AAECC 6, 353–376 (1995)

AAECC
Applicable Algebra in Engineering, Communication and Computing

Bounds for Traces in Complete Intersections and Degrees in the Nullstellensatz

Juan Sabia, Pablo Solernó

Departamento de Matemáticas, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires-1428-Buenos Aires, Argentina. jsabia@mate.dm.uba.ar and psolerno@mate.dm.uba.ar

Received May 13, 1993

Abstract. In this paper we obtain an effective Nullstellensatz using quantitative considerations of the classical duality theory in complete intersections. Let k be an infinite perfect field and let $f_1,\ldots,f_{n-r}\in k[X_1,\ldots,X_n]$ be a regular sequence with $d:=\max_j \deg f_j$. Denote by A the polynomial ring $k[X_1,\ldots,X_r]$ and by B the factor ring $k[X_1,\ldots,X_n]/(f_1,\ldots,f_{n-r})$; assume that the canonical morphism $A\to B$ is injective and integral and that the Jacobian determinant Δ with respect to the variables $X_{r+1},\ldots,X_n$ is not a zero divisor in B. Let finally $\sigma\in B^*:=\mathrm{Hom}_A(B,A)$ be the generator of B^* associated to the regular sequence.

We show that for each polynomial f the inequality $\deg \sigma(\bar{f})\leqq d^{n-r}(\delta+1)$ holds ($\bar{f}$ denotes the class of f in B and δ is an upper bound for $(n-r)d$ and $\deg f$). For the usual trace associated to the (free) extension $A\hookrightarrow B$ we obtain a somewhat more precise bound: $\deg \mathrm{Tr}(\bar{f})\leqq d^{n-r}\deg f$. From these bounds and Bertini's theorem we deduce an elementary proof of the following effective Nullstellensatz: let $f_1,\ldots,f_s$ be polynomials in $k[X_1,\ldots,X_n]$ with degrees bounded by a constant $d\geqq 2$; then $1\in(f_1,\ldots,f_s)$ if and only if there exist polynomials $p_1,\ldots,p_s\in k[X_1,\ldots,X_n]$ with degrees bounded by $4n(d+1)^n$ such that $1=\sum_i p_i f_i$. In the particular cases when the characteristic of the base field k is zero or $d=2$ the sharper bound $4nd^n$ is obtained.

Keywords: Complete intersection polynomial ideals, Trace theory, Bezout's inequality, Effective Nullstellensatz, Bertini's theorem.

1 Introduction

Old ideas on trace theory and more generally duality theory coming from Jacobi, Hermite and Sylvester play nowadays an important rôle for actual research in Computer Algebra, both from the theoretical and the algorithmical points of view (see e.g. [3], [8], [24], [27], [11], [1], [6]).

Partially supported by UBACYT and CONICET (Argentina)

In this sense the aim of this paper is to present new upper bound estimations for the degrees of trace functions in complete intersections in order to obtain an elementary proof of an effective Nullstellensatz.

Let k be an infinite perfect field with an algebraic closure denoted by $\bar{k}$, $\mathfrak{F}$ be a radical complete intersection ideal of the polynomial ring $k[X_1,\ldots,X_n]$. Denote by B the factor ring $k[X_1,\ldots,X_n]/\mathfrak{F}$, by $V\subset\mathbb{A}_k^n$ the affine variety defined by $\mathfrak{F}$ and assume that the canonical morphism $A:=k[X_1,\ldots,X_r]\to B$ is an integral monomorphism.

Under these conditions B is a finite free A-module and for any $b\in B$ the element $\mathrm{Tr}(b):=$ *trace of the multiplication by* b is a well defined polynomial of A.

In Theorem 13 we show that for any $f\in k[X_1,\ldots,X_n]$ the inequality

$$\deg \mathrm{Tr}(\bar{f})\leqq \deg(V)\deg f$$

holds (where $\bar{f}$ is the class of f in B).

Let us now consider the dual module $B^*:=\mathrm{Hom}_A(B,A)$ which has a simple structure of B-module; moreover, with this structure B^* is a free module of rank 1.

Any regular sequence $f_1,\ldots,f_{n-r}$ which generates the ideal $\mathfrak{F}$ induces then a basis σ of B^* called *the trace associated to* $f_1,\ldots,f_{n-r}$.

This trace function – well known in Commutative Algebra (see e.g. [25, 17]) – appears also as an useful tool in Computer Algebra ([3, 11, 6]).

Let Δ be the Jacobian determinant of the regular sequence $f_1,\ldots,f_{n-r}$ with respect to the dependent variables $X_{r+1},\ldots,X_n$ and assume that $\bar{\Delta}$ is not a zero divisor in B. Then for any $f\in k[X_1,\ldots,X_n]$ we obtain the following inequality (Theorem 10 below):

$$\deg\sigma(\bar{f})\leqq \deg(V)(1+\max\{\deg f,(n-r)d\})$$

where d denotes an upper bound for the degrees of the polynomials $f_j(1\leqq j\leqq n-r)$. The strong hypothesis we require on $\bar{\Delta}$ allows us to relate the trace function σ to the usual trace Tr and therefore to obtain the mentioned linear upper bound for σ (Lemma 9 and Theorem 10). If one doesn't impose such a condition it is possible to estimate the degree of a dual basis which leads to non linear bounds for $\sigma(\bar{f})$ of type $\deg(V)^c\deg f$ with $c\geqq 2$ (see [11] and Remark 12 below).

However for many applications one can expect that by means of standard tricks like Bertini's theorem, suitable Noether position, deformation, etc., one may often come down to our conditions. In this sense we present here an elementary proof of an effective Nullstellensatz, following ideas analogous to [11].

Now k denotes an arbitrary field and $\bar{k}$ an algebraic closure of k.

Classical Hilbert Nullstellensatz states that a finite family of polynomials $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ hasn't a common zero in $\bar{k}^n$ if and only if 1 belongs to the ideal generated by $f_1,\ldots,f_s$ in $k[X_1,\ldots,X_n]$.

Let $\delta(n,d)$ be the minimal integer which verifies: for any $s\in\mathbb{N}$ and for any family of polynomials $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ without common zeros in $\bar{k}^n$ with total degrees bounded by d, 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 $\deg p_j\leqq\delta(n,d)$.

Therefore an effective Nullstellensatz means to provide an upper bound for the quantity $\delta(n,d)$.

The most precise bound obtained up to now is due to J. Kollár [18] (see also [10]) and states that $\delta(n,d) \leqq \max\{3,d\}^n$; moreover a well known example ([4]) shows that this bound is asymptotically optimal (see [26, 2] for more details and bibliography about effective Nullstellensätze).

Our trace inequalities and Bertini's Theorem allow to obtain easily the general estimation $\delta(n,d) \leqq 4n(d+1)^n$ (Theorem 17) and the upper bound $4nd^n$ when the characteristic of the ground field k is 0 (Theorem 19). Even if our method doesn't give the mentioned sharp results of [18] or [10], it leads to a slightly more precise bound $n2^{n+2}$ instead of 3^n for the particular case of polynomials of degree 2 (see Theorem 24 below). We have recently known that a similar bound was simultaneously obtained by T. Dubé [9] by means of combinatorial tools.

The paper is organized as follows: in Sect. 3 we compute an upper bound for integral dependence equations using Bezout inequality. We summarize in Sect. 4.2 all the elements of trace theory in complete intersection algebras we need here, which are in fact borrowed from E. Kunz [19]. The upper bounds for the degrees of traces are then given in Sect. 4.3 and finally Sect. 5 is devoted to effective Nullstellensätze.

2 Preliminaries

Let k be an infinite perfect field, $\bar{k}$ be an algebraic closure of k, $X_1,\ldots,X_n$ 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 $\deg 0 := -1$).

We denote by $\mathbb{A}_k^n$ the affine space $\bar{k}^n$ equipped with the Zariski topology.

For any polynomial ideal $\mathfrak{F} \subset k[X_1,\ldots,X_n]$, we denote by $V(\mathfrak{F})$ (or simply V) the affine variety of $\mathbb{A}_k^n$ formed by the common zeros of all the polynomials which belong to the ideal $\mathfrak{F}$.

Following [14] we define the (set-theoretical) *degree* of an algebraic affine variety $V \subset \mathbb{A}_k^n$ as the sum of the degrees of its irreducible components. If $W \subset \mathbb{A}_k^n$ is another affine variety, Bezout Inequality states that $\deg(V \cap W) \leqq \deg(V)\deg(W)$ (see [14, Theorem 1] for an elementary proof).

We say that the variables $X_1,\ldots,X_n$ are in *Noether position* with respect to the polynomial ideal $\mathfrak{F}$ if there exists an index r, $0 \leqq r \leqq n$, such that the canonical morphism $k[X_1,\ldots,X_r] \to k[X_1,\ldots,X_n]/\mathfrak{F}$ is an integral monomorphism. In particular we have $r = \dim V$.

A classical elementary result in Commutative Algebra states that for any polynomial ideal $\mathfrak{F}$ there exist linear changes of coordinates providing new variables which are in Noether position (see for example [23]). If the ideal $\mathfrak{F}$ is given by a finite family of generators there exist several effective methods to compute linear changes of coordinates which give new variables in Noether position (see [20, 7, 12]).

We recall that a polynomial sequence $f_1,\ldots,f_{n-r}$ in $k[X_1,\ldots,X_n]$ is called a *regular sequence* if the following conditions are verified:

- $1 \notin (f_1,\ldots,f_{n-r})$
- f_{i+1} is not a zero divisor in the ring $k[X_1,\ldots,X_n]/(f_1,\ldots,f_i)$, $1 \leqq i < n-r$.

Suppose now that the ideal $\mathfrak{F}$ is generated by a regular sequence $f_1,\ldots,f_{n-r}$ (in this case $r = \dim V$). Suppose also that $X_1,\ldots,X_n$ are in Noether position with respect to $\mathfrak{F}$ and set $A := k[X_1,\ldots,X_r]$ and $B := k[X_1,\ldots,X_n]/\mathfrak{F}$.

Under these assumptions it is well known that B is a free A-algebra (see for instance [13, Lemma 3.3.1]). Moreover, as a consequence of Bezout Inequality, its rank is bounded by $\prod_j \deg f_j$ (see [13, Corollary 3.3.2]).

