On the computation of the radical of polynomial complete intersection ideals

Inés Armendáriz [1] ⋆ and Pablo Solernó [2] ⋆

[1] Departamento de Matemáticas. Facultad de Ciencias Exactas y Naturales. Universidad de Buenos Aires. -1428- Buenos Aires. ARGENTINA.
iarmend@mate.dm.uba.ar

[2] Departamento de Economía y Matemática. Universidad de San Andrés. Vito Dumas 284. -1644- Victoria, Buenos Aires. ARGENTINA.
psolerno@udesa.edu.ar

Abstract. This paper deals with the effective computation of the radical of certain polynomial ideals. Let k be a characteristic zero field, $f_1, \ldots, f_{n-r} \in k[X_1, \ldots, X_n]$ a regular sequence with $d := \max_j \deg f_j$, $\Im$ the generated ideal, $\sqrt{\Im}$ its radical, and suppose that the factor ring $k[X_1, \ldots, X_n]/\sqrt{\Im}$ is a Cohen-Macaulay ring. Under these assumptions we exhibit a single exponential algorithm which computes a system of generators of $\sqrt{\Im}$.

1 Introduction

Let k be a field of characteristic zero, $X_1, \ldots, X_n$ be indeterminates over k and $f_1, \ldots, f_s$ polynomials in $k[X_1, \ldots, X_n]$ generating an ideal $\Im$.
The present paper deals with the effective computation of a system of generators for the radical of $\Im$. This problem seems to be, in a quite natural way, the next step to follow, now that the quantitative versions of the Nullstellensätze, effective Noether normalization, membership problem for complete intersection ideals, equidimensional decomposition, etc. have been found (see, for instance, the surveys [3], [26] and [2] and their bibliography).

The general problem, without any hypothesis on the f_i's, has already been considered in [1], [17] and [9]. Even when the techniques vary from work to work (Gröbner basis and linear algebra in the first two, basic duality theory in the third), all of them resort to certain quotient ideals. It is well-known that quotients are essentially difficult to compute, at least from the complexity point of view, and lead to doubly exponential time algorithms in the best case ([17]). This constraint, also appearing in the present paper (see Theorem 4 below), can be satisfactorily solved if we assume that the input polynomials $f_1, \ldots, f_s$ form a regular sequence whose zeros define a Cohen-Macaulay variety V. This condition, satisfied for example if V is a non-singular variety defined by a regular sequence, allows to deduce a single exponential algorithm (see Section 5).

The problem, under the complete intersection hypothesis, has been treated in [8], also making use of duality tools. The authors observe that if a single exponential bound for the degree of a system of generators of $\sqrt{\Im}$ is *a priori* known, then there exists a single exponential algorithm to compute it (see also Section 5.3). Unfortunately, such an upper bound is not yet known for the complete intersection general case. The best results in this direction are the following : if Z is a smooth, purely dimensional *projective* variety, its associated ideal $I(Z)$ can be generated by forms of degree bounded by $(\dim(Z)+1)(\deg(Z)-2)+2$ ([2, Theorem 3.12]) (in the case $\dim(Z) \leq 3$, the upper bound $\deg(Z) - \operatorname{codim}(Z) + 1$ holds; see [13] and [2]). In the affin case it is possible to

⋆ Partially supported by UBACYT and CONICET.

show that if V is smooth, its ideal $I(V)$ can be generated by polynomials of degree bounded by $\deg(V)$ ([22]).
In this paper we are able to show the non-intrinsic upper bound :

$$\max_j\{\deg f_j\}\operatorname{codim}(V)\,(2\deg(V)^2+1)$$

when $V \subset \overline{k}^n$ (the zeros of the ideal $\Im$) is a Cohen-Macaulay variety (Theorem 13).

The paper is organized as follows : Section 3 is devoted to explain the basic facts in trace theory (borrowed from [18]) and the description of the radical as a quotient ideal (Theorem 4). The following section contains a characterization of Cohen-Macaulay algebras by means of a Noether position.
Finally, in Section 5, we describe $\sqrt{\Im}$ as the solutions of a polynomial linear system (see also [8], [9]) whose entries have single exponential degrees. Unfortunately, it is well known that the degrees of a basis of the solutions for a polynomial linear system don't depend polynomially on the parameters (see [21] or [6]). However, for the special case when $k[X_1,\ldots,X_n]/\sqrt{\Im}$ is a Cohen-Macaulay ring, a polynomial upper bound can be exhibited (sections 5.1 and 5.2). From this estimation we obtain a single exponential upper bound for a system of generators of $\sqrt{\Im}$ (Theorem 13) and therefore a single exponential time algorithm to compute this radical ideal (Theorem 14).

We thank the referees for many useful remarks and pertinent suggestions.

