A divide-and-conquer algorithm for computing Gröbner bases of syzygies in finite dimension

Simone Naldi, Vincent Neiger

A Divide-and-conquer Algorithm for Computing Gröbner Bases of Syzygies in Finite Dimension

Simone Naldi
Univ. Limoges, CNRS, XLIM, UMR 7252
F-87000 Limoges, France

Vincent Neiger
Univ. Limoges, CNRS, XLIM, UMR 7252
F-87000 Limoges, France

ABSTRACT

Let $f_1, \ldots, f_m$ be elements in a quotient $\mathcal{R}^n/\mathcal{N}$ which has finite dimension as a $\mathbb{K}$-vector space, where $\mathcal{R} = \mathbb{K}[X_1, \ldots, X_r]$ and $\mathcal{N}$ is an $\mathcal{R}$-submodule of $\mathcal{R}^n$. We address the problem of computing a Gröbner basis of the module of syzygies of $(f_1, \ldots, f_m)$, that is, of vectors $(p_1, \ldots, p_m) \in \mathcal{R}^m$ such that $p_1 f_1 + \cdots + p_m f_m = 0$.

An iterative algorithm for this problem was given by Marinari, Möller, and Mora (1993) using a dual representation of $\mathcal{R}^n/\mathcal{N}$ as the kernel of a collection of linear functionals. Following this viewpoint, we design a divide-and-conquer algorithm, which can be interpreted as a generalization to several variables of Beckermann and Labahn's recursive approach for matrix Padé and rational interpolation problems. To highlight the interest of this method, we focus on the specific case of bivariate Padé approximation and show that it improves upon the best known complexity bounds.

KEYWORDS

Syzygies; Gröbner basis; Padé approximation; divide and conquer

ACM Reference Format:
Simone Naldi and Vincent Neiger. 2020. A Divide-and-conquer Algorithm for Computing Gröbner Bases of Syzygies in Finite Dimension. In *International Symposium on Symbolic and Algebraic Computation (ISSAC '20), July 20–23, 2020, Athens, Greece.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3373207.3404059

1 INTRODUCTION

Context. Hereafter, $\mathcal{R} = \mathbb{K}[X_1, \ldots, X_r]$ is the ring of r-variate polynomials over a field $\mathbb{K}$. Given an $\mathcal{R}$-submodule $\mathcal{N} \subset \mathcal{R}^n$ such that $\mathcal{R}^n/\mathcal{N}$ has finite dimension D as a $\mathbb{K}$-vector space, as well as a matrix $\boldsymbol{F} \in \mathcal{R}^{m \times n}$ with rows $\boldsymbol{f}_1, \ldots, \boldsymbol{f}_m \in \mathcal{R}^n$, this paper studies the computation of a Gröbner basis of the module of syzygies

$$\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}) = \{\boldsymbol{p} = (p_i)_{1 \le i \le m} \in \mathcal{R}^m \mid \boldsymbol{p}\boldsymbol{F} = \textstyle\sum_{1 \le i \le m} p_i \boldsymbol{f}_i \in \mathcal{N}\},$$

where $\boldsymbol{p}$ is seen as a $1 \times m$ row vector. Note that $\mathcal{R}^m/\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ also has finite dimension, at most D, as a $\mathbb{K}$-vector space.

Following a path of work pioneered by Marinari, Möller and Mora [1, 25, 27], we focus on a specific situation where $\mathcal{N}$ is described using duality. That is, $\mathcal{N}$ is known through D linear functionals $\varphi_j : \mathcal{R}^n \to \mathbb{K}$ such that $\mathcal{N} = \cap_{1 \le j \le D} \ker(\varphi_j)$. In this context, it is customary to make an assumption equivalent to the following: $\mathcal{N}_i = \cap_{1 \le j \le i} \ker(\varphi_i)$ is an $\mathcal{R}$-module, for $1 \le i \le D$; see e.g. [25, Algo. 2] [16, Eqn. (4.1)] [30, Eqn. (5)] for such assumptions and related algorithms. Namely, this assumption allows one to design iterative algorithms which compute bases of $\mathrm{Syz}_{\mathcal{N}_i}(\boldsymbol{F})$ iteratively for increasing i, until reaching $i = D$ and obtaining the sought basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$. An efficient such iterative procedure is given in [25], specifically in Algorithm 2 (variant in Section 9 therein); note that it is written for $m = n = 1$ and $\boldsymbol{F} = [1]$, in which case $\mathrm{Syz}_{\mathcal{N}_i}(\boldsymbol{F}) = \mathcal{N}_i$, but directly extends to the case $m \ge 1$ and $\boldsymbol{F} \in \mathcal{R}^{m \times n}$.

Ideal of points and Padé approximation. One particular case of interest is when $\mathcal{N}$ is the vanishing ideal of a given set of points: $n = 1$, and $\mathcal{N}$ is the ideal of all polynomials in $\mathcal{R}$ which vanish at distinct points $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_D \in \mathbb{K}^r$. Here, one takes the linear functionals for evaluation: $\varphi_j : f \in \mathcal{R} \mapsto f(\boldsymbol{\alpha}_j) \in \mathbb{K}$. The question is, given the points, m polynomials as $\boldsymbol{F} \in \mathcal{R}^{m \times 1}$, and a monomial order $\preccurlyeq$, to compute a $\preccurlyeq$-Gröbner basis of the set of vectors $\boldsymbol{p}$ such that $\boldsymbol{p}\boldsymbol{F}$ vanishes at all the points. When $m = 1$ and $\boldsymbol{F} = [1]$, this means computing a $\preccurlyeq$-Gröbner basis of the ideal of the points, as studied in [25, 26].

