Journal of Symbolic Computation 115 (2023) 124–141

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

Bounds for degrees of syzygies of polynomials defining a grade two ideal

Teresa Cortadellas Benítez [a], Carlos D'Andrea [b,c], M. Eulàlia Montoro [b]

[a] Universitat de Barcelona, Facultat d'Educació, Passeig de la Vall d'Hebron 171, 08035 Barcelona, Spain
[b] Universitat de Barcelona, Departament de Matemàtiques i Informàtica, Universitat de Barcelona (UB), Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain
[c] Centre de Recerca Matemàtica, Edifici C, Campus Bellaterra, 08193 Bellaterra, Spain

ARTICLE INFO

Article history:
Available online 4 August 2022

MSC:
primary 13P20
secondary 13D02, 14Q20, 68W30

Keywords:
Effective Quillen-Suslin theorem
Hilbert-Burch theorem
Syzygyes
μ-bases
Degree bounds

ABSTRACT

We make explicit the exponential bound on the degrees of the polynomials appearing in the Effective Quillen-Suslin Theorem, and apply it jointly with the Hilbert-Burch Theorem to show that the syzygy module of a sequence of m polynomials in n variables defining a complete intersection ideal of grade two is free, and that a basis of it can be computed with bounded degrees. In the known cases, these bounds improve previous results.

1. Introduction

Let n and m be positive integers, $m \geq 2$, and $R := \mathbb{K}[x_1, \ldots, x_n]$ a polynomial ring in n variables with coefficients in an infinite field $\mathbb{K}$. Suppose that $a_1, \ldots, a_m$, $p, q \in R$ are such that the following equality of ideals in R holds:

$$I := \langle a_1, a_2, \ldots, a_m \rangle = \langle p, q \rangle. \tag{1}$$

E-mail addresses: terecortadellas@ub.edu (T. Cortadellas Benítez), cdandrea@ub.edu (C. D'Andrea), eula.montoro@ub.edu (M.E. Montoro).
URL: http://www.ub.edu/arcades/cdandrea.html (C. D'Andrea).

https://doi.org/10.1016/j.jsc.2022.08.004
0747-7171/

In this paper, we will show that $\mathrm{Syz}(a_1,\dots,a_m)$, the R-syzygy module of the sequence $(a_1,\dots,a_m)$ is a free R-module, and we will develop algorithms for a computation of a basis of it in terms of the matrices of converting the a_i's into p,q and vice versa. Our approach will be the use of the Effective Quillen-Suslin Theorem presented in Caniglia et al. (1993). We will also develop a bound on the degrees of the elements of such a basis as a function of the degrees of the input data.

Note that we are not assuming in principle that neither p and q are coprime, nor that the ideal they define equals the whole ring R. But our claim can be simplified in the first case by removing common factors without changing the syzygy module, and in the second case the problem is solved completely by applying the Effective Quillen-Suslin Theorem (cf. Caniglia et al., 1993) directly to the input data, with better bounds than those presented below. So we can assume w.l.o.g. for the rest of the text that $\gcd(p,q)=1$, and that they do not generate the unitary ideal, i.e. that the grade of I is equal to two. Let $\delta_a\in\mathbb{N}$ be a bound on the total degrees of $a_1,\dots,a_m$, and δ_0 a bound for the degrees of p and q. The main result of this paper is the following.

Theorem 1.1. *Given the data $a_1,\dots,a_m,p,q\in\mathbb{K}[x_1,\dots,x_n]$ satisfying (1), and δ_a, δ_0 as defined above. There is an algorithm which computes an R-basis of $\mathrm{Syz}(a_1,\dots,a_m)$ made by vectors of polynomials of degree bounded by $3n^2 4^n(\delta_0^2+\delta_a+1)^{2n}$.*

If in addition I is zero dimensional (for instance when $n=2$), then another basis of the same module can be computed with the following degree bound:

$$2\delta_0+2\delta_a+2\delta_a^2+\delta_0^2+3mn^2 4^n(2\delta_a^2+\delta_a+\delta_0+1)^{2n}. \tag{2}$$

The proof of this Theorem is given in Section 5.3. These results can be applied to the case treated in our ISSAC 2020 paper (Cortadellas Benítez et al., 2020), where $n=2$, $m=4$ and p,q a "Shape Lemma" representation of the radical ideal I. Our algorithm and main result there state that a basis of $\mathrm{Syz}(a_1,a_2,a_3,a_4)$ can be found with degree bounded by $5\delta_0^4(2\delta_a+1)^4$.

Note that in this case, δ_0 can be expressed in terms of δ_a thanks to Bézout Theorem, and we can set $\delta_0:=\delta_a^2$. The results in Cortadellas Benítez et al. (2020) amount then to a bound of size δ_a^{12}. In contrast, the first bound in Theorem 1.1 amounts to a constant times δ_a^{16}, while the second one is of the order of δ_a^8, which is an improvement with respect to this previous bound. In addition, we will see in Proposition 7.1 that a careful analysis of this situation can actually make the bound of size δ_a^{12} get smaller, comparable to the results in Cortadellas Benítez et al. (2020).

It should be pointed out, however, that even though the situation presented here contains the problem tackled in Cortadellas Benítez et al. (2020), this paper is not a generalization of the results given there, as our methods are slightly different despite the fact that in both cases we use Hilbert-Burch and Effective Quillen-Suslin theorems. Our ISSAC 2020 paper dealt with the case when p and q are "shape" basis of an ideal of 4 polynomials in 2 variables, and the results were restricted to that case. Here, we deal with any number of polynomials and variables, and even in the case $n=2$ we are not assuming that the ideal has a shape basis, just that it is a complete intersection of grade 2. In Section 7 we will compare both approaches.

The computation of syzygies of sequences of polynomials is of major interest in the Computer Aided Geometric Design community. In the cases of curves ($n=1$) and surfaces ($n=2$), these are called "μ-bases", see for instance Cox (2003); Chen and Wang (2003); Chen et al. (2005); Deng et al. (2005); Hong et al. (2017); Shen and Goldman (2017); Yao et al. (2019); Yao and Jia (2019) and the references therein. The situation for curves is quite well-understood and classical, see for instance Cox et al. (1998). The existence of μ-bases for surfaces has been proven in Chen et al. (2005), and several methods have been proposed for computing them in taylored situations (revolution, canal, translational, ... surfaces). In Deng et al. (2005), a concrete method for computing a μ-basis is proposed based on the Matrix Primitive Factorization Theorem given in Guiver and Bose (1982), but no concrete bounds on the outcome are given.

Even though the study of syzygies of ideals of grade 2 does not cover all the cases of interest in the literature —for instance, it is known that if $n=2$ the syzygy module of $a_1,\dots,a_m$ is always free independently of the fact that I can be generated by 2 polynomials, see Cid-Ruiz (2019) for general bounds for degrees in this case— the situation presented in (1) is quite general in the sense that to

have $\mathrm{Syz}(a_1,\dots,a_m)$ being a free module, if all the a_i's are coprime, then Hilbert-Burch Theorem 2.1 implies that this ideal must have grade 2, and hence they should be described —at least locally— with two polynomials.

The paper is organized as follows: in Section 2 we review both Hilbert-Burch and Effective Quillen-Suslin Theorems (Theorems 2.1 and 2.2 respectively), and give an explicit bound in Theorem 2.6 for the degree of a unimodular "inverse" matrix to a unimodular one. In Section 3 we show that the matrix of polynomials converting $(a_1 \dots a_m)$ into $(p\ q)$ is unimodular, while the one reversing this process is "almost" unimodular, see Proposition 3.3, but can be replaced by a unimodular one (cf. Proposition 3.4). This result allows a complete characterization of those data $a_1,\dots,a_m,p,q\in R$ satisfying (1) in terms of a unimodular conversion matrix, see Theorem 3.5.

All these results are then used in Section 4 to develop algorithms which compute an R-basis of $\mathrm{Syz}(a_1,\dots,a_m)$ based each of them in one of these conversion matrices.

In Section 5 we study degree bounds for the output of the algorithms presented, and also prove Theorem 1.1. In section 6 we show some examples illustrating our methods and tools. We conclude the paper by comparing our approach with the one presented in Cortadellas Benítez et al. (2020) in Section 7.