2 Notations

Throughout the paper we shall maintain the following notations :

- n and r are non-negative integers with $0 \le r < n$.
- k is a characteristic zero field and the polynomial ring $k[X_1,\ldots,X_r]$ is denoted by A.
- $f_1,\ldots,f_{n-r}$ is a polynomial regular sequence in $k[X_1,\ldots,X_n]$ which generates an ideal $\Im$. We write $\sqrt{\Im}$ for the radical of $\Im$. The set of zeros of $\Im$ in $\mathbb{A}^n_{\overline{k}}$ (the affine n-dimensional space over the algebraic closure $\overline{k}$) is denoted by V and its usual geometric degree by $\deg(V)$. The integer d is an upper bound for the total degrees of the polynomials f_i.
- B denotes the factor ring $k[X_1,\ldots,X_n]/\Im$ and the variables $X_1,\ldots,X_n$ are in Noether position w.r.t. $\Im$ (i.e. the canonical morphism $A \to B$ is an integral monomorphism). The reduced ring $k[X_1,\ldots,X_n]/\sqrt{\Im}$ shall be denoted by B_{red} (observe that the variables $X_1,\ldots,X_n$ are also in Noether position w.r.t. $\sqrt{\Im}$).
  For any polynomial $f \in k[X_1,\ldots,X_n]$ we denote by $\overline{f}$ its class in B.
- Δ denotes the determinant of the Jacobian matrix $\big(\dfrac{\partial f_i}{\partial X_{r+j}}\big)_{1\le i,j\le n-r}$.

3 Describing radicals by means of Trace Theory

3.1 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 [18, 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 N (see Corollary 6 below). Fix for the moment a basis of this module; each element $b \in B$ defines, by multiplication, a square matrix $M_b \in A^{N\times N}$. If we denote by $\mathrm{trace}\,(M_b)$ 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 tensor 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 $\mathcal{K}$ the kernel of μ. It is easy to show that $\mathcal{K}$ 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 $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})(b\otimes 1 - 1\otimes b) = 0$ for all $b \in B$, one infers that the induced structures of right and left B-modules over $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ coincide. In other words, if $\sum_i b_i \otimes b'_i$ belongs to $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ 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 $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ is a cyclic B-module ([18, Corollary F.10]).
Let us consider the application $\Phi : B \otimes_A B \to \mathrm{Hom}_A(B^*, B)$ defined by

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

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 $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ by Φ is exactly $\mathrm{Hom}_B(B^*, B)$.

For each generator $\Gamma := \sum_m b_m \otimes b'_m$ of the B-module $\mathrm{Ann}_{B\otimes_A B}(\mathcal{K})$ 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 $b \in B$:

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

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

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 [18, Corollary F.12]) :

$$\mu(\Gamma).\sigma_\Gamma \ = \ \mathrm{Tr} \tag{2}$$

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 write

$$f^{(Y)} := f(X_1, \ldots, X_r, Y_{r+1}, \ldots, Y_n)$$

in the polynomial ring $k[X_1, \ldots, X_r, Y_{r+1}, \ldots, Y_n]$.
Hence we have the canonical isomorphism of A-algebras :

$$B \otimes_A B \;\cong A[X_{r+1}, \ldots, X_n, Y_{r+1}, \ldots, Y_n]/(f_1, \ldots, f_{n-r}, f_1^{(Y)}, \ldots, f_{n-r}^{(Y)}). \tag{3}$$

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 $k[X_1, \ldots, X_n]$ $(1 \leq i \leq n-r)$, its Taylor expansion around the point $(X_{r+1}, \ldots, X_n)$ gives the relation :

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

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 $(f_1, \ldots, f_{n-r}, f_1^{(Y)}, .$ gives a generator of $\mathrm{Ann}_{B \otimes_A B}(\mathcal{K})$ by means of the identification (3).

In other words we have (see also [10, Section 3.4]) :

Proposition 1 *There exist polynomials a_m, c_m in $k[X_1, \ldots, X_n]$ satisfying the inequality $\deg(a_m) + \deg(c_m) \leq (n-r)d$, $(1 \leq m \leq M)$, such that $\sum_m \overline{a}_m \otimes \overline{c}_m$ is a generator of $\mathrm{Ann}_{B \otimes_A B}(\mathcal{K})$ and $\overline{\Delta} = \sum_m \overline{a}_m\, \overline{c}_m$. Either family $(\overline{a_m})_m$ or $(\overline{c_m})_m$ is a system of generators of B over A.* ■

Definition 2 The trace associated to the generator of $\mathrm{Ann}_{B \otimes_A B}(\mathcal{K})$ introduced in Proposition 1 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 (2) gives

$$\overline{\Delta}.\sigma_\Delta \;=\; \mathrm{Tr}. \tag{4}$$

3.2 Describing the radical by means of the Jacobian

In this section we give the well-known characterization of the radical of the complete intersection ideal $\Im$ as the quotient $(\Im : \Delta)$. This result can be found in several previous works (see for instance [8] for the complex case, or [9, Th.2.1] for the general case). For the sake of simplicity we include a proof of this fact.

We start with an elementary, well-known characterization of nilpotent matrices.