Another case is that of (multivariate) Padé approximation and its extensions, as studied in [14, 16, 17, 30], as well as in [6] in the context of the computation of multidimensional linear recurrence relations. The basic setting is for $n = 1$, with $\mathcal{N}$ an ideal of the form $\langle X_1^{d_1}, \ldots, X_r^{d_r} \rangle$, and $\boldsymbol{F} = \left[\begin{smallmatrix} f \\ -1 \end{smallmatrix}\right]$ for some given $f \in \mathcal{R}$. Then, elements of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ are vectors $(q, p) \in \mathcal{R}^2$ such that $f = p/q \bmod X_1^{d_1}, \ldots, X_r^{d_r}$. Here, the $D = d_1 \cdots d_r$ linear functionals correspond to the coefficients of multidegree less than $(d_1, \ldots, d_r)$; note that not all orderings of these functionals satisfy the assumption above.

For these two situations, as well as some extensions of them, the fastest known algorithms rely on linear algebra and have a cost bound of $O(mD^2 + rD^3)$ operations in $\mathbb{K}$ [16, 25]; this was recently improved in [28, Thm. 2.13] and [29] to $O(mD^{\omega-1} + rD^{\omega} \log(D))$ where $\omega < 2.38$ is the exponent of matrix multiplication [10, 24].

Based on work in [9, 15], in the specific case of an ideal of points $\mathcal{N}$ and the lexicographic order, Ceria and Mora gave a combinatorial algorithm to compute the $\preccurlyeq_{\mathrm{lex}}$-monomial basis of $\mathcal{R}/\mathcal{N}$, the Cerlienco-Mureddu correspondence, and squarefree separators for the points using $O(rD^2 \log(D))$ operations [8].

The univariate case. This problem has received attention in the case of a single variable ($r = 1$) notably thanks to the numerous applications of matrix rational interpolation and Hermite-Padé approximation, which are the two situations described above. Iterative algorithms were first given for Padé approximation in [18, 34] and then for Hermite-Padé approximation in [2, 4, 33]; the latter can be seen as univariate analogues of [25, Algo. 2] and [16, Algo. 4.7].

A breakthrough divide and conquer approach was designed by Beckermann and Labahn in [3, Algo. SPHPS], allowing one to take

ISSAC '20, July 20–23, 2020, Athens, Greece

advantage of univariate polynomial matrix multiplication while previous iterative algorithms only relied on naive linear algebra operations. This led to a line of work [19, 21, 22, 32, 35] which consistently improved the incorporation of fast linear algebra and fast polynomial multiplication in this divide and conquer framework, culminating in cost bounds for rational interpolation and Hermite-Padé approximation which are close asymptotically to the size of the problem (if $\omega = 2$, these cost bounds are quasi-linear in the size of the input). To the best of our knowledge, no similar divide and conquer technique has been developed in multivariate settings prior to this work.

Contribution. We propose a divide and conquer algorithm for the problem of computing a $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ in the multivariate case. This is based on the iterative algorithm [25, Algo. 2], observing that each step of the iteration can be interpreted as a left multiplication by a matrix which has a specific shape, which we call elementary Gröbner basis (see Section 3). The new algorithm reorganizes these matrix products through a divide and conquer strategy, and thus groups several products by elementary Gröbner bases into a single multivariate polynomial matrix multiplication.

Thus, both the existing iterative and the new divide and conquer approaches compute the same elementary Gröbner bases, but unlike the former, our algorithm does not explicitly compute Gröbner bases for all intermediate syzygy modules $\mathrm{Syz}_{\mathcal{N}_i}(\boldsymbol{F})$. By computing less, we expect to achieve better computational complexity. To illustrate this, we specialize our approach to multivariate matrix Padé approximation and derive complexity bounds for this case; we obtain the next result, which is a particular case of Proposition 5.5.

Theorem 1.1. *For $\mathcal{R} = \mathbb{K}[X, Y]$, let $f_1, \ldots, f_m \in \mathcal{R}$, and let $\preccurlyeq$ be a monomial order on $\mathcal{R}$. Then one can compute a minimal $\preccurlyeq$-Gröbner basis of the module of Hermite-Padé approximants*

$$\{(p_1, \ldots, p_m) \in \mathcal{R}^m \mid p_1 f_1 + \cdots + p_m f_m = 0 \bmod \langle X^d, Y^d \rangle\}$$

using $O\tilde{}(m^\omega d^{\omega+2})$ operations in $\mathbb{K}$, where $O\tilde{}(\cdot)$ means that polylogarithmic factors are omitted.

In this case the vector space dimension is $D = d^2$. Thus, as noted above and to the best of our knowledge, the fastest previously known algorithm for this task has a cost of $O\tilde{}(md^{2(\omega-1)} + d^{2\omega})$ operations in $\mathbb{K}$ and does not exploit fast polynomial multiplication.

Perspectives. The base case of our divide and conquer algorithm concerns the case $\mathcal{N} = \ker(\varphi)$ of a single linear functional, detailed in Section 3; we thus work in a vector space $\mathcal{R}^n/\mathcal{N}$ of dimension 1. A natural perspective is to improve the efficiency of our algorithm thanks to a better exploitation of fast linear algebra by grouping several base cases together; using fast linear algebra to accelerate the base case was a key strategy in obtaining efficient univariate algorithms [19, 22]. In the context of Padé approximation, where one can introduce the variables one after another, one could also try to incorporate known algorithms for the univariate case.

