ELSEVIER

Journal of Pure and Applied Algebra 162 (2001) 127–170

JOURNAL OF PURE AND APPLIED ALGEBRA

www.elsevier.com/locate/jpaa

Computing bases of complete intersection rings in Noether position ☆

Marcela Almeida[a], Manuela Blaum[b,*], Lisi D'Alfonso[a], Pablo Solernó[b]

[a] *Departamento de Matemática, Facultad Ciencias Exactas y Naturales, Universidad de Buenos Aires, 1428 Buenos Aires, Argentina*

[b] *Universidad de San Andrés, Departamento de Matemáticas, Vito Dumas 284, 1644 Victoria, Argentina*

Received 25 November 1999; received in revised form 22 May 2000
Communicated by M.-F. Roy

Abstract

Let k be an effective infinite perfect field, $k[x_1,\ldots,x_n]$ the polynomial ring in n variables and $F \in k[x_1,\ldots,x_n]^{M\times M}$ a square polynomial matrix verifying $F^2 = F$. Suppose that the entries of F are polynomials given by a straight-line program of size L and their total degrees are bounded by an integer D. We show that there exists a well parallelizable algorithm which computes bases of the kernel and the image of F in time $(nL)^{O(1)}(MD)^{O(n)}$. By means of this result we obtain a single exponential algorithm to compute a basis of a complete intersection ring in Noether position. More precisely, let $f_1,\ldots,f_{n-r} \in k[x_1,\ldots,x_n]$ be a regular sequence of polynomials given by a slp of size ℓ, whose degrees are bounded by d. Let $R := k[x_1,\ldots,x_r]$ and $S := k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$ such that S is integral over R; we show that there exists an algorithm running in time $O(n)\ell d^{O(n^2)}$ which computes a basis of S over R. Also, as a consequence of our techniques, we show a single exponential well parallelizable algorithm which decides the freeness of a finite $k[x_1,\ldots,x_n]$-module given by a presentation matrix, and in the affirmative case it computes a basis.

MSC: 68Q40; 13P10; 13C10

☆ Partially supported by the grants ANPCyT 03-00000-01593, UBA-CYT TW80 and PIP CONICET 4571.
* Corresponding author.
E-mail addresses: malmeida@dm.uba.ar (M. Almeida), mblaum@dm.uba.ar (M. Blaum), lisi@dm.uba.ar (L. D'Alfonso), psolerno@dm.uba.ar (P. Solernó).

0022-4049/01/$ - see front matter
PII: S0022-4049(00)00135-3

1. Introduction

The aim of this paper is the effective computation of bases of certain free modules over the polynomial ring $k[x_1,\ldots,x_n]$, where k is an arbitrary effective infinite perfect field. Essentially, we consider two main cases of free $k[x_1,\ldots,x_n]$-modules: the kernel and the image of a polynomial projection matrix (Theorem A below) and a complete intersection ring in Noether position (Theorem C below). We consider also the more general case of the freeness of $k[x_1,\ldots,x_n]$-modules given a presentation matrix (Theorem B below).

Before stating the main results of this paper we make a brief description of the computational model we use here: it follows the model presented in several previous articles (see for instance [18,20,19]), where an exhaustive study of its advantages and limitations with respect to other alternative ones is done. For this reason we give here only a minimum of notions and basic facts about it.

1.1. The computational model

Let k be an effective infinite perfect field. The algorithms we shall use are described by *arithmetic networks* (cf. [47]) represented by acyclic oriented graphs where each node represents a constant of k, an input variable, an arithmetic operation $* \in \{+,-,\times,\div\}$ in k, a Boolean operation, an equality test or a selection. We shall suppose that our arithmetic networks are always *division-free*: this means that when evaluating the network on a generic point (i.e. on its input variables) we execute only divisions by nonzero constants from k (therefore our arithmetic networks only compute polynomials with coefficients in k).

We compute arithmetic or Boolean operations, equality tests and selections at unit cost and so we associate to an arithmetic network two complexity measures: *the sequential time* or *size* (the quantity of nodes) and *the parallel time* or *depth* (the size of the longest oriented path in the graph). An arithmetic network without decision and selector nodes (and consequently, without Boolean operations) is called an *arithmetic circuit* or *straight-line program* (we write "slp"). Thus, our slp's will always compute polynomials in the input variables with coefficients in k. More precise definitions and properties of arithmetic networks and circuits can be found in [7,47,28].

We say that an algorithm is *well parallelizable* if its parallel time depends polynomially on $\log_2$(sequential time) and on the depth of the input slp's.

The polynomials we deal with will be encoded as arithmetic circuits which evaluate them. However, sometimes we will consider polynomials represented by a vector of coefficients (*dense form*) and also in a mixed form: polynomials encoded in dense form with respect to specific main variables whereas their coefficients with respect to these variables are encoded by an arithmetic circuit.

A key point in our algorithms, as well as in several elimination algorithms, is the problem of deciding if a polynomial is zero or not. Trivial interpolation procedures require the evaluation of the polynomial in many points (if d is the degree of the

polynomial and n the number of variables, one needs $(d+1)^n$ points), in a way that the complexity times increase in a meaningful way.

Nevertheless, when the polynomials are encoded by slp's the following remarkable result holds (see [25] or [18]):

Theorem (Correct test sequences). *Let $W(d,n,L)$ be the set of all the polynomials in $k[x_1,\ldots,x_n]$ of total degrees bounded by d, which may be evaluated by slp's of size L. Set $m := 6(L+n)(L+n+1)$ and let Γ be an arbitrary subset of k whose cardinality is $2L(d+1)^2$. Therefore, there exists a subset $Q = \{\gamma_1,\ldots,\gamma_m\} \subset \Gamma^n$, depending only on d,n,L and Γ, and verifying the following property: a polynomial $f \in W(d,n,L)$ is the zero-polynomial if and only if $f(\gamma_i) = 0$ for all $i = 1,\ldots,m$.*

The vectors $\gamma_1,\ldots,\gamma_m$ are called a *correct test sequence* for the set $W(d,n,L)$. Unfortunately, an efficient procedure to construct a correct test sequence is not known (the standard methods to compute it run in exponential complexity time). Since the degrees, number of variables and evaluation complexity of all polynomials which appear throughout our algorithms may be estimated a priori, in our model we will suppose the reasonable hypothesis that a correct test sequence for all these polynomials is given in a preprocessing step (see also [18]). Anyway, for the reader which remains circumspect because of this assumption, let us remark that an adequate and performing random version for the choice of a correct test sequence can be done (see [18, Section 2.1]); this fact will transform our algorithms in probabilistic algorithms with the same complexity bounds (see also [35]).

1.2. The results

After the seminal paper of Mayr and Meyer [36] (see also [12]) it is well known that the problem of solving linear equation systems over $k[x_1,\ldots,x_n]$ requires double exponential time and involves polynomials of degrees of similar order. In our previous paper [1], we have shown that this double exponential dependence on the degree may be avoided for those systems such that the image of its associated matrix is a free $k[x_1,\ldots,x_n]$-module (for example, projection matrices). Following the same mathematical ideas, combined with appropriate algorithmic constructions, we are able to exhibit a single exponential algorithm to compute bases of the kernel and the image of a projection polynomial matrix:

Theorem A (See Theorem 22 below). *Let $F \in k[x_1,\ldots,x_n]^{M\times M}$ be a polynomial matrix corresponding to a linear projection (i.e. $F^2 = F$) such that its entries are polynomials of degrees bounded by an integer D and are given by a straight-line program of size L. Then there exists a well parallelizable algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$ computing two subsets of $k[x_1,\ldots,x_n]^M$: $\{v_1,\ldots,v_s\}$*

and $\{v_{s+1},\dots,v_M\}$ *such that*

1. $\{v_1,\dots,v_M\}$ *is a basis of* $k[x_1,\dots,x_n]^M$.
2. $\{v_1,\dots,v_s\}$ *is a basis of* $\mathrm{Im}(F)$ *and* $\{v_{s+1},\dots,v_M\}$ *is a basis of* $\mathrm{Ker}(F)$.
3. *The coordinates of the vectors* v_i *are polynomials of degrees bounded by* $(MD)^{O(n)}$ *and they are given by a straight-line program of size* $(nL)^{O(1)}(MD)^{O(n)}$.

Besides, with worse complexity upper bounds (but always in the single exponential class) it is possible to generalize this result for arbitrary unimodular polynomial matrices (see Definition 1 and Theorem 25). This generalization allows to show a "freeness-test" of finitely generated $k[x_1,\dots,x_n]$-modules given by a presentation matrix (see Definition 3):

Theorem B (See Corollary 26 below)**.** Let P *be a* $k[x_1,\dots,x_n]$*-module of finite type and* $F \in k[x_1,\dots,x_n]^{N\times M}$ *a presentation matrix for* P. *Suppose that the entries of the matrix* F *have total degrees bounded by* D *and are given by a straight-line program of size* L. *Then there exists a well parallelizable algorithm which runs in sequential time* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *which decides if* P *is free and in the affirmative case computes a basis of* P.

The techniques we apply are based on the classical ideas of Quillen, Suslin and Vaserstein used to solve the so-called "Serre Conjecture". From the algorithmic point of view many of these ideas appear in several papers related to the computation of bases of free modules, combined with Groebner bases procedures (see for instance [31,33,34]) or with the effective Nullstellensatz (see [16,8]). This paper follows the second approach because the theoretical upper bounds which come from Groebner basis methods are too large for our "single exponential" purposes.

Theorem A plays a main role in our approach to compute bases for complete intersection rings in Noether position (Theorem C below). More precisely, let $f_1,\dots,f_{n-r} \in k[x_1,\dots,x_n]$ be a regular sequence in a polynomial ring over a perfect field k. Suppose that the variables are in Noether position, in other words the canonical morphism $R := k[x_1,\dots,x_r] \to S := k[x_1,\dots,x_n]/(f_1,\dots,f_{n-r})$ is injective and integral. It is well known that under these hypotheses the ring S is an R-free module of finite rank (see [15, Corollary 18.17; 21, Lemma 3.3.1; 41]). This situation appears in a very natural way when one looks for effective solutions of polynomial systems. This problem has been considered mainly in the zero-dimensional case, where the base ring R is the field k and the ring S is simply a finite k-vector space. In this case there exist "good" theoretical algorithms computing a k-basis of S but their techniques cannot be generalized in an obvious way for the positive dimensional case. In fact, up to now, we did not know single exponential algorithms for the general case. In this paper we obtain the following result:

Theorem C (See Theorem 40 below)**.** *Let* $f_1,\dots,f_{n-r} \in k[x_1,\dots,x_n]$ *be a regular sequence of polynomials of degree bounded by an integer* d *and given by a straight-line*

program of size ℓ, such that the canonical morphism $R := k[x_1,\ldots,x_r] \to S := k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$ is injective and integral ("*Noether position*") *and assume that the ring S is reduced* (*i.e. S has no nilpotent elements*). *Then there exists a well parallelizable algorithm running in sequential time $O(n)\ell d^{O(n^2)}$ which computes, from the input polynomials $f_1,\ldots,f_{n-r}$, a slp of size $n^{O(1)}d^{O(n^2)}$ which evaluates a family of polynomials in $k[x_1,\ldots,x_n]$ of degrees bounded by $nd^{O(n^2)}$, and whose classes in S are an R-basis.*

If S is not reduced, it is also possible to compute an R-basis of S by means of an algorithm (*not necessarily well parallelizable*) *which runs in the same sequential time.*

This result may be also reinterpreted from a topological point of view: let $V \subset \mathbb{A}^n$ be the algebraic variety defined by the polynomials $f_1,\ldots,f_{n-r}$ and let $\pi : V \to \mathbb{A}^r$ be the projection map induced by the injection $R \hookrightarrow S$; in terms of algebraic bundles, the freeness of S over R says that the variety V is a trivial bundle over $\mathbb{A}^r$. In this sense Theorem C provides an explicit and algorithmic description of this trivialization.

Our methods are close to those of our previous paper [1], where upper bounds for the degree of representatives of a basis of S are estimated. By means of arguments of traces for complete intersection rings it is possible to construct a matrix F with entries in R whose image is related to a basis of S (Sections 5.3 and 6). The matrix F has the additional property of being a projection matrix (i.e. $F^2 = F$); thus Theorem A allows to construct a basis of its image and, as a consequence, a basis of S verifying the statement of Theorem C. The increase of the complexity bounds in Theorem C with respect to Theorem A is due to the size of the matrix F (typically of order $d^{O(n)}$ from Bezout Theorem).

As we said above, the data structure of the considered algorithms corresponds to encoding polynomials by straight-line programs. However, the algorithms may be also interpreted in a mixed data structure: input polynomials given by a vector of coordinates ("dense representation") while the output is given by straight-line programs. In this case both theorems remain valid forgetting the quantities L and ℓ in the complexity upper bounds. In this model Theorem A may be seen as an algorithm which runs in polynomial time in the length of the input, since the typical length of a polynomial in n variables of degree D is of order D^n (this is not the case of Theorem C, because the exponent $O(n^2)$ appears in the complexity upper bound).

Obviously, our single exponential complexity bounds make hopeless any possible implementation. However, the knowledge of the algebraic structure of the ring associated to a polynomial equations system should play a main role in order to effectively solve it. In this sense this paper represents the first global result on the computation of bases of these rings for the complete intersection case.

The paper is organized as follows: In Section 2 we briefly sketch basic subroutines we shall use throughout the paper (Sections 2.1–2.3). The main result of this section is the elimination of superfluous minors of a polynomial unimodular matrix

that we describe in detail in Section 2.2. The routines described in Sections 2.1 and 2.3 are well known and then, we just quote them without their proofs. Section 3 is devoted to the effective computation of bases of the kernel and the image of a projection polynomial matrix. This is done by means of an effective local–global procedure: the local constructions are described in Sections 3.1–3.3, and the global passage in Section 3.4.

The results of Section 3 are generalized in Section 4 for the case of an arbitrary unimodular polynomial matrix. As a consequence we exhibit a single exponential method to decide the freeness of $k[x_1,\ldots,x_n]$-modules from a presentation matrix.

In Section 5 we apply the classical trace theory for Gorenstein rings in order to describe a basis of a complete intersection ring in Noether position. An overview of the trace theory is given in Section 5.1; meanwhile in Section 5.2 we exhibit explicit degree upper bounds for traces. We make use of these tools in Section 5.3 obtaining bounds for the degree of a certain basis of a complete intersection ring. Finally, in Section 6, we construct effectively this basis.

2. A toolkit of basic algorithms

In this section we describe a family of basic routines we shall use throughout this paper. Almost all of these subalgorithms are well known. We shall describe more explicitly one of them in Section 2.2 (a procedure to decide the unimodularity of a polynomial matrix avoiding superfluous minors) because we do not know a reference of such a result and it implies an apparently new decision procedure to determine the freeness of a $k[x_1,\ldots,x_n]$-module given by generators and their relations (see Proposition 4).

2.1. Basic algorithms

A – *Putting straight-line programs into dense form. Computing the homogeneous components*: Let f be a polynomial in $k[x_1,\ldots,x_n]$ given by a slp of size L. Let $m \in \mathbb{N}$, $1 \leq m \leq n$, and $d := \deg_{x_{n-m+1},\ldots,x_n}(f)$; there exists a well parallelizable algorithm which runs in sequential time $Ld^{O(m)}$ whose output is the coefficients of the polynomial f seen as a polynomial in $k[x_1,\ldots,x_{n-m}][x_{n-m+1},\ldots,x_n]$. Moreover, these coefficients are given by a slp of size $Ld^{O(m)}$ (see [40, Proposition 3.1.1]).

This procedure may be applied in order to obtain the homogeneous components of a given polynomial: let f be a polynomial in $k[x_1,\ldots,x_n]$, of degree D, given by a slp of size L and let t be a new variable; the polynomial $g := f(tx_1,\ldots,tx_n) \in k[x_1,\ldots,x_n,t]$ has degree in t bounded by D and it can be evaluated by a slp of size $L+n$. Interpolating with respect to the variable t, we obtain the homogeneous components of f in time $(L+n)D^{O(1)}$ and we may evaluate them by a slp of size $(L+n)D^{O(1)}$.

B – *Determinant, inverse and rank of polynomial matrices*: Let F be a matrix in $k[x_1,\ldots,x_n]^{N\times N}$ whose entries are polynomials given by a slp of size L. There exist

well parallelizable algorithms running in time $(LN)^{O(1)}$ computing:

1. A slp which evaluates the determinant and the coefficients in $k[x_1,\ldots,x_n]$ of the characteristic polynomial of F.
2. A slp which evaluates the entries of F^{-1} (if F is invertible).
3. The rank of F (as a matrix in $k(x_1,\ldots,x_n)^{N\times N}$) and a submatrix of maximal rank.

The first two items follow from Berkowitz [5] and the last one from Mulmuley [37] (see also a brief description of it in Section 2.2 below); in both cases the mentioned algorithms may be easily adapted for the case of multivariate polynomials given by slp's.

C – *Euclid's polynomial division*: Let f and g be polynomials in $k[x_1,\ldots,x_n]$, of degrees $D_1 \leq D$ and $D_2 \leq D$, respectively, given by a slp of size L, and assume that g is monic with respect to the variable x_n. There exists a well parallelizable algorithm running in time $(LD)^{O(1)}$ producing a slp which evaluates the quotient and the remainder of the Euclid's division of f by g with respect to x_n. Their total degrees are bounded by D_1D_2. This procedure is a straightforward consequence of Subroutine A and the Berkowitz algorithm.