Proposition 3 *Let K be a field of characteristic 0 and let $\phi \in K^{N \times N}$. Then ϕ is a nilpotent matrix if and only if $\mathrm{Tr}(\phi^i) = 0$ for all $i \in \mathbb{N}$.*

Proof.- Without loss of generality we may suppose that K is algebraically closed. Let $\lambda_1, \ldots, \lambda_t$ be the different non zero eigenvalues of ϕ and $k_1, \ldots, k_t$ the corresponding multiplicities in the characteristic polynomial of ϕ. It is easy to see (for instance by means of the Jordan form of ϕ) that for all $i \in \mathbb{N}$,

$$0 = \mathrm{Tr}(\phi^i) = \sum_{j=1}^{t} k_j \lambda_j^i.$$

Therefore $(k_1, \ldots, k_t)$ is a solution of an invertible Vandermonde matrix, which implies that $t = 0$ and hence 0 is the only eigenvalue of the matrix.
The converse is obvious. ■

Theorem 4 *Let f be an element of $k[X_1, \ldots, X_n]$ and $\overline{f}$ its class in the factor ring B. Then the following statements are equivalent :*

1. $f \in \sqrt{\Im}$;
2. $\mathrm{Tr}(\overline{f}\ b) = 0$, *for all* $b \in B$;
3. $f \in (\Im : \Delta)$.

Proof.- From Proposition 1 together with the relations (1) and (4) we obtain :

$$\overline{\Delta f} \ = \sum_{1 \le m \le M} \mathrm{Tr}(\overline{f}\ \overline{c_m})\ \overline{a_m} \ = \sum_{1 \le m \le M} \sigma_{\Delta}(\overline{\Delta f}\ \overline{c_m})\ \overline{a_m}.$$

Now conditions *2* and *3* become immediately equivalent.
If f belongs to $\sqrt{\Im}$ then $M_{\overline{f}b}$ (the matrix of multiplication by $\overline{f}b$) is nilpotent and Condition *2* follows from Proposition 3.
Conversely, the condition $\mathrm{Tr}(\overline{f}\ b) = 0$ for every $b \in B$ implies that $\mathrm{Tr}(\overline{f}^i) = 0$ for all index $i \in \mathbb{N}$ and the proposition already quoted shows that *1.* holds. ■

4 Cohen-Macaulayness via Noether Normalization Lemma

In this section we give a characterization of certain Cohen-Macaulay algebras as free modules over a polynomial ring in Noether position. This criterion has been treated in [12], [23] and [11].

We start by briefly recalling some basic definitions concerning Cohen-Macaulay rings (see [16] and [20]) that we shall use in the sequel.

Let $\mathcal{O}$ be a Noetherian local ring; we define the *depth* of $\mathcal{O}$ as the length of a maximal regular sequence. We say that $\mathcal{O}$ is a *Cohen-Macaulay ring* in case its depth and dimension coincide. An arbitrary Noetherian ring R is called Cohen-Macaulay if any localization in a maximal ideal is a Cohen Macaulay local ring. Finally, we shall say that an ideal is unmixed if the heights of its associated prime ideals are all equal.

The following key result (known as Hironaka's lemma) is classical; it can be found in [25, Ch.IV, Prop.22] for the local case, and in [11, Lemma 3.3.1] (in fact, our proof is essentially the same as the one of [11], even if the statements are slightly different).

Lemma 5 *Let $R := k[X_1, \ldots, X_n]/I$, where I is an unmixed ideal, $A := k[X_1, \ldots, X_r]$ and suppose that the canonical morphism $A \to R$ verifies the Noether Normalization Lemma. Then R is a Cohen-Macaulay ring if and only if R is $A-$ free.*

Proof.- ($\Rightarrow$) We proceed by induction on r. For the case $r = 0$ we observe that $A = k$ and that R is a k-vector space of finite dimension. Hence R is a free A-module.
It suffices now to show the lemma for fixed $0 < r \leq n-1$ supposing it true for $r-1$.
Quillen-Suslin Theorem ([19, Ch.III, Th.1.8]) states that the classes of finite projective modules and of finite free modules over a polynomial ring are the same, therefore it will be enough to show that R is A-projective.
First observe that $\overline{k}\otimes_k A$ is a faithfully flat A-algebra. Thus $\overline{k}\otimes_k R = (\overline{k}\otimes_k A)\otimes_A R$ is a projective $\overline{k}\otimes_k A$-module if and only if R is a projective A-module ([19, Ch.I, Prop.2.15]). Therefore we may suppose without loss of generality that k is algebraically closed.
Since R is a finite A-module it suffices to show that for any maximal ideal $\mathcal{M}$ of A the localized $A_{\mathcal{M}}$-module $R_{\mathcal{M}}$ is free.
Let $\mathcal{M}$ be a maximal ideal of $A = k[X_1, \ldots, X_r]$. Since k is by assumption algebraically closed there exist elements $a_1, \ldots, a_r$ of k such that $\mathcal{M} = (X_1 - a_1, \ldots, X_r - a_r)$. Without loss of generality we may assume $a_1 = \cdots = a_r = 0$. For the sake of simplicity, we shall write R for $R_{\mathcal{M}}$ and A for $A_{\mathcal{M}}$.
Since the canonical map $A \hookrightarrow R$ is integral and the ideal (0) is unmixed we conclude that X_r is not a zero divisor in R. It is easy to see that the rings $R' := R/(X_r)$ and $A' := A/(X_r)$ verify the hypothesis of the lemma : the Cohen-Macaulay theorem implies that R' is a Cohen-Macaulay ring (and therefore unmixed) and a standard dimension argument guarantees that $A' \hookrightarrow R'$ is in Noether position. Then, by our induction hypothesis, R' is a free A'-module of finite rank.
Let $e_1, \ldots, e_N$ be elements of R such that $e'_1, \ldots, e'_N$ (their classes modulo X_r) form a basis of the A'-free module R'. Thus $e_1, \ldots, e_N$ generate the $A/\mathcal{M}$-vector space $R/\mathcal{M}R \cong R'/\mathcal{M}R'$.
From Nakayama's Lemma we conclude that $e_1, \ldots, e_N$ generate the A-module R.
To finish the proof we are going to show that $e_1, \ldots, e_N$ form a free generator system.
Suppose on the contrary that there exists a nontrivial linear relation