Unfortunately no single exponential bound for the degrees of the elements of any basis of B is known up to now, even when precise estimations can be done if one considers the localized integral extension $K \subset\!\!\rightarrow K[X_{r+1}, \ldots, X_n]/(f_1, \ldots, f_{n-r})$ of K-vector spaces (K denotes the fraction field of the integral domain A): there exists a basis of elements with degrees bounded by d^{n-r}, obtainable by means of an algorithm with sequential complexity of the same order (see [11, Proposition 2.4]).

3 A Bound for the Degree of Integral Dependence Equations

Let $\mathfrak{F}$ be a *radical* ideal contained in $k[X_1, \ldots, X_n]$ and $V \subset \mathbb{A}_k^n$ be the set of zeros of $\mathfrak{F}$. Suppose that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the ideal $\mathfrak{F}$ and set $A := k[X_1, \ldots, X_r]$ and $B := k[X_1, \ldots, X_n]/\mathfrak{F}$.

Under these assumptions the following proposition allows to estimate degrees for integral dependence equations (for related results see [7, 12, 13]).

Proposition 1. *Let f be an element of the polynomial ring $k[X_1, \ldots, X_n]$ and denote by $\bar{f}$ its class in the factor ring B. Let T be a new variable, then there exists a monic polynomial $F \in A[T]$ which verifies $F(\bar{f}) = 0$ and whose total degree is bounded by* $\deg(V) \deg f$.

Proof. First let us consider the case $r = 0$. Here the ring A coincides with the base field k and then B is a finite dimensional k-vector space. Since $\mathfrak{F}$ is a radical ideal we have that $\dim_k B = \#(V) = \deg(V)$. In particular for each $\bar{f} \in B$ the sequence $1, \bar{f}, \bar{f}^2, \ldots, \bar{f}^{\deg V}$ is linearly dependent; therefore there exists a polynomial $F \in k[T]$ of degree bounded by $\deg(V)$ such that $F(\bar{f}) = 0$ and the proposition is proved.

Now we consider the case $r > 0$.

Let K be the quotient field of A. We write $B' := B \otimes_A K$, $\bar{A} := A \otimes_k \bar{k}$ and $\bar{B} := B \otimes_k \bar{k}$. From the integral inclusion $A \subset\!\!\rightarrow B$ we obtain (since $\bar{k}$ is flat) that the corresponding morphism $\bar{A} \subset\!\!\rightarrow \bar{B}$ is an integral extension too. This ring inclusion induces a projection map $\pi: V \to \mathbb{A}_k^r$ defined as $\pi(x_1, \ldots, x_n) := (x_1, \ldots, x_r)$. The Noether position assumption implies that the map π is surjective.

Now we consider a new map $\varphi: V \to \mathbb{A}_k^{r+1}$ defined as $\varphi(x) := (\pi(x), f(x))$ where $x := (x_1, \ldots, x_n)$.

Since the map φ is closed (the corresponding ring morphism is integral) the image of V under φ is an algebraic variety W contained in $\mathbb{A}_k^{r+1}$ of codimension 1 (i.e. r-dimensional). Then there exists a squarefree polynomial $F \in \bar{k}[Y_1, \ldots, Y_{r+1}]$ such that $W = \{y \in \mathbb{A}_k^{r+1}; F(y) = 0\}$ (see [23, Ch. I, §7, Prop. 4]). In particular we have:

$$F(x_1, \ldots, x_r, f(x)) = 0 \quad \text{for all } x := (x_1, \ldots, x_n) \in V. \tag{1}$$

In order to finish the proof of the proposition it suffices to show that:

(i) the total degree of F is bounded by $\deg(V) \deg f$.
(ii) F is monic in the variable Y_{r+1}.
(iii) F has coefficients in the ground field k and $F(X_1, \ldots, X_r, f)$ belongs to the ideal $\mathfrak{F}$.

• *Proof of (i).* Let $F = F_1 \ldots F_s$ be the decomposition of the squarefree polynomial F in irreducible factors on $\bar{k}[Y_1, \ldots, Y_{r+1}]$ and for each i, $1 \leqq i \leqq s$, let W_i be the irreducible hypersurface defined by the polynomial F_i. In particular $W = \bigcup_i W_i$ and $\deg F = \deg(W) = \sum_i \deg(W_i)$.

Let $S \subset \mathbb{A}_{\bar{k}}^{r+1}$ be an affine line such that the equalities $\#(W \cap S) = \deg(W)$ and $\#(W_i \cap S) = \deg(W_i)$ for all $1 \leqq i \leqq s$ hold simultaneously (the genericity property in the selection of the affine subspace which gives the degree and the equidimensionality of the hypersurface W guarantee the existence of such a line S; moreover we can assume that S is defined by r linear equations whose coefficients belong to the base field k).

Let $\ell_1, \ldots, \ell_r$ be independent affine linear forms from $k[Y_1, \ldots, Y_{r+1}]$ whose zeros define the line S. For each $1 \leqq j \leqq r$, let $\alpha_i^{(j)}$ $(1 \leqq i \leqq r+2)$ be elements of the field k such that:

$$\ell_j = \alpha_1^{(j)} Y_1 + \cdots + \alpha_{r+1}^{(j)} Y_{r+1} + \alpha_{r+2}^{(j)}.$$

The genericity of S also allows to suppose without loss of generality (changing the hyperplanes if necessary) that the coefficient $\alpha_{r+1}^{(1)}$ is equal to 1 and that all the remaining coefficients $\alpha_{r+1}^{(j)}$ are zero for $j \geqq 2$.

Let us consider the algebraic set $U \subset \mathbb{A}_{\bar{k}}^{n}$ defined by the equations:

$$\ell_1(X_1, \ldots, X_r, f) = \ell_2(X_1, \ldots, X_r) = \cdots = \ell_r(X_1, \ldots, X_r) = 0.$$

Let Z be an irreducible component of the algebraic variety $V \cap U$. The image of Z by the map φ is an irreducible subvariety of $W \cap S$ and is therefore a single point (recall that $W \cap S$ is 0-dimensional). Since the equality $\varphi(V \cap U) = W \cap S$ holds we obtain

$$\#(W \cap S) \leqq \deg(V \cap U).$$

Now, applying Bezout Inequality one infers

$$\deg(V \cap U) \leqq \deg(V) \deg(U) \leqq \deg(V) \deg f$$

(U is defined by one polynomial of degree $\deg f$ and $r-1$ linear equations).

Therefore we have:

$$\deg F = \deg(W) = \#(W \cap S) \leqq \deg(V \cap U) \leqq \deg(V) \deg f$$

and assertion (i) is proved.

• *Proof of (ii).* From the definition of F we infer that any polynomial in $\bar{k}[Y_1, \ldots, Y_{r+1}]$ which is zero over W must be divisible by F in the ring $\bar{k}[Y_1, \ldots, Y_{r+1}]$.

Let

$$\bar{f}^m + a_{m-1} \bar{f}^{m-1} + \cdots + a_1 \bar{f} + a_0 = 0$$

be an integral dependence relation for $\bar{f}$ over A.

Let $H \in k[Y_1, \ldots, Y_{r+1}]$ be the polynomial $Y_{r+1}^m + b_{m-1} Y_{r+1}^{m-1} + \cdots + b_1 Y_{r+1} + b_0$, where $b_j := a_j(Y_1, \ldots, Y_r)$, $0 \leqq j \leqq m-1$. Clearly we have that $H(x_1, \ldots, x_r, f(x)) = 0$ holds for any point $x \in V$. Thus H is zero over W and so F divides H in $\bar{k}[Y_1, \ldots, Y_{r+1}]$. Then F is also monic in the variable Y_{r+1} and (ii) is proved.

• *Proof of (iii).* Suppose for the moment that the polynomial F has coefficients in the base field k. From (1) and from the fact that $\mathfrak{F}$ is a radical ideal we conclude that $F(X_1, \ldots, X_r, f)$ belongs to $\mathfrak{F}$.

Therefore it suffices to prove that $F \in k[Y_1, \ldots, Y_{r+1}]$.

Since k is perfect one deduces that the extended ideal $\mathfrak{F}\bar{k}[X_1, \ldots, X_n]$ is radical too (see [21, Ch. 10, §7, Lemma 2]) and it is the ideal associated to the variety V.

Now let us consider the element $\bar{f}$ as an element of the ring $B'' := B' \otimes_k \bar{k}$ (which is a finite dimensional vector space over the field $K' := \bar{k}(X_1, \ldots, X_r)$).

Let η_f be the K'-endomorphism of B'' induced by the multiplication by $\bar{f}$. We assert that $F(X_1, \ldots, X_r, T)$ considered as an univariate polynomial in $K'[T]$ is the minimal polynomial of the endomorphism η_f.

In virtue of (1) let us observe that this polynomial annihilates η_f. Moreover, if $G \in \bar{k}[X_1, \ldots, X_r, T]$ verifies $G(X_1, \ldots, X_r, \eta_{\bar{f}}) = 0$ we have that $G(X_1, \ldots, X_r, f)$ belongs to the ideal $\mathfrak{F}\bar{k}[X_1, \ldots, X_n]$ and then $G(x_1, \ldots, x_r, f(x))$ is zero for all $x \in V$. This implies that F divides G and therefore $F(X_1, \ldots, X_r, T)$ is the minimal polynomial of η_f.

To finish the proof of (iii) let us consider the restriction of the endomorphism η_f to B'. We deduce that the minimal polynomial $F(X_1, \ldots, X_r, T)$ belongs to the subring $K[T] \cap \bar{k}[X_1, \ldots, X_r, T]$. Since the polynomial ring A is integrally closed it follows that $K[T] \cap \bar{k}[X_1, \ldots, X_r, T] = A[T]$ (see [22]) and then $F(X_1, \ldots, X_r, T)$ belongs to $A[T]$.