D – *Effective Nullstellensatz*: Let $f_1,\ldots,f_s$ be polynomials in $k[x_1,\ldots,x_n]$ of degrees bounded by D, given by a slp of size L. There exists a well parallelizable algorithm running in time $(nL)^{O(1)}D^{O(n)}$ which decides if 1 belongs to the ideal $(f_1,\ldots,f_s)$ and, if this is the case, it computes by means of a slp of the same size certain polynomials $p_1,\ldots,p_s \in k[x_1,\ldots,x_n]$ such that

1. $1 = p_1f_1 + \cdots + p_sf_s$.
2. $\max_j\{\deg(p_j)\} \leq 3n^2D^{n+1}$.

For a proof see for instance [18,20, Theorem 20] or [22] (for related articles about the Effective Nullstellensatz see also the research papers [6,9,27,43,16,4,10,39,21,42,28,44] and the surveys [3,45]).

E – *Consistence of a system of polynomial equations and inequalities*: Let $f_1,\ldots,f_s$, $g_1,\ldots,g_{s'}$ be polynomials in $k[x_1,\ldots,x_n]$ of degrees bounded by D given by a slp of size L, and let $P := \{f_1 = 0,\ldots,f_s = 0, g_1 \neq 0,\ldots,g_{s'} \neq 0\}$. There exists a well parallelizable algorithm running in time $L^2(ss')^{O(1)}D^{O(n)}$ which decides if P is empty (see [40, Remark 3.4.3]).

F – *Computation of cells*: Let $f_1,\ldots,f_s$ be polynomials in $k[x_1,\ldots,x_n]$. Any non-empty set of type $\{f_1\varepsilon_1 0,\ldots,f_s\varepsilon_s 0,\ \varepsilon_i \in \{=,\neq\}\forall i\}$ is called a *cell*. Following [40] and the "divide and conquer" argument of [17] it is possible to enumerate all the cells by means of a well parallelizable algorithm running in sequential time $L^2s^{O(1)}D^{O(n)}$, where D is an upper bound for the degrees of the polynomials f_i and L is the size of the slp which computes them.

2.2. Eliminating superfluous minors

Definition 1. Let F be a polynomial matrix in $k[x_1,\ldots,x_n]^{N\times M}$ of rank s; we say that F is *unimodular* if their $s\times s$ minors span the whole ring $k[x_1,\ldots,x_n]$.

Customarily the notion of unimodular matrix corresponds to the case of rectangular matrices in $k[x_1,\ldots,x_n]^{N\times M}$, where $N \leq M$ and their $N \times N$ minors generate the polynomial ring, or equivalently, F represents an epimorphism; our definition is slightly more general and corresponds to matrices whose image are direct summands of $k[x_1,\ldots,x_n]^N$ (in particular free by Quillen–Suslin Theorem). Let us observe that any projection matrix F (i.e. $F^2 = F$) is also unimodular, because in this case $N = M$ and $k[x_1,\ldots,x_n]^M = \mathrm{Ker}(F) \oplus \mathrm{Im}(F)$.

If F is a unimodular matrix there are $\binom{M}{s}\binom{N}{s}$ many $s \times s$ minors generating $k[x_1,\ldots,x_n]$; since we are interested in algorithms with complexities at most single exponential on the number of variables n, this quantity (exponential on the size of the matrix) is too large for our purposes. In this subsection we describe an algorithm based on a procedure to find the rank of a matrix over a field, due to Mulmuley (see [38]), which computes an admissible number of these minors and, in particular, it decides if a given polynomial matrix is unimodular (Lemma 2 below).

We start recalling briefly the mentioned Mulmuley's algorithm:

Let H be a matrix in $k^{N\times M}$. First, consider the symmetric square matrix

$$\begin{pmatrix} 0 & H \\ H^t & 0 \end{pmatrix} \in k^{(N+M)\times(N+M)}$$

whose rank is twice the rank of H. Then the matrix

$$H'(\lambda) := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda^{N+M-1} \end{pmatrix} \begin{pmatrix} 0 & H \\ H^t & 0 \end{pmatrix} \in k[\lambda]^{(N+M)\times(N+M)}$$

(where λ is a variable over k), verifies the relation

$$2\mathrm{rk}(H) = \mathrm{rk}(H'(\lambda)) = N + M - \mu,$$

where μ is the biggest power of t dividing the characteristic polynomial $P(t) \in k(\lambda)[t]$ of $H'(\lambda)$.

If $H = (h_{ij}) \in k^{N\times M}$ is a matrix of rank s, the previous procedure can be used to compute a submatrix $\tilde{H} \in k^{s\times s}$ with maximal rank, as follows: Let $R_1,\ldots,R_N$ be the rows of H and $C_1,\ldots,C_M$ be its columns. Using Mulmuley's algorithm, one computes the rank of the submatrices $H^{(i)} \in k^{i\times M}$ for $i = 1,\ldots,N$, whose rows are the first i rows of H. Let us consider the set I whose elements are those indices i, such that $\mathrm{rk}(H^{(i)}) > \mathrm{rk}(H^{(i-1)})$; clearly the cardinal of I is s. Set $\tilde{H}_1 \in k^{s\times M}$ the matrix $(h_{ij})_{i\in I,\ 1\leq j\leq M}$. Repeating this procedure with the columns of H, we have another set of indices J and another submatrix $\tilde{H}_2 \in k^{N\times s}$ with linearly independent columns C_j, with $j \in J$. Let us see that the submatrix $\tilde{H} := (h_{ij})_{i\in I,\ j\in J} \in k^{s\times s}$ is invertible. Actually, the matrix H can be reduced by elementary row operations into a matrix of type

$$\begin{pmatrix} \tilde{H}_1 \\ 0 \end{pmatrix} = UH,$$

where $U \in k^{N\times N}$ is an invertible matrix. Since the columns C_j, for $j \in J$, are linearly independent, this is true for the corresponding columns of UH too, and so $\tilde{H}$ is invertible.

From the previous procedure, we are able to eliminate "superfluous" minors of a given unimodular matrix, as follows:

Lemma 2. *Let F be a polynomial matrix in $k[x_1,\ldots,x_n]^{N\times M}$ of rank s, whose entries are polynomials of degrees bounded by D and given by a slp of size L. Then there exist $\delta_1,\ldots,\delta_Q \in k[x_1,\ldots,x_n]$, $s\times s$-non-zero minors of the matrix F, $Q \le ((M+N)^6D)^n$, such that $1 \in (\delta_1,\ldots,\delta_Q)$ if and only if F is a unimodular matrix (see Definition 1).*

These minors can be computed by means of a well parallelizable algorithm which runs in sequential time $(nL)^{O(1)}((N+M)D)^{O(n)}$, and they are given by a slp of size $(sL)^{O(1)}$. Moreover, this procedure gives a method to decide if a given matrix is unimodular in time $(nL)^{O(1)}((N+M)D)^{O(n)}$.

Proof. Let $F^{(i)} \in k[x_1,\ldots,x_n]^{i\times M}$ be the submatrix of F whose rows are the first i rows of F, $1 \le i \le N$. By Mulmuley, for each $\alpha \in k^n$, the rank of $F^{(i)}(\alpha)$ is equal to $(M+i-\mu_i)/2$, where μ_i is the biggest power of t dividing the characteristic polynomial $P_i(\alpha,\lambda,t)$ of the matrix:

$$F^{(i)'}(\alpha,\lambda) := \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & \lambda & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \lambda^{M+i-1} \end{pmatrix} \cdot \begin{pmatrix} 0 & F^{(i)}(\alpha) \\ F^{(i)}(\alpha)^t & 0 \end{pmatrix} \in k[\alpha,\lambda]^{(M+i)\times(M+i)}.$$

Clearly, $P_i(\alpha,\lambda,t)$ is a polynomial in the variables λ,t and also in the coordinates of the point α. The polynomial $P_i(x,\lambda,t) \in k[x_1,\ldots,x_n,\lambda,t]$ may be written as

$$t^{M+i} + a^i_{M+i-1}(x,\lambda)t^{M+i-1} + \cdots + a^i_{\mu_i}(x,\lambda)t^{\mu_i},$$

where each $a^i_j(x,\lambda) \in k[x_1,\ldots,x_n,\lambda]$ is a sum of determinants of square $(M+i-j)$-submatrices of $F^{(i)'}(x,\lambda)$ and then

$$\deg_\lambda a^i_j(x,\lambda) \le 1+2+\cdots+(M+i-1) = \frac{(M+i-1)(M+i)}{2} < \frac{(M+N)^2}{2}.$$

Repeating the previous arguments for the submatrices $C^{(k)}$ whose columns are the first k columns of F we obtain, in a similar way, polynomials $b^k_l(x,\lambda)$, $l=0,\ldots,N+k-1$, such that

$$\deg_\lambda b^k_l(x,\lambda) < \frac{(N+M)^2}{2}$$

for $k=1,\ldots,M$.

Let us consider now the set $\Gamma \subset k[x_1,\ldots,x_n]$, whose elements are all the coefficients of the polynomials a^i_j and $b^k_l \in k[x_1,\ldots,x_n][\lambda]$ for $i=1,\ldots,N$, $j=0,\ldots,M+i-1$, $k=1,\ldots,M$ and $l=0,\ldots,N+k-1$.

Since the polynomials a^i_j, b^k_l can be evaluated by a slp of size $((N+M)L)^{O(1)}$ (Berkowitz's algorithm), interpolating in the variable λ (cf. [40, Proposition 3.1.1] or Subroutine A), we obtain the polynomials of Γ also by means of a slp of size $((N+M)L)^{O(1)}$.

Remark that the cardinal of Γ is bounded by

$$N(N+M)\left(\frac{(N+M)^2}{2}+1\right)+M(N+M)\left(\frac{(N+M)^2}{2}+1\right)=(N+M)^{O(1)}.$$

Moreover, observe that each consistent sign condition over the polynomials of Γ determines uniquely the rank of the submatrices $F_1(\alpha),\ldots,F_N(\alpha),C_1(\alpha),\ldots,C_M(\alpha)$, for any point $\alpha\in\bar{k}^n$ verifying such a sign condition (where $\bar{k}$ denotes an algebraic closure of the field k).

Thus, if we fix now a consistent sign condition over Γ, the choice of rows and columns of F made as in Mulmuley's procedure is the same for any point $\alpha\in\bar{k}^n$ verifying the mentioned sign condition. In other words, there is an assignation between the set of consistent sign conditions over Γ and the set of certain submatrices of F of rank at most s, such that for any point α verifying a fixed sign condition its associated submatrix is invertible when it is evaluated in α.

In this way, computing all the consistent sign conditions over Γ by means of the algorithm described in [17] (see also Subroutine F) we obtain certain distinguished submatrices of F. Taking into account the cardinal of Γ, the degrees of its elements and the cost of computing them, these submatrices can be obtained in time$(nL)^{O(1)}((N+M)D)^{O(n)}$. Since the number of consistent sign conditions is bounded by $((N+M)^6D)^n$ (see [24, Section 3, Corollary 1]) the number of these submatrices can be bounded by the same constant. We take the polynomials $\delta_1,\ldots,\delta_Q$ as the determinants of those associated submatrices which have size $s\times s$.

In order to see that $\delta_1,\ldots,\delta_Q$ verify the statement of the lemma, let us observe that if F is unimodular the matrix in $k^{N\times M}$ obtained by evaluation in any arbitrary point $\alpha\in\bar{k}^n$ has also rank s, independently of the point α; in other words we have: $\mathrm{rk}(F)=\mathrm{rk}(F_N(\alpha))=\mathrm{rk}(C_M(\alpha))=s$ for all $\alpha\in\bar{k}^n$ (this fact is a consequence of the Nullstellensatz and Definition 1). Hence, since any point $\alpha\in\bar{k}^n$ satisfies at least one of the consistent sign conditions, the associated submatrix must have size $s\times s$ and its determinant is non-zero after the evaluation in α; then the polynomials $\delta_1,\ldots,\delta_Q$ generate the polynomial ring $k[x_1,\ldots,x_n]$. The converse implication is obvious.

Finally, in order to check the unimodularity of F, it suffices to compute the polynomials $\delta_1,\ldots,\delta_Q$ and to check if they generate the ring $k[x_1,\ldots,x_n]$ by means of the effective Nullstellensatz (see Subroutine D). This procedure does not increase in a meaningful way the previous complexity time. □

As an easy consequence of the previous lemma we are able to describe an effective decision test about the freeness of a finitely generated $k[x_1,\ldots,x_n]$-module, given by generators and relations. Up to our knowledge this method improves the previous results on the matter, at least from the complexity point of view (see also [34, Section 2]).

Definition 3. Let P be a $k[x_1,\ldots,x_n]$-module of finite type, a matrix $F \in k[x_1,\ldots,x_n]^{N\times M}$ is called a *presentation matrix for* P if there exists a surjective map $\varphi : k[x_1,\ldots,x_n]^M \to P$ such that the rows of F are a system of generators of $\mathrm{Ker}(\varphi)$.

If D is a bound for the degrees of the entries of F and L is a bound for the sizes of the slp which computes them, we have the following result (see also Corollary 26):

Proposition 4. *There exists a well parallelizable algorithm which decides, from the input presentation matrix F, the freeness of P in sequential time* $(nL)^{O(1)}((N+M)D)^{O(n)}$.

Proof. Let us consider the exact sequence:

$$0 \to \mathrm{Ker}(\varphi) \to k[x_1,\ldots,x_n]^M \to P \to 0.$$

If P is $k[x_1,\ldots,x_n]$-free, since the previous sequence splits, $\mathrm{Ker}(\varphi)$ must be a direct summand of $k[x_1,\ldots,x_n]^M$. Conversely, if $\mathrm{Ker}(\varphi)$ is a direct summand of $k[x_1,\ldots,x_n]^M$, we have $P \oplus \mathrm{Ker}(\varphi) \simeq k[x_1,\ldots,x_n]^M$ and then, by Quillen–Suslin Theorem, P must be free.

Therefore, it suffices to decide if $\mathrm{Ker}(\varphi) = \mathrm{Im}(F^t)$ is a direct summand of $k[x_1,\ldots,x_n]^M$, or equivalently, the unimodularity of the matrix F. Therefore, in order to decide the freeness of P it suffices to apply Lemma 2. □

2.3. A linear change of coordinates

Let F be a $N \times M$ polynomial matrix of rank s whose entries are polynomials of degrees bounded by a constant D and given by a slp of size L. Following Mulmuley's algorithm mentioned in Subroutine B item 3, it is possible to obtain, in time $(L(N+M))^{O(1)}$, a non-singular $s \times s$ submatrix of F whose determinant $\mu \in k[x_1,\ldots,x_n]$ can be evaluated by a slp of size $(sL)^{O(1)}$.

For technical reasons, in the sequel, we shall need the polynomial μ to be monic in all the variables $x_1,\ldots,x_n$. More precisely, if $\delta := \deg(\mu)$ we need that $\mu = \alpha_1 x_1^\delta + \cdots + \alpha_n x_n^\delta + \tilde{\mu}$ where $\alpha_1,\ldots,\alpha_n \in k$, $\alpha_j \neq 0\ \forall j = 1,\ldots,n$ and $\tilde{\mu} \in k[x_1,\ldots,x_n]$ has degree at most $\delta - 1$. This can be done making a linear change of coordinates in the ground ring $k[x_1,\ldots,x_n]$ as follows: let μ_K the homogeneous component of μ of maximal degree $K \leq sD$; this homogeneous polynomial μ_K can be computed from the matrix F by means of an algorithm which runs in sequential time $(Ln(N+M)D)^{O(1)}$, whose output is a slp of size $((sL)^{O(1)}+n)(sD)^{O(1)}$ which evaluates μ_K (see Subroutine A). It suffices to exhibit a linear change of coordinates making μ_K monic in all the variables.

For this, let us consider now n^2 new variables $(T_{ij})_{1\leq i,j\leq n}$ and set $G := \det(T_{ij}) \prod_{j=1}^n \mu_K(T_{1j},\ldots,T_{nj})$; the polynomial G is not the zero polynomial in n^2 variables, its degree is $n(K+1) \leq n(sD+1)$ and can be evaluated by a slp of size $(LnsD)^{O(1)}$.

From the theorem of correct test sequences mentioned in Section 1.1, there exists a subset $Q \subseteq k^{n^2}$, whose cardinal is $6((LnsD)^{O(1)} + n^2)((LnsD)^{O(1)} + n^2 + 1) = (LnsD)^{O(1)}$, such that, for all polynomial H in n^2 variables of degree at most $n(sD+1)$ and given by a slp of size at most $(LnsD)^{O(1)}$, we have

$$H = 0 \quad \Leftrightarrow \quad H(\gamma) = 0 \quad \forall \gamma \in Q.$$

Therefore, fixing $\gamma = (\gamma_{11}, \ldots, \gamma_{1n}, \ldots, \gamma_{n1}, \ldots, \gamma_{nn}) \in Q$ such that $G(\gamma) \neq 0$, the new variables $z_1, \ldots, z_n$ are defined by means of the following relations:

$$x_j := \gamma_{1j} z_1 + \cdots + \gamma_{nj} z_n, \quad j = 1, \ldots, n.$$

This change of variables can be done in time $(Ln(N+M)D)^{O(1)}$.