$$\alpha_1 e_1 + \cdots + \alpha_N e_N = 0 \tag{5}$$

in R, where $\alpha_1, \ldots, \alpha_N$ are elements from A, not all zero. Without loss of generality we may assume $\alpha_1, \ldots, \alpha_N$ belong to $k[X_1, \ldots, X_r]$. Dividing by a maximal power of X_r we obtain representations $\alpha_1 = X_r^\ell \beta_1, \ldots, \alpha_N = X_r^\ell \beta_N$, where $\beta_1, \ldots, \beta_N$ are elements of $k[X_1, \ldots, X_r]$, not all divisible by X_r, and ℓ is a nonnegative integer. Thus we obtain from (5) the equality

$$X_r^\ell(\beta_1 e_1 + \cdots + \beta_N e_N) = 0$$

which holds in R. Since X_r is not a zero divisor of R we conclude

$$\beta_1 e_1 + \cdots + \beta_N e_N = 0\,.$$

Hence we may suppose without loss of generality that α_1 is an element of $k[X_1, \ldots, X_r]$ which is not divisible by X_r. Thus the relation (5) implies that

$$\alpha'_1 e'_1 + \cdots + \alpha'_N e'_N = 0$$

holds in R' with $\alpha'_1, \ldots, \alpha'_N$ the classes of $\alpha_1, \ldots, \alpha_N$ in A' and $\alpha'_1 \neq 0$. This contradicts the fact that $e'_1, \ldots, e'_N$ is a A'-basis of R'.

($\Leftarrow$) Let's suppose that k is algebraically closed. Let $\mathcal{M}$ be a maximal ideal of R. Since $A \hookrightarrow R$ is an integral extension, $\mathcal{N} := \mathcal{M} \cap A$ is maximal too and therefore $\mathcal{N} = (X_1 - a_1, \ldots, X_r - a_r)$ for suitable $a_1, \ldots, a_r \in k$.
Following [20, Th.17.3] it is enough to show that $X_1 - a_1, \ldots, X_r - a_r$ is a regular sequence in $R_{\mathcal{M}}$. Our hypothesis about the freeness of R over A guarantee that $X_r - a_r$ is not a zero divisor

in R; moreover, if we denote by $R' := R/(X_1 - a_1)$ and $A' := k[X_1, \ldots, X_{r-1}]$, then A' and R' are in Noether position and R' is A'-free (the ideal $(0) \subset R'$ is also unmixed, however, this property will not be necessary for this implication). This reasoning can be repeated to conclude that $X_1 - a_1, \ldots, X_r - a_r$ is a R-regular sequence, and consequently, a $R_{\mathcal{M}}$ one.
Now we consider the general case, where k is an arbitrary field. Let $\overline{R} := \overline{k} \otimes_k R$ and $\mathcal{M}$ be a maximal ideal of R; by a faithful-flatness argument it is easy to show that there exists a maximal ideal $\overline{\mathcal{M}}$ in $\overline{R}$ lying over $\mathcal{M}$. The argument above guarantees that $\overline{R}_{\overline{\mathcal{M}}}$ is Cohen-Macaulay. Following [20, Th.23.3 and its corollary] we conclude that $R_{\mathcal{M}}$ is Cohen-Macaulay too. ■

With the notations introduced in Section 2 we have the following well-known corollaries.

Corollary 6 *The ring B is an A-free module of rank bounded by d^{n-r}.*

Proof.- Since $\Im$ is generated by a regular sequence, B is a Cohen-Macaulay ring and $(0) \subset B$ is unmixed. The upper bound for the rank is a consequence of Bezout inequality (tensoring by the rational field $k(X_1, \ldots, X_r)$ we may assume that B is 0-dimensional and then we apply, for instance [5, Theorem 17]). ■

Corollary 7 *B_{red} is a Cohen-Macaulay ring if and only if B_{red} is A-free. In this case, the rank of B_{red} is bounded by $\deg(V)$.*