The proposition is completely proved. □

From the proof of Proposition 1 we deduce:

Corollary 2. *Let $f_1, \ldots, f_{n-r}$ be a regular sequence in $k[X_1, \ldots, X_n]$ which generates a radical ideal $\mathfrak{F}$ defining an algebraic variety $V \subset \mathbb{A}_k^n$. Suppose that $X_1, \ldots, X_n$ are in Noether position with respect to $\mathfrak{F}$. Denote by A the ring $k[X_1, \ldots, X_r]$, by K the field of rational functions $k(X_1, \ldots, X_r)$, by B the free A-algebra $k[X_1, \ldots, X_n]/\mathfrak{F}$ and by B' the extended ring $B \otimes_A K$. Let f be an element of the polynomial ring $k[X_1, \ldots, X_n]$, $\bar{f}$ its class in B and let $\eta_f \in \mathrm{End}_K(B')$ be the morphism induced by the multiplication by $\bar{f}$. Then the minimal polynomial of η_f belongs to $A[T]$ and its total degree is bounded by* $\deg(V) \deg f$. □

4 Some Upper Bounds for the Degree of Traces

4.1 Notations and Assumptions

Throughout this section we shall maintain the following notations and assumptions:

- n and r are non-negative integers with $0 \leqq r < n$.
- k is an infinite perfect field and A is the polynomial ring $k[X_1, \ldots, X_r]$.
- $f_1, \ldots, f_{n-r}$ is a polynomial regular sequence contained in $k[X_1, \ldots, X_n]$ which generates an ideal $\mathfrak{F}$. The set of zeros of $\mathfrak{F}$ in $\mathbb{A}_k^n$ is denoted by V and d is an upper bound for the total degrees of the polynomials f_i.
- B denotes the factor ring $k[X_1, \ldots, X_n]/\mathfrak{F}$ and the variables $X_1, \ldots, X_n$ are inNoether position with respect to $\mathfrak{F}$ (i.e. the canonical morphism $A \to B$ is an

integral monomorphism). 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 $\left(\frac{\partial f_j}{\partial X_{r+j}}\right)_{1 \leq j \leq n-r}$ and we assume that $\bar{\Delta}$ is not a zero divisor in B (*therefore the Jacobian criterion implies that $\mathfrak{F}$ is a radical ideal*).
- K denotes the fraction field of A and $B' := B \otimes_A K$. If $\bar{K}$ is an algebraic closure of K we write $\tilde{B} := B' \otimes_K \bar{K}$. Finally $\bar{A}$ and $\bar{B}$ denote the rings $A \otimes_k \bar{k}$ and $B \otimes_k \bar{k}$ respectively.

Let us observe that under these assumptions $\tilde{B}$ is a reduced 0-dimensional $\bar{K}$-algebra.

4.2 *Basic General Trace Theory*

The Definition of the Trace. We consider the ring B as an A-algebra and we denote by B^* the dual space $\mathrm{Hom}_A(B, A)$. The A-module B^* admits a natural structure of B-module in the following way: for any pair (b, β) in $B \times B^*$ the product $b.\beta$ is the A-linear application of B^* defined by $(b.\beta)(x) := \beta(bx)$, for each x in B.

Our assumptions about A and B allow to show that the B-modules B and B^* are isomorphic (see [19, Example F.19 and Corollary F.10]) and therefore B^* can be generated by a single element. A generator σ of B^* is called a *trace* of B over A.

Under our hypothesis we have the additional property that B is a finite free A-module whose rank will be denoted by D. Fix for the moment a basis of this module; each element $b \in B$ defines, by multiplication, a square matrix $M_b \in A^{D \times D}$. If we denote by trace (M_b) the trace of the matrix M_b, the application $b \mapsto \mathrm{trace}(M_b)$ defines (independently of the basis of B) an element of B^* called the *usual trace* and denoted by Tr.

Unfortunately the usual trace is not always a generator of B^* (in other words the usual trace is not necessarily a trace).

The Trace Associated to a Regular Sequence. Let us consider now the tensorial product $B \otimes_A B$. This ring can be considered in a natural way as an A-algebra and as a B-bialgebra (with right and left multiplications).

Let $\mu : B \otimes_A B \to B$ be the morphism of A-algebras (or B-bialgebras) defined by $\mu(b \otimes b') := bb'$. Denote by $\mathscr{K}$ the kernel of μ. It is easy to show that $\mathscr{K}$ is the ideal generated by all the elements $b \otimes 1 - 1 \otimes b$, where b ranges over B (see for example [15, Proposition 1.3]).

From the fact that $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})(b \otimes 1 - 1 \otimes b) = 0$ for all $b \in B$, one infers that the induced structures of right and left B-modules over $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ coincide. In other words, if $\sum_i b_i \otimes b'_i$ belongs to $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ and b is an element of the ring B we have: $\sum_i bb_i \otimes b'_i = \sum_i b_i \otimes bb'_i$. Moreover it is possible to show that $\mathrm{Ann}_{B \otimes_A B}(\mathscr{K})$ is a cyclic B-module ([19, Corollary F.10]).

Let us consider the application $\Phi : B \otimes_A B \to \mathrm{Hom}_A(B^*, B)$ defined by

$$\Phi\left(\sum_i b_i \otimes b'_i\right)(\beta) := \sum_i b_i \beta(b'_i),$$

where $b_i, b'_i \in B$ and $\beta \in B^*$.

From the freeness of B it is easy to see that Φ is an isomorphism and the image of $\mathrm{Ann}_{B\otimes_A B}(\mathscr{K})$ by Φ is exactly $\mathrm{Hom}_B(B^*, B)$.

For each generator $\Gamma := \Sigma_m b_m \otimes b'_m$ of the B-module $\mathrm{Ann}_{B\otimes_A B}(\mathscr{K})$ the element $\Phi(\Gamma)$ is a generator of $\mathrm{Hom}_B(B^*, B)$ and then there exists a uniquely determinated $\sigma_\Gamma \in B^*$ such that $\Phi(\Gamma)(\sigma_\Gamma) = 1$. One deduces immediately that σ_Γ is a trace for B (which is called the *trace associated to* Γ).

From the definitions of Φ, Γ and σ_Γ we have the following "*trace formula*" for all $b \in B$:

$$b = \sum_{1 \leqq m \leqq M} \sigma_\Gamma(b\, b'_m) b_m. \tag{2}$$

In particular we observe that $b_1, \ldots, b_M$ is a system of generators of the A-module B. By means of the element Γ it is possible to obtain a relation between the trace σ_Γ and the "usual trace" Tr; more precisely (see [19, Corollary F.12]):

$$\mu(\Gamma) \cdot \sigma_\Gamma = \mathrm{Tr} \tag{3}$$

In terms of elements of B this formula says that for all $b \in B$ the equality $\sigma_\Gamma(\mu(\Gamma) b) = \mathrm{Tr}(b)$ holds.

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:

$$B \otimes_A B \cong A[X_{r+1}, \ldots, X_n, Y_{r+1}, \ldots, Y_n]/(f_1, \ldots, f_{n-r}, f_1^{(Y)}, \ldots, f_{n-r}^{(Y)}). \tag{4}$$

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 $(n-r)d$. Following [19, 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 (4).

In other words we have (see also [11, §3.4]):

Proposition 3. *There exist polynomials a_m, c_m in $k[X_1, \ldots, X_n]$ satisfying* $\deg(a_m) + \deg(c_m) \leqq (n-r)d$ $(1 \leqq m \leqq M)$ *such that* $\sum_m \bar{a}_m \otimes \bar{c}_m$ *is a generator of* $\mathrm{Ann}_{B\otimes_A B}(\mathscr{K})$ *and* $\Delta = \sum_m \bar{a}_m \bar{c}_m$. □

Definition 4. The trace associated to the generator of $\mathrm{Ann}_{B\otimes_A B}(\mathscr{K})$ introduced in Proposition 3 will be called *the trace associated to the regular sequence* $f_1, \ldots, f_{n-r}$ and we will denote it by σ_Δ.

Let us observe that in this case the relation (3) gives

$$\bar{\Delta} \cdot \sigma_\Delta = \mathrm{Tr}. \tag{5}$$

4.3 Upper Bounds for the Degree of Traces

This paragraph is enterely devoted to give some bounds for the degrees of traces associated to the extension $A \subset_{\to} B$.

Let $\mathfrak{F}^e$ be the extended ideal $\mathfrak{F}\bar{K}[X_{r+1},\ldots,X_n]$; our assumptions on Δ guarantee that $\mathfrak{F}^e$ is a radical 0-dimensional ideal (see [21, Ch. 10]). The rank of the A-module B (denoted by D) is the dimension of the $\bar{K}$-vector space $\tilde{B} = \bar{K}[X_{r+1},\ldots,X_n]/\mathfrak{F}^e$ and therefore it is also the cardinality of the set $\{p \in \bar{K}^{n-r};\ f_1(X_1,\ldots,X_r,p) = \cdots = f_{n-r}(X_1,\ldots,X_r,p) = 0\}$ (the set of zeros of $\mathfrak{F}^e$).

Let $p^1,\ldots,p^D$ be the different zeros of $\mathfrak{F}^e$ in $\bar{K}^{n-r}$ and for each point p^i, $1 \leqq i \leqq D$, write $(p^i_1,\ldots,p^i_{n-r})$ for its coordinates in $\bar{K}^{n-r}$.

Definition. Let g be an element of $\bar{K}[X_{r+1},\ldots,X_n]$, we say that g *distinguishes* (or *separates*) the points p^i, $1 \leqq i \leqq D$, if for each pair of different points p^i, p^j the values $g(p^i)$ and $g(p^j)$ are different too.

Notations. For any polynomial $g \in \bar{K}[X_{r+1},\ldots,X_n]$ we write m_g and $\mathscr{X}_g$ for the minimal and the characteristic polynomial of the endomorphism $\eta_g \in \mathrm{End}_{\bar{K}}(\tilde{B})$ respectively (we recall that η_g is the morphism induced by the multiplication by $\bar{g}$). Let us observe that if $g \in k[X_1,\ldots,X_n]$ then m_g and $\mathscr{X}_g$ are univariate polynomials with coefficients in A.

Proposition 5. *Let g be an element of the ring $\bar{K}[X_{r+1},\ldots,X_n]$ which distinguishes the zeros of $\mathfrak{F}^e$. Then $m_g = \mathscr{X}_g$.*

Proof. Let $m_g := T^s + \alpha_{s-1}T^{s-1} + \cdots + \alpha_0 \in \bar{K}[T]$ be the minimal polynomial of η_g. It suffices to show that we have $s \geqq D$ (recall that D is the dimension of the $\bar{K}$-vector space $\tilde{B}$ and therefore the degree of the characteristic polynomial of $\eta_{\bar{g}}$).