One reason why these improvements are not straightforward to do in the multivariate case is that there is no direct generalization of a property at the core of the correctness of univariate algorithms. This property (see [23, Lem. 2.4]) states that if $\boldsymbol{P}_1$ is a $\preccurlyeq_1$-Gröbner basis of $\mathcal{N}_1 \supset \mathcal{N}$ and $\boldsymbol{P}_2$ is a $\preccurlyeq_2$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{P}_1)$, then $\boldsymbol{P}_2\boldsymbol{P}_1$ is a $\preccurlyeq_1$-Gröbner basis of $\mathcal{N}$, provided that the order $\preccurlyeq_2$ is well chosen (a Schreyer order for $\boldsymbol{P}_1$ and $\preccurlyeq_1$, see Section 2.4). We give a counterexample to such a property in Example 3.6. It remains open to find a similar general property that would help to design algorithms based on matrix multiplication in the multivariate case.

Another difficulty arises in analyzing the complexity of our divide and conquer scheme in contexts where the number of elements in the sought Gröbner basis is not well controlled, such as rational interpolation. Indeed, this number corresponds to the size of the matrices used in the algorithm, and therefore is directly related to the cost of the matrix multiplication. In fact, the worst-case number of elements depends on the monomial order and is often pessimistic compared to what is observed in a generic situation. Thus, future work involves investigating complexity bounds for generic input and for interesting particular cases other than Padé approximation.

2 PRELIMINARIES

2.1 Notation

Here and hereafter, the coordinate vector with 1 at index i is denoted by $\boldsymbol{e}_i$; its dimension is inferred from the context. A monomial in $\mathcal{R}^m$ is an element of the form $v\boldsymbol{e}_i$ for some $1 \le i \le m$ and some monomial v in $\mathcal{R}$; i is called the support of $v\boldsymbol{e}_i$. We denote by $\mathrm{Mon}(\mathcal{R}^m)$ the set of all monomials in $\mathcal{R}^m$. A term is a monomial multiplied by a nonzero constant from $\mathbb{K}$. The elements of $\mathcal{R}^m$ are $\mathbb{K}$-linear combinations of elements of $\mathrm{Mon}(\mathcal{R}^m)$ and are called polynomials.

Elements in $\mathcal{R}$ are written in regular font (e.g. monomials μ and ν and polynomials f and p), while elements in $\mathcal{R}^m$ are boldfaced (e.g. monomials $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ and polynomials $\boldsymbol{f}$ and $\boldsymbol{p}$). Vectors or (ordered) lists of polynomials in $\mathcal{R}^m$ are seen as matrices, written in boldfaced capital letters; precisely, $(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_k) \in (\mathcal{R}^m)^k$ is seen as a matrix $\boldsymbol{P} \in \mathcal{R}^{k \times m}$ whose ith row is $\boldsymbol{p}_i$. In particular, in what follows the default orientation is to see an element of $\mathcal{R}^m$ as a *row* vector in $\mathcal{R}^{1\times m}$.

For the sake of completeness, we recall below in Sections 2.2 to 2.4 some classical definitions from commutative algebra concerning submodules of $\mathcal{R}^m$; we assume familiarity with the corresponding notions concerning ideals of $\mathcal{R}$. For a more detailed introduction the reader may refer to [11–13].

2.2 Monomial orders for modules

A monomial order on $\mathcal{R}^m$ is a total order $\preccurlyeq$ on $\mathrm{Mon}(\mathcal{R}^m)$ such that, for $v \in \mathrm{Mon}(\mathcal{R})$ and $\boldsymbol{\mu}_1, \boldsymbol{\mu}_2 \in \mathrm{Mon}(\mathcal{R}^m)$ with $\boldsymbol{\mu}_1 \preccurlyeq \boldsymbol{\mu}_2$, one has $\boldsymbol{\mu}_1 \preccurlyeq v\boldsymbol{\mu}_1 \preccurlyeq v\boldsymbol{\mu}_2$; hereafter $\boldsymbol{\mu}_1 \prec \boldsymbol{\mu}_2$ means that $\boldsymbol{\mu}_1 \preccurlyeq \boldsymbol{\mu}_2$ and $\boldsymbol{\mu}_1 \neq \boldsymbol{\mu}_2$. For $\boldsymbol{p} \in \mathcal{R}^m$, its $\preccurlyeq$-leading monomial is denoted by $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p})$ and is the largest of its monomials with respect to the order $\preccurlyeq$ (we take the convention $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{0}) = \boldsymbol{0}$ for $\boldsymbol{0} \in \mathcal{R}^m$ the zero element). We extend this notation to collections of polynomials $\mathcal{P} \subset \mathcal{R}^m$ with $\mathrm{lm}_{\preccurlyeq}(\mathcal{P}) = \{\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}) : \boldsymbol{p} \in \mathcal{P}\}$, and to matrices $\boldsymbol{P} \in \mathcal{R}^{k\times m}$ with $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{P})$ the $k \times m$ matrix whose ith row is the $\preccurlyeq$-leading monomial of the ith row of $\boldsymbol{P}$.

Example 2.1. The usual lexicographic comparison is a monomial order on $\mathbb{K}[X, Y]$: $X^a Y^b \preccurlyeq_{\mathrm{lex}} X^{a'} Y^{b'}$ if and only if $a < a'$ or ($a = a'$ and $b < b'$). It can be used to define a monomial order on $\mathbb{K}[X, Y]^2$, called the term-over-position lexicographic order: for

μ, ν in $\mathrm{Mon}(\mathbb{K}[X,Y])$ and i,j in $\{1,2\}$, $\mu \boldsymbol{e}_i \preccurlyeq^{\mathrm{top}}_{\mathrm{lex}} \nu \boldsymbol{e}_j$ if and only if $\mu \preccurlyeq_{\mathrm{lex}} \nu$ or ($\mu = \nu$ and $i < j$).

We refer to [11, Sec. 1.§2 and 5.§2] for other classical monomial orders, such as the degree reverse lexicographical order on $\mathcal{R}$, and the construction of term-over-position and position-over-term orders on $\mathcal{R}^m$ from monomial orders on $\mathcal{R}$.

