DEPARTAMENTO DE MATEMÁTICA
DOCUMENTO DE TRABAJO

“Sur les degrés des bases de modules libres sur l’anneau de polynomes”

Marcela Almeida, Lisi D’Alfonso y Pablo Solernó

D.T.: N° 8 Marzo 1997

Vito Dumas 284, (B1644BID) Victoria, Pcia. de Buenos Aires, Argentina
Tel: 4725-7053 Fax: 4725-7010
Email: matematica@udesa.edu.ar

On the degrees of bases of free modules over a polynomial ring

Marcela Almeida* Lisi D'Alfonso*

Departamento de Matemática. Facultad de Ciencias Exactas y Naturales.

Universidad de Buenos Aires. -1428- Buenos Aires. ARGENTINA.

malmeida@dm.uba.ar lisi@dm.uba.ar

Pablo Solernó*

Departamento de Economía y Matemática. Universidad de San Andrés.

Vito Dumas 284. -1644- Victoria, Buenos Aires. ARGENTINA.

psolerno@dm.uba.ar

Fax : 54-1-746-50-90

October 31, 2000

Abstract. Let k be an infinite field, A the polynomial ring $k[x_1, ..., x_n]$ and $F \in A^{N\times M}$ a matrix such that $\operatorname{Im} F \subset A^N$ is A-free (in particular, Quillen-Suslin Theorem implies that $\operatorname{Ker} F$ is also free). Let D be the maximum of the degrees of the entries of F and s the rank of F. We show that there exists a basis $\{v_1, \ldots, v_M\}$ of A^M such that $\{v_1, \ldots, v_{M-s}\}$ is a basis of $\operatorname{Ker} F$, $\{F(v_{M-s+1}), \ldots, F(v_M)\}$ is a basis of $\operatorname{Im} F$ and the degrees of their coordinates are of order $((M-s)sD)^{O(n^4)}$.

This result allows to obtain a single exponential degree upper bound for a basis of the coordinate ring of a reduced complete intersection variety in Noether position.

Keywords. Linear equation systems over polynomial rings. Quillen-Suslin Theorem. Effective Nullstellensatz. Complete intersection polynomial ideals. Duality theory in Gorenstein Rings.

*Partially supported by UBACYT and PID-CONICET.

1 Introduction

This article deals with the computation of the solutions of linear equation systems over a polynomial ring. After the seminal paper by E.Mayr and A.Meyer [20], it is well known the constraints of linear algebra methods as a tool in effective commutative algebra. In particular, Mayr-Meyer's monoid leads to an intrinsic hyperexponential growth of the degrees of the syzygies.

In terms of linear equation systems this fact can be restated saying that there exist families of polynomial matrices such that every system of generators of their kernels contains a vector with at least one coordinate of double exponential degree. More precisely, in [7, Corollaire, pag.10] the following result is shown :

Let $\varepsilon > 0$. *Let* n *and* D *be integers such that* $n \geq 10$, $D \geq 3$, $D \geq 2 + \frac{1}{32\varepsilon}$. *There exists a polynomial sequence* $P_1, \ldots, P_n$ *of degree bounded by* D *in* $A := k[x_1, \ldots, x_n]$ *(where* $P_1 := x_1$, $P_2 := x_2$*) such that any system of generators of the* A*-submodule of* A^n *consisting of all the sequences* U_i *with* $\sum_i U_i P_i = 0$, *contains at least one vector whose first coordinate has degree* $\geq N$, *where* $\log_2 \log_2 N > (\frac{1}{8} - \varepsilon)n + \log_2 \log_2 D - \frac{9}{4}$.

However, under certain additional hypothesis on the matrix associated to the linear system, more precise estimations can be done. For example, if the matrix is unimodular (i.e. the rows can be extended to a basis of the whole space), a single exponential upper bound for the degree of a basis of its kernel is given in [5, Corollary 3.2].

In the present paper we treat the more general case where the columns of the matrix generate a free A-module (in particular, Quillen-Suslin Theorem assures that the kernel is also free). In this case it is not too difficult to show a polynomial upper bound for the degree of a system of generators of the kernel (see [2, Corollary 10] or Lemma 1 below). Nevertheless our purpose here is to find bases of low degree for the kernel and the image.

More precisely, let k be an infinite field, $A := k[x_1, ..., x_n]$ be the polynomial ring in the indeterminates $x_1, \ldots, x_n$ and $F \in A^{N \times M}$ be a matrix such that $\operatorname{Im} F$ is A-free. Denote by D the maximum of the degrees of the entries of F and by s the rank of F. Therefore we have (see Theorem 19 below) :

Theorem *There exists a basis* $\{v_1, \ldots, v_M\}$ *of* A^M *such that :*

- $\{v_1, \ldots, v_{M-s}\}$ *is a basis of* $\operatorname{Ker} F$*;*
- *the coordinates of the vectors* v_j *have degrees of order* $((M-s)sD)^{O(n^3)}$ *for* $j = 1, \ldots, M-s$.
- $\{F(v_{M-s+1}), \ldots, F(v_M)\}$ *is a basis of* $\operatorname{Im} F$.
- *the coordinates of the vectors* v_j *have degrees of order* $((M-s)sD)^{O(n^4)}$ *for* $j = M-s+1, \ldots, M$.

Under suitable stronger conditions (for instance, if F corresponds to the matrix of a linear projection) the degree upper bounds of the Theorem can be slightly improved (see Section 6).

The methods we use in order to prove the main theorem (developed in Sections 2 to 5) are strongly inspired on the works of D.Quillen, A.Suslin, L.Vaserstein and M.Hochster related to the resolution of the so called "Serre's Conjecture" (on this subject let us mention the remarkable books of T.Y.Lam [17] and E.Kunz [15]). We combine this approach with the effective version of Hilbert Nullstellensatz (see [13], [9] and the references given in [3] and [23]) and its consequences in the quantitative study of polynomial unimodular matrices following [5]. Other approaches on effective Quillen-Suslin Theorem may be found in [18] and [19].

The last section is devoted to an application of the mentioned theorem in the frame of effective commutative algebra : let k be an infinite field and $f_1, \ldots, f_{n-r}$ be a regular sequence in $k[x_1, \ldots, x_n]$ of degrees bounded by an integer d. Suppose that the variables $x_1, \ldots, x_n$ are in Noether position with respect to the polynomials f_i (i.e. the natural map $k[x_1, \ldots, x_r] \to k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ is an injective and integral morphism). Write $R := k[x_1, \ldots, x_r]$ and $S := k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$. It is well known (see for example [8, Corollary 18.17] or [12, Lemma 3.3.1]) that, under these conditions, S is a locally free R-module of finite rank (bounded by d^{n-r} following Bezout's Inequality) and hence free (Quillen-Suslin Theorem).
This situation appears frequently in problems related to effective elimination theory (see [21], [12], [6], [1], [14], [11]). In this context it is natural to ask about quantitative properties of bases of the module S. To our knowledge the only significative result for this problem deals with the homogeneous case, where a basis whose coordinates have single exponential degree is obtained with the aid of elementary properties of Gröbner bases.
In this sense we obtain the following result (see Theorem 27 below) :

Theorem *Suppose that S is a reduced ring. Then, there exist a basis of S over R formed by polynomials of degrees of order $d^{O((n-r)r^4))}$.*

The proof of this theorem combines the previous results of linear algebra over the polynomial ring with consequences of Gorenstein duality theory.

The methods of the proofs of both theorems are explicit and they can be easily transformed into algorithmic procedures; however their complexity bounds are too bad, even for theoretical purposes. Therefore the problem of how to find single exponential algorithms remains open.

Aknowledgements: The third author (P.S.) thanks the Laboratoire GAGE, Ecole Polytechnique, Palaiseau, specially Prof. Marc Giusti, for its hospitality during the winter season 96-97.

2 A system of generators for the kernel of F

Let k be an infinite field, $A := k[x_1, ..., x_n]$ and $F \in A^{N \times M}$ a matrix verifying that $\operatorname{Im} F$ is a free A-module. In this case, Quillen-Suslin Theorem (see for instance [15, Ch.IV, Th.3.15.]) implies that $\operatorname{Ker} F$ is also free. Denote by D the maximum of the degrees of the entries of F and by s the rank of F. The columns of F will be denoted by $C_1, \ldots, C_M$.

With these notations we are able to estimate a system of generators of $\mathrm{Ker}\, F$ of low degree (see also [2, Corollary 10]) :

Lemma 1 *The kernel of the matrix* F *can be generated as an* A*-module by* $3(M-s)(sD)^n$ *polynomial vectors with degrees bounded by* sD*.*