Further, if $f \in k[x_1, \ldots, x_n]$ is given by a slp of size L, its corresponding polynomial after the mentioned linear change of coordinates, can be evaluated by a new slp on the variables $z_1, \ldots, z_n$ of size $L + n^2$.

Let us observe that a similar change can be done simultaneously for a given finite family of matrices (we shall use this fact for the matrices F and $\mathrm{Id} - F$, when F is a projection).

3. Construction of bases for the image and the kernel of a polynomial projection matrix

In this section we deal with the construction of bases for the image and the kernel of a polynomial projection matrix $F \in k[x_1, \ldots, x_n]^{M \times M}$. Our approach follows seminal ideas of several works concerning the proof of the ex-Serre's conjecture (see [32,29]): we shall construct bases and systems of generators of suitable localizations of the image and the kernel of F, which we shall be able to glue by means of a quantitative version of Vaserstein's Theorem via the effective Nullstellensatz. In this procedure the fact that we may consider only localizations in polynomials lying in the ring $k[x_1, \ldots, x_{n-1}]$ plays a main role in order to allow recursive methods. Thus we start with the construction of a free $k[x_1, \ldots, x_{n-1}]$-module related to the image of F.

We recall that k denotes a perfect infinite field and $\bar{k}$ its algebraic closure; we write $\mathbb{A}^n$ for the n-dimensional affine space $\bar{k}^n$ equipped with the Zariski topology.

We shall denote in the sequel $A := k[x_1, \ldots, x_n]$ and $B := k[x_1, \ldots, x_{n-1}]$; $F \in k[x_1, \ldots, x_n]^{M \times M}$ will be a projection matrix of rank s, that we shall call "the input matrix". The entries of F are polynomials whose total degrees are bounded by an integer D, and they are given by a slp of size L.

For the sake of simplicity we shall suppose also that the first $s \times s$ principal minor μ is monic in all the variables $x_1, \ldots, x_n$. In other words we assume that the linear change of coordinates described in Section 2.3 is done. The complexity cost and the modifications of the sizes of the slp's in the input polynomials will be taken into account only for the estimations of the main theorem (Theorem 22).

3.1. A free $k[x_1,\dots,x_{n-1}]$ -module related to $\mathrm{Im}(F)$

Denote by $C_1,\dots,C_M$ the columns of F and let $\mathscr{L}$ be the free $k[x_1,\dots,x_n]$-module generated by $C_1,\dots,C_s$. We consider the exact sequence

$$0 \to \mathscr{L} \to \mathrm{Im}(F) \to Q \to 0,$$

where $Q := \mathrm{Im}(F)/\mathscr{L}$.

Since μ is monic and $\mu Q = 0$, Q admits a natural structure of $k[x_1,\dots,x_{n-1}]$-module generated by the classes of $x_n^k C_i$ with $k = 0,\dots,d := \deg(\mu) - 1$, $i = s+1,\dots,M$. Moreover, Q is a free $k[x_1,\dots,x_{n-1}]$-module of finite rank (cf. [1, Proposition 3] or [29, Chapter 3, Proposition 3.4]).

Definition 5. Let $\varphi : B^m \to Q$ where $m := (d+1)(M-s)$ the epimorphism defined as follows: if $e_{0,s+1}, e_{1,s+1},\dots,e_{d,s+1},\dots,e_{d,M}$ is the canonical basis of B^m, $\varphi(e_{k,i}) := \overline{x_n^k C_i}$ (observe that $\mathrm{Ker}(\varphi)$ is also B-free by Quillen–Suslin).

From now on, we shall construct a system of generators for $\mathrm{Ker}(\varphi)$ as follows:

Let $w_1,\dots,w_M$ be the canonical generators of $\mathrm{Ker}(F)$ (i.e. $w_i := e_i - C_i$, $i = 1,\dots,M$, where $\{e_1,\dots,e_M\}$ is the canonical basis of A^M); in particular their coordinates have degrees bounded by D.

Since μ is monic in x_n, we can compute the euclidean division of each coordinate of w_j by μ in $B[x_n]$ following Subroutine C, obtaining vectors q_j and r_j in A^M, in time $M(DsL)^{O(1)}$ such that

$$w_j = \mu q_j + r_j. \tag{1}$$

The degree in x_n of each coordinate of r_j is bounded by d, meanwhile, its total degree is bounded by sD^2 and r_j can be evaluated by a slp of size $(DsL)^{O(1)}$.

Since there are M many vectors w_j, the total time to compute all vectors q_j and r_j is $M^2(DsL)^{O(1)}$.

Now, for each $x_n^k r_j \in A^M$ with $j = 1,\dots,M$ and $k = 0,\dots,d$, we compute again the euclidean division

$$x_n^k r_j = \mu q_{kj} + r_{kj}, \tag{2}$$

where $r_{kj} \in A^M$, $\deg r_{kj} = 2(sD)^3$ and $\deg_{x_n} r_{kj} \le d$. This can be done in time $M^2(DsL)^{O(1)}$ and each coordinate can be evaluated by a slp of size $(DsL)^{O(1)}$.

For each vector r_{kj}, we consider the vector V_{kj} consisting on their $M-s$ last coordinates. For simplicity, we replace the multi-index kj by $h = 1,\dots,M(d+1)$.

Interpolating the vectors V_h with respect to the variable x_n, we have

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

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

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

All the polynomials $V_{h,k,l}$ can be obtained by means of Subroutine A in time $M^2(DsL)^{O(1)}$ and each one can be evaluated by a slp of size $(DsL)^{O(1)}$.

Following [1, Proposition 5] one shows that 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 $h = 1, \ldots, M(d+1)$, are a system of generators of $\mathrm{Ker}(\varphi)$. Summarizing, we have the following result:

Proposition 6. *There exists a system of generators of* $\mathrm{Ker}(\varphi)$ *which can be constructed from the input matrix* F *means of an algorithm with complexity time* $(MDL)^{O(1)}$. *The coefficients of these vectors can be evaluated by a slp of size* $(DsL)^{O(1)}$.

This proposition can be restated as follows:

Lemma 7. *There exists a matrix* $G \in B^{m \times p}$, *where* $m := (M-s)(d+1)$, $p := M(d+1)$ *and* $\deg G \leq 2(sD)^3$, *such that* $\mathrm{Im}(G) = \mathrm{Ker}(\varphi)$.

This matrix can be computed from the input matrix F *in sequential time* $(MDL)^{O(1)}$. *The entries of* G *can be evaluated by a slp of size* $(DsL)^{O(1)}$.

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

In other words, we have obtained a matrix whose transposed is a presentation of the B-module Q. This presentation shall be used in the next section in order to compute local presentations for the A-module $\mathrm{Im}(F)$.

3.2. Another local presentation for $\mathrm{Im}(F)$

By means of an elementary argument based on Cramer's rule and Nakayama's Lemma, it is easy to exhibit bases for the image and the kernel of F under localizations by suitable polynomials of A (see for instance [1, Lemma 1]). Unfortunately, we do not know how to glue these local bases in order to obtain global bases; the essential constraint seems to be the fact that the polynomials used in the localizations lie in $k[x_1, \ldots, x_n]$ but not in $k[x_1, \ldots, x_{n-1}]$. In this section we show alternative presentations for the image of F under localizations by polynomials in B, where the recursive gluing methods inspired in Vaserstein's results can be applied as we shall see in Section 3.3.

We recall the notations introduced previously. We denote by s the rank of the projection matrix F and by $\mu \in A$ the first principal $s \times s$ minor of F; after the change of coordinates given in Section 2.3, μ is a monic polynomial in all the variables. Set $d := \deg_{x_n} \mu - 1$ and $m := (d+1)(M-s)$ (see Definition 5).

We set $\varphi : B^m \to \underline{Q} := \mathrm{Im}(F)/\mathscr{L}$ the B-linear application defined on the canonical basis by $\varphi(e_{ki}) := \overline{x_n^k C_i}$, for $k = 0, \ldots, d$ and $i = s+1, \ldots, M$ (where $\mathscr{L}$ is the A-free module generated by the first s columns of F, denoted by $C_1, \ldots, C_s$; see Definition 5).

Let $G \in B^{m \times p}$ be the matrix whose columns are a system of generators of the kernel of φ, following Lemma 7, and let $q \leq m$ be the rank of the B-module $\mathrm{Ker}(\varphi)$ (which is free because B is a polynomial ring and Q is B-free from [1, Proposition 3]).

The $q \times q$ minors of G generate the ring B (since $\mathrm{Im}(G) = \mathrm{Ker}(\varphi)$ is a direct summand of B^m) and their degrees are bounded by $2q(sD)^3$ (therefore by $2(M - s)(sD)^4$). Moreover we are able to compute an admissible number of them directly from the algorithm described in Lemmas 2 and 7:

Proposition 8. *It is possible to construct $q \times q$ minors $\xi_1, \ldots, \xi_l$ of the matrix G such that*

- $1 \in (\xi_1, \ldots, \xi_l)$,
- $l \leq ((m + p)^6 2(sD)^3)^{n-1} = (MD)^{\mathrm{O}(n)}$,
- $\deg(\xi_i) \leq 2q(sD)^3$.

This can be done from the input matrix F in sequential time $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$ and each minor ξ_i can be evaluated by a slp of size $(qsDL)^{\mathrm{O}(1)} = (MLD)^{\mathrm{O}(1)}$.

Unfortunately, despite of the polynomials $\xi_1, \ldots, \xi_l \in B$ generate the whole ring B, we are not able to construct a basis for the localized A_ξ-module $\mathrm{Im}(F_\xi)$, and we shall need to refine them by suitable multiplications (see Lemma 17 below).

From now on, we fix ξ among the non-zero $q \times q$ minors obtained in the previous proposition.

Without loss of generality, we may suppose that ξ involves the first q columns of G, that we will denote by $K_1, \ldots, K_q$ (in particular $\varphi(K_1) = \cdots = \varphi(K_q) = 0$).

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 5). For the sake of simplicity we will denote the vectors 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 ξ or $-\xi$. Let us observe that the matrix Z can be constructed directly from the matrix G (see the previous proposition).

Then we have:

Proposition 9. *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.*

The following definition allows to show a new local presentation for $\mathrm{Im}(F)$ which we shall consider in the sequel.

Definition 10. Let $\psi : A^{m-q+s} \to \mathrm{Im}(F)$ 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 9 and the definition of Q), and then $\mathrm{Ker}(\psi_\xi)$ is a projective A_ξ-module because $\mathrm{Im}(F_\xi)$ is A_ξ-free

Now, we shall study more deeply the structure of this morphism ψ when it is localized in the minor ξ. Let us 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 9 and the definition of the B-module Q, for each index ℓ, $\ell = 1,\ldots,m-q$, there exist unique $\tilde{\beta}_1^{(\ell)},\ldots,\tilde{\beta}_{m-q}^{(\ell)} \in B_\xi$ and $\tilde{\alpha}_1^{(\ell)},\ldots,\tilde{\alpha}_s^{(\ell)} \in A_\xi$ such that

$$-x_n x_n^{k_\ell} C_{i_\ell} = \sum_{j=1}^{m-q} \tilde{\beta}_j^{(\ell)} x_n^{k_j} C_{i_j} + \sum_{i=1}^{s} \tilde{\alpha}_i^{(\ell)} C_i. \tag{3}$$

In the following two propositions we shall describe more precisely the fractions $\tilde{\beta}_j^{(\ell)}$ and $\tilde{\alpha}_i^{(\ell)}$ (see also [1, Section 4, (12)]).

Proposition 11. *There exist polynomials $\beta_j^{(\ell)} \in B$, $j=1,\ldots,m-q$, with total degrees bounded by $2(M-s)(sD)^4$, such that for each index j we have*

$$\tilde{\beta}_j^{(\ell)} = \frac{\beta_j^{(\ell)}}{\xi}.$$

These polynomials can be constructed from the input matrix F by means of an algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$ and can be evaluated by a slp of size $(LMD)^{O(1)}$.

Proof. 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 5).

On the other hand, we can write in B_ξ^m:

$$-e = \lambda_1 K_1 + \cdots + \lambda_q K_q + \lambda_{q+1} u_1 + \cdots + \lambda_m u_{m-q} = Z \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix} \tag{4}$$

and then, obviously

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

Hence, applying φ we have

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

(recall that $\varphi(K_l) = 0$ for all l and $\varphi(u_j) = \overline{x_n^{k_j} C_{i_j}}$).

Therefore in (3) we have $\tilde{\beta}_j^{(\ell)} := \lambda_{q+j}$, for all $j = 1,\ldots,m-q$.

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

$$\tilde{\beta}_j^{(\ell)} = \frac{\beta_j^{(\ell)}}{\xi}, \tag{5}$$

where the $\beta_j^{(\ell)}$'s can be computed as determinants of suitable matrices in $B^{m\times m}$ (Cramer's rule and Subroutine B). Taking into account the complexity time to construct the matrix Z, the polynomials $\beta_j^{(\ell)}$'s can be computed in time $(nL)^{O(1)}(MD)^{O(n)}$ and can be evaluated by a slp of size $(LMD)^{O(1)}$.

For the case $k_\ell = d$, instead of $-x_n^{1+k_\ell}C_{i_\ell}$, we may write $(x_n^{d+1}-\mu)C_{i_\ell}$ (since their classes are the same in Q) and the construction runs similarly.

The degree upper bound for the polynomials $\beta_j^{(\ell)}$ is straightforward. □

Proposition 12. *There exist polynomials $\alpha_j^{(\ell)} \in A$, $j=1,\dots,m-q$, with total degrees bounded by $4(M-s)(sD)^4$, such that for each index j we have*

$$\tilde{\alpha}_j^{(\ell)} = \frac{\alpha_j^{(\ell)}}{\xi}.$$

These polynomials can be constructed from the input matrix F by means of an algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$ and can be evaluated by a slp of size $(MLD)^{O(1)}$.

Proof. First, let us show that $\xi\tilde{\alpha}_j^{(\ell)}$ belongs to A. Rewriting formula (3), from the previous proposition we have that there exist $Q_1,\dots,Q_{M-s} \in B_\xi[x_n]$ such that the equality

$$Q_1C_{s+1}+\cdots+Q_{M-s}C_M = \sum_{i=1}^{s}\tilde{\alpha}_i^{(\ell)}C_i$$

holds in A_ξ^N and ξQ_l are polynomials in A of degrees bounded by $d+4(M-s)(sD)^4$ for all $l=1,\dots,M-s$.

On the other hand, since the first s columns of F are linearly independent and the rank of F is s, the column vectors $\mu C_{s+1},\dots,\mu C_M$ can be written as A-linear combinations of the columns $C_1,\dots,C_s$ (Cramer's rule) as follows:

$$C_{s+l} = \sum_{r=1}^{s}\frac{b_{rl}}{\mu}C_r, \tag{6}$$

for certain $b_{rl}\in A$, with $1\le r\le s$ and $1\le l\le M-s$.

Then we have

$$Q_1C_{s+1}+\cdots+Q_{M-s}C_M = Q_1\sum_{r=1}^{s}\frac{b_{r1}}{\mu}C_r+\cdots+Q_{M-s}\sum_{r=1}^{s}\frac{b_{r\ M-s}}{\mu}C_r.$$

And thus, we deduce the equality:

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

for all $i=1,\dots,s$.

Let h be the minimal exponent such that $\xi^h\tilde{\alpha}_i^{(\ell)}\in A$. 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 $h \leq 1$, and then

$$\xi\tilde{\alpha}_i^{(\ell)} \in A \quad \text{and} \quad \mu \text{ divides } \xi \sum_{l=1}^{M-s} b_{il} Q_l \quad \text{in } A. \tag{7}$$

Therefore to construct the polynomials $\alpha_i^{(\ell)} := \xi\tilde{\alpha}_i^{(\ell)}$ we proceed as follows:

- Rewriting $-\xi x_n^{k_\ell+1} C_{i_\ell} - \sum_{j=1}^{m-q} \beta_j^{(\ell)} x_n^{k_j} C_{i_j}$ as an A-linear combination of the last columns $C_{s+1}, \ldots, C_M$ we obtain the polynomials $\xi Q_1, \ldots, \xi Q_{M-s}$ in A; these polynomials can be evaluated by a slp of size $(DLM)^{O(1)}$ and their degrees are bounded by $2(M-s)(sD)^4 + sD - 1$.
- Rewriting $\mu C_{s+1}, \ldots, \mu C_M$ in terms of the first columns $C_1, \ldots, C_s$ as in the relation (6), by means of Cramer's rule and Subroutine B, we obtain the polynomials $b_{il} \in A, 1 \leq i \leq s, 1 \leq l \leq M-s$ of degrees bounded by sD; these polynomials can be evaluated by a slp of size $(sL)^{O(1)}$.
- From the previous items we compute $\sum_{l=1}^{M-s} b_{il}\xi Q_l$ and then we obtain $\mu\alpha_j^{(\ell)}$. From the previous estimations this polynomial can be evaluated by a slp of size $(DLM)^{O(1)}$ and their degrees are bounded by $2(M-s)(sD)^4 + 2sD - 2$.
- Finally, in order to obtain $\alpha_j^{(\ell)}$ we compute the euclidean division of $\mu\alpha_j^{(\ell)}$ by μ with respect to x_n as in Subroutine C (recall that μ is monic in all the variables).