A monomial order $\preccurlyeq$ on $\mathcal{R}^m$ induces a monomial order $\preccurlyeq_i$ on $\mathcal{R}$ for each $1 \le i \le m$, by restricting to the ith coordinate: for $\nu_1, \nu_2 \in \mathrm{Mon}(\mathcal{R})$, $\nu_1 \preccurlyeq_i \nu_2$ if and only if $\nu_1 \boldsymbol{e}_i \preccurlyeq \nu_2 \boldsymbol{e}_i$. In particular, $\mathrm{lm}_{\preccurlyeq}(q\boldsymbol{p})$ is a multiple of $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p})$ for $q \in \mathcal{R}$ and $\boldsymbol{p} \in \mathcal{R}^m$:

Lemma 2.2. *Let $\bar{\imath}$ be the support of $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p})$. Then $\mathrm{lm}_{\preccurlyeq}(q\boldsymbol{p}) = \mathrm{lm}_{\preccurlyeq_i}(q)\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p})$.*

Proof. Write $q = \sum_\ell \nu_\ell$ and $\boldsymbol{p} = \sum_{i,j} \mu_{ij} \boldsymbol{e}_i$ for terms μ_{ij}, ν_ℓ in $\mathcal{R}$. Then $q\boldsymbol{p} = \sum_{\ell,i,j} \nu_\ell \mu_{ij} \boldsymbol{e}_i$, i.e. the terms of $q\boldsymbol{p}$ are all those of the form $\nu_\ell \mu_{ij} \boldsymbol{e}_i$. Now let $\bar{\ell}$ and $\bar{\jmath}$ be such that $\mathrm{lm}_{\preccurlyeq_i}(q) = \nu_{\bar{\ell}}$ and $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}) = \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}}$. Then $\nu_\ell \prec_{\bar{\imath}} \nu_{\bar{\ell}}$ for all $\ell \neq \bar{\ell}$, which implies that $\nu_\ell \mu_{\bar{\imath}\bar{\jmath}} \prec_{\bar{\imath}} \nu_{\bar{\ell}} \mu_{\bar{\imath}\bar{\jmath}}$ and thus, by definition of $\preccurlyeq_{\bar{\imath}}$, that $\nu_\ell \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}} \prec \nu_{\bar{\ell}} \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}}$. On the other hand, $\mu_{ij} \boldsymbol{e}_i \prec \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}}$ holds for all $(i,j) \neq (\bar{\imath}, \bar{\jmath})$, hence $\nu_\ell \mu_{ij} \boldsymbol{e}_i \prec \nu_\ell \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}}$. Therefore we obtain $\nu_\ell \mu_{ij} \boldsymbol{e}_i \preccurlyeq \nu_{\bar{\ell}} \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}}$ for all (i,j,ℓ), with equality only if $(i,j,\ell) = (\bar{\imath}, \bar{\jmath}, \bar{\ell})$. This proves that $\mathrm{lm}_{\preccurlyeq}(q\boldsymbol{p}) = \nu_{\bar{\ell}} \mu_{\bar{\imath}\bar{\jmath}} \boldsymbol{e}_{\bar{\imath}} = \mathrm{lm}_{\preccurlyeq_i}(q)\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p})$. □

2.3 Gröbner bases

As a consequence of Hilbert's Basis Theorem, any $\mathcal{R}$-submodule of $\mathcal{R}^m$ is finitely generated [13, Prop. 1.4]. For a (possibly infinite) collection of polynomials $\mathcal{P} \subset \mathcal{R}^m$, we denote by $\langle \mathcal{P} \rangle$ the $\mathcal{R}$-submodule of $\mathcal{R}^m$ generated by the elements of $\mathcal{P}$. Similarly, for a matrix $\boldsymbol{P}$ in $\mathcal{R}^{k\times m}$, $\langle \boldsymbol{P} \rangle$ stands for the $\mathcal{R}$-submodule of $\mathcal{R}^m$ generated by its rows, that is, $\langle \boldsymbol{P} \rangle = \{\boldsymbol{q}\boldsymbol{P} \mid \boldsymbol{q} \in \mathcal{R}^k\}$.

For a given submodule $\mathcal{M} \subset \mathcal{R}^m$, the $\preccurlyeq$-leading module of $\mathcal{M}$ is the module $\langle \mathrm{lm}_{\preccurlyeq}(\mathcal{M}) \rangle$ generated by the leading monomials of the elements of $\mathcal{M}$. Then, a matrix $\boldsymbol{P}$ in $\mathcal{R}^{k\times m}$ whose rows are in $\mathcal{M}$ is said to be a $\preccurlyeq$-Gröbner basis of $\mathcal{M}$ if

$$\langle \mathrm{lm}_{\preccurlyeq}(\mathcal{M}) \rangle = \langle \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P}) \rangle.$$

In this case we have $\langle \boldsymbol{P} \rangle = \mathcal{M}$ (see [11, Ch.5, Prop.2.7]), hence we will often omit the reference to the module $\mathcal{M}$ and just say that $\boldsymbol{P}$ is a $\preccurlyeq$-Gröbner basis.

A $\preccurlyeq$-Gröbner basis $\boldsymbol{P}$, whose rows are $(\boldsymbol{p}_1, \ldots, \boldsymbol{p}_k)$, is said to be minimal if $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}_i)$ is not divisible by $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}_j)$, for any $j \neq i$. It is said to be reduced if it is minimal and, for all $1 \le i \le k$, $\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}_i)$ is monic and none of the terms of $\boldsymbol{p}_i$ is divisible by any of $\{\mathrm{lm}_{\preccurlyeq}(\boldsymbol{p}_j) \mid j \neq i\}$. Given a monomial order $\preccurlyeq$ and an $\mathcal{R}$-submodule $\mathcal{M} \subset \mathcal{R}^m$, there is a reduced $\preccurlyeq$-Gröbner basis of $\mathcal{M}$ and it is unique (up to permutation of its elements) [13, Sec. 15.2].