The equality $m_g(\eta_g) = 0$ in $\mathrm{End}_{\bar{K}}(\tilde{B})$ says that the element $m_g(\bar{g})$ of the ring $\tilde{B}$ is 0. In other words the polynomial $m_g(g) \in \bar{K}[X_{r+1},\ldots,X_n]$ belongs to the extended ideal $\mathfrak{F}^e$ and then $m_g(g(p^i)) = 0$ for all $1 \leqq i \leqq D$. Thus the fact that g distinguishes the points p^i implies that $g(p^1),\ldots,g(p^D)$ are different roots of the univariate polynomial m_g. In particular we have the inequality $D \leqq s$. □

Combining Proposition 5 and Corollary 2 we obtain:

Corollary 6. *Let g be a polynomial in $k[X_1,\ldots,X_n]$ which distinguishes the zeros of the ideal $\mathfrak{F}^e \subset \bar{K}[X_{r+1},\ldots,X_n]$. Then the total degree of $\mathscr{X}_g$ is bounded by* $\deg(V)\deg g$. □

Remark. In [13, Lemma 3.3.3] the general bound $\deg \mathscr{X}_g \leqq r\deg(V)^2 \deg g$ is obtained without additional hypothesis on g.

The following proposition allows to modify non zero divisors of B by means of a generic linear form in order to obtain "separability properties" with respect to the zeros of the ideal $\mathfrak{F}^e$.

Proposition 7. *Let $g \in k[X_1,\ldots,X_n]$ such that its class $\bar{g}$ in B is not a zero divisor. Then there exists a non-empty Zariski open set $U \subset k^{n-r+1}$ (depending on g) such that for all $\beta := (\beta_1,\ldots,\beta_{n-r+1}) \in U$ the induced linear affine form $\ell_\beta := \beta_1 X_{r+1} + \cdots + \beta_{n-r}X_n + \beta_{n-r+1} \in k[X_{r+1},\ldots,X_n]$ verifies that $\ell_\beta g$ distinguishes the zeros of $\mathfrak{F}^e$.*

Proof. Fix i, j, with $1 \leqq i < j \leqq D$, and let us consider the following linear homogeneous equation in the variables $\beta_1, \ldots, \beta_{n-r+1}$ with coefficients in $\bar{K}$:

$$(\beta_1 p_1^i + \cdots + \beta_{n-r} p_{n-r}^i + \beta_{n-r+1}) g(p^i) - (\beta_1 p_1^j + \cdots + \beta_{n-r} p_{n-r}^j + \beta_{n-r+1}) g(p^j) = 0 \tag{6}$$

Since $\bar{g}$ is not a zero divisor in B one deduces that $g(p^i) \neq 0$ for all $1 \leqq i \leqq D$. Hence, taking also into account that the points p^i and p^j are different we deduce that the linear homogeneous equation (6) defines an hyperplane H_{ij} of $\bar{K}^{n-r+1}$. The intersection of this hyperplane with the affine space k^{n-r+1} determines a proper linear subspace of k^{n-r+1}. We define the set $U \subseteqq k^{n-r+1}$ as follows:

$$U := k^{n-r+1} \setminus \bigcup_{i,j} (H_{ij} \cap k^{n-r+1}).$$

Since k is an infinite field one infers that the set U is non-empty and its definition guarantees that for any β in U the corresponding polynomial $\ell_\beta g$ distinguishes the zeros of the ideal $\mathfrak{F}^e$. □

Corollary 8. *Let* $g \in k[X_1, \ldots, X_n]$. *Then* $\deg(\det(\eta_g)) \leqq \deg(V)(1 + \deg g)$.

Proof. The statement is obvious if g is a zero divisor. If this is not the case, following Proposition 7 let $\ell_\beta \in k[X_{r+1}, \ldots, X_n]$ be a linear form such that the morphism $\eta_{\ell_\beta g}$ distinguishes the zeros of $\mathfrak{F}^e$. Therefore Corollary 6 implies that the total degree of the characteristic polynomial of $\eta_{\ell_\beta g}$ is bounded by $\deg(V)\deg(\ell_\beta g) = \deg(V)(1 + \deg g)$. The claimed upper bound is clear from the equality $\det(\eta_{\ell_\beta g}) = \det(\eta_{\ell_\beta})\det(\eta_g)$. □

Notation Let g be a polynomial in $k[X_1, \ldots, X_n]$ such that its class $\bar{g} \in B$ is not a zero divisor (in particular $\det(\eta_g)$ is a non-zero element of the ring A) and let $\mathscr{X}_g = T^s + \alpha_{s-1} T^{s-1} + \cdots + \alpha_0 \in A[T]$ be the characteristic polynomial of the morphism η_g. We define a new polynomial $g^* \in k[X_1, \ldots, X_n]$ which depends on g in the following way:

$$g^* := g^{s-1} + \alpha_{s-1} g^{s-2} + \cdots + \alpha_2 g + \alpha_1. \tag{7}$$

Observe that $g g^* + \alpha_0 = \mathscr{X}_g(g)$ is an element of the ideal $\mathfrak{F}$.

With these notations we have the following key lemma:

Lemma 9. *Let* f *and* g *be two polynomials in* $k[X_1, \ldots, X_n]$ *such that* $\bar{g} \in B$ *is not a zero divisor. Then we have the inequality*:

$$\deg \mathrm{Tr}(\overline{g^* f}) \leqq \deg(V)(1 + \max\{\deg f, \deg g\}).$$

Proof. Let $a_0 := (-1)^{D+1} \det(\eta_{\bar{g}})$; from (7) we have $\bar{g}\overline{g^*} = a_0$.

Let T be a new indeterminate and let $\mathscr{X}_{g^* f} = T^D + b_{D-1} T^{D-1} + \cdots + b_1 T + b_0 \in A[T]$ be the characteristic polynomial of the morphism $\eta_{g^* f}$ considered as an element in $\mathrm{End}_K(B')$. Observe that $\mathrm{Tr}(\overline{g^* f}) = -b_{D-1}$.

Fix for the moment an arbitrary element λ of the base field k.

The polynomial $\mathscr{X}_{g^* f}(\lambda a_0)$ is an element of the polynomial ring A (because $\mathscr{X}_{g^* f}$ belongs to $A[T]$ and $\lambda a_0 \in A$).

Set $Q_\lambda := \det(\lambda\eta_g - \eta_f)$. Therefore we have the following equalities in the ring A:

$$\begin{aligned}\mathscr{X}_{g^*f}(\lambda a_0) &= \det(\lambda a_0 \mathrm{Id} - \eta_{g^*f}) = \det(\lambda\eta_{g^*g} - \eta_{g^*f}) = \\ &= \det(\eta_{g^*})\det(\lambda\eta_g - \eta_f) = \det(\eta_{g^*})Q_\lambda \end{aligned} \tag{8}$$

Now let $\lambda_1, \ldots, \lambda_{D+1}$ be different elements of the infinite field k.

The relation (8) implies that the coefficients $b_{D-1}, \ldots, b_1, b_0$ satisfy the following $(D+1)\times(D+1)$ linear system:

$$\begin{pmatrix} 1 & \lambda_1 a_0 & \cdots & (\lambda_1 a_0)^D \\ 1 & \lambda_2 a_0 & \cdots & (\lambda_2 a_0)^D \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \lambda_{D+1} a_0 & \cdots & (\lambda_{D+1} a_0)^D \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} \det(\eta_{g^*})Q_{\lambda_1} \\ \det(\eta_{g^*})Q_{\lambda_2} \\ \vdots \\ \det(\eta_{g^*})Q_{\lambda_{D+1}} \end{pmatrix}.$$

If we denote by $M \in A^{(D+1)\times(D+1)}$ the matrix of this linear system we have that $\det(M) = a_0^{D(D+1)/2}\prod_{i>j}(\lambda_i - \lambda_j)$ and by Cramer's rule one obtains

$$\det(M) b_{D-1} = \det(C),$$

where $C \in A^{(D+1)\times(D+1)}$ is the following matrix:

$$\begin{pmatrix} 1 & \lambda_1 a_0 & \cdots & (\lambda_1 a_0)^{D-2} & \det(\eta_{g^*})Q_{\lambda_1} & (\lambda_1 a_0)^D \\ 1 & \lambda_2 a_0 & \cdots & (\lambda_2 a_0)^{D-2} & \det(\eta_{g^*})Q_{\lambda_2} & (\lambda_2 a_0)^D \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \lambda_{D+1} a_0 & \cdots & (\lambda_{D+1} a_0)^{D-2} & \det(\eta_{g^*})Q_{\lambda_{D+1}} & (\lambda_{D+1} a_0)^D \end{pmatrix}.$$

Thus

$$\begin{aligned} & b_{D-1} a_0^{D(D+1)/2} \prod_{i>j}(\lambda_i - \lambda_j) = \\ & = a_0^{(D(D-1)/2)+1} \det(\eta_{g^*}) \det \begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{D-2} & Q_{\lambda_1} & \lambda_1^D \\ 1 & \lambda_2 & \cdots & \lambda_2^{D-2} & Q_{\lambda_2} & \lambda_2^D \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \lambda_{D+1} & \cdots & \lambda_{D+1}^{D-2} & Q_{\lambda_{D+1}} & \lambda_{D+1}^D \end{pmatrix}. \end{aligned}$$

Taking into account that $\det(\eta_{g^*}) = (-a_0)^{D-1}$ we have:

$$b_{D-1}\prod_{i>j}(\lambda_i - \lambda_j) = (-1)^{D-1}\det \begin{pmatrix} 1 & \lambda_1 & \cdots & \lambda_1^{D-2} & Q_{\lambda_1} & \lambda_1^D \\ 1 & \lambda_2 & \cdots & \lambda_2^{D-2} & Q_{\lambda_2} & \lambda_2^D \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & \lambda_{D+1} & \cdots & \lambda_{D+1}^{D-2} & Q_{\lambda_{D+1}} & \lambda_{D+1}^D \end{pmatrix} \tag{9}$$

This equality implies the estimation:

$$\deg \mathrm{Tr}(\overline{g^* f}) = \deg b_{D-1} \leqq \max_i \{\deg Q_{\lambda_i}\} = \max_i \{\deg(\det(\lambda_i\eta_g - \eta_f))\}.$$

Fix an index i, $1 \leqq i \leqq D+1$. Corollary 8 implies that the following inequality is satisfied:

$$\deg Q_{\lambda_i} = \deg(\det(\lambda_i\eta_g - \eta_f)) \leqq \deg(V)(1 + \max\{\deg f, \deg g\}).$$

Taking into account this inequality, from (9) one obtains:

$$\deg \mathrm{Tr}(\overline{g^*}\bar{f}) = \deg b_{D-1} \leqq \max_i \{\deg Q_{\lambda_i}\} \leqq \deg(V)(1 + \max\{\deg f, \deg g\})$$

and this concludes the proof of the lemma. □

This lemma allows us to estimate an upper bound for a trace associated to the sequence $f_1, \ldots, f_{n-r}$ (see Definition 4):