Acknowledgements: All our computations were done with the aid of the softwares Maple (Maple, 2020) and Mathematica (Wolfram Research, Inc., 2018). We also acknowledge useful conversations with Martín Sombra while working some of the results of this paper. T. Cortadellas was supported by the Spanish MICINN Research projects MTM2013-40775-P and PID 2019-104844GB-100. C. D'Andrea and M.E. Montoro were supported by the Spanish MICINN research projects MTM 2015-65361-P and PID2019-104047GB-I00. C. D'Andrea was also supported by the Spanish State Research Agency, through the Severo Ochoa and María de Maeztu Program for Centers and Units of Excellence in R&D (CEX2020-001084-M).

2. Hilbert-Burch and effective Quillen-Suslin theorems

We start by recalling the well-known Hilbert-Burch Theorem for resolutions of length 1.

Theorem 2.1. *(Eisenbud, 2005, Theorem 3.2) Suppose that an ideal I in a Noetherian commutative ring A admits a free resolution of length 1 as follows:*

$$0 \to F_1 \xrightarrow{G} F_2 \to I \to 0.$$

If the rank of the free module F_1 is ℓ, then the rank of F_2 is $\ell+1$, and there exists a nonzero divisor $a\in A$ such that I is equal to a times the ideal of $\ell\times\ell$ minors of the matrix G with respect with any given bases of F_1 and F_2. The generator of I that is the image of the i-th basis vector of F_2 is $\pm a$ times the determinant of the submatrix of G formed from all except the i-th row. Moreover, the grade of the ideal of maximal minors is 2.

Conversely, given an $(\ell+1)\times\ell$ matrix G with entries in A such that the grade of the ideal of $\ell\times\ell$ minors of G is at least 2, and a given nonzero divisor $a\in A$, the ideal I generated by a times the $\ell\times\ell$ minors of G admits a free resolution of length one as above. It has grade 2 if and only if a is a unit.

We bring also to the picture the main tool we will use in our paper, namely the Effective Quillen-Suslin Theorem. We recall that $R=\mathbb{K}[x_1,\dots,x_n]$ is a polynomial ring in n variables with coefficients in an infinite field $\mathbb{K}$. A matrix $U\in R^{r\times s}$ is called *unimodular* if the ideal generated by the maximal minors of it equals to the whole ring R. We denote by $\mathbf{I}_r$ the identity matrix of size $r\times r$. An elementary matrix is one that consists in exchanging two rows (or two columns) of $\mathbf{I}_r$, or adding to a row (or column) a polynomial multiple of another. The degree of a matrix equals the maximum of the degrees of its entries.

Theorem 2.2. *(Caniglia et al., 1993, Theorem 3.1) Assume that $F\in R^{r\times s}$ is unimodular, with $r\le s$. Then, there exists a square matrix $U\in R^{s\times s}$ such that*

(1) *U is unimodular,*

(2) $F \cdot U = [\mathbf{I}_r, \mathbf{0}] \in R^{r\times s}$,
(3) $\deg(U) = (rd)^{\mathcal{O}(n)}$, *and*
(4) U *is a product of* $\mathcal{O}(n^2 s^2 (rd)^{2n})$ *matrices, each of them being elementary or having the form* $T \oplus \mathbf{I}_{s-r-1}$ *for some* $T \in SL_{r+1}(R)$.

The proof given in Caniglia et al. (1993) of this result is constructive. In the rest of this section, we will review some steps of it to make explicit the exponent $\mathcal{O}(n)$ which appears in (3).

Assume then that a unimodular matrix $F \in R^{r\times s}$ is given. In a preliminary step in Caniglia et al. (1993), one has to make a linear change of coordinates, and then multiply F by the unimodular matrix $A = (a_{ij})_{1\le i,j\le s}$ defined by

$$a_{ij} = \begin{cases} x_n & \text{if } \ i = j \le r \\ 1 & \text{if } \ j = i+1 \\ 1 & \text{if } \ i = s,\ j = 1 \\ 0 & \text{everywhere else} \end{cases},$$

in such a way that the conditions of Assumption 2.8 in Caniglia et al. (1993) are satisfied, namely that the $r \times r$ minor of F made by choosing the first r columns is monic in all the variables $x_1, \dots, x_n$, and having total degree strictly larger than the degree of the remaining maximal minors of F. This may increase the value of d in 1, so we will have to keep track of this in order to get an explicit bound.

Next we will have to deal with a version of Hilbert's Nullstellensatz presented in that paper. To do this, consider the $s \times s$ matrix $Y = (y_{ij})_{1\le i,j\le s}$ where each of the y_{ij} is a new indeterminate. Set $F_Y := F \cdot Y \in (R \otimes \mathbb{K}[y_{ij}])^{r\times s}$. Denote with D_1 (resp. D_2) the determinant of the $r \times r$ submatrix of F_Y made by choosing its first r columns (resp. the columns $1, \dots, r-1, r+1$), and denote with $c \in \mathbb{K}[x_1, \dots, x_{n-1}, y_{ij},\ 1 \le i, j \le s]$, the resultant as defined in Walker (1978, Theorem 9.3) of D_1 and D_2 with respect to x_n. From Walker (1978, Theorem 10.9) we easily verify that

$$\deg_{x_1,\dots,x_{n-1}}(c) \le \big(r(d+1)\big)^2, \tag{3}$$

and moreover by applying the latter result and (Walker, 1978, Theorem 9.6) we deduce that there exist $A_1, A_2 \in \mathbb{K}[x_1, \dots, x_{n-1}, y_{ij},\ 1 \le i, j \le s]$ such that

$$c = A_1 D_1 + A_2 D_2, \text{ with } \deg_{x_1,\dots,x_{n-1}}(A_1, A_2) \le \big(r(d+1)\big)^2. \tag{4}$$

Lemma 2.3. *(Caniglia et al., 1993, Lemma 4.4) For all* $\xi \in \mathbb{K}^{n-1}$, *there exists* $\mathbf{y}_\xi \in \mathbb{K}^{s\times s}$ *such that* $c(\xi, \mathbf{y}_\xi) \neq 0$.

With this result in hand, we can prove the following effective version of Hilbert's Nullstellensatz.

Proposition 2.4. *There exist matrices* $\mathbf{y}^1, \dots, \mathbf{y}^n \in \mathbb{K}^{s\times s}$ *such that*

$$\langle c(x, \mathbf{y}^1), \dots, c(x, \mathbf{y}^n)\rangle = R. \tag{5}$$

Proof. Denote with $\overline{\mathbb{K}}$ the algebraic closure of $\mathbb{K}$. Start by picking any $\xi_1 \in \mathbb{K}^{n-1}$, and set $\mathbf{y}^1 \mapsto y(\xi_1)$. Thanks to Lemma 2.3 we have that $c(x, \mathbf{y}^1) \neq 0$, and hence the variety defined by its zeroes is a hypersurface in $\overline{\mathbb{K}}^{n-1}$.

Denote with $W_1, \dots, W_\ell$ the irreducible components of maximal dimension of this hypersurface, and pick $\chi_1, \dots, \chi_\ell \in \overline{\mathbb{K}}^{n-1}$ such that $\chi_j \in W_j$. By Lemma 2.3, none of the polynomials $c(\chi_j, y_{ij}) \in \mathbb{K}[y_{ij}]$ can be identically zero, so the product $\prod_{j=1}^{\ell} c(\chi_j, y_{ij})$ also is non-zero. As $\mathbb{K}$ is infinite, we can choose $\mathbf{y}^2 \in \mathbb{K}^{s\times s}$ such that $\prod_{j=1}^{\ell} c(\chi_j, \mathbf{y}^2) \neq 0$. With this choice, we have that the variety defined by the zeroes of $c(x, \mathbf{y}^1)$ and $c(x, \mathbf{y}^2)$ cannot have components of codimension 1 in $\overline{\mathbb{K}}^{n-1}$ as the latter polynomial cannot vanish identically in any of the W_j.