Proof.- Since $s = \mathrm{rk}F$ there exists at least one non zero $s \times s$ minor; without loss of generality, let us suppose that the first $s \times s$ principal minor δ is non zero (in particular, the first s columns are linearly independent). Therefore, by Cramer's rule, we have for $i = 1, ..., M-s$:

$$\delta\ C_{s+i} = b_{1i}C_1 + \cdots + b_{si}C_s\ , \tag{1}$$

where b_{ji} are polynomials in A uniquely determined, whose degrees are bounded by sD. Dividing relation (1) by the GCD of $b_{1i}, \ldots, b_{si}, \delta$ we obtain new relations

$$\delta_i\ C_{s+i} = b'_{1i}C_1 + \cdots + b'_{si}C_s. \tag{2}$$

Clearly, the vectors

$$w_i := (b'_{1i}, \ldots, b'_{si}, 0, \ldots, -\delta_i, \ldots, 0),$$

where $-\delta_i$ occurs in the coordinate $s+i$, belong to $\mathrm{Ker}\, F$.
Repeating this construction for all the $s \times s$ non zero minors of F, we get a family of vectors lying in the kernel.
We claim that this family generates $\mathrm{Ker}\, F$.
For this it is enough to show that for any maximal ideal $\mathcal{M} \subset A$ these vectors span the kernel of the corresponding localized application $F : A^M_{\mathcal{M}} \to A^N_{\mathcal{M}}$.
Clearly, the columns $C_1, \ldots, C_M$ generate $\mathrm{Im}\, F_{\mathcal{M}}$; by Nakayama's Lemma, since $\mathrm{Im}\, F_{\mathcal{M}}/\mathcal{M}\mathrm{Im}\, F_{\mathcal{M}}$ is a s-dimensional vector space, we deduce that there exists a basis of $\mathrm{Im}\, F_{\mathcal{M}}$ consisting of s suitable columns of the matrix F. Without loss of generality, we may suppose that $C_1, \ldots, C_s$ is an $A_{\mathcal{M}}$-basis of $\mathrm{Im}\, F_{\mathcal{M}}$ and therefore, there exist $p_{1i}, \ldots, p_{si} \in A$ and $q_i \in A \setminus \mathcal{M}$, such that

$$q_i C_{s+i} = p_{1i}C_1 + \ldots + p_{si}C_s, \tag{3}$$

for $i = 1, \ldots, M-s$.
We now show that no δ_i in (2) belongs to $\mathcal{M}$: suppose on the contrary that $\delta_j \in \mathcal{M}$, from the relations (2) and (3) we deduce :

$$q_j b'_{kj}\ =\ p_{kj}\delta_j$$

for $k = 1, \ldots, M-s$. In particular, since $q_j \notin \mathcal{M}$, all the irreducible factors of δ_j which belong to $\mathcal{M}$ are also factors of all the b'_{kj}'s. This contradicts the coprimality of $b'_{1j}, \ldots, b'_{sj}, \delta_j$.
We finish the claim remarking that the vectors w_i are an $A_{\mathcal{M}}$-basis of $\mathrm{Ker}\, F_{\mathcal{M}}$ because they are a basis of the vector space $\mathrm{Ker}\, F_{\mathcal{M}}/\mathcal{M}\mathrm{Ker}\, F_{\mathcal{M}}$ (they are $M-s$ linearly independent vectors).

In order to shrink the obtained system of generators, for every non zero minor δ we modify slightly the vectors w_i in the following way: let $g_\delta := \mathrm{mcm}(\delta_1, \ldots, \delta_{M-s})$ and set $\widetilde{w}_i := \dfrac{g_\delta}{\delta_i} w_i$.
Let us observe that:

- $\widetilde{w}_i \in A^M$.
- The coordinates of $\widetilde{w}_i$ have degrees bounded by sD (observe that g_δ divides δ).
- If $\delta_i \notin \mathcal{M}$ for $i = 1, \ldots M-s$, then $g_\delta \notin \mathcal{M}$. In particular the vectors $\widetilde{w}_i$ are a system of generators of $\operatorname{Ker} F_{\mathcal{M}}$ and the ideal generated by the polynomials g_δ is A.
- If δ runs over all the non zero $s \times s$ minors, the corresponding vectors $\widetilde{w}_i$ generate $\operatorname{Ker} F$.

Since g_δ divides δ, the degrees of the polynomials g_δ are bounded by sD and then they span a k vector space of dimension smaller than $\binom{n+sD}{sD} \leq e(sD)^n$.
Fix a maximal k-linearly independent family of g_δ's; for each one of these g_δ's consider the $M-s$ vectors associated to it. The collection of all these vectors is also a system of generators of $\operatorname{Ker} F$. ■

3 A free $k[x_1, \ldots, x_{n-1}]$-module related to $\operatorname{Im} F$

From now on we write B for the polynomial ring $k[x_1, \ldots, x_{n-1}]$.

Since $\operatorname{Im} F$ is a free A-module of rank $s > 0$, there is a non zero $s \times s$ minor of F; after a linear change of coordinates, we may assume that the first $s \times s$ principal minor, μ, is monic with respect to each variable $x_1, \ldots, x_n$.

Remark 2 Under this assumption the image of the matrix $F(0) \in B^{N \times M}$, obtained by replacing x_n by 0 in F, is B-free. Moreover, let $h_1, \ldots, h_s \in A^N$ be a basis of $\operatorname{Im} F$ and $w_1, \ldots, w_t \in A^M$ be the system of generators of $\operatorname{Ker} F$ constructed in Lemma 1. Then the corresponding vectors $h_1(0), \ldots, h_s(0)$ and $w_1(0), \ldots, w_t(0)$ are a B-basis of $\operatorname{Im} F(0)$ and a B-system of generators of $\operatorname{Ker} F(0)$ respectively.
In fact, let $v \in \operatorname{Im} F(0)$ and $v' \in B^M$ be such that $F(0)(v') = v$; since $F(v')$ is an A-linear combination of the vectors $h_1, \ldots, h_s$, replacing x_n by 0, one deduces that v is a B-linear combination of the vectors $h_j(0)$'s. The assumption about the $s \times s$ minor μ implies that the rank of $\operatorname{Im} F(0)$ over the fraction field of B is also s. Therefore $h_1(0), \ldots, h_s(0)$ are B-linearly independent.
In a similar way the assertion about the generators of $\operatorname{Ker} F(0)$ follows.

Let L be the free submodule of A^N generated by the first s columns $C_1, \ldots, C_s$. Consider the exact sequence

$$0 \to L \to \operatorname{Im} F \to Q \to 0 \tag{4}$$

where $Q := \mathrm{Im}\, F/L$.

Clearly, Q is generated by the images of the columns $C_{s+1}, \ldots, C_M$ and then $\mu Q = 0$ (due to the relations (1) for $\delta = \mu$).
We write $d := \deg_{x_n} \mu - 1$ (note that $d \leq sD - 1$).
Since μ is monic in x_n, Q admits a natural B-module structure of finite type generated by the images of the elements $x_n^j C_i$ with $j = 0, \ldots, d$ and $i = s+1, \ldots, M$.

Proposition 3 *The B-module Q is free of finite rank.*

Proof.- Let $\wp \subset B$ be a maximal ideal; tensoring the exact sequence (4) (as a sequence of B-modules) by $B/\wp$, we claim that the sequence of $B/\wp$-vector spaces

$$0 \to L/\wp L \to \mathrm{Im}\, F/\wp \mathrm{Im}\, F \to Q/\wp Q \to 0 \tag{5}$$

is exact.
To prove our claim it is enough to show that the injection $L \hookrightarrow \mathrm{Im}\, F$ is preserved after tensoring. In fact, let $w := \alpha_1 C_1 + \cdots + \alpha_s C_s$ be an element in $L \cap \wp \mathrm{Im}\, F$.
Then w may be written as a linear combination of the columns $C_1, \ldots, C_M$ with coefficients in $\wp A$.
Then we have :

$$\alpha_1 C_1 + \cdots + \alpha_s C_s = w = \beta_1 C_1 + \cdots + \beta_M C_M$$

with $\alpha_j \in A$ and $\beta_i \in \wp A$. Multiplying this equality by μ and using (1) we deduce the relations :

$$\mu \alpha_j = \mu \beta_j + \sum_{i=1}^{M-s} \beta_{s+i} b_{ji}$$

for $j = 1, ..., s$.
Regarding this formula as a polynomial identity in $B[x_n]$ and comparing coefficients (recall μ is monic) we observe that the α_j's belong to $\wp A$ and then $w \in \wp L$, i.e. $w = 0$ in $L/\wp L$.
From the exactness of (5) we deduce that Q is a locally projective B-module and then projective (see [15, Ch.IV, Prop.3.4]). Therefore it is a free B-module of finite type, by Quillen-Suslin. ■

Definition 4 For $k = 0, \ldots, d$ and $i = s+1, \ldots, M$, let $\overline{x_n^k C_i}$ be the canonical system of generators of Q over B, and let $m := (d+1)(M-s)$.
Let $e_{0,s+1}, e_{1,s+1}, \ldots, e_{d,s+1}, \ldots, e_{d,M}$ be the canonical basis of B^m. Therefore, we have a surjective map $\varphi : B^m \to Q$, defined as $\varphi(e_{ki}) := \overline{x_n^k C_i}$ (observe that $\mathrm{Ker}\, \varphi$ is B-free).

We are interested now in the computation of a system of generators for $\mathrm{Ker}\, \varphi$ of low degree.

Let $w_1, \ldots, w_t$ be a system of generators of $\operatorname{Ker} F$ as in Lemma 1 (in particular, $t \leq e(M-s)(sD)^n$). Since μ is monic in x_n, we can compute the euclidean division in $B[x_n]$ for each coordinate, and we write :

$$w_j \ = \ \mu q_j + r_j \tag{6}$$

where q_j and r_j are in A^M and the degree in x_n of each coordinate of r_j is bounded by d, meanwhile, the total degree is bounded by $(sD)^2$.

For each $x_n^k r_j \in A^M$ with $j = 1, \ldots, t$ and $k = 0, \ldots, d$, we compute again the euclidean division :

$$x_n^k r_j \ = \ \mu q_{kj} + r_{kj} \tag{7}$$

where $r_{kj} \in A^M$, $\deg r_{kj} = 2(sD)^3$ and $\deg_{x_n} r_{kj} \leq d$.

For each vector r_{kj}, we consider the vector V_{kj} consisting of the $M-s$ last coordinates. We replace the multi-index kj by $h = 1, \ldots, t(d+1)$.
For each h, V_h can be decomposed :

$$V_h \ = V_{h,0} + x_n V_{h,1} + \cdots + x_n^d V_{h,d}$$

and each $V_{h,k}$, being a vector in B^{M-s}, can be written

$$V_{h,k} = (V_{h,k,s+1}, \ldots, V_{h,k,M}).$$

Proposition 5 *The vectors* $(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d,s+1}, \ldots, V_{h,d,M}) \in B^{(d+1)(M-s)}$, *with* $h = 1, \ldots, t(d+1)$, *are a system of generators of* $\operatorname{Ker} \varphi$.