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:*

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

In particular for any polynomial $f \in k[X_1, \ldots, X_n]$ we have:

$$\deg \sigma_\Delta(\bar{f}) \leqq \deg(V)(1 + \max\{\deg f, (n-r)d\}).$$

Proof. Since $\bar{\Delta}$ is not a zero divisor in B (assumptions 4.1), from (5) and (7) we deduce the relation in B^*:

$$(\overline{\Delta^*}\bar{\Delta})\cdot\sigma_\Delta = \overline{\Delta^*}\cdot\mathrm{Tr}$$

Specializing this formula in $\overline{g^*}\bar{f} \in B$ one obtains:

$$\sigma_\Delta(\overline{\Delta^*}\bar{\Delta}\overline{g^*}\bar{f}) = \mathrm{Tr}(\overline{\Delta^* g^*}\bar{f}).$$

By (7) we have that $\overline{\Delta^*}\bar{\Delta}$ belongs to the ring A and then the previous formula can be rewritten as the following equality in the ring A:

$$\overline{\Delta^*}\bar{\Delta}\sigma_\Delta(\overline{g^*}\bar{f}) = \mathrm{Tr}(\overline{\Delta^* g^*}\bar{f}).$$

In particular we obtain the inequality

$$\deg \sigma_\Delta(\overline{g^*}\bar{f}) \leqq \deg \mathrm{Tr}(\overline{\Delta^* g^*}\bar{f}).$$

Taking into account that $\overline{\Delta^*}\,\overline{g^*} = (-1)^{D+1}\overline{(\Delta g)^*}$ and applying Proposition 3 and Lemma 9 we conclude that

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

and the theorem is proved. □

Remark 11. Combining Theorem 10 and Bezout Inequality we obtain:

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

Remark 12. In [8, Lemma 5.1] a different approach based essentially in theory of residues allows to obtain the inequality

$$\deg \sigma_\Delta(\bar{f}) \leqq \deg f + (n-r)d^n(1 + d^{n-r}). \tag{10}$$

Their method requires that the (dependent) variables $X_{r+1}, \ldots, X_n$ verify *semimonical* integral equations (i.e. for each j, $r+1 \leqq j \leqq n$, there exists $h_j \in A[X_j] \cap \mathfrak{F}$ non zero

such that $\deg_{X_j} h_j = \deg h_j$), it uses strongly the effective Nullstellensatz of [18] or [10] and is proved only for fields of characteristic zero. But on the other hand our assumption about the Jacobian doesn't appear.

Let us observe the different nature of this bound with respect to the result of the previous remark: in (10) the degree of the polynomial f appears in an additive form and the remaining part is essentially of order d^{2n} while our bound (Remark 11) is multiplicative in $\deg f$ but the exponent of d is $n-r+1$. Nevertheless our method is also adaptable in order to obtain an upper bound of the same kind: if, like in [8], we assume the existence of semimonical integral equations it is easy to show that every polynomial $f \in k[X_1, \ldots, X_n]$ can be represented modulo $\mathfrak{F}$ by a polynomial f' such that $\deg_{X_1,\ldots,X_r} f' \leqq \deg f$ and $\deg_{X_{r+1},\ldots,X_n} f' \leqq \deg(V)$; therefore using the A-linearity of σ_Δ one obtains:

$$\deg \sigma_\Delta(\bar{f}) = \deg \sigma_\Delta(\bar{f}') \leqq \deg f + \deg(V)(1 + \deg(V)) \leqq \deg f + d^{n-r}(1 + d^{n-r}).$$

The assumption on semimonical integral equations is unavoidable (see Remark 14 below).

Lemma 9 provides also an upper bound for the usual trace: taking the constant 1 as the polynomial g we have $\deg \mathrm{Tr}(\bar{f}) \leqq \deg(V)(1 + \deg f)$. Nevertheless a somewhat more precise upper bound is easily obtainable from Corollary 2 (see also [13, Lemma 3.3.3]).

Theorem 13. *Let f be a polynomial in $k[X_1, \ldots, X_n]$ and let $\bar{f}$ be its class in the ring B. Then* $\deg \mathrm{Tr}(\bar{f}) \leqq \deg(V) \deg f$. *In particular* $\deg \mathrm{Tr}(\bar{f}) \leqq d^{n-r} \deg f$.

Proof. Let $m_f = T^s + a_{s-1} T^{s-1} + \cdots + a_0 \in A[T]$ be the minimal polynomial of the morphism $\eta_f \in \mathrm{End}_K(B')$. In virtue of Corollary 2 the total degree of m_f is bounded by $\deg(V) \deg f$.

Let $m_f = \prod_{1 \leqq j \leqq J} Q_j$ be the decomposition of m_f in irreducible factors on $K[T]$. By Gauss Lemma one deduces that all the polynomials Q_j are monic and their coefficients are elements of the ring A of degrees bounded by $\deg(V) \deg f$.

For each index j, $1 \leqq j \leqq J$, denote by d_j the degree of Q_j and by β_j the coefficient of the monomial $T^{d_j - 1}$ in Q_j (in particular $\deg \beta_j \leqq \deg(V) \deg f$).

Let $\mathscr{X}_f = T^D + b_{D-1} T^{D-1} + \cdots + b_0$ be the characteristic polynomial of η_f. Therefore $\mathscr{X}_f = m_f \prod_j Q_j^{e_j}$ where $e_1, \ldots, e_J$ are non-negative integers.

By comparison of coefficients one deduces:

$$-\mathrm{Tr}(\bar{f}) = b_{D-1} = a_{s-1} + \sum_{\{j; e_j \neq 0\}} (e_j - 1)\beta_j.$$

Therefore $\deg \mathrm{Tr}(\bar{f}) \leqq \deg(V) \deg f$. □

Remark 14. The following very simple example shows that the upper bound of Theorem 13 is optimal: let $d \in \mathbb{N}$, $A := \mathbb{C}[X]$, $B := \mathbb{C}[X, Y]/(Y - X^d)$. Then $\mathrm{Tr}(\bar{Y}^t) = \mathrm{Tr}(X^{dt}) = X^{dt}$.

5 On Effective Nullstellensätze

In this section we apply the inequalities obtained in the previous paragraph in order to prove a quantitative version of the Hilbert Nullstellensatz.

5.1 The Complete Intersection Case

5.1.1 Assumptions. We follow essentially the notations introduced in Sect. 4. We denote by k an arbitrary field; since the statement of effective Nullstellensätze doesn't depend on algebraic extensions of k, we may however suppose without loss of generality that k is algebraically closed.

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 $\mathfrak{F}_j$ be the ideal generated by $f_1, \ldots, f_{n-j}$, $A_j := k[X_1, \ldots, X_j]$ and $B_j := k[X_1, \ldots, X_n]/\mathfrak{F}_j$. Suppose that the canonical morphism $A_j \to B_j$ is an integral monomorphism and that the 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 4.2 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 3. Its associated trace will be denoted by σ_j.

5.1.2 A Division Lemma. Under the previous assumptions we have the following division lemma (see [18, 7, 3, 26] for more precise bounds):

Lemma 15. *Let f be a polynomial in the ideal $\mathfrak{F}_r$. Then there exist polynomials $p_1, \ldots, p_{n-r}$ in $k[X_1, \ldots, X_n]$ such that:*

- $f = \sum_{i=1}^{n-r} p_i f_i$
- $\deg p_i \leqq d^{n-r}(3n-3r-2) + d^{n-r-1} \max\{\deg f, d\} \quad (1 \leqq i \leqq n-r)$.

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 $\mathfrak{F}_{j+1}$ (where $\mathfrak{F}_n$ 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 3 and $\alpha_m^{(j+1)}$ are polynomials in the ring A_{j+1} which degrees are uniformly bounded by a constant δ_j defined by:

$$d^{n-r}(n-r-1) + d^{n-r-1} \max\{\deg f, d\} + \sum_{1 \leqq s \leqq j-r} d^{n-r-s}(2(n-r-s)+1) + d^{n-j-1} \tag{11}$$

We start the recursive procedure at $j = r$.

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

$$f \equiv h f_{n-r} \mod \mathfrak{F}_{r+1}. \tag{12}$$

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 (2) implies that $p_{n-r} - h$ belongs to $\mathfrak{F}_{r+1}$. So p_{n-r} satisfies (I).

The element $\bar{f}_{n-r}$ is not a zero divisor in the ring B_{r+1} so, following (7), we can define the polynomials $f^*_{n-r} \in k[X_1, \ldots, X_n]$ and $\alpha \in A_{r+1}$ in such a way that $f^*_{n-r} f_{n-r} - \alpha$ is an element of the ideal $\mathfrak{F}_{r+1}$. Multiplying the equality (12) by f^*_{n-r} we obtain:

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

Thus the polynomial identity

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

holds.

Observe that α divides the polynomials $\sigma_{r+1}(\bar{f}^*_{n-r} \bar{f} \bar{c}^{(r+1)}_m)$ whose degrees are uniformly bounded by $d^{n-r-1}(1+(n-r-1)d + \max\{\deg f, d\}) = \delta_r$ (see Remark 11). Therefore defining

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

property (II) holds.

Let now j, $r \leqq j < n-1$, be an index such that there exist polynomials $p_{n-r}, \ldots, p_{n-j}$ satisfying conditions (I) and (II). We are going to repeat *mutatis mutandis* the same procedure used in the case $j = r$.

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

$$g \equiv h f_{n-j-1} \mod \mathfrak{F}_{j+2}. \tag{13}$$

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

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

The trace formula (2) implies that $p_{n-j-1} - h$ belongs to $\mathfrak{F}_{j+2}$. So condition (I) is verified. Following (7) let us consider the polynomials $f^*_{n-j-1} \in k[X_1, \ldots, X_n]$ and $\alpha \in A_{j+2}$ such that $f^*_{n-j-1} f_{n-j-1} - \alpha \in \mathfrak{F}_{j+2}$.