The same argument can be applied recursively as follows: given $c(x,\mathbf{y}^1),\dots,c(x,\mathbf{y}^i)$ such that the set of common zeroes of these polynomials has irreducible components of dimension at most $n-1-i$, there exist $\mathbf{y}^{i+1}\in\mathbb{K}^{s\times s}$ such that $c(x,\mathbf{y}^{i+1})$ cuts properly every component of maximal dimension of this algebraic set. We will eventually arrive to the situation where the system $c(x,\mathbf{y}^1),\dots,c(x,\mathbf{y}^n)$ defines the empty variety in $\overline{\mathbb{K}}^{n-1}$. Hilbert's Nullstellensatz then implies (5). □

We will also need the following refinement of the Effective Nullstellensatz for the degrees of polynomials involving a Bézout identity.

Proposition 2.5. *Let $c(x,\mathbf{y}^1),\dots,c(x,\mathbf{y}^n)$ be as in (5). Then one can have*

$$x_n = a_1\,c(x,\mathbf{y}^1)+\ldots+a_n\,c(x,\mathbf{y}^n)$$

with $a_1,\dots,a_n\in R$, and $\deg\big(a_i\,c_i(x,\mathbf{y}^i)\big)\le 2\big(r(d+1)\big)^{2(n-1)}$.

Proof. By the Effective Nullstellensatz (Theorem 1.1 in Jelonek, 2005), there exist $b_1,\dots,b_n\in\mathbb{K}[x_1,\dots,x_{n-1}]$ such that $1=b_1\,c(x,\mathbf{y}^1)+\ldots+b_n\,c_n(x,\mathbf{y}^n)$, with $\deg(b_i\,c(x,\mathbf{y}^i))\le 2(r(d+1))^{2(n-1)}-1$. The claim now follows by multiplying by x_n both sides of this equality. □

Theorem 2.6. *Assume that $F\in R^{r\times s}$ is unimodular, with $r\le s$. Then, the matrix $U\in R^{s\times s}$ of Theorem 2.2 can be computed with*

$$\deg(U)\le 3n^2(r(d+1))^{2n}.$$

Proof. We start by following the steps of the algorithms given in the proof of Proposition 4.1 (Procedure 4.3) in Caniglia et al. (1993) to compute a matrix U_n which "eliminates" the variable x_n from F by evaluating it to zero, i.e. $F\cdot U_n = F|_{x_n=0}$.

- In their step 1, their number N can be replaced by n thanks to Proposition 2.4.
- In their step 2, we have $\deg(a_i\,c_i(x,\mathbf{y}^i))\le 2\big(r(d+1)\big)^{2(n-1)}$ thanks to Proposition 2.5.
- The degree of what is called E_k in their step 3 is bounded by

$$\deg(E_k)\le r(d+1)(1+r(d+1))2\big(r(d+1)\big)^{2(n-1)}\le 3\big(r(d+1)\big)^{2n}.$$

- To compute the unimodular matrix U_n (matrix M in their notation), one has to multiply $N(=n)$ of these matrices E_k, so we have that

$$\deg(U_n)\le 3n\big(r(d+1)\big)^{2n}.$$

By applying this process recursively and eliminating all the variables, we see that the unimodular matrix U of Theorem 2.2 can be computed as a product of matrices $U_n\cdot U_{n-1}\dots U_1\cdot U_0$, where for $i>0$, each U_i eliminates the variable x_i, and $U_0\in\mathbb{K}^{s\times s}$ is a matrix of scalars. So, we have then that

$$\deg(U)\le 3n^2\big(r(d+1)\big)^{2n},$$

as claimed. □

3. Syzygies and unimodularity

In this section, we will relate the matrices converting $a_1,\dots,a_m$ into p,q, and vice versa, with unimodular matrices. This will allow us to use the Effective Quillen-Suslin Theorem 2.2 to produce an R-basis of $\mathrm{Syz}(a_1,\dots,a_m)$ of controlled degree.

Let then $a_1,\dots,a_m,\ p,q\in R$ be such that (1) holds. The syzygy module of the sequence $(a_1,\dots,a_m)$ is defined as

$$\mathrm{Syz}(a_1,\dots,a_m) := \{(u_1,\dots,u_m) \in R^m \mid u_1a_1 + \dots + u_ma_m = 0\} \subset R^m.$$

Note that we are not claiming that $\gcd(p,q) = 1$, but this can be assumed w.l.o.g. as $\mathrm{Syz}(a_1,\dots,a_m)$ does not change after removing a common factor of all these polynomials (which would be a common factor of p and q thanks to (1))).

From (1), we deduce that there exist matrices $M \in R^{2\times m}$ and $N \in R^{m\times 2}$ such that

$$(a_1\ a_2\ \dots\ a_m)\cdot N = (p\ q),\quad (p\ q)\cdot M = (a_1\ a_2\ \dots\ a_m). \tag{6}$$

In principle, there are infinite matrices M and N that satisfy (6). The results that we prove in the sequel hold for *any* of these choices. Denote with K the 2×2 matrix which is the product $M\cdot N$.

Lemma 3.1. *Assuming that* $\gcd(p,q) = 1$, *there exist* $e,\ f \in R$ *such that*

$$K = \begin{pmatrix} 1 - e\cdot q & f\cdot q \\ e\cdot p & 1 - f\cdot p \end{pmatrix}. \tag{7}$$

Proof. Write $K = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. From (6) we deduce straightforwardly that

$$(p\ q)\cdot K = (p\ q)\cdot M\cdot N = (p\ q).$$

So, we have

$$\begin{cases} p &= \alpha\cdot p + \gamma\cdot q \\ q &= \beta\cdot p + \delta\cdot q \end{cases}.$$

From here we deduce that

$$\begin{cases} (1-\alpha)p &= \gamma\cdot q \\ (1-\delta)q &= \beta\cdot p \end{cases},$$

so there exist $\lambda, \tilde{\lambda}$ in $Q(R)$, the field of fractions of R, such that

$$\begin{cases} 1-\alpha &= \lambda\cdot q \\ \gamma &= \lambda\cdot p \\ 1-\delta &= \tilde{\lambda}\cdot p \\ \beta &= \tilde{\lambda}\cdot q \end{cases}.$$

As $\lambda\cdot q$ and $\lambda\cdot p$ are elements of R and $\gcd(p,q) = 1$, then we deduce that $\lambda \in R$. The same happens with $\tilde{\lambda}$. The claim follows by setting $e \mapsto \lambda,\ f \mapsto \tilde{\lambda}$. □

We cannot claim that K is a unimodular matrix. As a matter of fact, with the notation above we have that $\det(K) = 1 - e\cdot q - f\cdot p$, which is an element of $\mathbb{K}$ if and only if $e\cdot q + f\cdot p \in \mathbb{K}$. If this is the case and $\det(K) \neq 1$, then I is principal, and the Quillen-Suslin Theorem 2.2 shows that $\mathrm{Syz}(a_1,\dots,a_m)$ is a free R-module, and gives bounds for the degrees of a basis of this module, which are better than those appearing in Theorem 4.1.

In any case, we can modify the matrix M so that we get $e = f = 0$. We start by denoting with

$$\tilde{K} := \begin{pmatrix} 1 - e\cdot q & f\cdot q & -q \\ e\cdot p & 1 - f\cdot p & p \end{pmatrix} \in R^{2\times 3}, \tag{8}$$

the matrix which consists in adding to K the column $\begin{pmatrix} -q \\ p \end{pmatrix}$.