Proof.- First, we show that these vectors belong to $\operatorname{Ker} \varphi$.
Applying the definition of φ, we have

$$\varphi(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d,s+1}, \ldots, V_{h,d,M}) = \sum_{i,k} V_{h,k,i} \overline{x_n^k C_i} = \sum_{i=s+1}^{N} Q_{h,i} \overline{C_i}.$$

with $Q_{h,i} := \sum_k V_{h,k,i} x_n^k$.
It suffices to show that $\sum_{i=s+1}^M Q_{h,i} C_i \in L$.
With the notations above; $V_h = (Q_{h,s+1}, \ldots, Q_{h,M})$, and then, reversing the euclidean divisions (7) and (6), there exist $P_1, \ldots, P_s \in A$ such that :

$$(P_1, \ldots, P_s, Q_{h,s+1}, \ldots, Q_{h,M}) = x_n^k w + \mu r$$

where $k \in \mathbb{N}$, $w \in \operatorname{Ker} F$ and $r \in A^M$.
Multiplying this identity by the "column vector" $(C_1, \ldots, C_M)$ we obtain :

$$\sum_{i=1}^{s} P_i C_i + \sum_{i=s+1}^{M} Q_{h,i} C_i = \mu \sum_{i=1}^{M} r_i C_i,$$

because $w \in \operatorname{Ker} F$.

Since $\mu C_i \in L$ for all $i = 1, \ldots, M$, we deduce that $\sum_i Q_{h,i} C_i \in L$, and so, the vectors are in $\operatorname{Ker} \varphi$.

Now, we will show that they are a system of generators of $\operatorname{Ker} \varphi$.
Let $(q_{0,s+1}, q_{1,s+1}, \ldots, q_{d,M})$ be an element in $\operatorname{Ker} \varphi \subset B^{(d+1)(M-s)}$; that is to say

$$q_{0,s+1} C_{s+1} + q_{1,s+1} x_n C_{s+1} + \ldots + q_{d,M} x_n^d C_M \in L.$$

Writing $Q_i := \sum_k q_{k,i} x_n^k$, we know that there exist $P_1, \ldots, P_s \in A$ such that

$$Q_{s+1} C_{s+1} + \cdots + Q_M C_M = P_1 C_1 + \cdots + P_s C_s.$$

This means that the vector $(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) \in A^M$ belong to $\operatorname{Ker} F$, and then, if $\{w_1, \ldots, w_t\}$ is the system of generators of $\operatorname{Ker} F$ constructed in Lemma 1, there exist $\alpha_1, \ldots \alpha_t \in A$ such that

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_N) = \sum \alpha_j w_j.$$

Dividing the α_j's and w_j's by μ, we can write, for a certain $w \in A^M$

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) = \mu w + \sum \beta_j r_j$$

where $\deg_{x_n} \beta_j \leq d$ and r_j are the ones defined in (6).
Repeating the division (7) we obtain

$$(-P_1, \ldots, -P_s, Q_{s+1}, \ldots, Q_M) = \mu w' + \sum \beta_{kj} r_{kj}$$

with $\beta_{kj} \in B$ (see (7)).
Comparing the last $M - s$ coordinates, and simplifying the notation, we have

$$(Q_{s+1}, \ldots, Q_M) = \mu v + \sum \beta_h V_h$$

for a certain $v \in A^{M-s}$.
Since $\beta_h \in B$ for all index h, and since $\deg_{x_n} Q_i$ and $\deg_{x_n} V_h$ are strictly lower than $\deg_{x_n} \mu$, we obtain that v is zero from the uniqueness of the euclidean algorithm in $B[x_n]$.
Then

$$(Q_{s+1}, \ldots, Q_M) \in BV_1 + \cdots + BV_{t(d+1)}.$$

The proof finishes developing this identity in powers of x_n. ∎

With the notations above, we observe that $t \leq e(M-s)(sD)^n$, $d \leq sD$ and $\deg V_h = 2(sD)^3$, and then we have the following result:

Lemma 6 *There exists a matrix $G \in B^{m \times p}$, where $m := (M-s)(d+1)$, $p := t(d+1) \leq e(M-s)(sD)^{n+1}$ and $\deg G = 2(sD)^3$, such that $\operatorname{Im} G = \operatorname{Ker} \varphi$.*

Proof.- Take G as the matrix whose columns are the vectors $(V_{h,0,s+1}, V_{h,1,s+1}, \ldots, V_{h,d,s+1}, \ldots, V_{h,d,M})$, $h = 1, \ldots, p$. ∎

Observe that $m \leq p$ since $M - s = \operatorname{rk} (\operatorname{Ker} F) \leq t$.

4 Another local presentation for $\operatorname{Im} F$

This section is devoted to exhibit a presentation of $\operatorname{Im} F$ under a suitable localization in an element of the ring B (Lemma 14 below).

Let $G \in B^{m \times p}$ be the matrix from Lemma 6 and let $q \leq m$ be the rank of the B-module $\operatorname{Ker} \varphi$ (which is free because Q is free and B is a polynomial ring). The $q \times q$ minors of G generate the ring B (since $\operatorname{Im} G = \operatorname{Ker} \varphi$ is a direct summand of B^m) and their degrees are bounded by $2q(sD)^3$ (therefore by $2(M-s)(sD)^4$).
Let ξ be a non zero $q \times q$ minor. Without loss of generality we may suppose that ξ involves the first q columns of G that we will denote by $K_1, \ldots, K_q$.

For the $m-q$ rows not used in the construction of the minor ξ, let $e_{k_1,i_1}, \ldots, e_{k_{m-q},i_{m-q}}$ be the corresponding $m-q$ vectors of the canonical basis of B^m (see Definition 4). For the sake of simplicity we will denote e_{k_j,i_j} by u_j, $j = 1, \ldots, m-q$.
Clearly $K_1, \ldots, K_q, u_1, \ldots, u_{m-q}$ are a basis of B_ξ^m since the determinant of the corresponding $m \times m$ matrix Z is $\pm\xi$.
Then we have

Proposition 7 *The vectors $\varphi(e_{k_j,i_j}) = \overline{x_n^{k_j} C_{i_j}}$, $j = 1, \ldots, m-q$, are a basis of the B_ξ-module Q_ξ.* ■

Meanwhile consider the vectors $x_n^{k_1} C_{i_1}, \ldots, x_n^{k_{m-q}} C_{i_{m-q}}, C_1, \ldots, C_s$.
From Proposition 7 and the definition of the B-module Q (see (4)), for each index ℓ, $\ell = 1, \ldots, m-q$, there exist unique $\widetilde{\beta}_1^{(\ell)}, \ldots, \widetilde{\beta}_{m-q}^{(\ell)} \in B_\xi$ and $\widetilde{\alpha}_1^{(\ell)}, \ldots, \widetilde{\alpha}_s^{(\ell)} \in A_\xi$ such that

$$-x_n\, x_n^{k_\ell} C_{i_\ell} = \sum_{j=1}^{m-q} \widetilde{\beta}_j^{(\ell)}\, x_n^{k_j} C_{i_j} + \sum_{i=1}^{s} \widetilde{\alpha}_i^{(\ell)} C_i. \tag{8}$$

We will analize this relations more deeply.

First assume $k_\ell < d$: then $-\overline{x_n^{1+k_\ell} C_{i_\ell}} = -\varphi(e)$ for a certain vector e of the canonical basis of B^m (see Definition 4).
On the other hand we can write in B_ξ^m :

$$-e = \lambda_1 K_1 + \cdots + \lambda_q K_q + \lambda_{q+1} u_1 + \cdots + \lambda_m u_{m-q} \tag{9}$$

for certain $(\lambda_1, \ldots, \lambda_m) \in B_\xi^m$.
Hence, applying φ we have

$$-\varphi(e) = -\overline{x_n^{1+k_\ell} C_{i_\ell}} = -x_n \varphi(u_\ell) = \sum_{j=1}^{m-q} \lambda_{q+j} \varphi(u_j)$$

(recall that $\varphi(K_l) = 0$ for all l). Therefore in (8) we can take $\widetilde{\beta}_j^{(\ell)} := \lambda_{q+j}$, for all j.
In order to estimate the degree of λ_{q+j} we consider the product of (9) by the matrix Z^{-1} :

$$-Z^{-1}\ e = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}.$$

In particular, the λ_{q+j}'s are the last $m-q$ entries of a column of the matrix $-Z^{-1}$. Since Z belongs to $B^{m\times m}$ and $\det(Z) = \pm\xi$ we can write

$$\widetilde{\beta}_j^{(\ell)} \ = \ \frac{\beta_j^{(\ell)}}{\xi} \tag{10}$$

where, by Cramer's rule, the $\beta_j^{(\ell)}$'s are polynomials in B whose degrees are bounded by $(m-1)2(sD)^3 \le 2m(sD)^3$.
For the case $k_\ell = d$, instead of $-x_n^{1+k_\ell} C_{i_\ell}$, we write $(x_n^{d+1} - \mu) C_{i_\ell}$ and the argument runs similarly. Here the upper bound for the polynomials $\beta_j^{(\ell)}$ is $2(m-1)(sD)^3 + (sD) \le 2m(sD)^3$.