Example 2.3. The syzygy module

$$\mathcal{M} = \{(p_1, p_2) \in \mathbb{K}[X,Y]^2 \mid p_1 - p_2 \in \langle X, Y \rangle\} = \mathrm{Syz}_{\langle X,Y \rangle}([\begin{smallmatrix} 1 \\ -1 \end{smallmatrix}])$$

is generated by $(X\boldsymbol{e}_1, Y\boldsymbol{e}_1, \boldsymbol{e}_1 + \boldsymbol{e}_2)$, that is, by the rows of

$$\boldsymbol{P} = \begin{bmatrix} X & 0 \\ Y & 0 \\ 1 & 1 \end{bmatrix} \in \mathbb{K}[X,Y]^{3\times 2}.$$

Furthermore, $\boldsymbol{P}$ is the reduced $\preccurlyeq^{\mathrm{top}}_{\mathrm{lex}}$-Gröbner basis of $\mathcal{M}$.

2.4 Schreyer orders

In the context of the computation of bases of syzygies it is generally beneficial to use a specific construction of monomial orders, as first highlighted by Schreyer [20, 31] (see also [13, Th. 15.10] and [5]).

In the univariate case, the notion of shifted degree plays the same role as Schreyer orders and is ubiquitous in the computation of bases of modules of syzygies [19, 21, 35]; an equivalent notion of defects was also used earlier for M-Padé and Hermite-Padé approximation algorithms [2, 3]. Specifically, this provides a monomial order on $\mathcal{R}^k$ constructed from a monomial order $\preccurlyeq$ on $\mathcal{R}^m$ and from the leading monomials of a $\preccurlyeq$-Gröbner basis in $\mathcal{R}^m$ of cardinality k.

Definition 2.4. Let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$, and let $\boldsymbol{L} = (\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_k)$ be a list of monomials of $\mathcal{R}^m$. A *Schreyer order for $\preccurlyeq$ and $\boldsymbol{L}$* is any monomial order on $\mathcal{R}^k$, denoted by $\preccurlyeq_{\boldsymbol{L}}$, such that for $\nu_1 \boldsymbol{e}_i, \nu_2 \boldsymbol{e}_j \in \mathrm{Mon}(\mathcal{R}^k)$, if $\nu_1 \boldsymbol{\mu}_i \prec \nu_2 \boldsymbol{\mu}_j$ then $\nu_1 \boldsymbol{e}_i \preccurlyeq_{\boldsymbol{L}} \nu_2 \boldsymbol{e}_j$.

As noted above, this notion is often used with $\boldsymbol{L} = \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P})$ for a list of polynomials $\boldsymbol{P} \in \mathcal{R}^{k\times m}$, which is typically a $\preccurlyeq$-Gröbner basis.

Remark that Definition 2.4 uses a strict inequality, and implies that if $\nu_1 \boldsymbol{e}_i \preccurlyeq_{\boldsymbol{L}} \nu_2 \boldsymbol{e}_j$, then $\nu_1 \boldsymbol{\mu}_i \prec \nu_2 \boldsymbol{\mu}_j$ or $\nu_1 \boldsymbol{\mu}_i = \nu_2 \boldsymbol{\mu}_j$. In particular, for $\nu_1 = \nu_2 = 1$ and assuming $\boldsymbol{\mu}_i \neq \boldsymbol{\mu}_j$ for all $i \neq j$ (for instance, if $\boldsymbol{L} = \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P})$ for a minimal $\preccurlyeq$-Gröbner basis $\boldsymbol{P}$), then $\boldsymbol{e}_i \preccurlyeq_{\boldsymbol{L}} \boldsymbol{e}_j$ if and only if $\boldsymbol{\mu}_i \prec \boldsymbol{\mu}_j$.

Furthermore, for every $\preccurlyeq$ and $\boldsymbol{L}$, a corresponding Schreyer order exists and can be constructed explicitly: for example, $\nu_1 \boldsymbol{e}_i \preccurlyeq_{\boldsymbol{L}} \nu_2 \boldsymbol{e}_j$ if and only if

$$\nu_1 \boldsymbol{\mu}_i \prec \nu_2 \boldsymbol{\mu}_j \text{ or } (\nu_1 \boldsymbol{\mu}_i = \nu_2 \boldsymbol{\mu}_j \text{ and } i < j).$$

This specific Schreyer order is the one used in the algorithms in this paper, where we write

$$\preccurlyeq_{\boldsymbol{L}} \leftarrow \textsc{SchreyerOrder}(\preccurlyeq, \boldsymbol{L})$$

to mean that the algorithm constructs it from $\preccurlyeq$ and $\boldsymbol{L}$.

3 BASE CASE OF THE DIVIDE AND CONQUER SCHEME

In this section we present the base case of our main algorithm. It constructs Gröbner bases for syzygies modulo the kernel of a single linear functional, which we call elementary Gröbner bases and describe in Section 3.1. Further in Section 3.2 we state properties that are useful to prove the correctness of the base case algorithm given in Section 3.3. Precisely, this correctness is written having in mind the design of an algorithm handling several functionals iteratively by repeating this basic procedure and multiplying the elementary bases together.