The complexity times of this procedure depend essentially on the construction of the polynomials $\beta_j^{(\ell)}$s and therefore they are of the same order than those stated in the previous proposition. □

Moreover, with the notations above we have the following result:

Proposition 13. *Let $U \in A_\xi^{(m-q)\times(m-q+s)}$ be the matrix whose ℓth 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 ℓth vector of the canonical basis of A^{m-q+s}). Then U 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 $\mathrm{Ker}(\psi_\xi)$ *(in particular* $\mathrm{Ker}(\psi_\xi)$ *is free).*

The matrix $\xi U \in A^{(m-q)\times(m-q+s)}$ can be computed from the input matrix F by an algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$. Moreover, each entry of ξU can be evaluated by a slp of size $(LMD)^{O(1)}$ and $\deg \xi U \leq 4(M-s)(sD)^4$.

Proof. The "purely mathematical"contents of the statement are proved in [1, Proposition 9] and the complexity estimations follow immediately from the previous constructions of the $\alpha_j^{(\ell)}$'s and $\beta_j^{(\ell)}$'s. □

Let us observe that the matrix U corresponds to a presentation of the A_ξ-module $\mathrm{Im}(\psi_\xi)$.

3.3. Construction of local bases for the image of F

The main results of this section (Proposition 14 and Lemmas 15 and 16 below) allow to construct adequate polynomials in B in order to obtain bases for localizations of $\mathrm{Im}(F)$ (see Lemma 17 below) by means of suitable changes of coordinates in $A_\xi^{(m-q+s)}$.

For the sake of simplicity we shall denote by $[\beta] := (\beta_j^{(\ell)})_{j,\ell} \in B^{(m-q)\times(m-q)}$ and by $[\alpha] := (\alpha_j^{(\ell)})_{j,\ell} \in A^{(m-q)\times s}$.

First, following [29, Chapter IV, Lemma 3.12], we are able to simplify the matrix U (introduced in Proposition 13) using "x_n-division with remainder" between the matrix $\frac{1}{\xi}[\alpha]$ (formed by the last s columns of U) and the matrix $x_n \,\mathrm{Id}_{m-q} + \frac{1}{\xi}[\beta]$ (consisting of the first $m-q$ columns of U) in the obvious way:

Proposition 14. *There exists a matrix $C \in A^{(m-q+s)\times(m-q+s)}$ whose determinant is a power of ξ (hence C is invertible as a matrix in $A_\xi^{(m-q+s)\times(m-q+s)}$) and matrices $U_1 \in A^{(m-q)\times(m-q)}$, $U_2 \in B^{(m-q)\times s}$, satisfying the following items*:

- $UC = (U_1 \mid U_2)$.
- $U_1 = \xi x_n \,\mathrm{Id}_{m-q} + [\beta]$.
- *C, U_1 and U_2 can be obtained from the input matrix F by an algorithm which runs in sequential time $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$.*
- *The entries of the matrices C, U_1 and U_2 can be evaluated by a slp of size $(MLD)^{\mathrm{O}(1)}$.*
- *The degrees of the entries of the matrices C and U_2 are bounded by $(MD)^{\mathrm{O}(1)}$ and those of U_1 by $2(M-s)(sD)^4$.*

Proof. Set $t := 4(M-s)(sD)^4$ the upper bound for the total degrees of the entries of the matrix $[\alpha]$. From Euclid's division algorithm, there exist unique matrices $q_0, \ldots, q_{t-1}, r \in B^{(m-q)\times s}$ such that the following formula holds:

$$\xi^t[\alpha] = (\xi x_n \,\mathrm{Id}_{m-q} + [\beta])(q_{t-1}x_n^{t-1} + \cdots + q_0) + r. \tag{8}$$

The entries of the columns of the matrices $q_0, \ldots, q_{t-1}, r$ are the solutions of s many $(t+1)(m-q)$-linear systems of equations over the ring B, and all these systems have the same associated matrix:

$$\begin{pmatrix} \xi \,\mathrm{Id}_{(m-q)} & 0 & \cdots & \cdots & 0 \\ [\beta] & \xi \,\mathrm{Id}_{(m-q)} & \cdots & \cdots & \vdots \\ 0 & \cdots & \ddots & \cdots & \vdots \\ \vdots & \cdots & [\beta] & \xi \,\mathrm{Id}_{(m-q)} & 0 \\ 0 & \cdots & 0 & [\beta] & \mathrm{Id}_{(m-q)} \end{pmatrix}.$$

Their inhomogeneous components are the entries of the columns of the matrices $\xi^t a_t, \ldots, \xi^t a_0$, where $[\alpha] = x_n^t a_t + \cdots + a_0$ (each a_i is a matrix in $B^{(m-q)\times s}$); these entries can be computed interpolating with respect to x_n the coefficients of $[\alpha]$ (see

Subroutine A or [40, Proposition 3.11]). This can be done from the input matrix F by an algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$ and evaluates each entry by a slp of size $(MLD)^{O(1)}$.

Since the determinant of the systems is equal to $\xi^{(m-q)t}$, using Cramer's rule without divisions, we obtain (only computing determinants) the entries of the unknown matrices $\xi^{(m-q)t}q_{t-1},\ldots,\xi^{(m-q)t}r$ with the same complexity bounds above.

Summarizing, we have constructed two polynomial matrices $Q\in A^{(m-q)\times s}$ and $R\in B^{(m-q)\times s}$ such that

$$\xi^{(m-q)t+t+1}\frac{[\alpha]}{\xi}=\left(x_n\,\mathrm{Id}_{m-q}+\frac{[\beta]}{\xi}\right)Q+R$$

(where $Q:=x_n^{t-1}\xi^{(m-q)t+1}q_{t-1}+\cdots+\xi^{(m-q)t+1}q_0$ and $R:=\xi^{(m-q)t}r$).

The matrix

$$C:=\begin{pmatrix}\xi\,\mathrm{Id}_{m-q} & -Q\\ 0 & \xi^{(m-q)t+t+1}\,\mathrm{Id}_s\end{pmatrix}$$

verifies the statements of the proposition. □

The matrix U can be modified by another change of coordinates in order to obtain all its entries belonging to a suitable localization of the ring B. For this purpose it is convenient to consider the matrix UC in Proposition 14 as a $k(x_1,\ldots,x_{n-1})[x_n]$-unimodular matrix in order to apply Suslin's reduction procedure following [32,8] (see the next two lemmas). Unfortunately, this approach requires the construction of certain new polynomials in B playing the role of the ξ's.

Lemma 15. *Let $V:=UC$ where U and C are the matrices defined in Propositions* 13 and 14, *respectively. There exist invertible matrices $\Lambda_1,\ldots,\Lambda_T\in k^{(m-q+s)\times(m-q+s)}$, with $T=((M-s)sD)^{O(1)}$, such that: if $V^{(i)}:=V\Lambda_i$, $\Delta_1^{(i)}:=\det[V_1^{(i)},\ldots,V_{m-q}^{(i)}]$ (the $(m-q)\times(m-q)$-minor built from the first $m-q$ columns of $V^{(i)}$), $\Delta_2^{(i)}:=\det[V_1^{(i)},\ldots,V_{m-q-1}^{(i)},V_{m-q+1}^{(i)}]$ and $c_i:=\mathrm{Res}_{x_n}(\Delta_1^{(i)},\Delta_2^{(i)})$ (the resultant of $\Delta_1^{(i)},\Delta_2^{(i)}$ with respect to the indeterminate x_n), then for each $z\in\mathbb{A}^{n-1}\setminus\{\xi=0\}$ there exists an index i, $1\le i\le T$, such that $c_i(z)\neq 0$ (in other words the polynomials $c_1,\ldots,c_T$ generate the ring B_ξ).*

Moreover, these polynomials (whose degrees are bounded by $(MD)^{O(1)}$) can be constructed from the input matrix F by an algorithm which runs in sequential time $(nL)^{O(1)}(MD)^{O(n)}$ and can be evaluated by slp's of size $(MLD)^{O(1)}$.

Proof. From [1, Lemma 11] we know that for each $z\in\mathbb{A}^{n-1}\setminus\{\xi=0\}$ there exists a matrix Λ (depending on z) such that $\mathrm{Res}_{x_n}(\Delta_1,\Delta_2)(z)\neq 0$. Following essentially the proof of that result, we are able to exhibit a procedure to find a finite number of matrices Λ and then a finite number of resultants generating B_ξ. The key point in the obtention of this finite family is the introduction of a correct test sequence as was pointed out in [35, Theorem 26].

Let us introduce $(m-q+s)^2$ new indeterminates over k that we denote by $y_{lj}, 1 \leq l,j \leq (m-q+s)$ and let Y be the $(m-q+s)$-square matrix whose entries are the variables y_{lj}.

Let z_0 be an arbitrary (but fixed) point in $\mathbb{A}^{n-1} \setminus \{\xi = 0\}$ and let $P_{z_0} \in k[y_{lj}]$ be the polynomial $\mathrm{Res}_{x_n}(\Delta_1, \Delta_2)\det(Y)$, where $\Delta_1 := \det[V'_1, \ldots, V'_{m-q}]$ is the $(m-q) \times (m-q)$-minor built from the first $m-q$ columns of $V' := V(z_0, x_n)Y$ and $\Delta_2 := \det[V'_1, \ldots, V'_{m-q-1}, V'_{m-q+1}]$.

The polynomial P_{z_0} is non-zero (cf. [1, proof of Lemma 11]) with degree bounded by $(m-q+s)^2$ and it can be evaluated by a slp of size $\lambda := (m-q+s)^{\mathrm{O}(1)}$. These estimations do not depend on the fixed point z_0, and then, if z_0 runs over all the points in $\mathbb{A}^{n-1} \setminus \{\xi = 0\}$, we have an infinite family $\mathscr{F}$ of polynomials in $k[y_{lj}]$ with the same upper bounds for their degrees and size of the slp's which evaluate them.

Therefore (see Section 1.1 or [25]) there exists a correct test sequence for $\mathscr{F}$, say $\gamma_1, \ldots, \gamma_T \in k^{(m-q+s)^2}$, where $T := 6(\lambda + (m-q+s)^2)(\lambda + (m-q+s)^2 + 1)$; in other words for each $z \in \mathbb{A}^{n-1} \setminus \{\xi = 0\}$ there exists at least one γ_i such that $P_z(\gamma_i) \neq 0$. Let Λ_i be the $(m-q+s)$-square matrix associated to γ_i; clearly the matrices $\Lambda_1, \ldots, \Lambda_T$ verify the statements of the lemma.

The complexity bounds follow in the obvious way (the computation involves only products of matrices, computation of determinants, and interpolation with respect to the variable x_n). □

Lemma 16 (Cf. [8 Lemma 4.5]). *Let $V := UC$ be the matrix defined in Lemma* 15. *With the notations of the previous lemma, let i be a fixed index, $1 \leq i \leq T$. Then there exists a matrix $\Omega_i \in A^{(m-q+s)\times(m-q+s)}$ whose determinant is a power of c_i (hence Ω_i is invertible as a matrix in $A_{c_i}^{(m-q+s)\times(m-q+s)}$), such that $V^{(i)}\Omega_i = c_i^2 V^{(i)}(0)$ (where $V^{(i)}(0)$ denotes the matrix $V^{(i)}$ after the evaluation $x_n \mapsto 0$).*

This matrix can be computed from the input matrix F by an algorithm which runs in sequential time $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$. The entries of Ω_i can be evaluated by slp's of size $(MLD)^{\mathrm{O}(1)}$ and their degrees are of order $(MD)^{\mathrm{O}(1)}$.

Proof. For the sake of simplicity we write $W := V^{(i)}, \Delta_1 := \Delta_1^{(i)}, \Delta_2 := \Delta_2^{(i)}$ and $c := c_i$. Let $g, h \in A$ be such that

$$c^2 = g\Delta_1 + h\Delta_2 \quad \text{and} \quad \deg_{x_n}(g), \deg_{x_n}(h) < \max\{\deg_{x_n}(\Delta_1), \deg_{x_n}(\Delta_2)\} \leq m-q.$$

These polynomials can be obtained computing the determinants of the Sylvester's matrix of Δ_1, Δ_2 where some column is replaced by the column

$$\begin{pmatrix} 0 \\ \vdots \\ c \end{pmatrix}$$

(we compute a representation of the polynomial c^2 instead of the resultant c in order to avoid divisions in Cramer's rule). This can be done (from the output of the algorithm underlying in the previous lemma) interpolating the polynomials Δ_1, Δ_2 with respect to

x_n, obtaining in this way the entries of the Sylvester's matrix; finally we compute the mentioned determinants. The complexity times of this procedure do not increase those previously obtained.

Let us consider the submatrices of W: $B_1 := [W_1, \ldots, W_{m-q}] \in A^{(m-q)\times(m-q)}$ and $B_2 := [W_1, \ldots, W_{m-q-1}, W_{m-q+1}] \in A^{(m-q)\times(m-q)}$.

For each j, $m-q+2 \le j \le m-q+s$, we have

$$\begin{aligned} c^2(W_j(0) - W_j) &= (g\Delta_1 + h\Delta_2)(W_j(0) - W_j) \\ &= gB_1 \operatorname{adj}(B_1)(W_j(0) - W_j) + hB_2 \operatorname{adj}(B_2)(W_j(0) - W_j), \end{aligned}$$

where $\operatorname{adj}(B_l)$ denotes the adjoint matrix of B_l, $l = 1, 2$.

Developing this identity we obtain polynomials $g_{kj} \in A$, $1 \le k \le m-q+1$, such that

$$c^2(W_j(0) - W_j) = g_{1j}W_1 + \cdots + g_{m-q+1\,j}W_{m-q+1}.$$

This holds for all index j, $m-q+2 \le j \le m-q+s$. Therefore the matrix Ω' in $A^{(m-q+s)\times(m-q+s)}$ defined as

$$\Omega' := \begin{pmatrix} \mathrm{Id}_{m-q+1} & (g_{kj})_{kj} \\ 0 & c^2\,\mathrm{Id}_{s-1} \end{pmatrix}$$

verifies

$$W\Omega' = [W_1, \ldots, W_{m-q+1}, c^2\,W_{m-q+2}(0), \ldots, c^2 W_{m-q+s}(0)].$$

Now let $\Theta \in A^{(m-q+1)\times(m-q+1)}$ be the matrix defined by

$$\Theta := c \operatorname{adj}\begin{pmatrix} W_1 & \cdots & W_{m-q} & W_{m-q+1} \\ 0 & \cdots & -h & g \end{pmatrix}\begin{pmatrix} W_1(0) & \cdots & W_{m-q}(0) & W_{m-q+1}(0) \\ 0 & \cdots & -h(0) & g(0) \end{pmatrix}.$$

Since c does not depend on x_n, we have that $\det(\Theta) = c^{3(m-q+1)}$, in particular $\Theta \in SL_{m-q+1}(A_c)$. It is easy to see that the matrix Θ verifies

$$[W_1, \ldots, W_{m-q+1}]\,\Theta = c^2[W_1(0), \ldots, W_{m-q+1}(0)].$$

One easily checks now that the matrix

$$\Omega := \Omega' \begin{pmatrix} \Theta & 0 \\ 0 & \mathrm{Id}_{s-1} \end{pmatrix}$$

verifies the assertion. □

From the previous lemmas 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 17. *There exists an algorithm which runs in sequential time* $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$ *from the input matrix* F, *computing polynomials* $\pi_1, \ldots, \pi_H \in B$ *such that*

- $1 \in (\pi_1, \ldots, \pi_H)$,
- $\deg \pi_j = (MD)^{\mathrm{O}(1)}$,

- $H = (MD)^{O(n)}$,
- *each* π_j *can be evaluated by a slp of size* $(MLD)^{O(1)}$.

Moreover, for each $j = 1, \ldots, H$, *the algorithm computes a basis of* $\mathrm{Im}(F_{\pi_j})$ *formed by polynomial vectors of degrees* $(MD)^{O(1)}$ *whose entries can be evaluated by a slp of size* $(MLD)^{O(1)}$.

Proof. The algorithm constructs the polynomials π_j as follows: first let G be the matrix defined in Lemma 7 and let $\xi_1, \ldots, \xi_l \in B$ be the $q \times q$ minors of G as in Proposition 8; for each ξ_k, let $c_1^{(k)}, \ldots, c_T^{(k)} \in B$ be the polynomials constructed in Lemma 15 for the case $\xi := \xi_k$. We have that the quantities l and T are of order $(MD)^{O(n)}$ and $(MD)^{O(1)}$, respectively. Moreover, since the polynomials $\xi_1, \ldots, \xi_l$ span the ring B and $c_1^{(k)}, \ldots, c_T^{(k)}$ the ring B_{ξ_k}, we infer that the polynomials $(\xi_k c_i^{(k)})_{k,i}$ generate the whole ring B.

Fix the indices k, i and let C, Λ_i and Ω_i be the matrices defined in Proposition 14, Lemmas 15 and 16, respectively (for $\xi := \xi_k$ and $c_i := c_i^{(k)}$).

Since $c_i^2 V^{(i)}(0) = V^{(i)}\Omega_i = U(C\Lambda_i\Omega_i)$ and the rows of U form a basis of $\mathrm{Ker}(\psi_\xi)$ (see Proposition 13), the rows of $V^{(i)}(0)$ form a basis of $\mathrm{Ker}(\psi_{\xi c_i})$ after the linear change of coordinates in $A_{\xi c_i}^{(m-q+s)}$ given by the matrix $c_i^{-2}(C\Lambda_i\Omega_i)$.