Proof.- It is an immediate consequence of Lemma 5, taking $R := B_{\mathrm{red}}$. In order to obtain the upper bound for the rank, we first observe that $\mathrm{rk}_A(B_{\mathrm{red}}) = \mathrm{rk}_{k(A)}(B_{\mathrm{red}} \otimes_A k(A))$, where $k(A)$ denotes $k(X_1, \ldots, X_r)$. Let $\wp_1, \ldots, \wp_t$ be the prime ideals associated to $\sqrt{\Im}$; since $B_{\mathrm{red}} \otimes_A k(A)$ is 0-dimensional and reduced, its rank is equal to $\sum_i \mathrm{rk}_{k(A)}(B_{\mathrm{red}}/\wp_i \otimes_A k(A))$, which in turn equals $\sum_i [k(B_{\mathrm{red}}/\wp_i) : k(A)]$.
For each index $i, 1 \leq i \leq t$, $[k(B_{\mathrm{red}}/\wp_i) : k(A)]$ is bounded by the degree of the affine variety in $\mathbb{A}^n_{\overline{k}}$ defined by the prime ideal $\wp_i$ (see, for example, [14, Proposition 1]). Adding these degrees we obtain the desired inequality. ■

5 Computing the radical

5.1 The radical as the solution of a linear system of equations

We follow the notations introduced in Section 2 .

Let $e_1, \ldots, e_N$ in $k[X_1, \ldots, X_n]$ be polynomials such that their classes in B, $\overline{e_1}, \ldots, \overline{e_N}$, form a basis over A (Corollary 6).
Following Theorem 4 one deduces that an element $b \in B$ belongs to the nilradical if and only if $\mathrm{Tr}(\overline{e_i}\, b) = 0$ for $1 \leq i \leq N$.

Let $\mathcal{T} \in A^{N \times N}$ be the matrix having $\mathrm{Tr}(\overline{e_i e_j})$ in the entry ij. For any element $b \in B$ let $\alpha_1, \ldots, \alpha_N \in A$ be its coordinates with respect to this basis. From the A-linearity of the trace it follows that b is nilpotent if and only if the vector $(\alpha_1, \ldots, \alpha_N)$ is in the kernel of $\mathcal{T}$.

At this stage we can restate Corollary 7 as follows :

Proposition 8 *B_{red} is Cohen-Macaulay if and only if the image of $\mathcal{T}$ is a free A-submodule of A^N. The fulfillment of this condition implies that the nilradical of B (isomorphic to the kernel of $\mathcal{T}$) is A-free.*

Proof.- Let $\tau : A^N \to A^N$ be the linear transformation associated to the matrix $\mathcal{T}$. Choosing an A-basis for B we have the following commutative diagram of A-modules :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}(\tau) & \longrightarrow & A^N & \xrightarrow{\tau} & \mathrm{Im}(\tau) & \longrightarrow & 0 \\ & & \downarrow \wr & & \downarrow \wr & & & & \\ 0 & \longrightarrow & \mathrm{Nil}(B) & \longrightarrow & B & \xrightarrow{\pi} & B_{\mathrm{red}} & \longrightarrow & 0 \end{array}$$

and then $B_{\mathrm{red}} \simeq \mathrm{Im}(\tau)$.
The second assertion is an immediate consequence of Quillen-Suslin Theorem. ■

5.2 A bound for the degrees of a system of generators of the radical

In the previous paragraph we connect the radical of the ideal $\Im$ with the solutions of a system of polynomial linear equations. Unfortunately, it is well known that there is no simple exponential upper bound for the degrees of a system of generators for such solutions (see [21] and [6]). However, this constraint can be avoided if we assume that B_{red} is a Cohen-Macaulay ring, as Lemma 9 and Corollary 10 below show (we recall that A denotes the polynomial ring $k[X_1, \ldots, X_r]$).

Lemma 9 *Let $M \in A^{N \times N}$ be a matrix whose entries are polynomials of degree bounded by an integer D, let $\mathcal{M}$ be a maximal ideal in A and $A_{\mathcal{M}}$ the associated local ring. Suppose that the columns of M, as vectors in $A^N_{\mathcal{M}}$, generate a free module of rank s (i.e. the image of M is isomorphic to $A^s_{\mathcal{M}}$). Then there exists an $A_{\mathcal{M}}$-basis of $\mathrm{Ker}(M) \subset A^N_{\mathcal{M}}$ which lies in A^N and has degree bounded by sD.*

Proof.- We denote by $c_1, \ldots, c_N \in A^N$ the columns of M and by $S \subset A^N_{\mathcal{M}}$ the s-rank free submodule generated by them (*i.e.* the image of M). We write K for the residual field $A/\mathcal{M}$.
Since S is $A_{\mathcal{M}}$-free of rank s, $S/\mathcal{M}S$ is a K-vector space of dimension s generated by the classes of $c_1, \ldots, c_N$. Without loss of generality we may suppose that the classes of the first s columns form a basis of this vector space.
By means of Nakayama's Lemma we conclude that $c_1, \ldots, c_s$ is a system of generators of S and hence an $A_{\mathcal{M}}$-basis.
We may also suppose that the determinant δ of the submatrix of M composed of the first s rows and s columns is not zero.
Cramer's Rule allows us to compute the A-linear combinations which write the columns $\delta c_{s+1}, \ldots, \delta c_N$ in terms of $c_1, \ldots, c_s$. We obtain an upper bound of type sD for the total degrees of the coefficients involved.
More precisely, there exist polynomials $a_{ij} \in A,\ 1 \leq i \leq s,\ 1 \leq j \leq N - s$ of degree bounded by sD such that