In order to obtain an estimation for the degrees in (8) it remains only to bound the degrees of the $\widetilde{\alpha}_i^{(\ell)}$'s.
Rewriting formula (8), we construct $Q_1, \dots, Q_{M-s} \in B_\xi[x_n]$ such that the equality

$$Q_1 C_{s+1} + \cdots + Q_{M-s} C_M = \sum_{i=1}^{s} \widetilde{\alpha}_i^{(\ell)} C_i$$

holds in A_ξ^N and $\xi Q_l \in A$ for all $l = 1, \dots, M-s$ are polynomials of degree bounded by $d + 2m(sD)^3$.
On the other hand, relation (1) for the first $s \times s$ minor μ of the matrix F yields the equality :

$$Q_1 C_{s+1} + \cdots + Q_{M-s} C_M = Q_1 \sum_{r=1}^{s} \frac{b_{r1}}{\mu} C_r + \cdots + Q_{M-s} \sum_{r=1}^{s} \frac{b_{r,M-s}}{\mu} C_r.$$

Taking into account that the columns $C_1, \dots, C_s$ are linearly independent, we deduce :

$$\widetilde{\alpha}_i^{(\ell)} \ = \ \frac{\sum_{l=1}^{M-s} b_{il} Q_l}{\mu}.$$

Let h be the minimal exponent such that $\xi^h \alpha_i^{(\ell)} \in A$. Since $\xi Q_l \in A$ for all l and the polynomials μ and ξ are relatively primes (because μ is monic in all the variables and ξ belongs to B), we deduce that $h \le 1$, and then

$$\xi \widetilde{\alpha}_i^{(\ell)} \in A \qquad \text{and} \qquad \mu \ \text{ divides } \ \xi \sum_{l=1}^{M-s} b_{il} Q_l \ \text{ in } A. \tag{11}$$

Therefore, by (1) , (10) and (11) :

$$\deg(\xi \widetilde{\alpha}_i^{(\ell)}) \ \le \max_l \{\deg(b_{il} \xi Q_l)\} \le (sD) + \max_j \{\deg \beta_j^{(\ell)}\} + d \le (sD) + 2m(sD)^3 + d.$$

Since $m \leq (M-s)sD$, we are able to rewrite (8) as follows :

$$-x_n\, x_n^{k_\ell} C_{i_\ell} = \sum_{j=1}^{m-q} \frac{\beta_j^{(\ell)}}{\xi}\, x_n^{k_j} C_{i_j} + \sum_{i=1}^{s} \frac{\alpha_i^{(\ell)}}{\xi} C_i\ , \tag{12}$$

where $\beta_j^{(\ell)} \in B$, $\alpha_i^{(\ell)} \in A$ and $\deg \beta_j^{(\ell)}$, $\deg \alpha_i^{(\ell)} \leq 4(M-s)(sD)^4$ for all indices j, i and ℓ.

The following definition allows to show a new local presentation of $\operatorname{Im} F$ which we will consider in the sequel.

Definition 8 Let $\psi\ : A^{m-q+s} \to \operatorname{Im} F$ be the linear application defined by :
– $\psi(e_j) = x_n^{k_j} C_{i_j}$, for all $j = 1, \ldots, m-q$,
– $\psi(e_j) = C_{j-m+q}$, for all $j = m-q+1, \ldots, m-q+s$.
Observe that ψ depends on the choice of the minor ξ.
The localized morphism ψ_ξ is surjective (Proposition 7 and the definition of Q), and then $\operatorname{Ker} \psi_\xi$ is a projective A_ξ-module because $\operatorname{Im} F_\xi$ is A_ξ-free

With the notations above we have the following result borrowed from [15, Ch.IV, page 115]:

Proposition 9 *The matrix $U \in A_\xi^{(m-q)\times(m-q+s)}$, where the ℓ-th row is the vector*

$$\left(\frac{\beta_1^{(\ell)}}{\xi}, \ldots, \frac{\beta_{m-q}^{(\ell)}}{\xi}, \frac{\alpha_1^{(\ell)}}{\xi}, \ldots, \frac{\alpha_s^{(\ell)}}{\xi}\right) + x_n e_\ell$$

(e_ℓ is the ℓ-th vector of the canonical basis of A^{m-q}), is a unimodular matrix in A_ξ (i.e. the $(m-q)\times(m-q)$ minors generate the ring A_ξ) and its rows are a basis of $\operatorname{Ker}\psi_\xi$ (in particular $\operatorname{Ker}\psi_\xi$ is free). Moreover $\xi U \in A^{(m-q)\times(m-q+s)}$ and $\deg \xi U \leq 4(M-s)(sD)^4$.

Proof.- Let $S \subset A_\xi^{m-q+s}$ be the submodule generated by the rows of the matrix U. From the relations (12) it is clear that $S \subset \operatorname{Ker}\psi_\xi$.
In order to see the other inclusion, we observe the following : for all $\ell = 1, \ldots, m-q$ and for all $p \in A_\xi$ there exist $\gamma_1, \ldots, \gamma_{m-q} \in B_\xi$ and $\gamma_{m-q+1}, \ldots, \gamma_{m-q+s} \in A_\xi$ (depending on ℓ and p) such that

$$pe_\ell - \sum_{j=1}^{m-q+s} \gamma_j e_j \in S.$$

This can be done developing p in powers of the variable x_n.
Therefore, if $(p_1, \ldots, p_{m-q+s}) \in \operatorname{Ker}\psi_\xi$, we can rewrite it as follows

$$(p_1, \ldots, p_{m-q+s}) = w\ +\ \sum_{j=1}^{m-q+s} \gamma_j e_j$$

where $w \in S$, $\gamma_1, \ldots, \gamma_{m-q} \in B_\xi$ and $\gamma_{m-q+1}, \ldots, \gamma_{m-q+s} \in A_\xi$.
Applying ψ we have the following identity in $\operatorname{Im} F_\xi$:

$$0 \;=\; \sum_{j=1}^{m-q} \gamma_j \, x_n^{k_j} C_{i_j} + \sum_{j=m-q+1}^{m-q+s} \gamma_j C_{j-m+q}. \tag{13}$$

Looking this equality modulo the free A_ξ-module L_ξ (see (4) in Section 3) one deduces the relation in Q_ξ :

$$0 \;=\; \sum_{j=1}^{m-q} \gamma_j \, \overline{x_n^{k_j} C_{i_j}},$$

and, since the elements $\overline{x_n^{k_j} C_{i_j}}$, $j = 1, \ldots, m-q$, are a B_ξ-basis of Q_ξ (see Proposition 7), we have $\gamma_j = 0$ for $j = 1, \ldots, m-q$.
Thus, the linear combination (13) can be reduced to

$$0 \;=\; \sum_{j=m-q+1}^{m-q+s} \gamma_j C_{j-m+q}.$$

Since the vectors $C_1, \ldots, C_s$ are linearly independent we have also $\gamma_j = 0$ for $j = m-q+1, \ldots, m-q+s$. Then $(p_1, \ldots, p_{m-q+s}) \in S$ and therefore $S = \operatorname{Ker} \psi_\xi$.
Moreover, the rows of the matrix U are a A_ξ-basis of $\operatorname{Ker} \psi_\xi$: $\operatorname{Im} F_\xi$ is A_ξ-free of rank s and then $\operatorname{Ker} \psi_\xi$ is locally free of rank $m-q$; since the rows of the matrix U generate $\operatorname{Ker} \psi_\xi$, by Nakayama's Lemma, they are a basis for the localization in any maximal ideal of A_ξ and then they are A_ξ-linearly independent.
The unimodularity of the matrix U follows from the decomposition $A_\xi^{m-q+s} \simeq \operatorname{Ker} \psi_\xi \oplus \operatorname{Im} F_\xi$. ■

Following [15, Ch.IV, Lemma 3.12] we are able to simplify the matrix U using "x_n-division with remainder" between the matrix formed by the last s columns of U and the matrix consisting of the first $m-q$ columns of U in the obvious way :

Proposition 10 *There exists an invertible matrix $C \in A_\xi^{(m-q+s)\times(m-q+s)}$ verifying*

$$UC = \left(\begin{array}{c|c} x_n \mathrm{Id}_{m-q} + U_1 & U_2 \end{array} \right)$$

where $\xi U_1 \in B^{(m-q)\times(m-q)}$, $\xi^{4(M-s)(sD)^4} U_2 \in B^{(m-q)\times s}$, et $\xi^{4(M-s)(sD)^4} C \in A^{(m-q+s)\times(m-q+s)}$ are matrices whose entries have degrees bounded by $16(M-s)^2(sD)^8$. ■

The matrix U can be modified by another change of coordinates in such a way that all its entries belong to a suitable localization of the ring B. For this purpose it is convenient to consider the matrix UC in Proposition 10 as a $k(x_1, \ldots, x_{n-1})[x_n]$-unimodular matrix in order to apply Suslin's reduction procedure following [17] and [5] (see the next two lemmas). Unfortunately this approach requires the introduction of certain polynomials in B playing the rôle of the ξ's. Fortunately their amount and degrees can be appropriately controlled (Corollary 13 below).

In the following two lemmas V will denote the matrix UC from Proposition 10.

Lemma 11 (cf. [5, Lemma 4.4]) *For each* $z \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$ *there exists an invertible matrix* $\Lambda_z \in k^{(m-q+s)\times(m-q+s)}$ *such that: if* $V' := V\Lambda_z$, $\Delta_1 := \det[V_1', \ldots, V_{m-q}']$, *(the* $(m-q)\times(m-q)$ *minor built from the first* $m-q$ *columns of* V'*),* $\Delta_2 := \det[V_1', \ldots, V_{m-q-1}', V_{m-q+1}']$ *and* $c_z := \mathrm{Res}_{x_n}(\Delta_1, \Delta_2)$ *the resultant of* Δ_1 *and* Δ_2 *with respect to the indeterminate* x_n*, then* $c_z(z) \neq 0$.