Lemma 3.2. *$\tilde{K}$ is a unimodular matrix.*

Proof. Indeed the 3 maximal minors of $\tilde{K}$ are p, q and $1 - e \cdot q - f \cdot p$. From here the claim follows straightforwardly. □

To connect $\tilde{K}$ with M and N, we write them down explicitly:

$$N = \begin{pmatrix} b_1 & c_1 \\ b_2 & c_2 \\ \vdots & \vdots \\ b_m & c_m \end{pmatrix} \text{ and } M = \begin{pmatrix} d_1 & d_2 & \dots & d_m \\ e_1 & e_2 & \dots & e_m \end{pmatrix}. \tag{9}$$

Proposition 3.3. *N is a unimodular matrix, and so is $\tilde{M}$, where*

$$\tilde{M} := \begin{pmatrix} d_1 & d_2 & \dots & d_m & -q \\ e_1 & e_2 & \dots & e_m & p \end{pmatrix} \in R^{2\times(m+1)}. \tag{10}$$

Proof. Set

$$\tilde{N} = \begin{pmatrix} b_1 & c_1 & 0 \\ b_2 & c_2 & 0 \\ \vdots & \vdots & \\ b_m & c_m & 0 \\ 0 & 0 & 1 \end{pmatrix} \in R^{(m+1)\times 3}. \tag{11}$$

We clearly have $\tilde{M} \cdot \tilde{N} = \tilde{K}$. As $\tilde{K}$ is unimodular, so are $\tilde{N}$ and $\tilde{M}$ (this can be seen for instance by using the Cauchy-Binet formula (Broida and Williamson, 1989, §4.6) for computing minors of a product of matrices). The fact that N is unimodular follows just by noting that all the nonzero maximal minors of it are —up to the sign— the nonzero maximal minors of $\tilde{N}$. □

Note that Proposition 3.3 states that *a*ny matrix N as in (6) is unimodular. That does not apply to M, see for instance Example 6.2. However, one can always replace M with a unimodular one as the following result shows.

Proposition 3.4. *M can be chosen as in (6) to be unimodular.*

Proof. Let $e, f \in R$ be such that (7) holds. If $(e, f) = (0, 0)$ we are done. If not, because N is unimodular, its rows generate R^2 as an R-module, so there exist $x_1 \dots x_m \in R$ such that

$$x_1 \cdot (b_1\ c_1) + x_2 \cdot (b_2\ c_2) + \dots + x_m \cdot (b_m\ c_m) = (e\ -f). \tag{12}$$

Set then

$$M' = M + \begin{pmatrix} x_1 q & x_2 q & \dots & x_m q \\ -x_1 p & -x_2 p & \dots & -x_m p \end{pmatrix}. \tag{13}$$

We clearly have that M' satisfies (6), and an easy computation shows that

$$M' \cdot N = \left(M + \begin{pmatrix} x_1 q & x_2 q & \dots & x_m q \\ -x_1 p & -x_2 p & \dots & -x_m p \end{pmatrix} \right) \cdot N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{14}$$

thanks to (12). So, M' is unimodular, as claimed. □

We conclude by showing a characterization of those ideals of grade 2 having the property (1) via the matrix M.

Theorem 3.5. *For $a_1 \dots, a_m,\ p,\ q \in R$, we have that $\langle a_1, \dots, a_m \rangle = \langle p, q \rangle$ if and only if there exists a unimodular matrix $M \in R^{2\times m}$ such that*

$$(p\ q) \cdot M = (a_1 \dots a_m).$$

Proof. The "if" part follows from Proposition 3.4. For the converse, apply Theorem 2.2 to the unimodular matrix M, and let $U \in R^{m\times m}$ be such that $M \cdot U = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \end{pmatrix}$. Set $N \in R^{m\times 2}$ to be the matrix consisting of the first two columns of U. We then have that (6) holds and so (1), which proves the claim. □

Remark 3.6. The role of M and N are different in the characterization of ideals satisfying (1). Indeed, having N unimodular is not enough to characterize these ideals, as for instance we may have $a_1, \dots, a_m \in R$ with $m \geq 3$ be such that $a_3 \notin \langle a_1, a_2 \rangle$. If we set $N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ \vdots & \vdots \\ 0 & 0 \end{pmatrix}$, then it is clear that we will never find an M such that (6) holds.

4. Algorithms

We will now exhibit algorithms to compute R-bases of $\mathrm{Syz}(a_1, \dots, a_m)$ by applying the Effective Quillen-Suslin Theorem 2.2 to $\tilde{M}$, M' or N.

4.1. Working with $\tilde{M}$

With notation as above, from Theorem 2.2 we deduce that there exists a square unimodular matrix $U \in R^{(m+1)\times(m+1)}$ such that

$$\tilde{M} \cdot U = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \end{pmatrix}. \tag{15}$$

Assume w.l.o.g. that $\det(U) = 1$. From (6) we deduce that $(p\ q) \cdot \tilde{M} = (a_1 \dots a_m\ 0)$, and hence we must have

$$(p\ q) \cdot \tilde{M} \cdot U = (p\ q\ 0 \dots 0) = (a_1 \dots a_m\ 0) \cdot U \tag{16}$$

Let $\widehat{U} \in R^{m\times(m-1)}$ the submatrix of U consisting in removing its first two columns and its last row. From (16) we deduce that the columns of $\widehat{U}$ are syzygies of $(a_1, \dots, a_m)$. Our main result is the following.

Theorem 4.1. *The columns of $\widehat{U}$ are an R-basis of $Syz(a_1, \dots, a_m)$.*

Proof. Let $U^1, \dots, U^{m+1}$ be the columns of U, and denote with $\tilde{U} \in R^{(m+1)\times m}$ the matrix whose columns are $-q \cdot U^1 + p \cdot U^2,\ U^3, \dots, U^{m+1}$, in this order. By applying Cramer's rule to the last equality of (16), we deduce that the signed maximal minors of this matrix are $a_1, \dots, a_m, 0$. Hence, the ideal generated by these maximal minors is I, which has grade 2 by our initial assumptions. By applying then the converse of the Hilbert-Burch Theorem 2.1, we deduce then that the columns of $\tilde{U}$ are a basis of $\mathrm{Syz}(a_1, \dots, a_m, 0)$.

We claim now that the first two rows of U^{-1}, the inverse matrix of U, are equal to $\tilde{M}$. Indeed, denote then by $U^{-1}_{2\times(m+1)}$ the submatrix of U^{-1} made by these rows. From (15) we deduce that

$$\tilde{M} \cdot U = U^{-1}_{2\times(m+1)} \cdot U,$$

and as U is invertible, the claim follows. In particular, the last column of U^{-1} is of the form $\begin{pmatrix} -q \\ p \\ r_3 \\ \vdots \\ r_{m+1} \end{pmatrix}$ for suitable $r_3, \ldots, r_{m+1} \in R$. From the identity $U \cdot U^{-1} = \mathbf{I}_{m+1}$, we deduce that

$$-q \cdot U^1 + p \cdot U^2 + r_3 \cdot U^3 + \ldots + r_{m+1} \cdot U^{m+1} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

This implies that if we perform the following column operation in $\tilde{U}$: to its first column (which is equal to $-q \cdot U^1 + p \cdot U^2$) we add $r_3 U^3 + \ldots + r_{m+1} U^{m+1}$, the fact that its columns are an R-basis of $\mathrm{Syz}(a_1, \ldots, a_m, 0)$ remains unchanged, but now the first column of the modified matrix is equal to $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$.

From here, we can perform new column operations in $U^3, U^4, \ldots, U^{m+1}$ in such a way that the last row of $\tilde{U}$ equals to $(1\ 0 \ldots\ 0)$, and the other coefficients of this matrix have not changed. So, we have shown that $\mathrm{Syz}(a_1, \ldots, a_m, 0)$ has an R-basis of the form

$$\begin{pmatrix} 0 & \widehat{U} \\ 1 & 0 \end{pmatrix}.$$

From here the claim follows straightforwardly. □

4.2. Working with a unimodular M

If M is already unimodular (which is for instance the case of the matrix M' defined in (13), although we are not requiring that $M \cdot N = \mathbf{I}_2$ as in (14)), we can apply directly the Effective Quillen-Suslin Theorem 2.2 to M and obtain a unimodular $U^* \in R^{m \times m}$ such that

$$M \cdot U^* = \begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \end{pmatrix}. \tag{17}$$

From (6) we now get that $(p\ q) \cdot M = (a_1 \ldots a_m)$, and hence

$$(p\ q) \cdot M \cdot U^* = (p\ q\ 0 \ldots 0) = (a_1 \ldots a_m) \cdot U^*. \tag{18}$$

Denote the columns of U^* with $U^{*1}\ U^{*2} \ldots, U^{*m}$. Let $\widehat{U^*} \in R^{m \times (m-1)}$ be the matrix

$$\widehat{U^*} = \left(qU^{*1} - pU^{*2},\ U^{*3}, \ldots,\ U^{*m} \right). \tag{19}$$

By applying Cramer's rule to (18), and using the converse of the Hilbert-Burch Theorem 2.1, we deduce straightforwardly that

Theorem 4.2. *The columns of $\widehat{U^*}$ defined in (19) are an R-basis of $\mathrm{Syz}(a_1, \ldots, a_m)$.*

4.3. Working with N

We can also work directly with the unimodular matrix N from (6) and construct an R basis of $\mathrm{Syz}(a_1, \ldots, a_m)$ as follows: denote with $N^* \in R^{m \times m}$ a matrix of determinant equals to 1 such that

it has N as its first 2 columns. This can be done by applying the Quillen-Suslin Theorem 2.2 to $N^{\mathbf{t}}$. The matrix N^* can be taken to be the inverse of matrix U in this claim. Denote its columns with $N^{*1}, \dots, N^{*m}$.