Since $V^{(i)}(0)$ is $B_{\xi c_i}$-unimodular (because U is $A_{\xi c_i}$-unimodular) its $(m-q)\times(m-q)$ minors generate the ring $B_{\xi c_i}$. By means of Lemma 2, we are able to construct effectively in admissible time, minors $\mu_1, \ldots, \mu_Q$ with $Q = (MD)^{O(n-1)}$ and $B_{\xi c_i} = (\mu_1, \ldots, \mu_Q)$ (the fact that in this case the whole ring is a suitable localization of B instead of a polynomial ring as in Lemma 2, does not make any difference because the enumeration of non-empty cells can be made in a similar way outside a given hypersurface, in this case it suffices to add the condition $\{\xi c_i \neq 0\}$). The degrees of these minors are clearly of order $(MD)^{O(1)}$.

We observe that for each minor μ_u it is easy to compute a basis of the image of the map ψ localized in the polynomial $\mu_u \xi c_i$: it is enough to take the image by ψ of those rows of $\mathrm{adj}(C\Lambda_i\Omega_i)$ corresponding to those columns of $V^{(i)}(0)$ not considered in the construction of μ_u.

We take the polynomials π_j as the polynomials $\mu_u \xi_k c_i^{(k)}$ where $1 \leq k \leq l, 1 \leq i \leq T$ and $1 \leq u \leq Q$. Let us observe that we have $(MD)^{O(n)}$ many polynomials π_j and they generate the ring B.

In this way we obtain a basis for the image of F localized in π_j, whose elements have degrees bounded by $(MD)^{O(1)}$.

The complexity statements follow from the previous construction in the obvious way. □

3.4. Gluing bases

In this section we exhibit a procedure which allows to glue the local bases constructed in Lemma 17. Our approach will make use *mutatis mutandis* of the

local–global techniques due to Vaserstein (see for example [29, Chapter IV, Theorem 1.18]). Let us remark that, at this point, the fact that the localizing polynomials π_j belong to the ring B is crucial in order to obtain an adequate recursive procedure (as well as in the classical proofs of the Serre's conjecture, see for instance [32] or [29]).

For technical reasons we need bases of $\mathrm{Im}(F)$ and $\mathrm{Ker}(F)$ under suitable localizations in elements of the ring B; since $\mathrm{Ker}(F)=\mathrm{Im}(\mathrm{Id}_M - F)$, this can be done applying Lemma 17 for the matrices F and $\mathrm{Id}_M - F$ simultaneously.

Theorem 18. *There exists an algorithm which runs in sequential time* $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$ *from the input matrix* F, *computing polynomials* $\pi_1,\ldots,\pi_H \in B$ *such that*

- $1 \in (\pi_1,\ldots,\pi_H)$,
- $\deg \pi_j = (MD)^{\mathrm{O}(1)}$,
- $H = (MD)^{\mathrm{O}(n)}$,
- *each* π_j *can be evaluated by a slp of size* $(MLD)^{\mathrm{O}(1)}$.

Moreover, for each $j=1,\ldots,H$, *the algorithm computes bases of* $\mathrm{Im}(F_{\pi_j})$ *and* $\mathrm{Im}((\mathrm{Id}-F)_{\pi_j})$ (*and then also a basis of* $\mathrm{Ker}(F_{\pi_j})$) *formed by polynomial vectors of degrees* $(MD)^{\mathrm{O}(1)}$ *whose coordinates can be evaluated by a slp of size* $(MLD)^{\mathrm{O}(1)}$.

Proof. As we have observed in Section 2.3, we can make the same linear change of coordinates for both matrices F and $\mathrm{Id}-F$ in order to obtain principal minors monic in all the variables $x_1,\ldots,x_n$ (this is an essential point because the procedure built in the previous sections is in some sense an elimination procedure of the variable x_n). Therefore, we can apply Lemma 17 to the matrices F and $\mathrm{Id}-F$, obtaining polynomials π_j and π'_k. We may take the polynomials claimed in the theorem as all the products $\pi_j\pi'_k$. Clearly this does not increase the order of the complexity considerations. □

The following result shows an explicit local equivalence between the matrices F and $F(0)$ (recall that $F(0)$ denotes the matrix obtained replacing the variable x_n by 0 in all the entries of F).

Lemma 19. *There exists an algorithm which runs in sequential time* $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$ *and computes, from the input matrix* F, *polynomials* $\delta_1,\ldots,\delta_H \in B$ *and matrices* $P_1,\ldots,P_H,Q_1,\ldots,Q_H \in A^{M\times M}$, *where* $H=(MD)^{\mathrm{O}(n)}$, *such that*

- $1 \in (\delta_1,\ldots,\delta_H)$ *and* $\deg \delta_j = (MD)^{\mathrm{O}(1)}$.
- $\det(P_j) = \det(Q_j) = \delta_j^M$, $j=1,\ldots,H$ (*in particular the matrices* P_j *and* Q_j *are invertible over* A_{δ_j}) *and the degrees of their entries are of order* $(MD)^{\mathrm{O}(1)}$.
- $\delta_j^2 F = P_j F(0) Q_j$.
- *each* δ_j *and each entry of the matrices* P_j *and* Q_j *can be evaluated by a slp of size* $(MLD)^{\mathrm{O}(1)}$.

Proof. For each index j as in Theorem 18, let $\{v_1,\ldots,v_s\}$ and $\{v_{s+1},\ldots,v_M\}$ be the bases of $\mathrm{Im}(F_{\pi_j})$ and $\mathrm{Ker}(F_{\pi_j})$ constructed there. Since F is a projection matrix,

$\mathscr{B}_j := \{v_1, \ldots, v_s, v_{s+1}, \ldots, v_M\}$ is a basis of $A^M_{\pi_j}$. Denote by W_j the matrix whose columns are the vectors $v_1, \ldots, v_M$; we define $\delta_j := \det(W_j)$.

Since the matrix W_j is invertible over A_{π_j}, the polynomial δ_j is a divisor of a suitable power of π_j, therefore δ_j belongs to B and the family $\delta_1, \ldots, \delta_H$ generates the ring B (because $\pi_1, \ldots, \pi_H$ had these properties).

We define, for each index j, the matrices $P_j := \mathrm{adj}(W_j)W_j(0)$ and $Q_j := \mathrm{adj}(W_j(0))W_j$. Clearly the polynomials δ_j and the matrices P_j and Q_j can be obtained directly from the output of the algorithm underlying in Theorem 18 and so, we have the stated complexity estimations.

In order to finish the proof of the lemma, it remains to show the validity of the third item. For this, let us observe that we have the following relations:

$$\delta_j F = \mathrm{adj}(W_j) \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} W_j \tag{9}$$

and

$$\delta_j F(0) = \mathrm{adj}(W_j(0)) \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} W_j(0). \tag{10}$$

From (10) we have

$$\delta_j \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix} = W_j(0)F(0)\mathrm{adj}(W_j(0)).$$

Then, multiplying the identity (9) by δ_j and replacing

$$\delta_j \begin{pmatrix} \mathrm{Id}_s & 0 \\ 0 & 0 \end{pmatrix}$$

by means of the last relation, the lemma follows. □

Now, we shall make use of Vaserstein's argument (see [29, Chapter IV, Theorem 1.18]) in order to "glue" the matrices P_j's and Q_j's.

Lemma 20. *There exists an algorithm which runs in sequential time* $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$ *that computes, from the input matrix* F, *two invertible matrices* $P \in A^{M\times M}$ *and* $Q \in A^{M\times M}$ *such that* $F = PF(0)Q$. *Each entry of these matrices have degree of order* $(MD)^{\mathrm{O}(n)}$ *and can be evaluated by a slp of size* $(nL)^{\mathrm{O}(1)}(MD)^{\mathrm{O}(n)}$.

Proof. Fix an index j, $j = 1, \ldots, H$, and let y be a new variable. With the notations of the previous lemma, let us consider the matrices with entries in $A_{\delta_j}[y]$:

$$\Gamma_j := \frac{P_j}{\delta_j}(x_n + \delta_j^M y)\left(\frac{P_j}{\delta_j}\right)^{-1} \quad \text{and} \quad \Lambda_j := \left(\frac{Q_j}{\delta_j}\right)^{-1} \frac{Q_j}{\delta_j}(x_n + \delta_j^M y),$$

where $(P_j/\delta_j)(x_n + \delta_j^M y)$ denotes the matrix P_j/δ_j after the evaluation $x_n \mapsto x_n + \delta^M y$ and similarly for $(Q_j/\delta_j)(x_n + \delta_j^M y)$.

We start by showing that these matrices belong to $A[y]^{M\times M}$.

Let $p_j^{(k,l)} \in A$ be the (k,l) entry of the matrix P_j; we can write

$$p_j^{(k,l)}(x_n + \delta_j^M y) = p_j^{(k,l)} + \delta_j^M \tilde{p}_j^{(k,l)}(y), \tag{11}$$

where $\tilde{p}_j^{(k,l)}(y)$ is a polynomial in $A[y]$. We denote by $\tilde{P}_j(y) \in A[y]^{M\times M}$ the matrix $(\tilde{p}_j^{(k,l)}(y))_{k,l}$. Since δ_j^M is the determinant of P_j, we have

$$\left(\frac{P_j}{\delta_j}\right)^{-1} = \mathrm{adj}\left(\frac{P_j}{\delta_j}\right) = \frac{\mathrm{adj}(P_j)}{\delta_j^{M-1}}$$

and therefore

$$\Gamma_j = \mathrm{Id}_M + \tilde{P}_j(y)\mathrm{adj}(P_j) \in A[y]^{M\times M}.$$

The same argument applied to the matrix $\Gamma_j^{-1} = (P_j/\delta_j)(P_j/\delta_j)^{-1}(x_n + \delta_j^M y)$ shows that it belongs to $A[y]^{M\times M}$, and therefore Γ_j is an invertible matrix in $A[y]^{M\times M}$.

Similarly one shows that Λ_j can be decomposed as

$$\Lambda_j = \mathrm{Id}_M + \mathrm{adj}(Q_j)\tilde{Q}_j(y),$$

where $\tilde{Q}_j(y)$ is an adequate matrix in $A[y]^{M\times M}$, and also that Λ_j becomes an invertible matrix in $A[y]^{M\times M}$.

In order to compute the matrices Γ_j and Λ_j, it suffices to obtain the matrices $\tilde{P}_j$ and $\tilde{Q}_j$: let z be a new indeterminate and consider the polynomials $p_j^{(k,l)}(x_n+z) - p_j^{(k,l)} \in A[z]$. Clearly, these new polynomials can be computed with the same complexity order as the matrix P_j; moreover, interpolating with respect to the variable z, we are able to obtain polynomials $r_1,\ldots,r_d$ in A (where $d := \deg_{x_n}(p_j^{(k,l)}) = (MD)^{\mathrm{O}(1)}$), such that

$$p_j^{(k,l)}(x_n + z) - p_j^{(k,l)} = \sum_{i=1}^{d} r_i z^i.$$

Therefore, from relation (11), the polynomial $\tilde{p}_j^{(k,l)}(y)$ can be computed evaluating the previous relation in $z \mapsto \delta_j^M y$ (in fact $\tilde{p}_j^{(k,l)}(y) = \sum_{i=1}^{d} r_i \delta_j^{Mi-M} y^i$). Analogously we compute the matrix $\tilde{Q}_j$.

Now we proceed to exhibit the construction of the matrices P and Q.

From Lemma 19, replacing x_n by $x_n + \delta_j^M y$ we have

$$F(x_n + \delta_j^M y) = \frac{P_j}{\delta_j}(x_n + \delta_j^M y)F(0)\frac{Q_j}{\delta_j}(x_n + \delta_j^M y)$$

for $j = 1,\ldots,H$. And then, since $F(0) = (P_j/\delta_j)^{-1}F(Q_j/\delta_j)^{-1}$ (again by Lemma 19), we get

$$F(x_n + \delta_j^M y) \ = \Gamma_j F \Lambda_j \tag{12}$$

for all j.

Since $1 \in (\delta_1^M,\ldots,\delta_H^M)$ (because, by Lemma 19, $1 \in (\delta_1,\ldots,\delta_H)$), applying the effective Nullstellensatz (see Subroutine D or [20, Theorem 20]), we obtain in

sequential time $L^{O(1)}(MD)^{O(n)}$ a slp of size $L^{O(1)}(MD)^{O(n)}$, which evaluates polynomials $\alpha_1,\ldots,\alpha_H \in x_nB$ verifying

$$x_n = \alpha_1\delta_1^M + \cdots + \alpha_H\delta_H^M \quad \text{and} \quad \deg\alpha_j = (MD)^{O(n)} \quad \forall j.$$

Considering identity (12) for $j := H$ and replacing $x_n \mapsto \sum_{q=1}^{H-1} \alpha_q\delta_q^M$ and $y \mapsto \alpha_H$, we get

$$F = \Gamma_H\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M, \alpha_H\right)\ F\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M\right)\ \Lambda_H\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M, \alpha_H\right).$$

Applying once again formula (12), with $j := H-1$, and replacing $x_n \mapsto \sum_{q=1}^{H-2}\alpha_q\delta^M$ and $y \mapsto \alpha_{H-1}$, we have

$$F\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M\right) = \Gamma_{H-1}\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M, \alpha_{H-1}\right) F\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M\right)$$

$$\cdot\Lambda_{H-1}\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M, \alpha_{H-1}\right)$$

and then F can be written as

$$\Gamma_H\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M, \alpha_H\right)\Gamma_{H-1}\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M, \alpha_{H-1}\right) F\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M\right)$$

$$\cdot\Lambda_{H-1}\left(\sum_{q=1}^{H-2}\alpha_q\delta_q^M, \alpha_{H-1}\right)\Lambda_H\left(\sum_{q=1}^{H-1}\alpha_q\delta_q^M, \alpha_H\right).$$

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

$$F = \left[\prod_{u=0}^{j}\Gamma_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right)\right] F\left(\sum_{q=1}^{H-j}\alpha_q\delta_q^M\right)$$

$$\cdot\left[\prod_{u=0}^{j}\Lambda_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right)\right].$$

In particular, for $j = H$,

$$F = \left[\prod_{u=0}^{H}\Gamma_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right)\right] F(0)\left[\prod_{u=0}^{H}\Lambda_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right)\right].$$

Therefore, we take

$$P := \prod_{u=0}^{H}\Gamma_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right) \quad \text{and} \quad Q := \prod_{u=0}^{H}\Lambda_{H-u}\left(\sum_{q=1}^{H-u-1}\alpha_q\delta_q^M, \alpha_{H-u}\right).$$

The complexity bounds follow directly from the computation of the matrices Γ_j and Λ_j and the polynomials α_i's. □

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

Corollary 21. *There exists an algorithm which runs in sequential time* $(nL)^{O(1)}(MD)^{O(n)}$ *from the input matrix* F *that computes two invertible matrices* $P \in A^{M\times M}$ *and* $Q \in A^{M\times M}$ *such that* $F = PF(0,\ldots,0)Q$. *Each entry of these matrices have degree of order* $(MD)^{O(n)}$ *and can be evaluated by a slp of size* $(nL)^{O(1)}(MD)^{O(n)}$.

Now, we are able to proof the main theorem. We remark that the complexity estimations (slightly worse than the previous ones) involve now also the computation of a convenient linear change of coordinates making the minor μ monic (see Section 2.3).

Theorem 22. *Let* $F \in k[x_1,\ldots,x_n]^{M\times M}$ *be a polynomial matrix corresponding to a linear projection (i.e.* $F^2 = F$*) such that its entries are polynomials of degrees bounded by an integer* D *and are given by a slp of size* L. *Then there exists a well parallelizable algorithm which runs in sequential time* $(nL)^{O(1)}(MD)^{O(n)}$ *computing two subsets of* $k[x_1,\ldots,x_n]^M$: $\{v_1,\ldots,v_s\}$ *and* $\{v_{s+1},\ldots,v_M\}$ *such that*

1. $\{v_1,\ldots,v_M\}$ *is a basis of* $k[x_1,\ldots,x_n]^M$.
2. $\{v_1,\ldots,v_s\}$ *is a basis of* $\mathrm{Im}(F)$ *and* $\{v_{s+1},\ldots,v_M\}$ *is a basis of* $\mathrm{Ker}(F)$.
3. *The coordinates of the vectors* v_i *are polynomials of degrees bounded by* $(MD)^{O(n)}$ *and they are given by a slp of size* $(nL)^{O(1)}(MD)^{O(n)}$.

Proof. By means of elementary linear algebra procedures over the ground field k, it is easy to construct a basis $\{w_1,\ldots,w_M\}$ of k^M whose first s vectors are a basis of the image of the matrix $F(0,\ldots,0)$ and the remaining ones, a basis of its kernel (let us observe that the matrix $F(0,\ldots,0) \in k^{M\times M}$ also corresponds to a projection map).

Then, from Corollary 21, we take $v_1,\ldots,v_s$ as the vectors $Pw_1,\ldots,Pw_s$ and $v_{s+1},\ldots,v_M$ as the vectors $Q^{-1}w_{s+1},\ldots,Q^{-1}w_M$.

The estimations for the degrees and complexity times follow immediately from Corollary 21 and the linear change of coordinates described in Section 2.3. □

4. The case of a unimodular matrix

In this section we briefly sketch a result similar to Theorem 22 for the more general case of a unimodular polynomial matrix (see Definition 1). We shall not describe in detail the algorithms to compute bases for the kernel and the image of an arbitrary unimodular matrix because the arguments are almost the same as those used in the case of a projection matrix; however the complexity upper bounds are worse, even if they remain in the single exponential class.