Proof.- Let $z = (z_1, \ldots, z_{n-1}) \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$ be given; let $k[y_{ij};\ 1 \leq i, j \leq m-q+s]$ be the polynomial ring in $(m-q+s)^2$ new indeterminates over k. By Y we denote the $m-q+s$ square matrix $[y_{ij}]$ with columns $Y_1, \ldots, Y_{m-q+s}$. We write Y' and Y'' for the $(m-q+s)\times(m-q)$ matrices $[Y_1, \ldots, Y_{m-q}]$ and $[Y_1, \ldots, Y_{m-q-1}, Y_{m-q+1}]$ respectively. Let $V' := VY$.
From the Binet-Cauchy formula ([10, Ch.2]) we see that:

$$\Delta_1 := \det[V_1', \ldots, V_{m-q}'] = \sum_I \det(V_I)\det(({}^tY')_I) \tag{14}$$

$$\Delta_2 := \det[V_1', \ldots, V_{m-q-1}', V_{m-q+1}'] = \sum_I \det(V_I)\det(({}^tY'')_I)$$

where I runs through all sequences $(i_1, \ldots, i_{m-q})$ such that $1 \leq i_1 < \cdots < i_{m-q} \leq m-q+s$.
Let $c := c(x_1, \ldots, x_{n-1}, Y) := \mathrm{Res}_{x_n}(\Delta_1, \Delta_2)$ be the resultant of Δ_1 and Δ_2 with respect to the indeterminate x_n.
Claim.- $c(z, Y) = c(z_1, \ldots, z_{n-1}, Y) \neq 0$.
Proof of the claim. From Proposition 10 we have that the polynomial $\det[V_1, \ldots, V_{m-q}]$ is monic in x_n and $m-q = \deg_{x_n}(\det[V_1, \ldots, V_{m-q}]) > \deg_{x_n}(\det(V_I))$ for all sequences of natural numbers $I = (i_1, \ldots, i_{m-q})$ with $1 \leq i_1 < \cdots < i_{m-q} \leq m-q+s$ and $I \neq (1, \ldots, m-q)$.
Thus (14) implies that $c(z, Y) = c(z_1, \ldots, z_{n-1}, Y) = \mathrm{Res}_{x_n}(\Delta_1(z, x_n, Y'), \Delta_2(z, x_n, Y''))$.
Suppose now that $c(z, Y) = 0$. Then there exists $p \in \bar{k}[x_n, Y]$ with $\deg_{x_n}(p) \geq 1$ such that p divides both $\Delta_1(z, x_n, Y')$ and $\Delta_2(z, x_n, Y'')$. In particular we have $p \in \bar{k}[x_n, Y_1, \ldots, Y_{m-q-1}]$. Let $h \in \bar{k}[x_n, Y']$ be such that

$$ph = \Delta_1 = \sum_I \det(V_I(z, x_n))\det(({}^tY')_I). \tag{15}$$

Let $\mathcal{I} \subset \bar{k}[x_n][Y']$ be the ideal generated by all the determinants $\det(({}^tY')_I)$; $\mathcal{I}$ is a homogeneous prime ideal (see [4, Ch.2, Th.2.10]). From (15) we see that p and h must be homogeneous in Y' and that $\deg_{Y'}(p) + \deg_{Y'}(h) = m-q$. The polynomial p doesn't belong to $\mathcal{I}$ since it is independent from Y_{m-q}.
Since $\Delta_1 \in \mathcal{I}$ by (15) and $\mathcal{I}$ is prime we conclude $h \in \mathcal{I}$ and $\deg_{Y'}(h) \geq m-q$. Thus $\deg_{Y'}(p) = 0$, i.e. $p \in \bar{k}[x_n]$. Now, again by (15), we see that p divides all $\det(V_I(z, x_n))$. The unimodularity of V (Propositions 9 and 10) implies that the ideal generated by all polynomials $\det(V_I(z, x_n))$ is trivial in $k[x_n]$. Therefore $p \in \bar{k}$, which contradicts $\deg_{x_n}(p) \geq 1$. This finishes the proof of the claim.
Since k is infinite and since $c(z, Y) \neq 0$ there exists $\Lambda_z \in GL_{m-q+s}(k)$ such that $c(z, \Lambda_z) \neq 0$. ∎

Lemma 12 (cf. [5, Lemma 4.5]) *Let* $z \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$, $\Lambda_z \in GL_{m-q+s}(k)$, $V' = V\Lambda_z$, Δ_1, Δ_2 *and* $c_z \in B_\xi$ *be as in Lemma 11. Then there exists an invertible matrix* $\Omega \in A_{c_z\xi}^{(m-q+s)\times(m-q+s)}$ *such that* $V\Omega = V(0)$ *(where* $V(0)$ *denotes the matrix* V *after the evaluation* $x_n \mapsto 0$ *) and* $(c_z\xi^u)^l\Omega$ *is a polynomial matrix in* $A^{(m-q+s)\times(m-q+s)}$. *The degrees of the entries of* $(c_z\xi^u)^l\Omega$ *and the integers* u *and* l *are of order* $((M-s)sD)^{O(1)}$, *independently of* z.

Proof.- Let $z \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$, $c := c_z$ and $g, h \in B_\xi[x_n]$ be such that $c = g\Delta_1 + h\Delta_2$. From Proposition 10, without loss of generality, we may assume that there exists a constant $\eta \in \mathbb{N}$ independent of z, of order $((M-s)sD)^{O(1)}$, such that $\xi^\eta g$, $\xi^\eta h$ are polynomials in A, $\xi^\eta c$ belongs to B, and the total degrees of these polynomials are bounded by another constant of size $((M-s)sD)^{O(1)}$.

For each j, $m-q+2 \le j \le m-q+s$, there exists a column vector $G_j \in A_{c\xi}^{(m-q)\times 1}$ with controlled degrees such that $V'_j(0) - V'_j = cG_j$. Therefore $V'_j(0) - V'_j = g\Delta_1 G_j + h\Delta_2 G_j$. Let $B_1 := \operatorname{adj}[V'_1, \ldots, V'_{m-q}]$ be the adjoint matrix of the $(m-q)\times(m-q)$ matrix $[V'_1, \ldots, V'_{m-q}]$. Simmilarly, let B_2 be the adjoint of the matrix $[V'_1, \ldots, V'_{m-q-1}, V'_{m-q+1}]$. Thus:

$$\Delta_1 g G_j = [V'_1, \ldots, V'_{m-q}](B_1 g G_j)$$

and

$$\Delta_2 h G_j = [V'_1, \ldots, V'_{m-q-1}, V'_{m-q+1}](B_2 h G_j).$$

From these equalities we conclude that

$$V'_j(0) - V'_j = g_1 V'_1 + \cdots + g_{m-q+1} V'_{m-q+1}$$

for suitable $g_1, \ldots, g_{m-q+1} \in A_{c\xi}$.

This holds for all $m-q+2 \le j \le m-q+s$. Therefore there exists a unimodular matrix Ω' in $A_{c\xi}$ which is a product of $(m-q+1)(s-1)$ elementary matrices and such that:

$$V\Omega' = [V'_1, \ldots, V'_{m-q+1}, V'_{m-q+2}(0), \ldots, V'_{m-q+s}(0)].$$

Let T be the $(m-q+1)\times(m-q+1)$ matrix defined by

$$T := \frac{1}{c}\operatorname{adj}\left(\begin{pmatrix} V'_1 & \cdots & V'_{m-q} & V'_{m-q+1} \\ 0 & \cdots & -h & g \end{pmatrix}\right)\begin{pmatrix} V'_1(0) & \cdots & V'_{m-q}(0) & V'_{m-q+1}(0) \\ 0 & \cdots & -h(0) & g(0) \end{pmatrix}.$$

Since c does not depend on x_n it is easy to see that $T \in A_{c\xi}^{(m-q+1)\times(m-q+1)}$ and $\det(T) = 1$. Therefore $T \in SL_{m-q+1}(A_{c\xi})$. Moreover, we have

$$[V'_1, \ldots, V'_{m-q+1}]\,T = [V'_1(0), \ldots, V'_{m-q+1}(0)].$$

One easily checks now that $\Omega := \Omega' \begin{pmatrix} T & 0 \\ 0 & \mathrm{Id}_{s-1} \end{pmatrix}$ verifies the assertion. ∎

From Lemma 11 and Lemma 12 one deduces:

Corollary 13 *For each non zero* $q \times q$ *minor* ξ *of the matrix* G *(see Lemma 6) there exist polynomials* $\xi_1, \ldots, \xi_L \in B$ *whose degrees are of order* $((M-s)sD)^{O(1)}$ *and* $L = ((M-s)sD)^{O(n)}$, *such that*

1. *The ring B is generated by the polynomials $\xi\xi_j$ where ξ runs over all the non zero $q\times q$ minors of G and $j=1,\ldots,L$.*

2. *The image of the localized map $\psi_{\xi\xi_j}$ (Definition 8) is $\operatorname{Im} F_{\xi\xi_j}$.*

3. *The kernel of $\psi_{\xi\xi_j}$ is a free module generated by $m-q$ polynomial vectors in B^{m-q+s} of degrees of order $((M-s)sD)^{O(1)}$.*

Proof.- For each minor ξ we construct the polynomials ξ_j as follows : consider the k-linear space generated by the polynomials $c_z\xi^u \in B$ of Lemma 12, where z runs in the set $\mathbb{A}^{n-1}\setminus\{\xi=0\}$; since $\deg(c_z\xi^u)=((M-s)sD)^{O(1)}$, the dimension of this space is bounded by $((M-s)sD)^{O(n)}$. The polynomials ξ_j's are chosen as a basis of this space. From Lemma 11 and Hilbert Nullstellensatz one deduces that the polynomials $\xi\xi_j$ generate B_ξ; on the other hand the minors ξ generate the ring B (recall that $\operatorname{Im} G$ is a direct summand of B^m) and then the first condition is verified.
The second condition follows from Definition 8.
Fix $\xi\xi_j$ and let $z\in\mathbb{A}^{n-1}$ be such that $\xi_j=c_z\xi^u$. Let $\Omega\in A_{\xi\xi_j}^{(m-q+s)\times(m-q+s)}$ be the matrix from Lemma 12 associated to z. Therefore the rows of $V\Omega=V(0)$ form a basis of $\operatorname{Ker}\psi_{\xi\xi_j}$. Multiplying these vectors by a suitable power of ξ as in Proposition 10 we finish the proof. ■

Consider now a polynomial $\xi\xi_j$ and let $W\in B^{(m-q)\times(m-q+s)}$ be the matrix whose rows are a basis of $\operatorname{Ker}\psi_{\xi\xi_j}$ as in the previous corollary. Since W is $B_{\xi\xi_j}$-unimodular (because $\operatorname{Im}\psi_{\xi\xi_j}$ is free) its $(m-q)\times(m-q)$ minors $\gamma_i,\ i\in I$, generate the ring $B_{\xi\xi_j}$. The degrees of these minors are clearly bounded by $((M-s)sD)^{O(1)}$, and then, we may consider again only $((M-s)sD)^{O(n-1)}$ of them.
For each γ_i it is easy to exhibit a basis of the image of the map ψ localized in the polynomial $\gamma_i\xi\xi_j$: it suffices to take the image by ψ of those vectors e_k of the canonical basis, where the k-th column of W is not considered in the construction of γ_i. In this way we obtain a basis for the image of F localized in $\gamma_i\xi\xi_j$ of degrees bounded by $((M-s)sD)^{O(1)}$.