$$\delta c_{s+j} = a_{1j}c_1 + \cdots + a_{sj}c_s \tag{6}$$

holds in A^N (in fact the polynomials a_{ij} are $s \times s$ minors of the matrix M).
For each index j set $\varepsilon_j := \mathrm{g.c.d}(\delta, a_{1j}, \ldots, a_{sj})$, $\delta_j := \delta\varepsilon_j^{-1}$ and $b_{ij} := a_{ij}\varepsilon_j^{-1}$.
Then we obtain from (6) :

$$\delta_j c_{s+j} = b_{1j}c_1 + \cdots + b_{sj}c_s. \tag{7}$$

From the fact that $c_1, \ldots, c_s$ is a $A_{\mathcal{M}}$-basis of S and that $\delta_j, b_{1j}, \ldots, b_{sj}$ are relatively prime, one deduces that $\delta_j \notin \mathcal{M}$. Therefore the $N - s$ vectors

$$w_j := (b_{1j}, \ldots, b_{sj}, 0, \ldots, -\delta_j, \ldots, 0),$$

where $-\delta_j$ occurs in the coordinate $s + j$, $1 \leq j \leq N - s$, form a basis for the free $A_{\mathcal{M}}$-module $\mathrm{Ker}(M)$ and the lemma follows. ■

From this lemma we obtain the following global version :

Corollary 10 *Let $M \in A^{N \times N}$ be a matrix whose entries are polynomials of degree bounded by an integer D. Suppose that the columns of M, as vectors in A^N, generate a free module of rank s (i.e. the image of M is isomorphic to A^s). Then there exists a finite system of generators of* $\mathrm{Ker}(M)$ *having degree bounded by sD.*

Proof.- Let I and J be subsets of s rows and s columns of the matrix M and $D_{I,J}$ be the minor of the associated $s \times s$-submatrix. By Cramer's rule in the fraction field of A, if $D_{I,J} \neq 0$, one infers that, for any column c that is not in J, the identity

$$c\, D_{I,J} = \sum_{h \in J} \pm h\, D_{I,(J \cup \{c\}) \setminus \{h\}}$$

holds in A^N.
Dividing this equality by the greatest common divisor of $D_{I,J}$ and $D_{I,(J\cup\{c\})\setminus\{h\}}$ (for all $h \in J$) as in (7), we obtain an identity which induces an element $w_{I,J,c}$ in $\mathrm{Ker}(M)$ having coordinates of degree bounded by sD.
We claim that the submodule W generated by these elements is exactly the kernel of M. Clearly we have $W \subset \mathrm{Ker}(M)$.
In order to prove the other inclusion it suffices to consider the situation under localization by a maximal ideal $\mathcal{M} \subset A$. The argument runs as the one of the previous lemma (the flatness of the localization implies the fulfillment of its hypothesis).
From Nakayama's Lemma one sees that there exist a subset of rows I_0 and a subset of columns J_0 such that the corresponding elements $w_{I_0,J_0,c}$ (where c ranges over the set of columns in the complement of J_0) form a $A_{\mathcal{M}}$-basis of $\mathrm{Ker}(M)_{\mathcal{M}}$. In particular, we have $\mathrm{Ker}(M)_{\mathcal{M}} \subset W_{\mathcal{M}}$ for any maximal ideal $\mathcal{M}$. The corollary follows from the local-global principle. ■

In the next proposition we estimate the degree of the elements of a polynomial local basis for the free A-module B (we recall that no similar bound is known up to now for the global case).

Proposition 11 *Let $\mathcal{M}$ be a maximal ideal of A. There exist polynomials $e_1, \ldots, e_N \in k[X_1, \ldots, X_n]$ having degrees bounded by $(n - r)d$ such that their classes in the ring $B_{\mathcal{M}}$ form a $A_{\mathcal{M}}$-basis.*

Proof.- Let $\overline{a_1}, \ldots, \overline{a_M} \in B$ be the system of generators constructed in Proposition 1; they are such that the total degree of each $a_m \in k[X_1, \ldots, X_n]$ is bounded by $(n - r)d$.
The classes of these polynomials in the factor ring $B/\mathcal{M}B \simeq B_{\mathcal{M}}/\mathcal{M}B_{\mathcal{M}}$ also form a system of generators over the field $A/\mathcal{M}$. Without loss of generality we may suppose that the classes of $a_1, \ldots, a_N$ form a basis of this vector space.
Nakayama's Lemma implies that these elements are a system of generators of $B_{\mathcal{M}}$. Since they are as many as the rank of the free module $B_{\mathcal{M}}$ one infers that they are actually a basis. ■

The following proposition allows us to estimate an upper bound for the degree of the entries in the trace matrix :

Proposition 12 *Let f be an element in the polynomial ring $k[X_1,\ldots,X_n]$ and denote by $\overline{f}$ its class in the factor ring B. Then the inequality*

$$\deg \mathrm{Tr}(\overline{f}) \leq \deg(V)\deg f$$

holds.