Even if Theorem 22 above will be enough to obtain bases for complete intersection rings in Noether position, its generalization to unimodular polynomial matrices (Theorem 25 below) leads to an effective decision procedure for the freeness of $k[x_1,\dots,x_n]$-modules given by a presentation matrix (see Proposition 4 and Corollary 26).

Throughout this section F will denote a unimodular matrix in $k[x_1,\dots,x_n]^{N\times M}$ of rank s, whose entries are polynomials of degrees bounded by a constant D, given by a slp of size L. The polynomial ring $k[x_1,\dots,x_n]$ will be denoted by A.

The first difference between the unimodular and the projection cases, is the construction of a system of generators for the kernel of F; while this is obvious for projection matrices, it requires a more careful treatment in the unimodular case (cf. [1, Lemma 1] and [46, Corollary 2.4.1]).

Lemma 23. *The kernel of the matrix F can be generated as an A-module by $(M-s)((M+N)^6D)^n$ many polynomial vectors that can be calculated by an algorithm which runs in sequential time $(nL)^{O(1)}((N+M)D)^{O(n)}$. The coordinates of these vectors are polynomials of degrees at most sD that can be evaluated by a slp of size $(sL)^{O(1)}$.*

Proof. Let us consider the $s\times s$ minors $\delta_1,\dots,\delta_Q$ as in Lemma 2; then we have $Q\le((M+N)^6D)^n$. Without loss of generality, we may suppose that δ_1 is the first principal minor; in this case the first s columns $C_1,\dots,C_s$ of the matrix F are linearly independent over $k(x_1,\dots,x_n)$, and then (by Cramer's rule) we have the relations:

$$\delta_1 C_{s+i} = b^1_{1i}C_1+\cdots+b^1_{si}C_s \quad \text{for } i=1,\dots,M-s,$$

where $b^1_{ji}\in A$ have degrees bounded by sD and can be computed and evaluated (by Cramer's rule and Subroutine B) in time $(sL)^{O(1)}$.

Therefore, the vectors

$$w^1_i := (b^1_{1i},\dots,b^1_{si},0,\dots,-\delta_1,\dots,0),$$

where $-\delta_1$ occurs in the coordinate $s+i$, belong to $\mathrm{Ker}(F)$.

Repeating this construction for $\delta_2,\dots,\delta_Q$, we get a family $\mathscr{F}$ of $(M-s)((M+N)^6D)^n$ many vectors lying in $\mathrm{Ker}(F)$.

We claim that this family generates $\mathrm{Ker}(F)$. For this it is enough to show that for any maximal ideal $\mathfrak{M}\subset A$ these vectors span the kernel of the localized application $F_{\mathscr{M}}: A^M_{\mathfrak{M}}\to A^N_{\mathfrak{M}}$. Clearly, for each maximal ideal $\mathfrak{M}$, there exists some index $j\in\{1,\dots,Q\}$, such that $\delta_j\notin\mathfrak{M}$ (because $1\in(\delta_1,\dots,\delta_Q)$), and then, the $M-s$ vectors $\overline{w^j_i}$ are $A/\mathfrak{M}$-linearly independent in $\mathrm{Ker}(F_{\mathfrak{M}})/\mathfrak{M}\mathrm{Ker}(F_{\mathfrak{M}})$. That means (by Nakayama's Lemma), that $\mathscr{F}$ spans $\mathrm{Ker}(F_{\mathfrak{M}})$. □

From this point, the constructions for a unimodular matrix are *mutatis mutandis* the same as those made in the projection case until the computation of bases for the image of F under suitable localizations in the ring $B:=k[x_1,\dots,x_{n-1}]$ (cf. Sections 3.1–3.3). The growth of the complexity times is due essentially to the single exponential upper

bound for the cardinal of a system of generators of $\mathrm{Ker}(F)$ (see Lemma 23), which produces an increment in the size of the matrix G (see Lemma 7). Summarizing we have:

Lemma 24. *There exists an algorithm which runs in sequential time* $(nL)^{O(1)}((M+N)D)^{O(n^2)}$ *from the input matrix* F, *computing polynomials* $\pi_1,\ldots,\pi_H \in B$ *such that*

- $1 \in (\pi_1,\ldots,\pi_H)$,
- $\deg\pi_j = ((M+N)D)^{O(1)}$,
- $H = ((M+N)D)^{O(n^2)}$,
- *each* π_j *can be evaluated by a slp of size* $((M+N)LD)^{O(1)}$.

Moreover, for each $j = 1,\ldots,H$, *the algorithm computes a basis of* $\mathrm{Im}(F_{\pi_j})$ *formed by polynomial vectors of degree* $((M+N)D)^{O(1)}$ *whose entries can be evaluated by a slp of size* $((M+N)LD)^{O(1)}$.

Now, in order to execute the gluing procedures as in Section 3.4 we need also localized bases for the kernel of F (see Theorem 18); in the projection case it was enough to apply the same argument for the matrix $\mathrm{Id} - F$, unfortunately in this case we do not know how to do this in a direct way, and, as in [1, Section 4, Definition 14], we must introduce two auxiliary related unimodular matrices and repeat all the arguments of Sections 3.1–3.3 for them.

For the sake of simplicity we shall avoid here the description of this argument, which also increases the complexity bounds. The correctness of this procedure follows from [1] combined with Section 3.

In this way we obtain the analogous of Theorem 22 for unimodular matrices:

Theorem 25. *Let* $F \in k[x_1,\ldots,x_n]^{N\times M}$ *be a polynomial unimodular matrix whose entries are polynomials of degrees bounded by an integer* D *and are given by a slp of size* L. *Then there exists a well parallelizable algorithm which runs in sequential time* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *computing a basis* $\{v_1,\ldots,v_M\}$ of $k[x_1,\ldots,x_n]^M$ *and a basis* $\{w_1,\ldots,w_N\}$ of $k[x_1,\ldots,x_n]^N$ *such that*

1. $\{w_1,\ldots,w_s\}$ *is a basis of* $\mathrm{Im}(F)$ *and* $\{v_{s+1},\ldots,v_M\}$ *is a basis of* $\mathrm{Ker}(F)$.
2. *The coordinates of the vectors of both bases are polynomials of degrees bounded by* $((M+N)D)^{O(n^4)}$ *and they are given by a slp of size* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$.

Corollary 26. *Let* P *be a* $k[x_1,\ldots,x_n]$*-module of finite type and* $F \in k[x_1,\ldots,x_n]^{N\times M}$ *a presentation matrix for* P (*see Definition* 3). *Suppose that the entries of the matrix* F *have total degrees bounded by* D *and are given by a straight-line program of size* L. *Then there exists a well parallelizable algorithm which runs in sequential time* $(nL)^{O(1)}((M+N)D)^{O(n^4)}$ *which decides if* P *is free and in the affirmative case computes a basis of* P.

Proof. The part of the algorithm that decides the freeness of P has been explained in Proposition 4. Therefore if P is free, the matrix F^t is unimodular and then Theorem 25 applied to F^t gives a basis $w_1,\ldots,w_M$ of $k[x_1,\ldots,x_n]^M$ such that $w_1,\ldots,w_s$ is a basis of $\mathrm{Im}(F^t)$. Hence the vectors $w_{s+1},\ldots,w_M$ leads to a basis of P. The complexity bounds follow directly from Proposition 4 and Theorem 25. □

5. Traces and bases of complete intersection rings

This section deals with the relation between the classical notion of trace in Gorenstein rings and the estimation of degrees of bases of complete intersection rings.

We introduce the notations and notions we shall use throughout this section.

Let k be an infinite perfect field, $\bar{k}$ be its algebraic closure, $f_1,\ldots,f_{n-r}$ be polynomials in $k[x_1,\ldots,x_n]$ of degrees bounded by an integer d forming a regular sequence and whose zeros define an affine algebraic variety $V\subset\mathbb{A}^n$. We denote by $\deg(V)$ the "set theoretical" degree of the variety V (see for instance [38, Chapter 5] or [24, Definition 1]); Bezout Inequality states that $\deg(V)\leq d^{n-r}$ (see [24, Theorem 1]).

We assume that the variables $x_1,\ldots,x_n$ are in Noether position with respect to the polynomials f_i; more precisely, 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 $S:=k[x_1,\ldots,x_n]/(f_1,\ldots,f_{n-r})$. For any polynomial $f\in k[x_1,\ldots,x_n]$ we denote by $\bar{f}$ its class in S. The determinant of the Jacobian matrix $(\partial f_i/\partial x_{r+j})_{1\leq i,j\leq n-r}$ is denoted by Δ.

It is well known that under these hypothesis the ring S becomes a free R-module of finite rank (see for instance [15, Corollary 18.17] or [21, Lemma 3.3.1]). The goal of this section is to exhibit an explicit description of an R-basis of S as the basis of the image of certain polynomial projection matrix associated to a trace of S over R (Theorem 34 below). This property will be used also in the next section, in order to obtain an algorithm to compute this basis, in the reduced case, in single exponential time by means of Theorem 22.

We start borrowing some well-known facts about the algebraic theory of traces in complete intersection or Gorenstein rings following [30]. For a treatment from the complex-residual point of view see for instance [11,23] or [14].

5.1. Basic general trace theory

With the notations and assumptions stated above, we consider the ring S as an R-algebra and 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 [30, 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.

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

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

Let us consider now the tensor product $S \otimes_R S$. This ring can be considered in a natural way as an R-algebra and as an S-bialgebra (with right and left multiplications).

Let $\mu : S \otimes_R S \to S$ be the morphism of R-algebras (or S-bialgebras) defined by $\mu(b \otimes b') := bb'$. Denote by $\mathscr{K}$ the kernel of μ. It is easy to show that $\mathscr{K}$ is the ideal generated by all the elements $b \otimes 1 - 1 \otimes b$, where b ranges over S (see for example [26, Proposition 1.3]).

From the fact that $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})(b \otimes 1 - 1 \otimes b) = 0$ for all $b \in S$, one infers that the induced structures of right and left S-modules over $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ coincide. In other words, if $\sum_i b_i \otimes b'_i$ belongs to $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ and b is an element of the ring S, we have: $\sum_i bb_i \otimes b'_i = \sum_i b_i \otimes bb'_i$. Moreover it is possible to show that $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ is a cyclic S-module (see [30, Corollary F.10]).

Let us consider the application $\Phi : S \otimes_R S \to \mathrm{Hom}_R(S^*, S)$ defined by

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

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

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

For each generator $\Gamma := \sum_m b_m \otimes b'_m$ of the S-module $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$, the element $\Phi(\Gamma)$ is a generator of $\mathrm{Hom}_S(S^*, S)$ and then there exists a uniquely determined $\sigma_\Gamma \in S^*$ such that $\Phi(\Gamma)(\sigma_\Gamma) = 1$. One deduces immediately that σ_Γ is a trace for S (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 $b \in S$:

$$b = \sum_{1\le m\le M} \sigma_\Gamma(b\, b'_m) b_m. \tag{13}$$

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

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 [30, Corollary F.12]):

$$\mu(\Gamma).\sigma_\Gamma = \mathrm{Tr}. \tag{14}$$

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

The trace associated to a regular sequence: In our case (i.e. the regular sequence, which makes S a complete intersection ring, is given) it is possible to exhibit explicitly a generator Γ of $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$.

For this, let us consider new indeterminates over k, denoted by $y_{r+1},\dots,y_n$; for each polynomial $f\in k[x_1,\dots,x_n]$ we write

$$f^{(Y)} := f(x_1,\dots,x_r,y_{r+1},\dots,y_n)$$

in the polynomial ring $k[x_1,\dots,x_r,y_{r+1},\dots,y_n]$.

Hence we have the canonical isomorphism of R-algebras:

$$S\otimes_R S \cong R[x_{r+1},\dots,x_n,y_{r+1},\dots,y_n]/(f_1,\dots,f_{n-r},f_1^{(Y)},\dots,f_{n-r}^{(Y)}). \tag{15}$$

Clearly, each polynomial $f_i^{(Y)}-f_i\in k[x_1,\dots,x_n,y_{r+1},\dots,y_n]$ belongs to the ideal $(y_{r+1}-x_{r+1},\dots,y_n-x_n)$ and therefore it can be written as

$$f_i^{(Y)}-f_i=\sum_{j=1}^{n-r} l_{ij}(y_{r+j}-x_{r+j}), \tag{16}$$

where $l_{ij}\in k[x_1,\dots,x_n,y_{r+1},\dots,y_n]$. Moreover, if one considers each polynomial $f_i^{(Y)}-f_i$ as a polynomial in the variables $y_{r+1},\dots,y_n$ with coefficients in $k[x_1,\dots,x_n]$ $(1\le i\le n-r)$, its Taylor expansion around the point $(x_{r+1},\dots,x_n)$ gives a particular representation where the polynomials l_{ij} have total degree bounded by $d-1$.

Following [30, Corollary E.19 and Example F.19] the class of $\det(l_{ij})$ modulo the ideal $(f_1,\dots,f_{n-r},f_1^{(Y)},\dots,f_{n-r}^{(Y)})$ gives a generator of $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ by means of the identification (15), independently of the choice of the l_{ij} verifying (16).

Developing $\det(l_{ij})$ as a sum of products of polynomials in the variables $x_1,\dots,x_n$ and $y_{r+1},\dots,y_n$, respectively, and taking into account the trace formula (13) we have (see [30, Corollary E.19 and Example F.19] and [18, Section 3.4] or [42, Proposition 3]):

Proposition 27. *There exists a finite family of polynomials a_m,c_m in $k[x_1,\dots,x_n]$, such that $\Gamma:=\sum_{m=1}^{M}\bar{a}_m\otimes\bar{c}_m$ is a generator of $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ and $\mu(\Gamma)=\sum_{m=1}^{M}\bar{a}_m\bar{c}_m=\bar{\Delta}$ (the class of the Jacobian). Both families $(\overline{a_m})_m$ and $(\overline{c_m})_m$ are systems of generators of S over R.*

In the particular case that the polynomials l_{ij} come from the Taylor expansion of $f_i^{(Y)}-f_i$, the polynomials a_m, c_m verify the inequality $(a_m)+\deg(c_m)\le(n-r)(d-1)$ and $M<3(nd)^{n-r}$.

Definition 28. From [30, Lemma E.19] the generator Γ defined in Proposition 27 does not depend on the choice of the polynomials l_{ij}, and then we define *the trace associated to the regular sequence* $f_1,\dots,f_{n-r}$ as the trace associated to the generator of $\mathrm{Ann}_{S\otimes_R S}(\mathscr{K})$ introduced in Proposition 27. Let us observe that if σ denotes this trace, the trace formula (13) is

$$b=\sum_m \sigma(\bar{a}_m b)\,\bar{c}_m \tag{17}$$

for any $b\in S$; in particular $\sigma(\bar{a}_m b)=0$ for all m if and only if $b=0$.

Definition 29. In the particular case when $r = n - 1$ and the polynomial f_1 is monic in the variable x_n, the trace σ associated to f_1 is the so-called "*Tate trace*" (see [30, Example F.22]): for an arbitrary element $b := \alpha_{e-1}x_n^{e-1} + \cdots + \alpha_1 x_n + \alpha_0$ (where $e := \deg_{x_n}(f_1)$ and $\alpha_i \in R$, $i = 0, \ldots, e-1$), we have $\sigma(b) = \alpha_{e-1}$.

5.2. An upper bound for the degree of the associated trace

Let σ be the trace introduced in Proposition 27 and Definition 28. In this section we shall estimate an upper bound for the degree of $\sigma(\bar{f})$ involving the parameters $\deg(f), d, n, r$ and $\deg(V)$.

Our approach is quite similar to that in [14] reinterpreting the complex-residual tools from the algebraic duality point of view. As a consequence, we obtain analogous results without restrictions on the characteristic of the ground field. On the other hand we also generalize the results of [42] without hypothesis about the radicality of the ideal $(f_1, \ldots, f_{n-r})$.

Following [14] the strategy consists on replacing the regular sequence $f_1, \ldots, f_{n-r}$ by another one $g_1, \ldots, g_{n-r}$, where each polynomial g_i belongs to $R[x_{r+i}] \cap (f_1, \ldots, f_{n-r})$. In this situation we may use the "Tate trace formula" in one variable (see Definition 29), and then, by tensoring, we obtain upper bounds for the degree of a new trace σ' of $S' := k[x_1, \ldots, x_n]/(g_1, \ldots, g_{n-r})$ over R.

Finally, rewriting the polynomials g_i as linear combinations of the f_i's using polynomials with bounded degrees, we are able to relate both traces σ and σ' and thus to estimate bounds for the original trace σ.

First, we introduce a new regular sequence $g_1, \ldots, g_{n-r}$ defined as integral dependence equations of the variables $x_{r+1}, \ldots, x_n$ over R respectively (see also [13, Proposition 1.12]):

Proposition 30. *There exist polynomials $g_1, \ldots, g_{n-r}$ such that each g_i belongs to $R[x_{r+i}] \cap (f_1, \ldots, f_{n-r})$, $i = 1, \ldots, n-r$, is monic in the variable x_{r+i} and its total degree is bounded by $d^n \deg(V)$. Clearly these polynomials form a regular sequence in $k[x_1, \ldots, x_n]$.*

Proof. From [42, Proposition 1] for each $i = 1, \ldots, n-r$, there exists a polynomial $q_i \in R[x_{r+i}] \cap \sqrt{(f_1, \ldots, f_{n-r})}$, monic in x_{r+i}, whose total degree is bounded by $\deg(V)$. Therefore, from [27] or [13, Remark 1.6], $g_i := q_i^{d^n}$ verifies the statement. □

Let $S' := k[x_1, \ldots, x_n]/(g_1, \ldots, g_{n-r})$; clearly $R \hookrightarrow S'$ is an integral and injective morphism. Following Definition 28, now for the rings S' and R, there exists an associated trace to the regular sequence $g_1, \ldots, g_{n-r}$ which will be denoted by σ'.

