shiffman, B.: Degree bounds for the division problem in polynomial ideals. Michigan Math. J. **36**, 163–171 (1989)
22. Sombra, M.: Bounds for the Hilbert function of polynomial ideals. Preprint, Universidad de Buenos Aires (1996)
23. Teissier, B.: Résultats récents d'algèbre commutative effective. Séminaire Bourbaki 1989–1990, Astérisque Vol. 189–190, 107–131 (1991)
24. Vasconcelos, W.: Jacobian Matrices and Constructions in Algebra. Proc. 9th Int. Conf. Applied Algebra. Algebraic Algorithms and Error Correcting Codes AAECC-9, New Orleans, 1991, Lecture Notes Comput. Sci., Vol. 539, pp. 48–64. Berlin, Heidelberg, New York: Springer 1992