From (13) we obtain:

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

Therefore

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

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

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

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

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

From the definition of the polynomial g we have:

$$\deg \sigma_{j+2}(\bar{f}^*_{n-j-1}\bar{g}\bar{c}^{(j+2)}_m) = \deg \sigma_{j+2}\left(\bar{f}^*_{n-j-1}\bar{f}\bar{c}^{(j+2)}_m - \sum_{l=r}^{j} \bar{f}^*_{n-j-1}\bar{p}_{n-l}\bar{f}_{n-l}\bar{c}^{(j+2)}_m\right)$$

$$\leqq \max\left\{\deg \sigma_{j+2}(\bar{f}^*_{n-j-1}\bar{f}\bar{c}^{(j+2)}_m), \deg \sigma_{j+2}\left(\sum_{l=r}^{j} \bar{f}^*_{n-j-1}\bar{p}_{n-l}\bar{f}_{n-l}\bar{c}^{(j+2)}_m\right)\right\} \tag{14}$$

Remark 11 implies:

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

In order to bound the remainder part of (14), we use condition (II) to replace each polynomial p_{n-l}, $r \leqq l \leqq j$:

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

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

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

From Remark 11 and condition (II) for l we deduce:

$$\deg \alpha^{(l+1)}_{m'} + \deg \sigma_{j+2}(\bar{f}^*_{n-j-1}\bar{a}^{(l+1)}_{m'}\bar{f}_{n-l}\bar{c}^{(j+2)}_m) \leqq \delta_l + d^{n-j-2}(1+(2n-l-j-2)d).$$

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

$$\max\left\{d^{n-j-2}(1+(n-j-2)d + \max\{d, \deg f\}),\right.$$

$$\left.\max_{r\leqq l\leqq j}\{\delta_l + d^{n-j-2}(1+(2n-l-j-2)d)\}\right\}.$$

From the definition of δ_j (11) it is clear that:

$$d^{n-j-2}(1+(n-j-2)d + \max\{d, \deg f\}) \leqq \delta_j.$$

Then

$$\deg \alpha^{(j+2)}_m \leqq \max_{r\leqq l\leqq j}\{\delta_l + d^{n-j-2}(1+(2n-l-j-2)d)\}. \tag{15}$$

On the other hand a simple computation shows that:

$$\delta_{l+1} = \delta_l + 2d^{n-l-1}(n-l-1) + d^{n-l-2} \tag{16}$$

and therefore

$$\delta_l + d^{n-j-2}(1+(2n-l-j-2)d) \leqq \delta_l + d^{n-l-2}(1+2(n-l-1)d) = \delta_{l+1}.$$

Replacing in (15) we conclude:

$$\deg \alpha_m^{(j+2)} \leqq \max_{r \leqq l \leqq j} \{\delta_{l+1}\} = \delta_{j+1}.$$

Thus, this recursive method produces polynomials $p_1, \ldots, p_{n-r}$ in $k[X_1, \ldots, X_n]$ which verify:

- $f = \sum_{i=1}^{n-r} p_i f_i$
- for every index i, $1 \leqq i \leqq n-r$, the inequality $\deg p_i \leqq \delta_{n-i} + (i-1)d \leqq \delta_{n-1}$ holds (see condition (II) and (16)).

In order to finish the proof of the lemma it suffices to estimate an upper bound for δ_{n-1}:

$$\begin{aligned}
\delta_{n-1} &= d^{n-r}(n-r-1) + d^{n-r-1} \max\{\deg f, d\} \\
&\quad + \sum_{1 \leqq s \leqq n-1-r} d^{n-r-s}(2(n-r-s)+1) + 1 \\
&= d^{n-r}(n-r-1) + d^{n-r-1} \max\{\deg f, d\} + \sum_{1 \leqq s \leqq n-r} d^{n-r-s}(2(n-r-s)+1) \\
&\leqq d^{n-r}(n-r-1) + d^{n-r-1} \max\{\deg f, d\} + (2(n-r)-1) \sum_{1 \leqq s \leqq n-r} d^{n-r-s} \\
&\leqq d^{n-r}(n-r-1) + d^{n-r-1} \max\{\deg f, d\} + (2(n-r)-1)(d^{n-r}-1) \\
&\leqq d^{n-r}(3n-3r-2) + d^{n-r-1} \max\{\deg f, d\}.
\end{aligned}$$

Thus the lemma follows. □

Now we are able to prove the following particular quantitative version of the Nullstellensatz:

Lemma 16. *Let $s \in \mathbb{N}$, $0 \leqq s \leqq n+1$, $f_1, \ldots, f_s$ be polynomials in $k[X_1, \ldots, X_n]$ such that $f_1, \ldots, f_{s-1}$ verify the assumptions 5.1.1 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 there exist polynomials $p_1, \ldots, p_s$ in $k[X_1, \ldots, X_n]$ verifying:*

- $1 = \sum_{i=1}^{s} p_i f_i$
- $\deg p_i \leqq 4nd^n$ $(1 \leqq i \leqq s)$.

Proof. First suppose $s < n+1$. Taking into account that in the first step of the proof of Lemma 15 we didn't use the fact that the ideal is generated by a regular sequence we obtain $1 = \sum_j p_j f_j$ where $\deg p_j \leqq 3sd^s \leqq 4nd^n (1 \leqq j \leqq s)$.

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

Formula (2) and Proposition 3 in the case $A = k$ and $B = k[X_1, \ldots, X_n]/\mathfrak{F}_0$ imply that there exist polynomials $a_m \in k[X_1, \ldots, X_n]$ $(1 \leqq m \leqq M)$ with degrees bounded by nd such that for any polynomial g one can find $\lambda_1, \ldots, \lambda_M$ in the field

k satisfying:

$$g - \sum_{m=1}^{M} \lambda_m a_m \in \mathfrak{F}_0.$$

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

Finally applying Lemma 15 to the polynomial $f := 1 - p_{n+1} f_{n+1}$ which belongs to the ideal $\mathfrak{F}_0$ and has degree bounded by $(n+1)d$ we obtain polynomials $p_1, \ldots, p_n$ such that:

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

$$-\deg p_i \leqq d^n(3n-2) + d^{n-1}(n+1)d \leqq 4nd^n. \qquad \square$$

5.2 *The General Case*

Now our goal is to obtain an effective Nullstellensatz in a general context. For this purpose we repeat the arguments applied in [13] in order to prepare our list of input polynomials.

Let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ such that $1 \in (f_1, \ldots, f_s)$ and let $d := \max_j \{\deg f_j\}$. Set $\rho := (n+1)s$. We consider the family of polynomials

$$g_1 := f_1, \ldots, g_s := f_s, g_{s+1} := x_1 f_1, \ldots, g_{s+n} := x_n f_1, \ldots, g_{(n+1)s-n+1}$$
$$:= x_1 f_s, \ldots, g_\rho = g_{(n+1)s} := x_n f_s.$$

Let us observe that the degrees of $g_1, \ldots, g_\rho$ are bounded by $d+1$ and that $g_1, \ldots, g_\rho$ generate the trivial ideal of $k[X_1, \ldots, X_n]$.

For any index j, $1 \leqq j \leqq s$, let $U_j := \{x \in \mathbb{A}_k^n; f_j(x) \neq 0\}$ and let $\Psi_j : U_j \to \mathbb{A}_k^{\rho-1}$ be the morphism of affine varieties defined by

$$\Psi_j(x) := \left(\frac{g_1(x)}{f_j(x)}, \ldots, \frac{g_{j-1}(x)}{f_j(x)}, \frac{g_{j+1}(x)}{f_j(x)}, \ldots, \frac{g_\rho(x)}{f_j(x)} \right)$$

for $x \in U_j$.

By construction, Ψ_j is unramified (the associated ring morphism is a localization inclusion, see [15, Ch. I, 2.2.i]) and the Zariski closure of its image is an irreducible subvariety of $\mathbb{A}_k^{\rho-1}$ of dimension n. The finite family $(U_j)_{1 \leqq j \leqq s}$ forms an open covering of $\mathbb{A}_k^n$. Let $f'_1, \ldots, f'_{n+1}$ be a family of generic k-linear combinations of $g_1, \ldots, g_\rho$. The degrees of the polynomials $f'_1, \ldots, f'_{n+1}$ are bounded by $d+1$ and they generate the trivial ideal of $k[X_1, \ldots, X_n]$.

Now fix r, $0 \leqq r \leqq n-1$. We analyze the ideal $(f'_1, \ldots, f'_{n-r})$ by means of Bertini's theorem and the geometric properties of the morphism Ψ_j, $1 \leqq j \leqq s$.

Let us for the moment fix j, $1 \leqq j \leqq s$. First observe that for each t, $1 \leqq t \leqq n+1$, the rational function $\frac{f'_t}{f_j}$ is a generic affine k-linear combination of $\frac{g_1}{f_j}, \ldots, \frac{g_{j-1}}{f_j}$, $\frac{g_{j+1}}{f_j}, \ldots, \frac{g_\rho}{f_j}$. We use Bertini's Theorem in the version of Jouanolou [16, Corollaire 6.7]. Applied to our context it has the following form: the fact that Ψ_j is an

unramified morphism from the irreducible smooth affine variety U_j to the affine space $\mathbb{A}_k^{\rho-1}$ having an n-dimensional image and being defined by the rational functions $\frac{g_1}{f_j},\ldots,\frac{g_{j-1}}{f_j},\frac{g_{j+1}}{f_j},\ldots,\frac{g_\rho}{f_j}$ implies that any set of at most n generic affine linear combinations of $\frac{g_1}{f_j},\ldots,\frac{g_{j-1}}{f_j},\frac{g_{j+1}}{f_j},\ldots,\frac{g_\rho}{f_j}$ defines a (nonempty) smooth affine subvariety of U_j and generates a (proper) radical ideal of the fraction ring $k[X_1,\ldots,X_n]_{f_j}$. Thus the rational functions $\frac{f'_1}{f_j},\ldots,\frac{f'_{n-r}}{f_j}$ define a smooth subvariety of U_j of dimension r and generate a radical ideal of $k[X_1,\ldots,X_n]_{f_j}$. (In fact the variety is irreducible and the ideal is prime for $1\leqq r\leqq n-1$.)

Since the U_j, for $1\leqq j\leqq s$, form an open covering of $\mathbb{A}_k^n$ we conclude that the subvariety of $\mathbb{A}_k^n$ defined by $f'_1,\ldots,f'_{n-r}$ is smooth and of dimension r, and that the ideal $(f'_1,\ldots,f'_{n-r})$ is radical for every $0\leqq r\leqq n-1$. (We call an eventually reducible closed subvariety of $\mathbb{A}_k^n$ smooth if it is equidimensional and all its local rings are regular.) In particular $f'_1,\ldots,f'_n$ form a regular sequence of $k[X_1,\ldots,X_n]$.

From these arguments one deduces that the sequence $f'_1,\ldots,f'_n,f'_{n+1}$ satisfies the assumptions of Lemma 16 (moreover each Jacobian Δ_j is a unit in the corresponding factor ring B_j) and that $\deg f'_j\leqq d+1$ for all j.