For each index i, $i = 1, \ldots, n-r$, denote by S_i' the ring $R[x_{r+i}]/(g_i)$. In this case the associated trace σ_i' is the *Tate trace* (see Definition 29).

Hence, for any polynomial $f \in R[x_{r+i}]$, if $\bar{f}$ is its class in S_i' after the division by g_i, we have that $\sigma_i'(\bar{f})$ is the principal coefficient of $\bar{f}$ (seen as a polynomial in x_{r+i}).

Therefore from Euclid's algorithm we deduce the inequality (see Subroutine C):

$$\deg \sigma_i'(\bar{f}) \leq \deg(g_i)\deg(f). \tag{18}$$

Now, we are able to estimate the degree of $\sigma'(\bar{f})$, with $\bar{f} \in S'$:

Proposition 31. *For each* $\bar{f} \in S'$, *the following inequality holds*:

$$\deg \sigma'(\bar{f}) \leq \deg(f) d^n \deg(V).$$

Proof. Clearly, $S' \simeq S_1' \otimes_R S_2' \otimes_R \ldots \otimes_R S_{n-r}'$ by means of the natural correspondence:

$$\sum_{\beta} a_\beta x_{r+1}^{\beta_1} \ldots x_n^{\beta_{n-r}} \mapsto \sum_{\beta} a_\beta x_{r+1}^{\beta_1} \otimes \ldots \otimes x_n^{\beta_{n-r}}, \quad a_\beta \in R$$

which goes down to the quotients.

From [30, Propositions F.16a and F.17] one has the formula

$$\sigma'(\bar{f}) = \sum_{\beta} a_\beta \sigma_1'(\bar{x}_{r+1}^{\beta_1}) \ldots \sigma_{n-r}'(\bar{x}_n^{\beta_{n-r}}),$$

for each $f = \sum a_\beta x_{r+1}^{\beta_1} \ldots x_n^{\beta_{n-r}} \in k[x_1, \ldots, x_n]$.

Then, from Proposition 30 and inequality (18), one obtains the following degree bound:

$$\begin{aligned}
\deg \sigma'(\bar{f}) &\leq \max_\beta \{\deg(a_\beta) + \deg(\sigma_1'(\bar{x}_{r+1}^{\beta_1})) + \cdots + \deg(\sigma_{n-r}'(\bar{x}_n^{\beta_{n-r}}))\} \\
&\leq \max_\beta \{\deg(a_\beta) + \deg(g_1)\beta_1 + \cdots + \deg(g_{n-r})\beta_{n-r}\} \\
&\leq \max_\beta \{\deg(a_\beta) + d^n \deg(V)\beta_1 + \cdots + d^n \deg(V)\beta_{n-r}\} \\
&\leq \deg(f) d^n \deg(V). \qquad \square
\end{aligned}$$

From this proposition we infer a degree upper bound for the associated trace σ as follows:

Theorem 32. *Let* $R := k[x_1, \ldots, x_r]$ *and* $S := k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$. *Let* $\sigma \in S^*$ *be the trace associated to the regular sequence* (*Definition* 28). *Then, for each* $\bar{f} \in S$, *the following inequality holds*:

$$\deg \sigma(\bar{f}) \leq \{\deg(f) + (n-r)(d^{n-r} + d^n \deg(V))\} d^n \deg(V).$$

Proof. Since the ideal $(g_1, \ldots, g_{n-r})$ is contained in $(f_1, \ldots, f_{n-r})$, there exist polynomials $\alpha_{ij} \in k[x_1, \ldots, x_n]$; $i, j = 1, \ldots, n-r$ whose degrees are bounded by $d^{n-r} + d^n \deg(V)$, such that

$$g_j = \sum_{i=1}^{n-r} \alpha_{ij} f_i$$

(see [13, Theorem 5.1]).

Following [30, p. 374], for any polynomial $f \in k[x_1,\ldots,x_n]$ we have the identity in $k[x_1,\ldots,x_r]$:

$$\sigma(\bar{f}) = \sigma'(\overline{\det(\alpha_{ij})}\bar{f}),$$

where the bars denote the classes in the rings S and S', respectively.

Proposition 31 and the arguments above yield the stated degree upper bound for $\sigma(\bar{f})$ as follows:

$$\begin{aligned}\deg\sigma(\bar{f}) = \deg\sigma'(\overline{\det(\alpha_{ij})f}) &\leq \deg(\det(\alpha_{ij})f)d^n\deg(V)\\ &\leq (\deg(f)+(n-r)\max_{ij}\deg(\alpha_{ij}))d^n\deg(V)\\ &\leq \{\deg(f)+(n-r)(d^{n-r}+d^n\deg(V))\}d^n\deg(V). \qquad \square\end{aligned}$$

Remark. When $(f_1,\ldots,f_{n-r})$ is a reduced ideal of $k[x_1,\ldots,x_n]$ the bounds we have just obtained can be slightly improved. In fact, in this case, in Proposition 30 we have $\deg(g_i) \leq \deg(V)$ for all $i=1,\ldots,n-r$ (see [42, Proposition 1]), and thus in Theorem 32, we get the inequality

$$\deg\sigma(\bar{f}) \leq \{\deg(f)+(n-r)(d^{n-r}+\deg(V))\}\deg(V).$$

However, in this case a more precise bound can be obtained (see [42, Theorem 10]):

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

5.3. Traces and bases

In this section we shall apply the trace theory tools previously introduced in order to bound the degrees of an R-basis of the complete intersection ring S. This will be done considering a matrix of a projection map whose image is isomorphic to S. Even if the strategy we follow here is essentially the same as the one applied throughout the last section of [1], the estimations we obtain improve those obtained in that paper and we drop the hypothesis of reduceness for S.

Following the notations introduced in Proposition 27, let $F \in R^{M\times M}$ be the matrix whose entries are defined by $F_{ij} := \sigma(\overline{a_i c_j})$ (where σ is the trace associated to the regular sequence $f_1,\ldots,f_{n-r}$, see Definition 28). The next lemma allows to apply Theorem 22 to the matrix F:

Lemma 33. *The matrix $F \in R^{M\times M}$ is a projection matrix whose entries are polynomials of degrees bounded by $D := 3(n-r)d^{4n-2r}$.*

Proof. In order to prove that F is a projection matrix it is enough to show that $F^2 = F$. From the R-linearity of σ and the trace formula (17) we have

$$(F^2)_{ij} = \sum_{k=1}^{M}\sigma(\bar{a}_i\bar{c}_k)\sigma(\bar{a}_k\bar{c}_j) = \sigma\left(\left(\sum_{k=1}^{M}\sigma(\bar{a}_i\bar{c}_k)\bar{a}_k\right)\bar{c}_j\right) = \sigma(\bar{a}_i\bar{c}_j) = F_{ij}.$$

The degree bounds obtained in Theorem 32 and Proposition 27 and Bezout inequality, yield the stated degree bounds as follows:

$$\begin{aligned}\deg(F_{ij}) = \deg\sigma(\bar{a}_i\bar{c}_j) &\leq \{\deg(a_ic_j) + (n-r)(d^{n-r} + d^n\deg(V))\}d^n\deg(V)\\ &\leq \{(n-r)(d-1) + (n-r)(d^{n-r} + d^n\deg(V))\}d^n\deg(V)\\ &\leq 3(n-r)d^{4n-2r}. \qquad \square\end{aligned}$$

The next theorem relates explicitly each basis of the image of the projection F with another one of S. This relation allows to estimate the degrees of a basis of S by means of Theorem 22:

Theorem 34. *Let* $w_k = (w_{k1},\ldots,w_{kM}) \in R^M$, $1 \leq k \leq s$, be an R-basis of $\mathrm{Im}(F)$, *then the elements* $\sum_{j=1}^M w_{kj}\overline{c_j}$, *with* $1 \leq k \leq s$, *form an* R*-basis of* S.

In particular, there exists an R*-basis of* S *whose elements are the classes of polynomials in* $k[x_1,\ldots,x_n]$ *with degrees bounded by* $(nd)^{\mathrm{O}((n-r)r)}$.

Proof. Let us consider the following diagram:

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

where $G : R^M \to S$ is the morphism mapping each element e_i of the canonical basis of R^M to $\bar{c}_i \in S$ and φ is the map defined by $\varphi(w) := \sum_{j=1}^M w_j\overline{c_j}$ for any $w = (w_1,\ldots,w_M) \in \mathrm{Im}(F)$. Let us observe that G is an epimorphism because the elements $\overline{c_i}$ are a system of generators of S over R (Proposition 27).

By the trace formula (17) we have for any e_i the following equality:

$$\varphi(F(e_i)) = \varphi(\sigma(\overline{a_1c_i}),\ldots,\sigma(\overline{a_Mc_i})) = \sum_{j=1}^M \sigma(\overline{a_jc_i})\overline{c_j} = \overline{c_i} = G(e_i).$$

On the other hand, $(w_1,\ldots,w_M) \in \mathrm{Ker}(F)$ if and only if $\sum_{j=1}^M \sigma(\overline{a_ic_j})w_j = 0$ for all $i = 1,\ldots,M$, or equivalently $\sigma\left(\overline{a_i}\sum_{j=1}^M \overline{c_j}w_j\right) = 0$ for all $i = 1,\ldots,M$. From the trace formula (17) this relation implies $\sum_{j=1}^M \overline{c_j}w_j = 0$, in other words $(w_1,\ldots,w_M) \in \mathrm{Ker}(G)$. Summarizing, we have seen that $\mathrm{Ker}(F) = \mathrm{Ker}(G)$.

Therefore the previous diagram is commutative. Hence φ is an isomorphism and if $w_1,\ldots,w_s \in R^M$ is an R-basis of $\mathrm{Im}(F)$, the elements $\varphi(w_1),\ldots,\varphi(w_s)$ form an R-basis of S.

In order to finish the proof, it suffices to see the existence of a basis of S with the claimed degree bounds.

Applying Theorem 22 to the projection matrix F, one obtains an R-basis of $\mathrm{Im}(F)$ formed by polynomial vectors w_k with coordinates w_{ki} of degrees bounded by $(MD)^{\mathrm{O}(r)}$

(recall that $R = k[x_1, \ldots, x_r]$ and D is the degree upper bound for the entries of F obtained in Lemma 33). Taking into account that $M \leq 3(nd)^{n-r}$ (Proposition 27), we have

$$(MD)^{O(r)} < \left(3(nd)^{n-r}3(n-r)d^{4n-2r}\right)^{O(r)} = (nd)^{O((n-r)r)}.$$

Hence, by means of the isomorphism φ, the elements $(\sum_{j=1}^{M} w_k^j \overline{c_j})$ are a basis of S and we have the following degree bounds for their representatives in $k[x_1, \ldots, x_n]$:

$$\deg\left(\sum_{j=1}^{M} w_k^j c_j\right) \leq \max_{kj} \deg(w_k^j c_j) \leq (nd)^{O((n-r)r)} + (n-r)(d-1)$$
$$= (nd)^{O((n-r)r)}. \qquad \square$$

6. Computing bases in single exponential time

Throughout this section we shall keep the notations previously introduced: k is a perfect field and $x_1, \ldots, x_n$ are indeterminates over k. Let $f_1, \ldots, f_{n-r}$ be a regular sequence of polynomials in $k[x_1, \ldots, x_n]$ of degrees bounded by an integer d and given by a slp of size ℓ, defining a variety V. We denote by S the ring $k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-r})$ and $R := k[x_1, \ldots, x_r]$, and we assume that the canonical morphism $R \to S$ is integral and injective. We also maintain the notations related to the trace tools introduced in Section 5.1 and we shall not repeat them here.

Under these hypotheses S is a free R-module of rank $\eta \leq d^{n-r} \leq d^n$ (see for instance [21, Corollary 3.3.2] or [2, Corollary 6]). The goal of this section is the computation of polynomials in $k[x_1, \ldots, x_n]$ whose classes are an R-basis of S.

For this purpose, following Theorem 34 and Theorem 22, it suffices to construct explicitly the projection matrix F with entries in R, introduced in Section 5.3.

The first step will be to give an effective version of Proposition 27 in order to construct the polynomials $a_m, c_m \in k[x_1, \ldots, x_n]$. Recall that these polynomials are not uniquely determined but they must verify the equality:

$$\det(l_{ij}) = \sum_m a_m(x_1, \ldots, x_r, x_{r+1}, \ldots, x_n) c_m(x_1, \ldots, x_r, y_{r+1}, \ldots, y_n). \tag{19}$$

Although the coefficients $l_{ij} \in k[x_1, \ldots, x_n, y_{r+1}, \ldots, y_n]$ are also not uniquely determined, they satisfy the relations:

$$f_i^{(Y)} - f_i = \sum_{j=1}^{n-r} l_{ij}(y_{r+j} - x_{r+j}) \tag{20}$$

for all $i = 1, \ldots, n-r$ (see formula (16)).

The Taylor expansion of $f_i^{(Y)} - f_i$ as polynomials with coefficients in $k[x_1, \ldots, x_n]$ and variables $y_{r+1}, \ldots, y_n$ around the point $(x_{r+1}, \ldots, x_n)$ assures the existence of the polynomials l_{ij}, but this method is not totally convenient from our complexity point of view. Thus, in order to construct the polynomials l_{ij}, we can see relations (20) as an

effective membership problem of the polynomials $f_i^{(Y)} - f_i$ with respect to the ideal generated by $(y_{r+j} - x_{r+j})$ in $k[x_1,\ldots,x_n,y_{r+1},\ldots,y_n]$. Remark that the polynomials we find in this way are not necessarily the same as those we could obtain from the Taylor expansion. At this point we shall make use of the following result of [20]:

Theorem 35 (Giusti et al. [20, Theorem 19]). *Let $g_1,\ldots,g_s$ and g be polynomials of $k[x_1,\ldots,x_n]$ such that $g_1,\ldots,g_s$ form a regular sequence and g belongs to the ideal $(g_1,\ldots,g_s)$. For $1 \le j \le s$ denote by $\delta_j := \deg(V(g_1,\ldots,g_j))$ the degree of the affine variety defined by the ideal $(g_1,\ldots,g_j)$ which we suppose to be radical. Write $\delta := \max_{1\le j\le s-1}\{\delta_j\}$ and $e := \max_{1\le j\le s}\{\deg(g_j)\}$. Assume that the polynomials $g_1,\ldots,g_s,g$ are given by a slp of size L. Then there exists a well parallelizable algorithm which runs in sequential time $(se\delta L)^{O(1)}$ and computes polynomials $p_1,\ldots,p_s \in k[x_1,\ldots,x_n]$ with the following properties*:

1. $g = p_1g_1 + \cdots + p_sg_s$.
2. $\max_{1\le j\le s}\{\deg(p_j)\} \le (2s^2e + \max\{e,\deg(g)\})\delta$.

Moreover the polynomials $p_1,\ldots,p_s$ are given by a slp of size $\deg^2(g)\,(se\delta L)^{O(1)}$.

Applying this theorem we have in our case:

Corollary 36. *There exists a well parallelizable algorithm running in sequential time $((n-r)\ell)^{O(1)}$ from the input polynomials $f_1,\ldots,f_{n-r}$, whose output is a slp of size $d^2((n-r)\ell)^{O(1)}$ which evaluates a family of polynomials l_{ij}, $i,j=1,\ldots,n-r$ satisfying relations* (20) *and* $\max_{ij}\{\deg(l_{ij})\} \le 2(n-r)^2 + d$.

Proof. For each fixed index $i = 1,\ldots,n-r$, it is easy to see that the polynomials $g_j := y_{r+j} - x_{r+j}$, $j = 1,\ldots,n-r$, and $g := f_i^{(Y)} - f_i$ verify all the hypotheses of the previous theorem over the polynomial ring $k[x_1,\ldots,x_n,y_{r+1},\ldots,y_n]$. Moreover, in this case we have: $s = n-r$, $\delta = e = 1$, $\deg(g) = d$ and $L = 2\ell + 1$.

Therefore, we can apply $(n-r)$-times Theorem 35 and get the polynomials l_{ij} verifying the statement of the corollary. □

With the polynomials l_{ij} just obtained we are able to compute the polynomials a_m, c_m as follows:

Proposition 37. *There exists a well parallelizable algorithm running in sequential time $\ell^{O(1)}((n-r)d)^{O(n-r)}$ from the input polynomials $f_1,\ldots,f_{n-r}$, whose output is a slp of the same size which evaluates two families of polynomials: $a_m \in k[x_1,\ldots,x_r,x_{r+1},\ldots,x_n]$, $c_m \in k[x_1,\ldots,x_r,y_{r+1},\ldots,y_n]$, $m=1,\ldots,M := ((n-r)d)^{O(n-r)}$, verifying the statement of Proposition* 27.