Proof.- The proof runs almost exactly as the one of [24, Prop.1 and Th.13] even if the ideal $\Im$ generated by the regular sequence is not radical, as was the case in the quoted paper.
Roughly speaking, we consider the map $\varphi : \mathbb{A}_{\overline{k}}^{n} \to \mathbb{A}_{\overline{k}}^{r+1}$ defined by

$$\varphi(x_1,\ldots,x_n) = (x_1,\ldots,x_r,f).$$

By means of this application one deduces that the minimal integral dependence equation $F \in k[X_1,\ldots,X_r,T]$ for the class of f modulo $\sqrt{\Im}$ has total degree bounded by $\deg(V)\deg f$. Moreover, F coincides with the minimal polynomial of the endomorphism η_f of $B_{\mathrm{red}} \otimes_A k(A)$ defined by multiplication by f. It is easy to see that the prime factors of this minimal polynomial, which lie in $A[T]$, are the same than the ones of the characteristic polynomial of the same endomorphism, now considered in $B \otimes_A k(A)$.
Let $F = \prod_{1\leq j\leq J} Q_j$ be the decomposition of F in irreducible factors on $A[T]$ (we recall that each Q_j is monic with total degree bounded by $\deg(V)\deg f$). For any index j, $1 \leq j \leq J$, denote by d_j the degree of Q_j and by $\beta_j \in A$ the coefficient of the monomial T^{d_j-1} in Q_j (in particular $\deg \beta_j \leq \deg(V)\deg f$).
Let $\mathcal{X}_f = T^D + b_{D-1}T^{D-1} + \ldots + b_0$ be the characteristic polynomial of η_f in $B \otimes_A k(A)$. Therefore $\mathcal{X}_f = \prod_j Q_j^{e_j}$, where $e_1,\ldots,e_J$ are positive integers.
By comparison of coefficients one deduces :

$$-\mathrm{Tr}(\overline{f}) = b_{D-1} = \sum_{1\leq j\leq J} e_j\beta_j.$$

Therefore $\deg \mathrm{Tr}(\overline{f}) \leq \deg(V)\deg f$. ■

Now, we are able to show an upper bound for the degrees of a system of generators for $\sqrt{\Im}$:

Theorem 13 *Suppose that B_{red} is a Cohen-Macaulay ring. Then the radical $\sqrt{\Im}$ can be generated by polynomials whose degrees are bounded by the integer $(n-r)d(2\deg(V)^2+1)$.*

Proof.- Let $\mathcal{M}$ be a maximal ideal of A and $e_1,\ldots,e_N \in k[X_1,\ldots,X_n]$ as in Proposition 11.
By Proposition 12 the matrix $\mathcal{T} \in A^{N\times N}$ associated to the bilinear form Tr in the basis $\overline{e_1},\ldots,\overline{e_N}$ have entries bounded by $2(n-r)d\deg(V)$.
From Proposition 8 and Corollary 7 the matrix $\mathcal{T}$ verifies the hypothesis of Corollary 10 with $s \leq \deg(V)$ and $D \leq 2(n-r)d\deg(V)$.
Hence there exists a finite system of generators of $\mathrm{Nil}(B_{\mathcal{M}})$ corresponding to polynomials of $k[X_1,\ldots,X_n]$ whose degrees are bounded by

$$\begin{aligned}&\mathrm{rk}_A(B_{\mathrm{red}})2(n-r)d\deg(V) + (n-r)d \leq\\ &\leq 2\deg(V)(n-r)d\deg(V) + (n-r)d \leq\\ &\leq (n-r)d(2\deg(V)^2+1).\end{aligned}$$

By the local-global principle one infers that $\sqrt{\Im}$ can be generated by polynomials of total degree bounded by $(n-r)d(2\deg(V)^2+1)$. ■

5.3 The algorithm

We continue with the same notations, assuming that B_{red} is a Cohen-Macaulay ring.
By Theorem 13 we know that the radical $\sqrt{\Im}$ can be generated by polynomials whose degrees are bounded by $D := (n-r)d(2\deg(V)^2+1) \leq 3d^{3(n-r)}$.
Let $\mathcal{A} \subset k[X_1,\ldots,X_n]$ be the set of all polynomials with total degree bounded by D, and for each multi-index $\alpha := (\alpha_1,\ldots,\alpha_n)$ such that $\alpha_1+\ldots+\alpha_n \leq D$, let $X^\alpha := {X_1}^{\alpha_1}\ldots{X_n}^{\alpha_n}$.
Theorem 4 says that a polynomial f belongs to the radical of $\Im$ if and only if $\Delta f = 0$ in the factor ring B.
Let $f \in \sqrt{\Im}\cap\mathcal{A}$, there exist constants $(\lambda_\alpha)_\alpha$ in the ground field k and polynomials $g_1,\ldots,g_{n-r} \in k[X_1,\ldots,X_n]$ such that :

- $f = \sum_\alpha \lambda_\alpha X^\alpha$
- $\Delta f = \sum_i g_i f_i$, with $\deg(g_i f_i) \leq 2D$, $1 \leq i \leq n-r$ (see [7, Theorem 5.1.]).