Summarizing, we are able to show local estimations for the degree of a basis of the image of F. We emphasize the fact that the localizing polynomials involve only the variables $x_1,\ldots,x_{n-1}$.

Lemma 14 *There exist polynomials $\pi_1,\ldots,\pi_H\in B$ such that*

1. $1\in(\pi_1,\ldots,\pi_H)$.

2. $\deg\pi_j=((M-s)sD)^{O(1)}$.

3. $H=((M-s)sD)^{O(n)}$.

4. *for all $j=1,\ldots,H$ there exists a basis of $\operatorname{Im} F_{\pi_j}$ formed by polynomial vectors of degree $((M-s)sD)^{O(1)}$.*

Proof.- Take the polynomials π_k as the polynomials $\gamma_i\xi\xi_j$ where ξ runs over all the $q\times q$ minors of G, ξ_j as in Corollary 13, and γ_i as in the previous argument. ■

Definition 15 Let $\widetilde{F} \in A^{\widetilde{N} \times \widetilde{M}}$ be the matrix whose columns are the generators of $\operatorname{Ker} F$ constructed in Lemma 1. Therefore we have :
– $\deg \widetilde{F} \leq sD$.
– $\widetilde{N} := M$.
– $\widetilde{M} \leq 3(M-s)(sD)^n$.
– $\operatorname{Im} \widetilde{F}$ is A-free.
– $\widetilde{s} :=$ the rank of $\widetilde{F}$ (we have $\widetilde{s} = M - s$).
Analogously, let $\widehat{F} \in A^{\widehat{N} \times \widehat{M}}$ be the matrix whose columns are the generators of $\operatorname{Ker} \widetilde{F}$ constructed applying Lemma 1 to $\widetilde{F}$.
– $\deg \widehat{F} \leq (M-s)sD$.
– $\widehat{N} \leq 3(M-s)(sD)^n$.
– $\widehat{M} = ((M-s)sD)^{O(n^2)}$.
– $\operatorname{Im} \widehat{F}$ is A-free.
– $\widehat{s} :=$ the rank of $\widehat{F}$ (where $\widehat{s} = \widetilde{M} - \widetilde{s}$).

For technical reasons we need a similar lemma for $\widetilde{F}$ and $\widehat{F}$. This can be done repeating the arguments used for F. We note that the change of coordinates in Section 3 that assures the existence of a minor monic in all the variables can be made simultaneously for the three matrices F, $\widetilde{F}$ and $\widehat{F}$.

Lemma 16 *There exist polynomials* $\widetilde{\pi}_1, \ldots, \widetilde{\pi}_{\widetilde{H}} \in B$ *such that*

1. $1 \in (\widetilde{\pi}_1, \ldots, \widetilde{\pi}_{\widetilde{H}})$.
2. $\deg \widetilde{\pi}_j = ((M-s)sD)^{O(n)}$.
3. $\widetilde{H} = ((M-s)sD)^{O(n^2)}$.
4. *for all* $j = 1, \ldots, \widetilde{H}$ *there exists a basis of* $\operatorname{Im} \widetilde{F}_{\widetilde{\pi}_j} = \operatorname{Ker} F_{\widetilde{\pi}_j}$ *formed by polynomial vectors of degree* $((M-s)sD)^{O(n)}$. $\blacksquare$

Lemma 17 *There exist polynomials* $\widehat{\pi}_1, \ldots, \widehat{\pi}_{\widehat{H}} \in B$ *such that*

1. $1 \in (\widehat{\pi}_1, \ldots, \widehat{\pi}_{\widehat{H}})$.
2. $\deg \widehat{\pi}_j = ((M-s)sD)^{O(n^2)}$.
3. $\widehat{H} = ((M-s)sD)^{O(n^3)}$.
4. *for all* $j = 1, \ldots, \widehat{H}$ *there exists a basis of* $\operatorname{Im} \widehat{F}_{\widehat{\pi}_j} = \operatorname{Ker} \widetilde{F}_{\widehat{\pi}_j}$ *formed by polynomial vectors of degree* $((M-s)sD)^{O(n^2)}$. $\blacksquare$

Remark 18 Taking the products $\pi_i \widetilde{\pi}_j \widehat{\pi}_k$, we will suppose that the polynomials π_j, $\widetilde{\pi_j}$ and $\widehat{\pi_j}$ are the same in Lemma 14, 16 and 17, with the last estimations for the degree and the number of the polynomials.

5 The main Theorem

This section is devoted to the proof of our main result :

Theorem 19 *Let $F \in A^{N\times M}$ be a polynomial matrix whose image is an A-free module of rank s and whose entries have total degrees bounded by an integer D. Then there exists a basis $\{v_1, \ldots, v_M\}$ of A^M such that:*

- *$\{v_1, \ldots, v_{M-s}\}$ is a basis of $\operatorname{Ker} F$.*
- *the coordinates of the vectors v_j, for $j = 1, \ldots, M-s$, have degree of order $((M-s)sD)^{O(n^3)}$.*
- *$\{F(v_{M-s+1}), \ldots, F(v_M)\}$ is a basis of $\operatorname{Im} F$.*
- *the coordinates of the vectors v_j, for $j = M-s+1, \ldots, M$, have degree of order $((M-s)sD)^{O(n^4)}$.*

On our way to prove this theorem, we will make use *mutatis mutandis* of the local-global techniques due to Vaserstein (see for example [15, Ch.IV, Th.1.18.]) in combination with the effective version of Quillen-Suslin Theorem given in [5].

Recall that for any matrix G with entries in a polynomial ring, $G(0)$ denotes the new matrix obtained by replacing the last variable by 0.

With the notations introduced in the previous section, we will prove the following local result :

Proposition 20 *For all $\pi_j \in B$ chosen after Remark 18 (for $j = 1, \ldots, H$), there exist a non negative integer η and invertible matrices $P_j \in A_{\pi_j}^{M\times M}$ and $Q_j \in A_{\pi_j}^{\widetilde{M}\times\widetilde{M}}$ such that :*

1. $\eta = ((M-s)sD)^{O(n^2)}$.
2. $\pi_j^\eta P_j \in A^{M\times M}$ *and* $\deg(\pi_j^\eta P_j) = ((M-s)sD)^{O(n^2)}$.
3. $\pi_j^\eta Q_j \in A^{\widetilde{M}\times\widetilde{M}}$ *and* $\deg(\pi_j^\eta Q_j) = ((M-s)sD)^{O(n^2)}$.
4. $\widetilde{F} = P_j \widetilde{F}(0) Q_j$.

Proof.- Fix an index j. From Remark 18 one can take the polynomials π_j unifying the Lemmas 14, 16 and 17 and obtains bases for $\operatorname{Im} F_{\pi_j}$, $\operatorname{Im} \widetilde{F}_{\pi_j}$, and $\operatorname{Im} \widehat{F}_{\pi_j}$ of appropriate degrees.
Consider now the exact sequences associated to the matrices F and $\widetilde{F}$:

$$0 \to \operatorname{Im} \widetilde{F}_{\pi_j} \to A_{\pi_j}^M \to \operatorname{Im} F_{\pi_j} \to 0$$

$$0 \to \operatorname{Im} \widehat{F}_{\pi_j} \to A_{\pi_j}^{\widetilde{M}} \to \operatorname{Im} \widetilde{F}_{\pi_j} \to 0$$

From the first sequence, one obtains a basis of $A_{\pi_j}^M$ lifting the s vectors of the basis of $\operatorname{Im} F_{\pi_j}$ and adding the $M-s$ vectors of the basis of $\operatorname{Im} \widetilde{F}_{\pi_j}$. Write $\mathcal{B}_j$ for this basis.
In the same way one obtains a basis $\mathcal{C}_j$ of $A_{\pi_j}^{\widetilde{M}}$ from the second exact sequence completing the basis of $\operatorname{Im} \widehat{F}_{\pi_j}$ with the preimages of the basis of $\operatorname{Im} \widetilde{F}_{\pi_j}$ in $A_{\pi_j}^{\widetilde{M}}$. From the previous results one infers that all the polynomial vectors of $\mathcal{B}_j$ and $\mathcal{C}_j$ have degree bounded by $((M-s)sD)^{O(n^2)}$.
For all integer q, denote by $\mathcal{E}_q$ the canonical basis of A^q.
Then, we have

$$\widetilde{F} = P\ C\ Q,$$

where

- $P := [\ \mathrm{Id}\ ]_{\mathcal{B}_j \mathcal{E}_M} \in A_{\pi_j}^{M\times M}$,
- $Q := [\ \mathrm{Id}\ ]_{\mathcal{E}_{\widetilde{M}} \mathcal{C}_j} \in A_{\pi_j}^{\widetilde{M}\times \widetilde{M}}$
- C is the diagonal matrix : $\begin{pmatrix} \mathrm{Id}_{M-s} & 0 \\ 0 & 0 \end{pmatrix}$.

Moreover, the matrices $\pi_j^\eta P$ and $\pi_j^\eta Q$ have all their entries in A and their degrees of order $((M-s)(sD))^{O(n^2)}$, for a certain $\eta \in \mathbb{N}$ of order $((M-s)sD)^{O(n^2)}$.
Finally, replacing x_n by 0, one has :

$$\widetilde{F}(0) = P(0)\ C\ Q(0).$$

And then :

$$\widetilde{F} = P_j\ \widetilde{F}(0)\ Q_j$$

where $P_j := PP^{-1}(0)$ and $Q_j := Q^{-1}(0)Q$ are invertible matrices in A_{π_j}, with controlled degrees (recall that $\pi_j \in B$). ∎

Now we make use of the argument of [15, Ch.IV, Th.1.18.] in order to "glue" the matrices P_j's and the matrices Q_j's.