From (6), we clearly have that $(a_1 \dots a_m) \cdot N^{*1} = p$, and $(a_1 \dots a_m) \cdot N^{*2} = q$. As for all $i = 1, \dots, m$, we have that $(a_1 \dots a_m) \cdot N^{*i} \in \langle a_1, \dots, a_m \rangle = \langle p, q \rangle$, for $i = 3, \dots, m$ we write $(a_1 \dots a_m) \cdot N^{*i} = \lambda_i p + \delta_i q$ for suitable λ_i, $\delta_i \in R$.

Perform then the following elementary column operations in N^*: for $i = 3, 4, \dots, m$, replace column N^{*i} with $N^{*i} - \lambda_i N^{*1} - \delta_i N^{*2}$. Call the remaining matrix N^{**}. By construction:

- $\det(N^{**}) = 1$, i.e. N^{**} is unimodular;
- $(a_1 \dots a_m) \cdot N^{**} = (p \ q \ 0 \dots 0)$

Denote then with $N^{**1}, N^{**2}, \dots$ the columns of N^{**}, and let $\widehat{N} \in R^{m \times (m-1)}$ the matrix whose columns are

$$\widehat{N} = \left(qN^{**1} - pN^{**2} \ N^{**3} \dots N^{**m} \right) \tag{20}$$

Theorem 4.3. *The columns of $\widehat{N}$ are an R-basis of Syz$(a_1, \dots, a_m)$.*

Proof. As before, by taking into account that $(a_1 \dots a_m) \cdot N^{**} = (p \ q \ 0 \dots 0)$, and applying Cramer's rule to this matrix, it is easy to see that the signed maximal minors of $\widehat{N}$ are $a_1, \dots a_m$. The converse of the Hilbert-Burch Theorem 2.1 then proves the claim. □

4.4. Relations among the bases

In the following, we will show that if one picks convenient unimodular matrices in the process of computing the several R-basis of Syz$(a_1, \dots, a_m)$ described above, the ansatz is essentially the same. We begin by proving the following straightforward relation between U^* and N^* if M is already unimodular.

Proposition 4.4. *Suppose that $M \cdot N = \mathbf{I}_2$ (in particular, we have that M is unimodular). Then, one can find a unimodular $m \times m$ matrix which can be used as U^* in (17) and also as N^{**} from §4.3. Moreover, we get $\widehat{U^*} = \widehat{N}$, i.e. the bases from Theorems 4.2 and 4.3 coincide.*

Proof. Start by picking any $U_0^* \in R^{m \times m}$ satisfying (17). Denote its columns with $U_0^{*1} \dots U_0^{*m}$. As we have

$$M \cdot \left(U_0^{*1} \ U_0^{*2} \right) = M \cdot N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

we deduce that each of the columns of $\left(U_0^{*1} \ U_0^{*2} \right) - N$ belongs to the right-kernel of M. Denote also with N^1 and N^2 the columns of N. As M is unimodular, its right-kernel is a free R-module, with basis $U_0^{*3}, \dots, U_0^{*m}$. So there exist $y_{i3}, \dots, y_{im} \in R$ such that

$$U_0^{*i} - N^i = y_{i3} U_0^{*3} + \dots + y_{im} U_0^{*m}, \ i = 1, 2$$

Set now U^* to be the matrix obtained from U_0^* by substracting to the column i the following linear combination of columns: $y_{i3} U_0^{*3} + \dots + y_{im} U_0^{*m}$, $i = 1, 2$. Clearly U^* is unimodular, and has N as its first two columns, so the first part of the claim follows.

To see the second part, note that as we have

$$(a_1 \dots a_n) \cdot N^* = (p \ q) \cdot M \cdot U^* = (p \ q \ 0 \dots 0),$$

we deduce that λ_i, δ_i, $i = 3, \dots, m$ from §4.3 are all equal to zero, and hence the matrix N^{**} defined in that section equals to N^* (which is equal to U^*). As the process to convert N^{**} into $\widehat{N}$ and U^*

into $\widehat{U^*}$ is the same (replace the first two columns with q times the first column minus p times the second column), we deduce straightforwardly that $\widehat{U^*} = \widehat{N}$, which concludes with the proof of the proposition. □

If M is not unimodular anymore, we will have to work with matrices $\tilde{M}$ and $\tilde{N}$ which were defined in (10) and (11) respectively. The following result then holds.

Proposition 4.5. *The matrices U and N^* from (15) and §4.3 respectively can be chosen in such a way that the latter is a submatrix of the first, and that $\widehat{U^*} = \widehat{N}$, i.e. the bases from Theorems 4.2 and 4.3 coincide.*

Note that we are not having any requirement about the result of the product between $\tilde{M}$ and $\tilde{N}$ as it may be hinted by the situation in Proposition 4.4.

Proof. Denote the columns of N with N^1, N^2, and set

$$\tilde{N}^* = \begin{pmatrix} N^1 & N^2 & qN^1 - pN^2 \\ -e & f & 1 - eq - fp \end{pmatrix} \in R^{(m+1)\times 3}, \tag{21}$$

with $e, f \in R$ as in (3.1). As $\tilde{M} \cdot \tilde{N} = \tilde{K}$, with $\tilde{K}$ defined in (8), we deduce that

$$\tilde{M} \cdot \tilde{N}^* = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

This implies that $\tilde{N}^*$ is unimodular, and hence can be extended to an invertible $U \in R^{(m+1)\times(m+1)}$ such that (15) holds and having $\tilde{N}^*$ as its first columns. We have then that

$$U = \begin{pmatrix} N^1 & N^2 & qN^1 - pN^2 & N^4 & \dots & N_{m+1} \\ -e & f & 1 - eq - fp & r_4 & \dots & r_{m+1} \end{pmatrix}$$

for suitable columns $N^4, \dots, N^{m+1}$ in $R^{m\times 1}$ and suitable $r_4, \dots, r_{m+1} \in R$. As by performing elementary operations in the first columns of U we can get $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$, we deduce then that, by picking

$N^* = (N^1 \ N^2 \ N^4 \dots N^{m+1}) \in R^{m\times m}$,

- N^* is unimodular and has as first two columns N^1 and N^2, i.e. it is a valid N^* in the sense of the algorithm described in §4.3.
- Following the steps of that algorithm, $N^{**} = N^*$.
- $\widehat{N}$ from (20) equals to $\left(qN^1 - pN^2 \ N^4 \dots N^{m+1}\right) = \widehat{U}$ from Theorem 4.1.

This concludes with the proof of the Proposition. □

5. Degree bounds and proof of the main theorem

In this section, we will apply our explicit bound given in Theorem 2.6 to give bounds for $\deg(\widehat{U})$ from Theorem 4.1, $\deg(\widehat{U^*})$ from Theorem 4.2, and $\deg(\widehat{N})$ from Theorem 4.3. These bounds are given in terms of the degrees of both the input polynomials, but also of the transition matrices. We will show also some relations among the input bounds, and conclude by proving Theorem 1.1 from the Introduction.