3.1 Elementary Gröbner basis

If $\mathcal{I} \subset \mathcal{R}$ is an ideal such that $\mathcal{R}/\mathcal{I}$ has dimension 1 as a $\mathbb{K}$-vector space, then $\mathcal{I}$ is maximal: it is of the form $\langle X_1 - \alpha_1, \ldots, X_r - \alpha_r \rangle$ for some point $(\alpha_1, \ldots, \alpha_r) \in \mathbb{K}^r$, which directly yields the reduced Gröbner basis of $\mathcal{I}$, for any monomial order. In this paper, we will make use of a similar property for submodules of $\mathcal{R}^m$; such submodules have Gröbner bases of the form

$$\boldsymbol{E} = \begin{bmatrix} \boldsymbol{I}_{\pi-1} & \boldsymbol{\lambda}_1 & \\ & \boldsymbol{X} - \boldsymbol{\alpha} & \\ & \boldsymbol{\lambda}_2 & \boldsymbol{I}_{m-\pi} \end{bmatrix} \in \mathcal{R}^{(m+r-1)\times m}, \tag{1}$$

for the vector of variables $\boldsymbol{X} = [X_1 \ \cdots \ X_r]^\mathsf{T}$ and vectors of values $\boldsymbol{\alpha} = [\alpha_1 \ \cdots \ \alpha_r]^\mathsf{T} \in \mathbb{K}^{r\times 1}$, $\boldsymbol{\lambda}_1 = [\lambda_1 \ \cdots \ \lambda_{\pi-1}]^\mathsf{T} \in \mathbb{K}^{(\pi-1)\times 1}$, and $\boldsymbol{\lambda}_2 = [\lambda_{\pi+1} \ \cdots \ \lambda_m]^\mathsf{T} \in \mathbb{K}^{(m-\pi)\times 1}$. In what follows, such matrices are called elementary Gröbner bases.

Theorem 3.1. *Let $\mathcal{M}$ be an $\mathcal{R}$-submodule of $\mathcal{R}^m$ such that $\mathcal{R}^m/\mathcal{M}$ has dimension 1 as a $\mathbb{K}$-vector space, then for any monomial order $\preccurlyeq$ on $\mathcal{R}^m$, the reduced $\preccurlyeq$-Gröbner basis $\boldsymbol{E}$ of $\mathcal{M}$ is as in Eq. (1) with $\lambda_i = 0$ if $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ for all $i \neq \pi$. Conversely, any matrix $\boldsymbol{E}$ as in Eq. (1) defines a submodule $\mathcal{M} = \langle \boldsymbol{E} \rangle$ such that $\mathcal{R}^m/\mathcal{M}$ has dimension 1 as a $\mathbb{K}$-vector space, and $\boldsymbol{E}$ is a reduced $\preccurlyeq$-Gröbner basis for any monomial order $\preccurlyeq$ such that $\lambda_i = 0$ if $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ for all $i \neq \pi$.*

Proof. By [13, Thm. 15.3], a basis of $\mathcal{R}^m/\mathcal{M}$ as a $\mathbb{K}$-vector space is given by the monomials not in $\mathrm{lm}_\preccurlyeq(\mathcal{M})$; since the dimension of $\mathcal{R}^m/\mathcal{M}$ as a $\mathbb{K}$-vector space is 1, there exists a unique monomial which is not in $\mathrm{lm}_\preccurlyeq(\mathcal{M})$. Thus there is a unique $\pi \in \{1, \ldots, m\}$ such that

$$\mathrm{lm}_\preccurlyeq(\boldsymbol{E}) = (\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{\pi-1}, X_1\boldsymbol{e}_\pi, \ldots, X_r\boldsymbol{e}_\pi, \boldsymbol{e}_{\pi+1}, \ldots, \boldsymbol{e}_m). \quad (2)$$

By definition of reduced Gröbner bases, the jth polynomial in $\boldsymbol{E}$ is the sum of the jth element of $\mathrm{lm}_\preccurlyeq(\boldsymbol{E})$ and a constant multiple of $\boldsymbol{e}_\pi$; hence $\boldsymbol{E}$ has the form in Eq. (1). In addition, for $i \neq \pi$, the equality $\mathrm{lm}_\preccurlyeq(\boldsymbol{e}_i + \lambda_i\boldsymbol{e}_\pi) = \boldsymbol{e}_i$ implies that $\lambda_i = 0$ whenever $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$.

For the converse, let $\preccurlyeq$ be such that $\lambda_i = 0$ if $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ for all $i \neq \pi$ (such an order exists since there are orders for which $\boldsymbol{e}_\pi$ is the smallest coordinate vector). Then $\mathrm{lm}_\preccurlyeq(\boldsymbol{E})$ is as in Eq. (2); in particular, the monomials in $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{E}) \rangle$ are precisely $\mathrm{Mon}(\mathcal{R}^m) \setminus \{\boldsymbol{e}_\pi\}$. It follows that either $\boldsymbol{e}_\pi \in \mathrm{lm}_\preccurlyeq(\mathcal{M})$ and $\langle \mathrm{lm}_\preccurlyeq(\mathcal{M}) \rangle = \mathcal{R}^m$, or $\boldsymbol{e}_\pi \notin \mathrm{lm}_\preccurlyeq(\mathcal{M})$ and $\langle \mathrm{lm}_\preccurlyeq(\mathcal{M}) \rangle = \langle \mathrm{lm}_\preccurlyeq(\boldsymbol{E}) \rangle$. In the second case $\boldsymbol{E}$ is a reduced $\preccurlyeq$-Gröbner-basis and $\mathcal{R}^m/\mathcal{M}$ has dimension 1 by [13, Thm. 15.3]. To conclude the proof, we show that $\boldsymbol{e}_\pi \in \mathrm{lm}_\preccurlyeq(\mathcal{M})$ cannot occur; by contradiction, suppose there exists $\boldsymbol{q} \in \mathcal{M}$ such that $\mathrm{lm}_\preccurlyeq(\boldsymbol{q}) = \boldsymbol{e}_\pi$. Since the rows of $\boldsymbol{E}$ generate $\mathcal{M}$, we can write

$$\begin{aligned}\boldsymbol{q} &= (q_1, \ldots, q_{\pi-1}, p_1, \ldots, p_r, q_{\pi+1}, \ldots, q_m)\,\boldsymbol{E} \\ &= \left(q_1, \ldots, q_{\pi-1}, \sum_{i\neq\pi} q_i\lambda_i + \sum_{j=1}^{r}(X_j - \alpha_j)p_j, q_{\pi+1}, \ldots, q_m\right).\end{aligned}$$