Applying now Lemma 16 we obtain:

Theorem 17. *Let $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ be polynomials of degree bounded by d such that $1\in(f_1,\ldots,f_s)$. Then there exist polynomials $p_1,\ldots,p_s\in k[X_1,\ldots,X_n]$ which verify:*

- $1=\sum_{i=1}^{s} p_i f_i$
- $\deg p_i\leqq 4n(d+1)^n$ $(1\leqq i\leqq n+1)$. □

5.2.1 The Case of Characteristic Zero. When the characteristic of the ground field is zero, the unramified condition can be avoided (see [16, Corollaire 6.7]) and the previous argument can be simplified. First we need a well known result concerning generic linear combinations:

Proposition 18. *Let k be an infinite field, $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ be polynomials such that $1\in(f_1,\ldots,f_s)$. Then there exist $t\in\mathbb{N}$, $t\leqq n$, and k-linear combinations $g_1,\ldots,g_{t+1}$ of the polynomials f_i such that:*

- $1\in(g_1,\ldots,g_{t+1})$,
- *$g_1,\ldots,g_{j-1},g_{j+1},\ldots,g_{t+1}$ is a regular sequence, for all index j, $1\leqq j\leqq t+1$.*

Proof. Let t be the minimal integer such that there exist k-linear combinations $f'_1,\ldots,f'_t,f'_{t+1}$ of the polynomials $f_1,\ldots,f_s$ verifying:

- $1\in(f'_1,\ldots,f'_{t+1})$,
- $f'_1,\ldots,f'_t$ is a regular sequence (in particular $t\leqq n$).

It is easy to see that t is positive and well defined (see for example [5, Theorem 14]).

For each vector $\alpha:=(\alpha_1,\ldots,\alpha_t)\in k^t$ we define $g^{(\alpha)}:=\alpha_1 f'_1+\cdots+\alpha_t f'_t+f'_{t+1}$. Clearly $1\in(f'_1,\ldots,f'_t,g^{(\alpha)})$ (there are no common zeros) and $g^{(\alpha)}$ is a linear combination of

$f_1, \ldots, f_s$. It suffices to show that there exists an adequate α such that $f'_1, \ldots, f'_{j-1}$, $f'_{j+1}, \ldots, f'_t, g^{(\alpha)}$ is a regular sequence for all j, $1 \leqq j \leqq t$.

Fix j, $1 \leqq j \leqq t$, and denote by $V^{(\alpha)} \subset \mathbb{A}_k^n$ the variety defined by the polynomials $f'_1, \ldots, f'_{j-1}, f'_{j+1}, \ldots, f'_t, g^{(\alpha)}$.

From the minimality of t we deduce that $V^{(\alpha)} \neq \varnothing$ and since the variety W defined by $f'_1, \ldots, f'_{j-1}, f'_{j+1}, \ldots, f'_t$ is equidimensional (it is defined by a regular sequence) we have:

$$n-(t-1) \leqq \dim V^{(\alpha)} \leqq n-(t-2).$$

If $\dim V^{(\alpha)} = n-(t-1)$ one infers that $f'_1, \ldots, f'_{j-1}, f'_{j+1}, \ldots, f'_t, g^{(\alpha)}$ is a regular sequence. Let $W = C_1 \cup \cdots \cup C_m$ be the decomposition of W in irreducible components. Since $(f'_1, \ldots, f'_t)$ is a regular sequence, for each index i, $1 \leqq i \leqq m$, there exists $x_i \in C_i$ such that $f'_j(x_i) \neq 0$. Now we take the coefficient α_j in the non empty set (we recall that k is infinite):

$$k \setminus \left\{ \frac{-f'_{t+1}(x_i)}{f'_j(x_i)}; \quad 1 \leqq i \leqq m \right\}.$$

In particular we have $g^{(\alpha)}(x_i) \neq 0$ for all i and therefore the strict inequality $\dim V^{(\alpha)} < n-(t-2)$ holds. □

Now we are able to state an effective Nullstellensatz for characteristic zero (see also [4]).

Theorem 19. *Let k be a field of characteristic zero and let $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ be polynomials of degree bounded by d such that $1 \in (f_1, \ldots, f_s)$. Then there exist polynomials $p_1, \ldots, p_s \in k[X_1, \ldots, X_n]$ which verify:*

- $1 = \sum_{i=1}^{s} p_i f_i$
- $\deg p_i \leqq 4nd^n$ $(1 \leqq i \leqq s)$.

Proof. Without loss of generality, by means of generic linear combinations (Proposition 18), we can suppose:

- $s \leqq n+1$,
- $f_1, \ldots, f_{j-1}, f_{j+1}, \ldots, f_s$ is a regular sequence for all j, $1 \leqq j \leqq s$.

We finish the proof applying the same kind of arguments than in the proof of Theorem 17 to the dominant regular morphisms $\Psi'_j \colon U_j \to \mathbb{A}_k^{s-1}$ defined by:

$$\Psi'_j(x) := \left(\frac{f_1(x)}{f_j(x)}, \ldots, \frac{f_{j-1}(x)}{f_j(x)}, \frac{f_{j+1}(x)}{f_j(x)}, \ldots, \frac{f_s(x)}{f_j(x)} \right).$$

Let us observe that, since the characteristic of k is 0, we need no unramified conditions (in particular no variable multiplications) and therefore the degrees don't increase. □

5.3 An Effective Nullstellensatz for Degree 2

In the particular case when all the polynomials are of degree bounded by 2, an adequate version of Bertini's Theorem allows us to obtain the sharper estimation

$\deg p_j \leqq n2^{n+2}$ in Theorem 17 for fields of characteristic distinct from 2. This bound, obtained simultaneously and independently by T. Dubé [9], improves the upper bound 3^n given in [18] and [10].

5.3.1 On Bertini's Theorem for Degree 2. Let us suppose for the moment that k is an algebraically closed field and that are given polynomials $f_1, \ldots, f_s \in k[X_1, \ldots, X_n]$ such that $f_1, \ldots, f_{s-1}$ is a regular sequence and $1 \in (f_1, \ldots, f_s)$.

We denote by R the fraction ring $k[X_1, \ldots, X_n]_{f_s}$, by K its fractions field and by X the affine scheme Spec(R). We consider the (regular and dominant) morphism $\Psi: X \to \mathbb{A}_k^{s-1}$ defined by the rational functions $\psi_1 := f_1/f_s, \ldots, \psi_{s-1} := f_{s-1}/f_s$.

Let $t \in \mathbb{N}$, $1 \leqq t \leqq s-1$, be a fixed integer; denote by $Z^{(t)} \subset X \times (\mathbb{A}_k^s)^t$ the closed subscheme defined by the equations:

$$z_{l0} + \sum_{1 \leqq j \leqq s-1} z_{lj}\psi_j = 0 \quad 1 \leqq l \leqq t,$$

(where (z_{lj}) refers to the coordinates of $(\mathbb{A}_k^s)^t$) and denote by $\pi: Z^{(t)} \to (\mathbb{A}_k^s)^t$ the second projection.

Under these notations we have the following result (see [16, Prop. 6.8] and its proof):

Theorem 20. *The generic fiber of π is geometrically reduced if and only if the differentials $d\psi_1, \ldots, d\psi_{s-1} \in \Omega^1_{K/k}$ generate a K-subspace of dimension at least t (or in terms of Jacobian matrices, the rank of $\left(\frac{\partial \psi_j}{\partial X_i}\right)_{i,j} \in K^{n \times (s-1)}$ is at least t).* □

This theorem allows us to show:

Lemma 21. *Suppose that the characteristic of k is different from 2 and that* $\deg f_j \leqq 2$, *for all $1 \leqq j \leqq s$. Therefore the generic fiber of π is geometrically reduced.*

In order to prove Lemma 21 we need the following intermediate proposition:

Proposition 22. *Let L be an arbitrary field of characteristic different from 2 and let $h_1, \ldots, h_n, h_{n+1} \in L[X_1, \ldots, X_n]$ be polynomials of degree bounded by 2 such that $h_1, \ldots, h_n$ is a regular sequence and $1 \in (h_1, \ldots, h_{n+1})$. Let $J \in L(X_1, \ldots, X_n)^{(n+1)\times(n+1)}$ be the matrix defined by $J_{ij} := \frac{\partial h_j}{\partial X_i}$ $(1 \leqq i \leqq n, 1 \leqq j \leqq n+1)$ and $J_{n+1,j} := h_j$ $(1 \leqq j \leqq n+1)$. Therefore J is invertible.*

Proof. Without loss of generality we may suppose that L is algebraically closed, that $h_i(0) = 0$ for all $1 \leqq i \leqq n$, and that $h_{n+1}(0) \neq 0$. Let $g_1, \ldots, g_{n+1} \in L[X_1, \ldots, X_n, U]$ be defined by the matricial product:

$$(X_1, \ldots, X_n, U)\, J = (g_1, \ldots, g_n, g_{n+1}) \tag{17}$$

If q_i and l_i denote the homogeneous components of h_i of degree 2 and 1 respectively, we have $g_i = 2q_i + l_i + Uh_i$. Hence a simple computation gives for all i, $1 \leqq i \leqq n+1$:

$$g_i = \frac{(U+1)^2}{(U+2)}\left(h_i\left(\frac{U+2}{U+1}X_1, \ldots, \frac{U+2}{U+1}X_n\right) - h_i(0)\right) + Uh_i(0). \tag{18}$$

Let S be the fraction ring $L[X_1, \ldots, X_n, U]_{(U+1)(U+2)}$ and $\mathscr{U} \subset \mathbb{A}_L^{n+1}$ be the Zariski open set defined by S.

We claim that $g_1, \ldots, g_n, g_{n+1}$ is a regular sequence in S.

From (18) it is clear that $g_1, \ldots, g_n$ is a regular sequence (since $U+1$ and $U+2$ are invertible elements of S and $h_i(0)=0$, for $1 \leqq i \leqq n$).

Thus it is enough to show that the algebraic set of $\mathscr{U}$ defined by $g_1, \ldots, g_{n+1}$ is 0-dimensional.

First, let us observe that if a point $(\alpha, v) \in \mathscr{U} \subset \mathbb{A}_L^n \times \mathbb{A}_L^1$ is a common zero of $g_1, \ldots, g_{n+1}$ then the point $\beta_{\alpha,v} := \dfrac{v+2}{v+1}\alpha$ is a common zero of $h_1, \ldots, h_n$ in $\mathbb{A}_L^n$ (in particular there are only finitely many points $\beta_{\alpha,v}$ and they satisfy $h_{n+1}(\beta_{\alpha,v}) \neq 0$).