Lemma 21 *There exist two invertible matrices $P \in A^{M\times M}$ and $Q \in A^{\widetilde{M}\times\widetilde{M}}$ of degrees of order $((M-s)sD)^{O(n^3)}$ such that $\widetilde{F} = P\widetilde{F}(0)Q$.*

Proof.- Fix an index j, $j = 1, \ldots, H$, and let y be a new variable. Consider the matrices with entries in $A_{\pi_j}[y]$:

$$P_j(x_n+y)P_j^{-1}\ ,\ P_jP_j^{-1}(x_n+y)\ ,\ Q_j^{-1}(x_n+y)Q_j\ ,\ Q_j^{-1}Q_j(x_n+y).$$

From Proposition 20 (modifying slightly η, if necessary), we may suppose that the matrices

$$P_j(x_n+\pi_j^\eta y)P_j^{-1}\ ,\ P_jP_j^{-1}(x_n+\pi_j^\eta y)\ ,\ Q_j^{-1}(x_n+y\pi_j^\eta)Q_j\ ,\ Q_j^{-1}Q_j(x_n+\pi_j^\eta y)$$

have all the entries in $A[y]$ (it suffices to take an appropriate power of π_j in order to eliminate the denominators).

Then, the matrices

$$\Gamma_j := P_j(x_n + \pi_j^\eta y)P_j^{-1} \quad \text{and} \quad \Lambda_j := Q_j^{-1}Q_j(x_n + \pi_j^\eta y)$$

are invertible in $A[y]^{M\times M}$ and $A[y]^{\widetilde{M}\times\widetilde{M}}$ respectively, with entries of degree of order $((M-s)sD)^{O(n^2)}$.
Again after Proposition 20 we have the relation :

$$\widetilde{F}(x_n + \pi_j^\eta y) \;=\; \Gamma_j\;\widetilde{F}\;\Lambda_j \tag{16}$$

for $j = 1, \ldots, H$.
From item 1 of Lemmas 14-17 and Remark 18, we have $1 \in (\pi_1^\eta, \ldots, \pi_H^\eta)$ and, applying the effective Nullstellensatz (see [13] or [9]), there exist $\alpha_1, \ldots, \alpha_H \in x_nB$ such that :

$$x_n = \alpha_1\pi_1^\eta + \cdots + \alpha_H\pi_H^\eta \quad \text{and} \quad \deg\alpha_j = ((M-s)sD)^{O(n^3)} \;\; \forall j.$$

Considering the identity (16) for $j := H$ and replacing $x_n \mapsto \sum_{q=1}^{H-1}\alpha_q\pi_q^\eta$ and $y \mapsto \alpha_H$, we get :

$$\widetilde{F} \;=\Gamma_H(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta, \alpha_H)\;\widetilde{F}(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta)\;\Lambda_H(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta, \alpha_H).$$

Applying once again the formula (16), with $j := H-1$, and replacing $x_n \mapsto \sum_{q=1}^{H-2}\alpha_q\pi_q^\eta$ and $y \mapsto \alpha_{H-1}$, we have

$$\widetilde{F}(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta) \;=\Gamma_{H-1}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta, \alpha_{H-1})\;\widetilde{F}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta)\;\Lambda_{H-1}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta, \alpha_{H-1}),$$

and then $\widetilde{F}$ can be written

$$\Gamma_H(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta, \alpha_H)\Gamma_{H-1}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta, \alpha_{H-1})\;\widetilde{F}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta)\;\Lambda_{H-1}(\sum_{q=1}^{H-2}\alpha_q\pi_q^\eta, \alpha_{H-1})\Lambda_H(\sum_{q=1}^{H-1}\alpha_q\pi_q^\eta, \alpha_H).$$

Thus, we obtain for all index u, $u = 0, \ldots, j$, where $j = 1, \ldots, H$ a relation of the type :

$$\widetilde{F} \;=\; \Big[\prod_{u=0}^{j}\Gamma_{H-u}(\sum_{q=1}^{H-u-1}\alpha_q\pi_q^\eta, \alpha_{H-u})\Big]\;\widetilde{F}(\sum_{u=1}^{H-j}\alpha_q\pi_q^\eta)\;\Big[\prod_{u=0}^{j}\Lambda_{H-u}(\sum_{q=1}^{H-u-1}\alpha_q\pi_q^\eta, \alpha_{H-u})\Big].$$

In particular, for $j = H$, the assertion follows. ■

Applying the same argument in a recurrent way on the number of variables, one deduces :

Corollary 22 *There exist two invertible matrices* $V \in A^{M\times M}$ *and* $W \in A^{\widetilde{M}\times\widetilde{M}}$ *of degrees of order* $((M-s)sD)^{O(n^3)}$ *such that*

$$\widetilde{F} \;=\; V\widetilde{F}(0,\ldots,0)W.$$

In particular, there exists a basis of $\operatorname{Im}\widetilde{F}$ *formed by vectors of degree of order* $((M-s)sD)^{O(n^3)}$.

Proof.- From Remark 2 we have that $F(0)$ verifies the same conditions as F and that $\widetilde{F(0)} = \widetilde{F}(0)$ (since the vectors $w_j(0)$ are a system of generators of $\operatorname{Ker} F(0)$). Therefore we can apply again the same argument as in Lemma 21 to the matrix $\widetilde{F}(0)$. $\blacksquare$

Now, we are able to prove Theorem 19.

<u>Proof of Theorem 19.-</u> Since $\operatorname{Im}\widetilde{F} = \operatorname{Ker} F$, Corollary 22 allows us to estimate the degrees of a certain basis $v_1,\ldots,v_{M-s}$ of $\operatorname{Ker} F$. Applying [5, Th.3.1.] for the unimodular matrix in $A^{(M-s)\times M}$ formed by these vectors, we infer the existence of s vectors $v_{M-s+1},\ldots,v_M$ in A^M such that $\{v_1,\ldots v_M\}$ is a basis of A^M and $\deg v_i \le ((M-s)sD)^{O(n^4)}$, for $i = M-s+1,\ldots,M$.
Clearly $\{F(v_{M-s+1}),\ldots,F(v_M)\}$ is a basis of $\operatorname{Im} F$ and the theorem is proved. $\blacksquare$

6 The case of the matrix of a projection map

In this section $F \in A^{M\times M}$ denotes a polynomial matrix such that $F^2 = F$ (i.e. F is the matrix of a projection map of A^M). It is well known that in this case $A^M = \operatorname{Ker} F \oplus \operatorname{Im} F$ and, in particular, $\operatorname{Im} F$ and $\operatorname{Ker} F$ are both A-free.
Since $F' := \operatorname{Id} - F$ corresponds also to a projection map and since the bases of $\operatorname{Ker} F$ and $\operatorname{Im} F$ form a basis of A^M, several arguments of the last two sections can be simplified and the degree bounds in Theorem 19 may be improved.
We observe first that the Lemmas 14, 16 and 17 can be replaced by the following result (which doesn't involve neither the auxiliar matrix $\widetilde{F}$ nor the matrix $\widehat{F}$) :

Lemma 23 *Let* $F \in A^{M\times M}$ *be the matrix of a projection map whose entries are polynomials with total degrees bounded by an integer* D *and let* s *be the rank of* F. *Then there exist polynomials* $\pi_1,\ldots,\pi_H \in B$ *such that :*

1. $1 \in (\pi_1,\ldots,\pi_H)$.
2. $\deg \pi_j = ((M-s)sD)^{O(1)}$.
3. $H = ((M-s)sD)^{O(n)}$.
4. *for all index* $j = 1,\ldots,H$, *there exist bases of* $\operatorname{Im} F_{\pi_j}$ *and* $\operatorname{Ker} F_{\pi_j}$ *consisting of polynomial vectors of degrees of order* $((M-s)sD)^{O(1)}$.

Proof.- Applying Lemma 14 to F and F' one obtains a family of polynomials $\pi_j \in B$ and bases for $\operatorname{Im} F_{\pi_j}$ and $\operatorname{Im} F'_{\pi_j}$ with appropriate degrees (indeed, the polynomials π_j for F and F' are different but this constraint can be avoided multiplying them as in Remark 18). Since $\operatorname{Im} F'_{\pi_j} = \operatorname{Ker} F_{\pi_j}$ the lemma follows. ■

With the aid of this lemma, we are able to simplify the proof of Proposition 20 observing that the join of a basis of $\operatorname{Im} F$ and a basis of $\operatorname{Im} F'$ gives a basis of the whole space A^M. Since Lemma 21 and Corollary 22 follow directly from Proposition 20, we obtain analougous results for the matrix F instead of the matrix $\widetilde{F}$. The improvement of the degree upper bounds in this case is due to the fact that the introduction of the matrices $\widetilde{F}$ and $\widehat{F}$ is unnecessary.
We can summarize these facts in the following more precise statement of Theorem 19 :

Theorem 24 *Let $F \in A^{M\times M}$ be the matrix of a projection map involving polynomials whose degrees are bounded by an integer D and let s be the rank of F. Then there exists a basis $\{v_1, \dots, v_M\}$ of A^M, such that the first $M-s$ vectors form a basis of $\operatorname{Ker} F$, the last s vectors are a basis of $\operatorname{Im} F$ and the degrees of the coordinates of these vectors are of order $((M-s)sD)^{O(n)}$.* ■

We observe that if the matrix F does not correspond to a projection map, but the space A^M is decomposed as $\operatorname{Ker} F \oplus \operatorname{Im} F$, the arguments of the last two sections can be also simplified. In this case it is enough to consider the Lemmas 14 and 16, in order to obtain Proposition 20, Lemma 21 and Corollary 22 for the matrix F. In fact, for these three results it is only necessary to know how to complete the bases of the image and the kernel to bases of the whole space under a suitable localization; the matrix $\widetilde{F}$ must be introduced in order to obtain a basis of a localization of $\operatorname{Ker} F$ and then the bases of the kernel and the image can be completed.
In other words we have :

Theorem 25 *Let $F \in A^{M\times M}$ be a matrix such that $A^M = \operatorname{Ker} F \oplus \operatorname{Im} F$. Suppose that F involves polynomials whose degrees are bounded by an integer D and that s is the rank of F. Then there exists a basis $\{v_1, \dots, v_M\}$ of A^M, such that the first $M-s$ vectors form a basis of $\operatorname{Ker} F$ and have degrees of order $((M-s)sD)^{O(n^2)}$, and the last s vectors are a basis of $\operatorname{Im} F$ and have degrees of order $((M-s)sD)^{O(n^3)}$.* ■

7 An application to reduced complete intersections

Let k be an infinite field and $f_1, \dots, f_{n-r}$ be a regular sequence in $k[x_1, \dots, x_n]$ of degrees bounded by an integer $d > 1$. Suppose that the variables $x_1, \dots, x_n$ are in Noether position with respect to the polynomials f_i. More precisely, the natural map $k[x_1, \dots, x_r] \to k[x_1, \dots, x_n]/(f_1, \dots, f_{n-r})$ is an injective and integral morphism.