For $i \neq \pi$ such that $\boldsymbol{e}_\pi \prec \boldsymbol{e}_i$, any nonzero term of $q_i\boldsymbol{e}_i$ would appear in $\boldsymbol{q}$ and be greater than $\boldsymbol{e}_\pi$, hence $q_i = 0$. Moreover, for $i \neq \pi$ such that $\boldsymbol{e}_i \prec \boldsymbol{e}_\pi$ we have $\lambda_i = 0$. Thus, considering the πth component of $\boldsymbol{q}$ yields the equality

$$1 = \sum_{i\neq\pi} q_i\lambda_i + \sum_{j=1}^{r}(X_j - \alpha_j)p_j = \sum_{j=1}^{r}(X_j - \alpha_j)p_j$$

which is a contradiction since $1 \notin \langle X_1 - \alpha_1, \ldots, X_r - \alpha_r \rangle$. □

Remark that in the module case ($m \geq 2$) the reduced $\preccurlyeq$-Gröbner basis depends on the order $\preccurlyeq$, more precisely on how the $\boldsymbol{e}_i$'s are ordered by $\preccurlyeq$. For instance, the matrix in Example 2.3 is a reduced $\preccurlyeq$-Gröbner basis for every order such that $\boldsymbol{e}_1 \preccurlyeq \boldsymbol{e}_2$, whereas for orders such that $\boldsymbol{e}_2 \preccurlyeq \boldsymbol{e}_1$ the reduced $\preccurlyeq$-Gröbner basis of the same module is

$$\boldsymbol{E} = \begin{bmatrix} 1 & 1 \\ 0 & X \\ 0 & Y \end{bmatrix} \in \mathbb{K}[X, Y]^{3\times 2}.$$

3.2 Multiplying by elementary Gröbner bases

Let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$ and let $\boldsymbol{P} = (\boldsymbol{p}_1, \ldots, \boldsymbol{p}_k) \in \mathcal{R}^{k\times m}$ be a $\preccurlyeq$-Gröbner basis. In this section, we show conditions on an elementary Gröbner basis $\boldsymbol{E}$ to ensure that $\boldsymbol{EP}$ is a $\preccurlyeq$-Gröbner basis.

We write $\boldsymbol{L} = (\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_k)$ for $\mathrm{lm}_\preccurlyeq(\boldsymbol{P})$, that is, $\boldsymbol{\mu}_i = \mathrm{lm}_\preccurlyeq(\boldsymbol{p}_i)$ for $1 \leq i \leq k$. Let $\preccurlyeq_{\boldsymbol{L}}$ be a Schreyer order for $\preccurlyeq$ and $\boldsymbol{P}$, and consider a reduced $\preccurlyeq_{\boldsymbol{L}}$-Gröbner basis $\boldsymbol{E} \in \mathcal{R}^{(k+r-1)\times k}$ which has the form in Eq. (1); thus

$$\begin{aligned}\boldsymbol{EP} = (&\boldsymbol{p}_1 + \lambda_1\boldsymbol{p}_\pi, \ldots, \boldsymbol{p}_{\pi-1} + \lambda_{\pi-1}\boldsymbol{p}_\pi, \\ &(X_1 - \alpha_1)\boldsymbol{p}_\pi, \ldots, (X_r - \alpha_r)\boldsymbol{p}_\pi, \\ &\lambda_{\pi+1}\boldsymbol{p}_\pi + \boldsymbol{p}_{\pi+1}, \ldots, \lambda_k\boldsymbol{p}_\pi + \boldsymbol{p}_k)\end{aligned}$$

which is in $\mathcal{R}^{(k+r-1)\times m}$. We will show that, under suitable assumptions, $\boldsymbol{EP}$ is a $\preccurlyeq$-Gröbner basis; the next lemmas use the above notation. We start by describing the leading terms of $\boldsymbol{EP}$.

Lemma 3.2. *If $\boldsymbol{\mu}_i \neq \boldsymbol{\mu}_\pi$ for all $i \neq \pi$, then*

$$\begin{aligned}\mathrm{lm}_\preccurlyeq(\boldsymbol{EP}) &= \mathrm{lm}_{\preccurlyeq_{\boldsymbol{L}}}(\boldsymbol{E})\,\boldsymbol{L} \\ &= (\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{\pi-1}, X_1\boldsymbol{\mu}_\pi, \ldots, X_r\boldsymbol{\mu}_\pi, \boldsymbol{\mu}_{\pi+1}, \ldots, \boldsymbol{\mu}_k).\end{aligned}$$

Proof. First, $\mathrm{lm}_\preccurlyeq((X_j - \alpha_j)\boldsymbol{p}_\pi) = X_j\boldsymbol{\mu}_\pi$ for $1 \leq j \leq r$. Next we claim that $\mathrm{lm}_\preccurlyeq(\boldsymbol{p}_i + \lambda_i\boldsymbol{p}_\pi) = \boldsymbol{\mu}_i$ for all $i \neq \pi$. If $\lambda_i = 0$, the identity is obvious. If $\lambda_i \neq 0$, then $\boldsymbol{e}_\pi \preccurlyeq_{\boldsymbol{L}} \boldsymbol{e}_i$ (see Section 3.1), and from the definition of a Schreyer order and the assumption $\boldsymbol{\mu}_\pi \neq \boldsymbol{\mu}_i$, we deduce $\boldsymbol{\mu}_\pi \prec \boldsymbol{\mu}_i$ and hence $\mathrm{lm}_\preccurlyeq(\boldsymbol{p}_i + \lambda_i\boldsymbol{p}_\pi) = \boldsymbol{\mu}_i$. □

Next, we characterize the fact that $\boldsymbol{EP}$ generates a submodule which differs from the one generated by $\boldsymbol{P}$.