Recall that we have δ_0 being a bound for the degrees of p and q, and δ_a being a bound on the degrees of $a_1, \dots, a_m$. In addition, we set δ_N (resp. δ_M) being a bound for the degrees of the elements in N (resp. M).

Proposition 5.1. *With notation as above, if* $\delta \geq \max\{\delta_M, \delta_0\}$, *we have that*

$$\deg(\widehat{U}) \leq 3n^2 4^n (\delta + 1)^{2n}.$$

Proof. Note that $\widehat{U}$ is a submatrix of the unimodular matrix U. The result is then consequence of Theorem 2.6 with $r = 2$. □

Proposition 5.2. *With notation as above, if* M *is unimodular, we have that*

$$\deg(\widehat{U^*}) \leq 3n^2 4^n (\delta_M + 1)^{2n} + \delta_0.$$

Proof. By applying Theorem 2.6 to the unimodular matrix M we obtain U^* as in (17) with

$$\deg(U^*) \leq 3n^2 4^n (\delta_M + 1)^{2n}.$$

To get $\widehat{U^*}$ we only have to modify the first column of U^* and multiply a couple of columns of the latter by $-q$ and p. From here, the claim follows straightforwardly. □

Interestingly, the computation of a basis of syzygies starting from N will give us degree bounds which can differentiate the degrees of the different actors involved. The drawback is that this bound depends also on m, the number of elements of the sequence. Sometimes this leads to lower bounds as in the case of parametric curves, see Section 7.

Proposition 5.3. *With notation as above, we have that*

$$\deg(\widehat{N}) \leq \delta_0 + \delta_N + \delta_M + 3mn^2 4^n (\delta_N + 1)^{2n}.$$

Proof. By applying the Effective Quillen-Suslin procedure to the unimodular matrix N, we deduce that the matrix U of Theorem 2.2 has degree bounded by $3n^2 4^n (\delta_N + 1)^{2n}$, thanks to Theorem 2.6 with $r = 2$.

The matrix N^* from §4.3 is then the inverse of U, and can be computed by using cofactors. Hence, its entries have degree bounded by

$$3mn^2 4^n (\delta_N + 1)^{2n}.$$

As we have $(p\ q) \cdot M = (a_1\ a_2 \dots a_m)$ from (6), we get

$$(a_1 \dots a_m) \cdot N^{*i} = \lambda_i p + \delta_i q = (p\ q) \cdot M \cdot N^{*i},$$

and deduce then that $\deg(\lambda_i), \deg(\delta_i) \leq \delta_N + \delta_M$ for all $i = 3, \dots, m$. By construction, we have that

$$\deg(N^{**}) \leq \delta_N + \delta_M + 3mn^2 4^n (\delta_N + 1)^{2n}.$$

To pass from N^{**} to $\widehat{N}$, the matrix encoding a basis of $\mathrm{Syz}(a_1, \dots, a_m)$, we only need to modify the first column of N^{**}, and we have

$$\deg(\widehat{N}) \leq \delta_0 + \delta_N + \delta_M + 3mn^2 4^n (\delta_N + 1)^{2n},$$

as claimed. □

5.1. From $\tilde{M}$ to an unimodular M

The bounds on the degrees of the bases computed via $\tilde{M}$ or M if the latter is unimodular are not very comparable, for instance they depend on whether $\delta_0 > \delta_M$ or vice versa. We will compute for completion of our study of the degrees appearing in these matrices a bound on the unimodular matrix M' defined in (13) in terms of the input degrees of the problem.

Proposition 5.4. *With notation as above, a matrix M' as in (13) can be computed with*

$$\deg(M') \leq 3n^2 4^n (\delta_N + 1)^{2n} + \delta_M + \delta_N + \delta_0.$$

Proof. Note that e and f from (7) have degrees bounded by $\delta_M + \delta_N$. Let $U_N \in R^{m\times m}$ the unimodular matrix such that $N^{\mathbf{t}} \cdot U_N = (\mathbf{I}_2\, \mathbf{0}) \in R^{2\times m}$. By Theorem 2.6, U_N can be computed with $\deg(U_N) \leq 3n^2 4^n (\delta_N + 1)^{2n}$. As usual, denote the columns of U_N with $U_N^1, \dots U_N^m$. If we set,

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix} := eU_N^1 + fU_N^2$$

we deduce that (12) is satisfied. By computing explicitly, we get

$$\deg(x_i) \leq 3n^2 4^n (\delta_N + 1)^{2n} + \delta_M + \delta_N.$$

To compute M' from M as in (13), we have to add to the latter a matrix with coefficients then bounded by $3n^2 4^n (\delta_N + 1)^{2n} + \delta_M + \delta_N + \delta_0$. From here, the claim follows straightforwardly, as this bound is larger than δ_M, which bounds the degree of M. □

5.2. Relations among bounds

So far, we have

- δ_M, a bound on the degree of the elements of M;
- δ_N, a bound on the degree of the elements of N;
- δ_0, a bound on the degrees of p and q;
- δ_a, a bound on the degrees of $a_1, \dots, a_m$.

Is there any relation among these bounds? Clearly, from (6) we deduce straightforwardly that

- given δ_a and δ_N, one can set $\delta_0 := \delta_a + \delta_N$;
- given δ_0 and δ_M, one can set $\delta_a := \delta_0 + \delta_M$.

The following relation is less subtle.

Proposition 5.5. *Given δ_0 and δ_a, there exists a matrix M such that one can take $\delta_M := \delta_0^2 + \delta_a$.*

Proof. As we are assuming $\gcd(p, q) = 1$, we get these polynomials are an affine complete intersection in $\mathbb{K}^n$. The result then follows straightforwardly from Corollary 5.2 in Dickenstein et al. (1991). □

The connection between M and N given via Theorem 3.5 gives a bound for δ_N in terms of δ_M and δ_0 but not a very optimal one.

Proposition 5.6. *Given δ_M and δ_0, there exists a matrix N such that one can take $\delta_N = 3n^2 4^n (\max\{\delta_0, \delta_M\} + 1)^{2n}$.*

Proof. A possible matrix N can be taken by using the first columns (except the last row) of a unimodular $U \in R^{(m+1)\times(m+1)}$ such that (15) holds. Thanks to Theorem 2.6, we have that the degree of N is bounded by $3n^2 4^n (\max\{\delta_0, \delta_M\} + 1)^{2n}$, which proves the claim. □

In the zero-dimensional case, one can have a sharper bound for δ_N.

Proposition 5.7. *If the ideal I is zero-dimensional, given δ_0 and δ_a, there exists a matrix N such that one can take $\delta_N = 2\delta_a^2 + \delta_a + \delta_0$.*

Proof. This follows essentially from Theorem 2.5 in Hashemi (2009). □

We conclude this section by giving the proof of the main result announced in the Introduction.

5.3. Proof of Theorem 1.1

The first algorithm essentially consists in computing the matrix U from (15), and extract the submatrix $\widehat{U}$ which —thanks to Theorem 4.1— encodes an R-basis of $\mathrm{Syz}(a_1, \ldots, a_m)$.

A degree bound for $\widehat{U}$ is given in Proposition 5.1 in terms of the degrees of δ_M and δ_0. By using Proposition 5.5, we can replace this bound by $\delta_0^2 + \delta_a$, and then the first part of the claim follows straightforwardly.

For the second part, we will work with the matrix N as in §4.3. The algorithm proposed there computes $\widehat{N}$ which —thanks to Theorem 4.3— encodes also an R-basis of $\mathrm{Syz}(a_1, \ldots, a_m)$, having the degree bounds given in Proposition 5.3. Note that we are not assuming yet that I is zero-dimensional. This would be used to replace δ_N and δ_M with the bounds given in Propositions 5.5 and 5.7 to get (2). □

6. Examples

We present here the computation of two examples. The first one is the running example in Cortadellas Benítez et al. (2020) and has already M being unimodular, while the second does not. To be consistent with the notation of Cortadellas Benítez et al. (2020), we label the variables as s, t. So in both examples we have that $n = 2$.