Proof. It is enough to find a decomposition of $\det(l_{ij})$ as in equality (19). The polynomial $\det(l_{ij})$ of degree bounded by $(n-r)(2(n-r)^2+d)$ can be found by means of

Subroutine B item 1, in time $(d(n-r)\ell)^{O(1)}$ and it is given by a slp of the same size. In order to obtain the polynomials a_m, c_m it suffices to write $\det(l_{ij})$ in dense form with respect to the variables $y_{r+1},\ldots,y_n$ by means of Subroutine A, obtaining in this way the polynomials $a_m \in k[x_1,\ldots,x_n]$ in time $\ell^{O(1)}((n-r)d)^{O(n-r)}$ given by a slp of the same size. The polynomials c_m are the corresponding monomials of degrees bounded by $\deg(\det(l_{ij}))$ in the variables $y_{r+1},\ldots,y_n$ and can be evaluated in the obvious way by a slp of size $(n-r)\log(\deg(\det(l_{ij}))) = (n-r)^{O(1)}\log(d)$. Since there are at most $\deg(\det(l_{ij}))^{(n-r)} = ((n-r)d)^{O(n-r)}$ many monomials we get the bounds. □

The next step is the computation of each ij-entry, $\sigma(\overline{a_i c_j})$, of the projection matrix F (where σ is the trace associated to the regular sequence $f_1,\ldots,f_{n-r}$ as in Definition 28). This problem, the explicit construction of the trace, has been considered in previous articles (see for example [18, Lemma 3.4.1] and [29]) in order to obtain efficient effective Nullstellensätze; the results shown in these papers are essentially enough for our purposes and thus we shall only repeat here their statements adapting them to our situation.

We denote by $K := k(x_1,\ldots,x_r)$ the quotient field of R and $S' := S \otimes_R K \simeq k(x_1,\ldots,x_r)[x_{r+1},\ldots,x_n]/(f_1,\ldots,f_{n-r})$ (observe that under our assumptions S' is a K-vector space of dimension $\eta = \operatorname{rank}_R(S)$). Let $\sigma' := \sigma \otimes_R \mathrm{Id} : S' \to K$ be the canonical extension of the trace σ. The next lemma (see [18, Section 3.4.1]) computes explicitly a K-basis of S' and the matrix of the map σ' in this basis. Unfortunately, this lemma requires the additional hypothesis of the reduceness of the ring S in order to obtain a well parallelizable algorithm, if this condition is dropped the sequential complexity remains single exponential but the parallel one increases exponentially in n (see also [18, Section 2.4.1]).

Lemma 38. *Suppose that the regular sequence $f_1,\ldots,f_{n-r}$ generates a radical ideal. There exists a well parallelizable algorithm running in time $(n-r)\ell d^{O(n)}$ whose input are the polynomials $f_1,\ldots,f_{n-r}$, and whose output are the following items*:

1. *a slp of size $d^{O(n)}$ which evaluates a non zero polynomial τ in R of degree $d^{O(n)}$,*
2. *a slp of size $d^{O(n)}$ which evaluates a family of polynomials $e_1 := 1,\ldots,e_\eta$ in $k[x_1,\ldots,x_n]$ such that the set $\mathscr{E}$ formed by their classes $\overline{e_1},\ldots,\overline{e_\eta}$ in S' is a K-basis of S',*
3. *a slp of size $d^{O(n)}$ which evaluates the entries of a family of polynomial matrices $M_{r+1},\ldots,M_n$ in $R^\eta \times \eta$ such that: the degrees of their coefficients are bounded by $d^{O(n)}$ and $(1/\tau)M_{r+1},\ldots,(1/\tau)M_n$ are the matrices of the K-endomorphisms of S', induced by the multiplications by $\overline{x_{r+1}},\ldots,\overline{x_n}$, in the basis $\mathscr{E}$,*
4. *a slp of size $d^{O(n)}$ which evaluates a family of polynomials $\theta_1,\ldots,\theta_\eta$ in R of degrees $d^{O(n)}$ such that the matrix of the extended trace σ' of S' in the basis $\mathscr{E}$ is the matrix $(\theta_1,\ldots,\theta_\eta)$.*

Proof. A proof of this lemma can be found in [18, Section 3.4.1] for the case of input polynomials given in dense representation. Our statement (inputs given by a slp)

follows immediately from Subroutine A which allows to compute all the coefficients of the polynomials $f_1,\ldots,f_{n-r}$ in time $(n-r)\ell d^{O(n)}$. □

By means of the previous lemma we are able to construct explicitly the matrix F:

Corollary 39. *Suppose that the regular sequence $f_1,\ldots,f_{n-r}$ generates a radical ideal. There exists a well parallelizable algorithm running in time $O(n)\ell d^{O(n)}$ from the input polynomials $f_1,\ldots,f_{n-r}$ whose output is a slp of size $d^{O(n)}$ which evaluates the entries of the matrix F.*

Proof. Since the entries of F are the polynomials $\sigma(\overline{a_i c_j})$ it suffices to compute them. From Proposition 37, we can compute the polynomials $a_i c_j$ as a sum of their monomials (whose degrees are bounded by $(n-r)(d-1)$). Hence, in order to compute $\sigma(\overline{a_i c_j})$ it is enough to compute the image by σ of the class of each of these monomials. Therefore without loss of generality, we shall compute $\sigma\left(\overline{\prod_{k=1}^{n} x_k^{\alpha_k}}\right)$.

For any $f \in k[x_1,\ldots,x_n]$, we denote by M_f the matrix in $K^{\eta\times\eta}$ associated to the endomorphism of S' induced by the multiplication by $\bar{f}$ in the basis $\mathscr{E}$ of Lemma 38 item 2. In the particular case that $f := \prod_{k=1}^{n} x_k^{\alpha_k}$ we have that $M_f = \prod_{k=1}^{r} x_k^{\alpha_k} \prod_{k=r+1}^{n} M_{x_k}^{\alpha_k} = \prod_{k=1}^{r} x_k^{\alpha_k} \prod_{k=r+1}^{n} (1/\tau^{\alpha_k}) M_k^{\alpha_k}$, where M_k are the matrices obtained by means of Lemma 38 (item 3). The first column of the matrix M_f is a vector of the form $(\beta_1/\tau^T,\ldots,\beta_\eta/\tau^T)$ where $T := \alpha_{r+1} + \cdots + \alpha_n$ and each $\beta_t \in R, 1 \le t \le \eta$, can be explicitly computed.

Since $\overline{e_1} = 1$, we deduce that $\overline{\prod_{k=1}^{n} x_k^{\alpha_k}} = \sum_{t=1}^{\eta} (\beta_t/\tau^T)\overline{e_t}$ and therefore $\sigma(\overline{\prod_{k=1}^{n} x_k^{\alpha_k}}) = \sum_{t=1}^{\eta} (\beta_t/\tau^T)\theta_t \in R$.

The polynomial $\sum_{t=1}^{\eta} (\beta_t/\tau^T)\theta_t$ has degree $d^{O(n)}$ and is given by a slp (with divisions!) of size $d^{O(n)}$. Avoiding the divisions by means of Strassen's procedure (see also [18, Section 2.2]), we can compute in time $O(r)d^{O(n)}$ a division free slp of size $d^{O(n)}$ which evaluates the mentioned polynomial.

Finally, adding all the complexity costs, we get the stated sequential time. □

At this point, we are able to compute easily an R-basis of S:

Theorem 40. *Suppose that the regular sequence $f_1,\ldots,f_{n-r}$ generates a radical ideal. There exists a well parallelizable algorithm running in sequential time $O(n)\ell d^{O(n^2)}$ which computes, from the input polynomials $f_1,\ldots,f_{n-r}$, a slp of size $n^{O(1)}d^{O(n^2)}$ which evaluates a family of polynomials in $k[x_1,\ldots,x_n]$ of degrees bounded by $nd^{O(n^2)}$, and whose classes in S form an R-basis of this module.*

Proof. After applying the algorithm of Theorem 22 to the matrix F, obtained by means of the previous corollary, we get in time $O(n)\ell d^{O(n^2)}$ an R-basis $\{w_1,\ldots,w_s\}$ of the image of the F, where each w_k is a polynomial vector $(w_{k1},\ldots,w_{kM})$, $M := d^{O(n)}$, their coordinates have degrees bounded by $d^{O(n^2)}$ and they are given by a slp of size $n^{O(1)}d^{O(n^2)}$.

Therefore (see Theorem 34), the polynomials $\sum_{j=1}^{M} w_{kj}\overline{c_j}$, $k=1,\ldots,s$, are an R-basis of S. □

Remark. Let us observe, that the hypothesis of the reduceness of the ring S can be dropped if we are not interested in the parallel complexity. This fact follows from the observation preceding Lemma 38.

Acknowledgements

We thank Alicia Dickenstein, Joos Heintz and Guillermo Matera for many helpful suggestions and remarks.

References

[1] M. Almeida, L. D'Alfonso, P. Solernó, On the degrees of bases of free modules over a polynomial ring, Math. Z. 231 (1999) 679–706.
[2] I. Armendáriz, P. Solernó, On the computation of the radical of polynomial complete intersection ideals in: G. Cohen, M. Giusti, T. Mora (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, 1995, Lecture Notes in Computer Science, vol. 948, Springer, Berlin, 1995, pp. 106–119.
[3] C. Berenstein, D. Struppa, Recent improvements in the complexity of the effective Nullstellensatz, Linear Algebra Appl. 157 (1991) 203–215.
[4] C. Berenstein, A. Yger, Bounds for the degrees in the division problem, Mich. Math. J. 37 (1990) 25–43.
[5] S. Berkowitz, On computing the determinant in small parallel time using a small number of processors, Inform. Process. Lett. 18 (1984) 147–150.
[6] D. Brownawell, Bounds for the degrees in the Nullstellensatz, Ann. Math. Second Ser. 126 (3) (1987) 577–591.
[7] P. Bürguisser, M. Clausen, M. Amin Shokrollahi, Algebraic Complexity Theory, Grundlehren der mathematischen Wissenschaften, vol. 315, Springer, Berlin, 1997.
[8] L. Caniglia, G. Cortiñas, S. Danón, J. Heintz, T. Krick, P. Solernó, Algorithmic aspects of Suslin's proof of Serre's Conjecture, Comput. Complexity 3 (1993) 31–55.
[9] L. Caniglia, A. Galligo, J. Heintz, Some new effectivity bounds in computational geometry, Proceedings of 6th International Conference on Applied Algebra, Algebraic Algorithms and Error Correcting Codes, AAECC-6, Roma, 1988, Lecture Notes Computer Science, vol. 357, Springer, Berlin, 1989, pp. 131–151.
[10] L. Caniglia, J.A. Guccione, J.J. Guccione, Local membership problems for polynomial ideals, in: T. Mora, C. Traverso (Eds.), Effective Methods in Algebraic Geometry, MEGA 90, Progress in Mathematics, vol. 94, Birkhäuser, Basel, 1991, pp. 31–45.
[11] N. Coleff, M. Herrera, Les Courants Residuels Associés à une Forme Meromorphe, Lecture Notes in Mathematics, vol. 633, Springer, Berlin, 1978.
[12] M. Demazure, Le monoïde de Mayr et Meyer, Notes Informelles de Calcul Formel, Ecole Polytechnique, Palaiseau, 1984.
[13] A. Dickenstein, N. Fitchas, M. Giusti, C. Sessa, The membership problem for unmixed polynomial ideals is solvable in single exponential time, Discrete Appl. Math. 33 (1991) 73–94.
[14] A. Dickenstein, C. Sessa, Duality methods for the membership problem, in: T. Mora, C. Traverso (Eds.), Effective Methods in Algebraic Geometry, MEGA '90, Progress in Mathematics, vol. 94, Birkhäuser, Basel, 1990, pp. 89–103.
[15] D. Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, Graduate Texts in Mathematics, vol. 150, Springer, Berlin, 1994.

[16] N. Fitchas, A. Galligo, Nullstellensatz effectif et Conjecture de Serre (théorème de Quillen–Suslin) pour le Calcul Formel, Math. Nachr. 149 (1990) 231–253.
[17] N. Fitchas, A. Galligo, J. Morgenstern, Precise sequential and parallel bounds for quantifier elimination over algebraically closed fields, J. Pure Appl. Algebra 67 (1990) 1–14.
[18] N. Fitchas, M. Giusti, F. Smietanski, Sur la complexité du théorème de zéros, in: J. Guddat et al. (Eds.), Approximation and Optimization in the Caribbean II, Proceedings of Second International Conference on Non-Linear Optimization and Approximation, Approximation and Optimization, vol. 8, Peter Lange Verlag, 1995, pp. 247–329.
[19] M. Giusti, J. Heintz, J. Morais, L. Pardo, When polynomial equation systems can be "solved" fast? in: G. Cohen, M. Giusti, T. Mora (Eds.), Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-11, Paris, 1995, Lecture Notes in Computer Science, vol. 948, Springer, Berlin, 1995 pp. 205–231.
[20] M. Giusti, J. Heintz, J. Morais, J. Morgenstern, L. Pardo, Straight-line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1998) 101–146.
[21] M. Giusti, J. Heintz, J. Sabia, On the efficiency of effective Nullstellensatz, Comput. Complexity 3 (1993) 56–95.
[22] K. Hägele, J.E. Morais, L.M. Pardo, M. Sombra, On the intrinsic complexity of the arithmetic Nullstellensatz, J. Pure Appl. Algebra 146 (2000) 103–183.
[23] R. Hartshorne, Residues and Duality, Lecture Notes in Mathematics, vol. 20, Springer, Berlin, 1966.
[24] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.
[25] J. Heintz, C. Schnorr, Testing polynomials which are easy to compute, in: Logic and Algorithmic, an International Symposium held in Honour of E. Specker, Monographie de l'Enseignement Mathématique, vol. 30, Genève, 1982, pp. 237–254.
[26] B. Iversen, Generic Local Structure in Commutative Algebra, Lecture Notes in Mathmatics vol. 310, Springer, Berlin, 1973.
[27] J. Kollár, Sharp effective Nullstellensatz, J. Amer. Math. Soc. 1 (1988) 963–975.
[28] T. Krick, L. Pardo, A computational method for diophantine approximation, in: Effective Methods in Algebraic Geometry, MEGA '94, Progress in Mathematics, vol. 143, Birkhäuser, Basel, 1996, pp. 193–253.
[29] E. Kunz, Introduction to Commutative Algebra and Algebraic Geometry, Birkhäuser, Basel, 1985.
[30] E. Kunz, Kähler Differentials, Adv. Lect. in Math., Vieweg, Braunschweig, 1986.
[31] A. Logar, B. Sturmfels, Algorithms for Quillen–Suslin Theorem, J. Algebra 145 (1992) 231–239.
[32] T. Lam, Serre's Conjecture, Lecture Notes in Mathmatics, vol. 635, Springer, Berlin, 1978.
[33] R. Laudenbacher, C. Woodburn, An algorithm for the Quillen–Suslin theorem for monoid rings, J. Pure Appl. Algebra 117 & 118 (1997) 395–429.
[34] R. Laudenbacher, K. Schlauch, An algorithm for the Quillen–Suslin theorem for quotients of polynomial rings by monomial ideals, Preprint, 1999.
[35] G. Matera, Probabilistic algorithms for geometric elimination, Appl. Algebra in Eng., Communication and Comput. (AAECC J.) 9 (1999) 463–520.
[36] E. Mayr, A. Meyer, The complexity of the word problem for commutative semigroups and polynomial ideals, Adv. in Math. 46 (1982) 305–329.
[37] K. Mulmuley, A fast parallel algorithm to compute the rank of a matrix over an arbitrary field, Proceedings of 18th Annual ACM Symposium on Theory of Computing, 1986, pp. 338–339.
[38] D. Mumford, Algebraic Geometry I: Complex Projective Varieties, Class. in Mathematics, Springer, Berlin, 1995.
[39] P. Philippon, Dénominateurs dans le théorème des zéros de Hilbert, Acta. Arith. 58 (1991) 1–25.
[40] S. Puddu, J. Sabia, An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs, J. Pure Appl. Algebra 129 (1998) 173–200.
[41] F. Rossi, W. Spangher, Some effective methods in the openness of loci for Cohen–Macaulay and Gorenstein properties, in: T. Mora, C. Traverso (Eds.), Effective Methods in Algebraic Geometry, MEGA '90, Progress in Mathematics, vol. 94, Birkhäuser, Basel, 1990, pp. 441–455.
[42] J. Sabia, P. Solernó, Bounds for traces in complete intersections and degrees in the Nullstellensatz, AAECC J. 6 (6) (1995) 353–376.
[43] B. Shiffman, Degree bounds for the division problem in polynomial ideals, Michigan Math. J. 36 (1989) 163–171.

[44] A. Sombra, Bounds for the Hilbert function of polynomial ideal and for the degrees in the Nullstellensatz, J. Pure Appl. Algebra 117 & 118 (1997) 565–599.
[45] B. Teissier, Résultats récents d'algèbre commutative effective, Séminaire Bourbaki 1989–1990, Astérisque 189–190 (1991) 107–131.
[46] W. Vasconcelos, Computational Methods in Commutative Algebra and Algebraic Geometry, Algorithms and Computations in Mathmatics, vol. 2, Springer, Berlin, 1998.
[47] J. Von zur Gathen, Parallel arithmetic computations: a survey, Proceedings of 13th Symposium on MFCS 1986, Lecture Notes in Computer Science, vol. 233, Springer, Berlin, 1986, pp. 93–112.