Write $R := k[x_1, \dots, x_r]$ and $S := k[x_1, \dots, x_n]/(f_1, \dots, f_{n-r})$.
It is well known (see for example [8, Corollary 18.17] or [12, Lemma 3.3.1]) that, under these conditions, S is a locally free R-module of finite rank (bounded by d^{n-r} following Bezout's Inequality) and hence free (Quillen-Suslin Theorem).

This context ("polynomial regular sequence + Noether position") appears frequently in several approaches related to effectivity problems in Computer Algebra, even in the positive dimensional case (see for instance [21], [11], [22]). At this point it is quite natural to look for properties of R-bases of S (degree bounds, algorithms to compute them, etc.), but we have been unable to find any significative result related to this subject in the literature.
In this frame we are interested in the study of the existence of a basis consisting of polynomials with single exponential degrees, in the case where the ring S is reduced.
For this purpose we combine our previous results with quantitative facts about duality in complete intersection rings (following [16] and [22]).

We start by recalling some known facts about duality theory.
We denote by S^* the dual space $\mathrm{Hom}_R(S,R)$. The R-module S^* admits a natural structure of S-module in the following way : for any pair (b,β) in $S\times S^*$ the product $b.\beta$ is the R-linear application of S^* defined by $(b.\beta)(x):=\beta(bx)$, for each x in S.
Our assumptions about R and S allow to show that the S-modules S and S^* are isomorphic (see [16, Example F.19 and Corollary F.10]) and therefore S^* can be generated by a single element.
A generator σ of S^* is called a *trace* of S over R. If char(k)=0 it is well known that, under our hypothesis, the application $b\mapsto \mathrm{Tr}(\eta_b)$ is a trace of S over R (where η_b is the endomorphism induced by the multiplication by $b\in B$ and Tr is the usual trace).
Therefore we have the following :

Proposition 26 (see [22, Proposition 3]) *There exist a trace $\sigma\in S^*$ and polynomials a_m and c_m in $k[x_1,\ldots,x_n]$, $1\le m\le M$, such that :*
– $\deg(a_m)+\deg(c_m)\le (n-r)(d-1)$ *;*
– $M\le 3(n-r)(d-1)^{n-r}$ *;*
– *the "trace formula" : $b=\sum_m \sigma(b\overline{c}_m)\overline{a}_m$ holds for all $b\in S$.* ∎

From this proposition we infer that the classes of the polynomials a_m, $1\le m\le M$, are a system of generators of S over R and that the R-bilinear form $\Phi: S\times S\to R$ defined by $\Phi(b,b'):=\sigma(bb')$ is non degenerate.

By means of Proposition 26 we are able to apply our previous results about polynomial matrices in order to obtain the following :

Theorem 27 *There exists a basis of S over R formed by polynomials of degrees of order $d^{O((n-r)r^4))}$.*

Proof.- Let $F: R^M\to R^M$ be the linear map defined by the matrix $(\Phi(\overline{a}_i,\overline{a}_j))_{ij}$ and let $G: R^M\to S$ be the map defined by $e_j\mapsto \overline{a}_j$. Since S is free, $\mathrm{Ker}\, G$ is a free R-submodule of R^M.
From the fact that Φ is non degenerate, it is easy to see that $\mathrm{Ker}\, F=\mathrm{Ker}\, G$ and that the following diagram is commutative :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \operatorname{Ker} F & \longrightarrow & R^M & \xrightarrow{F} & \operatorname{Im} F & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \varphi} & & \\
0 & \longrightarrow & \operatorname{Ker} G & \longrightarrow & R^M & \xrightarrow{G} & S & \longrightarrow & 0
\end{array}$$

where φ is an isomorphism.
In particular, $\operatorname{Im} F$ is also a free R-module.
From [22, Theorem 13], one has

$$\deg \Phi(\overline{a}_i, \overline{a}_j) = \deg \sigma(\overline{a}_i \overline{a}_j) \leq \deg(V)(1+\max\{\deg(a_i a_j), (n-r)d\}) \leq \deg(V)(1+2(n-r)(d-1))$$

(where V is the set of all the common zeros of $f_1, \ldots, f_{n-r}$). By means of Bezout Inequality we deduce :

$$\deg(F) = \max_{i,j}\{\deg \Phi(\overline{a}_i, \overline{a}_j)\} \leq d^{n-r}(1 + 2(n-r)(d-1)).$$

Applying Theorem 19 to the matrix F we obtain a basis for $\operatorname{Ker} F$ of degrees of order $d^{O((n-r)r^3)}$ and then, a basis for $\operatorname{Im} F$ of degrees of order $d^{O((n-r)r^4)}$. Through φ we get a basis for S with the same degree upper bounds. ∎

References

[1] Alonso M., Becker E., Roy M.-F., Wörmann T. : Zeros, Multiplicities and Idempotents for Zerodimensional Systems.- Effective Methods in Alg. Geom. (MEGA '94), Progress in Math. **143**, Birkhäuser Verlag (1996)

[2] Armendáriz I., Solernó P. : On the computation of the radical of polynomial complete intersection ideals.- Appl. Algebra, Algebraic Algorithms and Error-Correcting Codes (G.Cohen, M.Giusti & T.Mora, eds.), Lect. Notes Comp. Sci. **948** Springer-Verlag (1995) 106-119.

[3] Berenstein C., Struppa D. : Recent improvements in the Complexity of the Effective Nullstellensatz.- Linear Algebra and its Appl. **157** (1991) 203-215.

[4] Bruns W., Vetter U. : *Determinantal Rings.*- Springer Lect. Notes in Math. **1327** (1988).

[5] Caniglia L., Cortiñas G., Danón S., Heintz J., Krick T., Solernó P. : Algorithmic aspects of Suslin's Proof of Serre's Conjecture.- Comput. Complexity **3**, Birkhäuser (1993) 31-55.

[6] Cardinal J.-P. : Dualité et algorithmes itératifs pour la résolution de systèmes polynomiaux.- Thesis Université de Rennes (1993).

[7] Demazure M. : Le monoïde Mayr et Meyer.- Notes Informelles de Calcul Formel, Ecole Polytechnique, Palaiseau (1984).

[8] Eisenbud D. : *Commutative Algebra with a view toward Algebraic Geometry.*- Graduate Texts in Math. **150**, Springer-Verlag (1994).

[9] Fitchas N., Galligo A. : Nullstellensatz effectif et Conjecture de Serre (théorème de Quillen-Suslin) pour le Calcul Formel.- Math. Nachr. **149** (1990) 231-253.

[10] Gantmacher F. : *Matrix Theory, Vol.I* .- Chelsea Publ. Co., New York (1960).

[11] Giusti M., Heintz J., Morais J., Morgenstern J., Pardo L. : Straight-line Programs in Geometric Elimination Theory.- J. Pure and Appl. Algebra (1997).

[12] Giusti M., Heintz J., Sabia J. : On the efficiency of effective Nullstellensatz.- Comput. Complexity **3** Birkhäuser (1993) 56-95.

[13] Kollár J. : Sharp effective Nullstellensatz.- J. Am. Math. Soc. **1** (1988) 963-975.

[14] Krick T., Pardo L. : A computational Method for Diophantine Approximation.- Effective Methods in Alg. Geom. (MEGA '94), Progress in Math. **143**, Birkhäuser Verlag (1996) 193-253.

[15] Kunz E. : *Introduction to Commutative Algebra and Algebraic Geometry.*- Birkhäuser (1985).

[16] Kunz E. : *Kähler Differentials.*- Adv.Lect. in Math. Vieweg Verlag (1986).

[17] Lam T. : *Serre's Conjecture.*- Springer LN Math. **635** Springer-Verlag (1978).

[18] Logar A., Sturmfels B. : Algorithms for Quillen-Suslin Theorem.- J. Algebra **145** (1992) 231-239.

[19] Lombardi H. : La structure d'un module projectif de type fini et le contenu constructif d'un principe local-global.- Preprint (1996).

[20] Mayr E., Meyer A. : The complexity of the word problem for commutative semigroups and polynomial ideals.- Adv. in Math. **46** (1982) 305-329.

[21] Rossi F., Spangher W. : Some effective methods in the openness of loci for Cohen-Macaulay and Gorenstein properties.- Effective Methods in Alg. Geom. (MEGA '90) (T.Mora & C.Traverso, eds.), Progress in Math. **94**, Birkhäuser (1990) 441-455.

[22] Sabia J., Solernó P. : Bounds for traces in Complete Intersections and Degrees in the Nullstellensatz.- AAECC Journal **6**, No.6, Springer-Verlag (1995) 353-376.

[23] Teissier B.: Résultats récents d'algèbre commutative effective.- Séminaire Bourbaki 1989-1990, Astérisque vol **189-190** (1991) 107-131.