Comparing coefficients, these identities lead to a non-homogeneous system of linear equations over the ground field k of size of order $D^{O(n)}$.
Solving this system via well-known symbolic procedures (see for instance [4]), one obtains generators for the k-vector space $\sqrt{\Im}\cap\mathcal{A}$ and therefore for the ideal $\sqrt{\Im}$.
Since all these computations, as well as the effective Noether normalization position, can be done by single exponential, well-parallelizable algorithms, we deduce :

Theorem 14 *Following the notations introduced in Section 2 and assuming that B_{red} is a Cohen-Macaulay ring, there exists a single exponential, well-parallelizable algorithm which computes the radical $\sqrt{\Im}$.* ■

References

1. Alonso M., Mora T. and Raimondo M.: Local decomposition algorithms.- Proc. 8th. Int. Conf. Applied Algebra, Algebraic Algorithms and Error Correcting Codes AAECC-8, Springer Lect. Notes Comput.Sci. **508** (1991) 208-221.
2. Bayer D. and Mumford D.: What Can Be Computed in Algebraic Geometry ? Computational Algebraic Geometry and Commutative Algebra, Cortona 1991, D. Eisenbud and L. Robbiano, eds. Symposia Math. XXXIV, Cambridge Univ. Press (1993) 1-48.
3. Berenstein C. and Struppa D.: Recent improvements in the Complexity of the Effective Nullstellensatz.- Linear Algebra and its Appl. **157** (1991) 203-215.
4. Berkowitz S.: On computing the determinant in small parallel time using a small number of processors.- Inform. Process. Lett. **18** (1984) 147-150.
5. Caniglia L., Galligo A. and 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, Springer Lect. Notes Comput.Sci. **357** (1989) 131-151.
6. Demazure M.: Le monoïde de Mayr et Meyer.- Notes Informelles de Calcul Formel, Ecole Polytechnique, Palaiseau (1984).
7. Dickenstein A., Giusti M., Fitchas N. and Sessa C.: The membership problem for unmixed polynomial ideals is solvable in single exponential time.- Discrete Appl. Math. **33** (1991) 73-94.
8. Dickenstein A. and Sessa C.: Duality methods for the membership problem.- Effective Methods in Algebraic Geometry MEGA 90, T. Mora and C. Traverso, eds., Progress in Mathematics Vol. **94**, Birkhäuser (1991) 89-103.
9. Eisenbud D., Huneke C. and Vasconcelos W.: Direct methods for primary decomposition.- Inv. Math. **110** (1992) 207-235.
10. Fitchas N., Giusti M. and Smietanski F.: Sur la complexité du théorème des zéros.- Preprint Ecole Polytechnique Palaiseau (1992).

11. Giusti M., Heintz J. and Sabia J.: On the efficiency of effective Nullstellensätze.- Comput. Complexity **3**, Birkhaüser (1993) 56-95.
12. Grothendieck A. and Dieudonné J.: *Éléments de géometrie algébrique IV*.- Publ. Math. Inst. Hautes Étud. Sci. **32** (1967).
13. Gruson L., Lazarsfeld R. and Peskine C.: On a Theorem of Castelnuovo, and the Equations Defining Space Curves.- Inv. Math. **72** (1983) 493-506.
14. Heintz J.: Definability and Fast Quantifier Elimination in Algebraically Closed Fields.- Theoret. Comput. Sci. **24** (1983) 239-277.
15. Iversen B.: *Generic Local Structures in Commutative Algebra*.- Lect. Notes in Math. **310**, Springer-Verlag (1973).
16. Kaplansky I.: *Commutative rings*.- Allyn and Bacon (1970).
17. Krick T. and Logar A.: An algorithm for the computation of the radical of an ideal in the ring of polynomials.- Proc. AAECC–9, New Orleans 1991. LN Comp. Sci. **539**. Springer–Verlag (1992) 195-205.
18. Kunz E.: *Kälher Differentials*.- Adv. Lect. in Math., Vieweg Verlag (1986).
19. Lam T.Y.: *Serre's Conjecture*.- Springer Lect. Notes in Math. **635** (1978).
20. Matsumura H.: *Commutative ring theory*.- Cambridge Studies in Adv. Math. **8** Cambridge University Press (1989).
21. Mayr E. and Meyer A.: The complexity of the word problem for commutative semigroups and polynomial ideals.- Adv. in Math. **46** (1982) 305-329.
22. Mumford D.: Varieties defined by quadratic equations.- Questions on Algebraic Varieties, Centro Internationale de Matematica Estivo, Cremonese, Roma (1970) 29-100.
23. Rossi F. and Spangher W.: Some effective methods in the openness of loci for Cohen-Macaulay and Gorenstein properties.- Effective Methods in Algebraic Geometry, Proc. Intern. Conf. MEGA 90, Castiglioncello 1990, T. Mora and C. Traverso, eds., Progress in Mathematics Vol. **94** Birkhäuser (1990) 441–455.
24. Sabia J. and Solernó P.: Bounds for traces in Complete Intersections and Degrees in the Nullstellensatz.- To appear in AAECC Journal, Springer-Verlag (1994).
25. Serre J.-P.: *Algèbre Locale - Multiplicités*.- Springer Lect. Notes in Math. **11** (1965).
26. Teissier B.: Résultats récents d'algèbre commutative effective.- Séminaire Bourbaki 1989-1990, Astérisque vol **189-190** (1991) 107-131.