Now relation (18) for $i = n+1$ implies the equality

$$(v+1)^2(h_{n+1}(\beta_{\alpha,v}) - h_{n+1}(0)) + v(v+2)h_{n+1}(0) = 0$$

or equivalently:

$$h_{n+1}(\beta_{\alpha,v})v^2 + 2h_{n+1}(\beta_{\alpha,v})v + h_{n+1}(\beta_{\alpha,v}) - h_{n+1}(0) = 0.$$

Hence there are finitely many (α, v) and therefore we only need to show that there exists at least one of them.

For this purpose it suffices to verify that for a common zero β of $h_1, \ldots, h_n$, -1 and -2 are not the unique solutions of the (quadratic) equation:

$$h_{n+1}(\beta)v^2 + 2h_{n+1}(\beta)v + h_{n+1}(\beta) - h_{n+1}(0) = 0.$$

Obviously -1 cannot be a solution ($h_{n+1}(0) \neq 0$). If -2 is a double root one infers $2h_{n+1}(\beta) = 0$, which is impossible since $h_{n+1}(\beta) \neq 0$ and char $(L) \neq 2$.

Summarizing, $g_1, \ldots, g_{n+1}$ and $X_1, \ldots, X_n, U$ are two regular sequences in S (recall that U isn't a unit in S because $2 \neq 0$).

Applying the Northcott-Wiebe principle (see for example [19, Corollary E.21]) to (17) we conclude that the ideal $(X_1, \ldots, X_n, U)$ is the ideal quotient

$$\{z \in S;\, z \det(J) \in (g_1, \ldots, g_{n+1})\}.$$

In particular $\det(J) \neq 0$. □

Now we are able to give the proof of Lemma 21.

Proof of Lemma 21. As in the previous Proposition, let $J \in K^{(n+1)\times s}$ be the matrix defined by:

$-J_{ij} := \dfrac{\partial f_j}{\partial X_i}$, $1 \leqq i \leqq n$, $1 \leqq j \leqq s$,

$-J_{n+1,j} := f_j$, $1 \leqq j \leqq s$.

By means of elementary operations on J, it is easy to restate Theorem 20 as follows: *the generic fiber of π is geometrically reduced if and only if the rank of J is at least $t+1$.*

Thus it suffices to prove that J has maximal rank s. For the case $s = n+1$ this is exactly the statement of Proposition 22 (where $L := k$ and $h_j := f_j$).

If $s < n+1$ we can suppose without loss of generality that the variables $X_1, \ldots, X_n$ are in Noether position with respect to the ideal $(f_1, \ldots, f_{s-1})$. Then we apply Proposition 22 to the base field $L := k(X_1, \ldots, X_{n-s+1})$ and the polynomials $f_1, \ldots, f_s$ (considered as elements of $L[X_{n-s+2}, \ldots, X_n]$).

This concludes the proof of Lemma 21. □

Corollary 23. *Let k be an infinite field of characteristic different from 2. Suppose that $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ are polynomials of degree bounded by 2 which verify that $1\in(f_1,\ldots,f_s)$ and that $f_1,\ldots,f_{j-1},f_{j+1},\ldots,f_s$ is a regular sequence for all j, $1\leqq j\leqq s$. Then there exist generic linear combinations $f'_1,\ldots,f'_s$ of the polynomials f_j such that:*

- $1\in(f'_1,\ldots,f'_s)$,
- $f'_1,\ldots,f'_{s-1}$ *is a regular sequence,*
- $(f'_1,\ldots,f'_{n-r})$ *is a radical ideal for all* r, $n-s+1\leqq r\leqq n-1$.

Proof. Let $f'_1,\ldots,f'_{s-1}$ be generic linear combinations of the polynomials $f_1,\ldots,f_s$. According to Lemma 21 the ideal $(f'_1/f_j,\ldots,f'_t/f_j)$ is a radical ideal in $k[X_1,\ldots,X_n]_{f_j}$ for all t, j, $1\leqq t\leqq s-1$, $1\leqq j\leqq s$.

Since $1\in(f_1,\ldots,f_s)$ one deduces as in 5.2 that $(f'_1,\ldots,f'_t)$ is a radical ideal of the polynomial ring $k[X_1,\ldots,X_n]$ (moreover the fiber theorem implies that the typical fiber of π has dimension $n-t$ and hence $f'_1,\ldots,f'_t$ is also a regular sequence).

Finally we add a last generic linear combination f'_{t+1} which verifies $(f_1,\ldots,f_{t+1})=(f'_1,\ldots,f'_{t+1})$ and we put $r:=n-t$. □

5.3.2 An Effective Nullstellensatz for Degree 2

Theorem 24. *Let k be a field of characteristic different from 2 and let $f_1,\ldots,f_s\in k[X_1,\ldots,X_n]$ be polynomials of degree at most 2 such that $1\in(f_1,\ldots,f_s)$. Then there exist polynomials $p_1,\ldots,p_s\in k[X_1,\ldots,X_n]$ which verify:*

- $1=\sum_{i=1}^{s} p_i f_i$
- $\deg p_i\leqq n2^{n+2}$ $(1\leqq i\leqq s)$.

Proof. Without loss of generality we may suppose that the field k is algebraically closed. Proposition 18 allows us to assume that $s\leqq n+1$, that $f_1,\ldots,f_{j-1}$, $f_{j+1},\ldots,f_s$ is a regular sequence for all j and therefore, by means of Corollary 23, that $(f_1,\ldots,f_{n-r})$ is a radical ideal for all $n-s+1\leqq r\leqq n-1$.

Following [14, Lemma 1] we can choose the variables $X_1,\ldots,X_n$ in such a way that for all r, $n-s+1\leqq r\leqq n-1$, the following conditions hold:

– the morphism $k[X_1,\ldots,X_r]\to k[X_1,\ldots,X_n]/(f_1,\ldots,f_{n-r})$ is injective and integral (Noether position),
– the class of the Jacobian determinant of $f_1,\ldots,f_{n-r}$ with respect to the variables $X_{r+1},\ldots,X_n$ is not a zero divisor in $k[X_1,\ldots,X_n]/(f_1,\ldots,f_{n-r})$.

Now we can apply Lemma 16. □

Acknowledgements. The authors thank Alicia Dickenstein, Joos Heintz and Teresa Krick for many helpful discussions and remarks. The second author (P.S.) wishes to thank the Département de Mathématiques of the University of Limoges for its hospitality during his stay in 1993, when a part of this paper was written.

References

1. Becker, E., Wörman, T.: On the trace formula for quadratic forms and some applications. To appear in Proc. RASQUAD, Berkeley
2. Berenstein, C., Struppa, D.: Recent improvements in the Complexity of the Effective Nullstellensatz. Linear Algebra Its Appl. **157**, 203–215 (1991)
3. Berenstein, C., Yger, A.: Bounds for the degrees in the division problem. Mich. Math. J. **37**, 25–43 (1990)
4. Brownawell, D.: Bounds for the degrees in the Nullstellensatz. Ann. Math. Second Series **126**(3), 577–591 (1987)
5. 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 in Computer Sciences. Berlin, Hiedelberg, New York: Springer vol. **357**, 131–151 (1989)
6. Cardinal, J.-P.: Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux. Thesis Université de Rennes (1993)
7. Dickenstein, A., Giusti, M., Fitchas, N., Sessa, C.: The membership problem for unmixed polynomial ideals is solvable in single exponential time. Discrete Appl. Math. **33**, 73–94 (1991)
8. Dickenstein, A., Sessa, C.: An effective residual criterion for the membership problem in $\mathbb{C}[z_1, \ldots, z_n]$. J. Pure Appl. Algebra **74**, 149–158 (1991)
9. Dubé, T.: A Combinatorial Proof of the Effective Nullstellensatz. J. Symb. Comp. **15**, 277–296 (1993)
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. Preprint Ecole Polytechnique Palaiseau (1992)
12. Giusti, M., Heintz, J.: La détermination des points isolés et de la dimension d'une variété algébrique peut se faire en temps polynomial. To appear in Proc. Int. Meeting on Commutative Algebra, Cortona, 1991
13. Giusti, M., Heintz, J., Sabia, J.: On the efficiency of effective Nullstellensätze. Comput. Complexity **3**, 56–95 (1993)
14. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theoret. Comput. Sci. **24**, 239–277 (1983)
15. Iversen, B.: Generic Local Structures in Commutative Algebra. Lect. Notes in Math. vol. **310**. Berlin, Heidelberg, New York: Springer 1973
16. Jouanolou, J.-P.: Théorèmes de Bertini et applications. Progress in Math. vol. **42**. Basel: Birkhäuser (1983)
17. Kreuzer, M., Kunz, E.: Traces in strict Frobenius algebras and strict complete intersections. J. Reine Angew. Math. **381**, 181–204 (1987)
18. Kollár, J.: Sharp effective Nullstellensatz. J. AMS **1**, 963–975 (1988)
19. Kunz, E.: Kälher Differentials. Adv. Lect. in Math. Vieweg Verlag (1986)
20. Logar, A.: A computational proof of the Noether normalization lemma. Proc. 6th Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC-6, Roma 1988, Lecture Notes in Computer Sciences vol. **357**, pp. 259–273. Berlin, Heidelberg, New York: Springer 1989
21. Matsumura, H.: Commutative Algebra. Benjamin (1970)
22. Matsumura, H.: Commutative ring theory. Cambridge Studies in Adv. Math. vol. **8**. Cambridge University Press (1989)
23. Mumford, D.: The Red Book of Varieties and Schemes. Lect. Notes in Math. vol. **1358**. Berlin, Heidelberg, New York: Springer 1988
24. Pedersen, P., Roy, M.-F., Szpirglas, A.: Counting real zeros in the multivariate case. To appear in Proc. MEGA 92
25. Scheja, G., Storch, U.: Über Spurfunktionen bei vollständigen Durchschnitten. J. Reine Angew. Math. **278**, 174–190 (1975)
26. Teissier, B.: Résultats récents d'algèbre commutative effective. Séminaire Bourbaki 1989–1990, Astérisque vol. **189–190**, 107–131 (1991)
27. 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, LN Comput. Sci. vol. **539**, pp. 48–64. Berlin, Heidelberg, New York: Springer 1992