6.1. Example 4.1 in Cortadellas Benítez et al. (2020)

Here we have $m = 4$, $p = t - s + 2$, $q = s^2 + 1$ and

$$\begin{cases} a_1(s,t) &= 11 - 4s + 3s^2 + 4t \\ a_2(s,t) &= 5 - 4s + 2s^2 + 4t - 2st + t^2 \\ a_3(s,t) &= 1 + 3s^2 - s^3 + s^2 t \\ a_4(s,t) &= 7 - 3s + s^2 + 3t. \end{cases}$$

As it was shown in Cortadellas Benítez et al. (2020), one can take for this case

$$M = \begin{pmatrix} 4 & t-s+2 & s^2 & 3 \\ 3 & 1 & 1 & 1 \end{pmatrix}.$$

In addition, a simple N is the following:

$$N = \begin{pmatrix} -\frac{1}{5} & \frac{3}{5} \\ 0 & 0 \\ 0 & 0 \\ \frac{3}{5} & -\frac{4}{5} \end{pmatrix}. \tag{22}$$

In this case, as the columns 1 and 4 of M are already an invertible matrix in $\mathbb{K}[s,t]$. The same happens with the rows 1 and 4 of N. By pivoting the 2×2 invertible submatrix of M, it is easy to compute a matrix 4×4 unimodular matrix U^* such that

$$M\cdot U^* = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

we get:

$$U^* = \begin{pmatrix} -\frac{1}{5} & -\frac{s}{5}+\frac{t}{5}+\frac{2}{5} & \frac{s^2}{5}+\frac{s}{5}-\frac{t}{5}-\frac{2}{5} & \frac{s}{5}-\frac{t}{5}+\frac{1}{5} \\ 0 & 1 & -1 & -1 \\ 0 & 0 & 1 & 0 \\ \frac{3}{5} & \frac{3s}{5}-\frac{3t}{5}-\frac{6}{5} & -\frac{3s^2}{5}-\frac{3s}{5}+\frac{3t}{5}+\frac{6}{5} & -\frac{3s}{5}+\frac{3t}{5}+\frac{2}{5} \end{pmatrix}.$$

To pass from U^* to $\widehat{U^*}$ we proceed as in (19) and get that

$$\widehat{U^*} = \begin{pmatrix} -\frac{2s^2}{5}+\frac{st}{5}+\frac{9s}{5}-\frac{7t}{5}-3 & \frac{s^2}{5}+\frac{s}{5}-\frac{t}{5}-\frac{2}{5} & \frac{s}{5}-\frac{t}{5}+\frac{1}{5} \\ s-t-2 & -1 & -1 \\ 0 & 1 & 0 \\ \frac{6s^2}{5}-\frac{6st}{5}-\frac{12s}{5}+\frac{3t^2}{5}+\frac{12t}{5}+3 & -\frac{3s^2}{5}-\frac{3s}{5}+\frac{3t}{5}+\frac{6}{5} & -\frac{3s}{5}+\frac{3t}{5}+\frac{2}{5} \end{pmatrix}.$$

Thanks to Theorem 4.2, the columns of $\widehat{U^*}$ encode a basis of $\mathrm{Syz}(a_1,a_2,a_3,a_4)$. Note that what we obtained with this procedure is quite different than the basis obtained in Cortadellas Benítez et al. (2020). For instance, the degree of this basis is 2, which is lower than the one obtained in that paper (equal to 5).

Now we work with N. From (22) it is easy to extend N to a 4×4 unimodular matrix, we chose

$$N^* = \begin{pmatrix} -\frac{1}{5} & \frac{3}{5} & 0 & 0 \\ 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{3}{5} & -\frac{4}{5} & 0 & 0 \end{pmatrix}.$$

To produce the matrix N^{**} of the algorithm, we have to modify the columns 3 and 4 of N^* by using M. We obtain

$$N^{**} = \begin{pmatrix} -\frac{1}{5} & \frac{3}{5} & s-t+1 & \frac{s^2}{5}-\frac{3}{5} \\ 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 1 \\ \frac{3}{5} & -\frac{4}{5} & -3s+3t+2 & \frac{4}{5}-\frac{3s^2}{5} \end{pmatrix}.$$

Finally, to obtain $\widehat{N}$ we must replace the columns 1 and 2 of N^{**} with the first column multiplied by $-q$ plus the second column multiply by p:

$$\widehat{N} = \begin{pmatrix} \frac{s^2}{5}-\frac{3s}{5}+\frac{3t}{5}+\frac{7}{5} & s-t+1 & \frac{s^2}{5}-\frac{3}{5} \\ 0 & -5 & 0 \\ 0 & 0 & 1 \\ -\frac{3s^2}{5}+\frac{4s}{5}-\frac{4t}{5}-\frac{11}{5} & -3s+3t+2 & \frac{4}{5}-\frac{3s^2}{5} \end{pmatrix}.$$

By Theorem 4.3, the columns of $\widehat{N}$ encode another R-basis of $\mathrm{Syz}(a_1,a_2,a_3,a_4)$. Note that the bases obtained via $\widehat{N}$ and $\widehat{U^*}$ are essentially different. For instance, the first column of $\widehat{N}$ is a relation that only involves a_1 and a_4, but nothing of this nature can be found from the columns of $\widehat{U^*}$. This is because the relation $M\cdot N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ does not hold.

6.2. Another example

Set now $m = 4$ again, and $p = t + 2s + 1$, $q = -2t - s$ which are not under the conditions of the Shape Lemma as all the results in Cortadellas Benítez et al. (2020) are. Consider the following sequence of polynomials:

$$\begin{cases} a_1 &= s + 3s^2 + t + 4st - t^2 \\ a_2 &= -s^2 + t + t^2 \\ a_3 &= s + 2s^2 - 2t^2 \\ a_4 &= 1 + s - t. \end{cases}$$

In this case, we can take

$$M = \begin{pmatrix} s+t & t & s & 1 \\ -s+t & s & t & 1 \end{pmatrix},$$

and note that M is not unimodular (setting $s = t = 0$ makes the rank of M drops). In contrast, we have that

$$\tilde{M} = \begin{pmatrix} s+t & t & s & 1 & s+2t \\ -s+t & s & t & 1 & t+2s+1 \end{pmatrix}$$

is unimodular, and by applying Quillen-Suslin to this matrix we obtain U such that

$$\tilde{M} \cdot U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}.$$

In our case, we get

$$U = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 2 & -2 & 2t-2s & -4s & 2s-2t+1 \\ 1 & -1 & -s+t+1 & -2s & s-t \\ 1 & 0 & -s & -s-t & -t \\ -1 & 1 & s-t & 2s & t-s \end{pmatrix},$$

and hence

$$\widehat{U} = \begin{pmatrix} 0 & 1 & 0 \\ 2t-2s & -4s & 2s-2t+1 \\ -s+t+1 & -2s & s-t \\ -s & -s-t & -t \end{pmatrix}$$

is a basis of $\mathrm{Syz}(a_1, a_2, a_3, a_4)$. Note that the first columns of U (except the last row) encode the matrix N, i.e. we can take this matrix as

$$N = \begin{pmatrix} 0 & 0 \\ 2 & -2 \\ 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

From here, we can extend it easily to a unimodular

$$N^* = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & -2 & 0 & 1 \\ 1 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix},$$

and then we get

$$N^{**} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 2 & -2 & -4s & 2s-2t+1 \\ 1 & -1 & -2s & s-t \\ 1 & 0 & -s-t & -t \end{pmatrix}.$$

To conclude, we need to replace the first two columns by a combination of them, to get

$$\widehat{N} = \begin{pmatrix} 0 & 1 & 0 \\ -2s+2t-2 & -4s & 2s-2t+1 \\ -s+t-1 & -2s & s-t \\ s+2t & -s-t & -t \end{pmatrix}$$

which encodes another basis of $\mathrm{Syz}(a_1, a_2, a_3, a_4)$. This basis is quite similar than the one we found via U. Indeed, the second and the third columns of both matrices coincide, while the first column of $\widehat{N}$ equals to the first minus 2 times the last column of $\tilde{U}$. This "coincidence" is explained by our choice of N from the first two columns of the matrix U above.

7. Minimal μ-bases of parametric surfaces

From a geometric point of view, the sequence $(a_1, \ldots, a_m)$ of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ can be regarded as the parametrization of a variety $Y \subset \mathbb{K}^m$ being the image of the map $(a_1, \ldots, a_m) : \mathbb{K}^n \to \mathbb{K}^m$. Understanding the role of $\mathrm{Syz}(a_1, \ldots, a_m)$ in the study of geometric properties of Y is an active area of research, and several results and challenges are well identified there, see for instance Cox (2003). In particular, when $n = 2$, this map represents typically a surface in $\mathbb{K}^m$, and bounding the degrees of generators of the syzygy module has been posed as an open problem in Chen et al. (2005) for the case $m = 4$, i.e. surfaces in 3-dimensional space.

A first answer to this problem was posted in Cid-Ruiz (2019), where the author exhibits a general bound of order δ_a^{33} to solve this problem ($n = 2$, $m = 4$). In Cortadellas Benítez et al. (2020) we improved this bound to δ_a^{12} in the case the ideal I has a so-called "shape basis", meaning that one can take p and q in (1) as $x_2 - r$ and s respectively, with $r, s \in \mathbb{K}[x_1]$. Indeed, our main result there (Cortadellas Benítez et al., 2020, Theorem 1.2) is that a basis of $\mathrm{Syz}(a_1, a_2, a_3, a_4)$ in that case can be found with degree bounded by

$$5\delta_0^4(2\delta_a + 1)^4. \tag{23}$$

The approach to solve that problem differs significantly than the one presented here. For instance we only used there the "simplified" Effective Quillen-Suslin Theorem presented in Fitchas and Galligo (1990), which is essentially Theorem 2.2 in the case $r = 1$. We only worked with the matrix which is called M in (6), and took advantage of the fact that one of its rows only depends on the variable x_1 in the shape-basis case. From there, after applying the Effective Quillen-Suslin algorithm to that univariate row ($r = 1$), a tricky manipulation of the remaining row would allow us to perform again the same simplified Effective Quillen-Suslin algorithm to the second row. The basis would come then after some simplifications and substitutions of these calculations.

In the present paper, we only apply once the Effective Quillen-Suslin algorithm described in Caniglia et al. (1993) with $r = 2$ to the modified matrix $\tilde{M}$ instead of M. As a result, we obtain the matrix $\widehat{U}$ which encodes the elements of a basis of $\mathrm{Syz}(a_1, \ldots, a_m)$ (Theorem 4.1). In addition, we also get another algorithm over the matrix N which gives another basis for this module (Theorem 4.3). This approach was not considered in Cortadellas Benítez et al. (2020).

When applied to the case $n = 2$, $m = 4$, and using the fact that thanks to Bézout's Theorem one can take $\delta_0 \leq \delta_a^2$, the first bound in Theorem 1.1 then amounts to a constant times δ_a^{16}, while the second one is of the order of δ_a^8, which is better than the results obtained in Cortadellas Benítez et al. (2020) if one substitutes δ_0 with δ_a^2.

But we can actually improve the bound of δ_a^{16} from Theorem 1.1 if we inspect carefully the structure of a matrix M converting a shape basis into the input sequence $a_1 \ldots a_4$, as it was done in Cortadellas Benítez et al. (2020). Indeed, we have

Proposition 7.1. *If $a_1, a_2, a_3, a_4 \in \mathbb{K}[s,t]$ have degrees bounded by δ_1 and the ideal generated by them has a shape basis as in Cortadellas Benítez et al. (2020) of degree δ_0, a basis of $Syz(a_1, a_2, a_3, a_4)$ can be found with degree bounded by $192(\delta_0\delta_a + 1)^4$.*

Proof. From the proof of Theorem 1.2 in Cortadellas Benítez et al. (2020), we get that the matrix M converting the shape basis into the original sequence has $\delta_M \leq \delta_a\delta_0$. The result now follows by applying Theorem 2.6 to $\tilde{M}$ with $n = r = 2$. □

Remark 7.2. Note that the bound obtained in Proposition 7.1 is of the same order than the one in (23) in terms of δ_0 and δ_a.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Broida, Joel G., Williamson, S. Gill, 1989. A Comprehensive Introduction to Linear Algebra. Addison–Wesley Publishing Company, Advanced Book Program, Redwood City, CA.

Caniglia, Leandro, Cortiñas, Guillermo, Danón, Silvia, Heinz, Joos, Krick, Teresa, Solernó, Pablo, 1993. Algorithmic aspects of Suslin's proof of Serre's conjecture. Comput. Complex. 3, 31–55.

Chen, Falai, Wang, Wenping, 2003. Revisiting the μ-basis of a rational ruled surface. J. Symb. Comput. 36 (5), 699–716.

Chen, Falai, Cox, David, Liu, Yang, 2005. The μ-basis and implicitization of a rational parametric surface. J. Symb. Comput. 39 (6), 689–706.

Cid-Ruiz, Yairon, 2019. Bounding the degrees of a minimal μ-basis for a rational surface parametrization. J. Symb. Comput. 95, 134–150.

Cortadellas Benítez, Teresa, D'Andrea, Carlos, Montoro, Eulàlia, 2020. Bounds for degrees of minimal μ-bases of parametric surfaces. In: Proc. ACM Intern. Symp. on Symbolic and Algebraic Computation, pp. 107–113.

Cox, David, 2003. Curves, surfaces, and syzygies. In: Topics in Algebraic Geometry and Geometric Modeling. In: Contemp. Math., vol. 334. Amer. Math. Soc., Providence, RI, pp. 131–150.

Cox, David A., Sederberg, Thomas W., Chen, Falai, 1998. The moving line ideal basis of planar rational curves. Comput. Aided Geom. Des. 15 (8), 803–827.

Deng, Jiansong, Chen, Falai, Shen, Liyong, 2005. Computing μ-bases of rational curves and surfaces using polynomial matrix factorization. In: ISSAC'05. ACM, New York, pp. 132–139.

Dickenstein, Alicia, Fitchas, Noaï, Giusti, Marc, Sessa, Carmen, 1991. The membership problem for unmixed polynomial ideals is solvable in single exponential time. In: Applied algebra, algebraic algorithms, and error-correcting codes, Toulouse, 1989. Discrete Appl. Math. 33 (1–3), 73–94.

Eisenbud, David, 2005. The Geometry of Syzygies: A Second Course in Commutative Algebra and Algebraic Geometry. Graduate Texts in Mathematics, vol. 229. Springer-Verlag, New York.

Fitchas, Noaï, Galligo, André, 1990. Nullstellensatz effectif et conjecture de Serre (théorème de Quillen-Suslin) pour le calcul formel. Math. Nachr. 149, 231–253.

Guiver, John P., Bose, N.K., 1982. Polynomial matrix primitive factorization over arbitrary coefficient field and related results. IEEE Trans. Circuits Syst. 29 (10), 649–657.

Hashemi, Amir, 2009. Nullstellensätze for zero-dimensional Gröbner bases. Comput. Complex. 18 (1), 155–168.

Hong, Hoon, Hough, Zachary, Kogan, Irina A., 2017. Algorithm for computing μ-bases of univariate polynomials. J. Symb. Comput. 80 (part 3), 844–874.

Jelonek, Zbigniew, 2005. On the effective Nullstellensatz. Invent. Math. 162 (1), 1–17.

Maple 2020.1, 2020. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario.

Shen, Li-Yong, Goldman, Ron, 2017. Algorithms for computing strong μ-bases for rational tensor product surfaces. Comput. Aided Geom. Des. 52/53, 48–62.

Walker, Robert J., 1978. Algebraic Curves, Reprint of the 1950 edition. Springer-Verlag, New York-Heidelberg.

Wolfram Research, Inc., 2018. Mathematica, Version 11. Champaign, IL.

Yao, Shanshan, Feng, Yifei, Jia, Xiaohong, Shen, Li-Yong, 2019. A package to compute implicit equations for rational curves and surfaces. ACM Commun. Comput. Algebra 53 (2), 33–36.

Yao, Shanshan, Jia, Xiaohong, 2019. μ-bases for rational canal surfaces. Comput. Aided Geom. Des. 69, 11–26.