Lemma 3.3. *If $\boldsymbol{\mu}_i \neq \boldsymbol{\mu}_\pi$ for all $i \neq \pi$, then*

$$\langle \boldsymbol{EP} \rangle \neq \langle \boldsymbol{P} \rangle \ \Leftrightarrow\ \boldsymbol{p}_\pi \notin \langle \boldsymbol{EP} \rangle \ \Leftrightarrow\ \boldsymbol{\mu}_\pi \notin \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle.$$

Proof. First, remark that $\langle \boldsymbol{EP} \rangle = \langle \boldsymbol{P} \rangle \Rightarrow \boldsymbol{p}_\pi \in \langle \boldsymbol{EP} \rangle \Rightarrow \boldsymbol{\mu}_\pi \in \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$ is obvious; thus, to conclude the proof it remains to show that $\langle \boldsymbol{EP} \rangle = \langle \boldsymbol{P} \rangle \Leftarrow \boldsymbol{\mu}_\pi \in \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$. Suppose that $\boldsymbol{\mu}_\pi \in \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$. Then, since $\boldsymbol{\mu}_i \in \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$ for all $i \neq \pi$ by Lemma 3.2, we have $\mathrm{lm}_\preccurlyeq(\boldsymbol{P}) \subset \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$, hence $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{P}) \rangle \subset \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$. Furthermore, recall that $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{P}) \rangle = \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{P} \rangle) \rangle$ since $\boldsymbol{P}$ is a $\preccurlyeq$-Gröbner basis, and that $\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle \subset \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{P} \rangle) \rangle$ since $\langle \boldsymbol{EP} \rangle \subset \langle \boldsymbol{P} \rangle$: we obtain $\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{P} \rangle) \rangle = \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$. Then, [13, Lemma 15.5] shows that $\langle \boldsymbol{EP} \rangle = \langle \boldsymbol{P} \rangle$. □

For example, if $\boldsymbol{P}$ is a *minimal* $\preccurlyeq$-Gröbner basis, then the assumption in the previous lemma is satisfied. Example 3.6 below exhibits a case where $\boldsymbol{P}$ is a minimal $\preccurlyeq$-Gröbner basis and $\boldsymbol{p}_\pi$ does belong to $\langle \boldsymbol{EP} \rangle$. In that case, $\langle \boldsymbol{EP} \rangle = \langle \boldsymbol{P} \rangle$ and $\boldsymbol{EP}$ is not a Gröbner basis since $\boldsymbol{\mu}_\pi$ is in $\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$ but not in $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{EP}) \rangle$.

Lemma 3.4. *If $\boldsymbol{\mu}_i \neq \boldsymbol{\mu}_\pi$ for all $i \neq \pi$ and $\langle \boldsymbol{EP} \rangle \neq \langle \boldsymbol{P} \rangle$, then $\boldsymbol{EP}$ is a $\preccurlyeq$-Gröbner basis.*

Proof. Suppose by contradiction that $\boldsymbol{EP}$ is not a $\preccurlyeq$-Gröbner basis. Then there exists a nonzero $\boldsymbol{h} \in \langle \boldsymbol{EP} \rangle$ such that $\mathrm{lm}_\preccurlyeq(\boldsymbol{h}) \notin \langle \mathrm{lm}_\preccurlyeq(\boldsymbol{EP}) \rangle$, that is, by Lemma 3.2, $\mathrm{lm}_\preccurlyeq(\boldsymbol{h})$ is not divisible by any of the elements $\boldsymbol{\mu}_i$ for $i \neq \pi$ and $X_j\boldsymbol{\mu}_\pi$ for $1 \leq j \leq r$. On the other hand, $\mathrm{lm}_\preccurlyeq(\boldsymbol{h})$ is in $\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$ and therefore in $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{P}) \rangle$, hence $\mathrm{lm}_\preccurlyeq(\boldsymbol{h})$ is divisible by at least one $\boldsymbol{\mu}_i$, $1 \leq i \leq k$. These divisibility constraints lead to $\mathrm{lm}_\preccurlyeq(\boldsymbol{h}) = \boldsymbol{\mu}_\pi$, which implies $\boldsymbol{\mu}_\pi \in \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP} \rangle) \rangle$. From Lemma 3.3 one deduces $\langle \boldsymbol{EP} \rangle = \langle \boldsymbol{P} \rangle$, which is absurd. □

Corollary 3.5. *Assume that $\langle \boldsymbol{EP}\rangle \neq \langle \boldsymbol{P}\rangle$ and that $\boldsymbol{P}$ is a minimal $\preccurlyeq$-Gröbner basis. Let $j_1 < \cdots < j_\ell$ be the indices $j \in \{1,\dots,r\}$ such that $X_j\boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi\rangle$. Then, the submatrix*

$$\boldsymbol{Q} = \begin{bmatrix} \boldsymbol{I}_{\pi-1} & \boldsymbol{\lambda}_1 & \\ & X_{j_1} - \alpha_{j_1} & \\ & \vdots & \\ & X_{j_\ell} - \alpha_{j_\ell} & \\ & \boldsymbol{\lambda}_2 & \boldsymbol{I}_{m-\pi} \end{bmatrix} \in \mathcal{R}^{(k+\ell-1)\times k} \tag{3}$$

of $\boldsymbol{E}$ is such that $\boldsymbol{QP}$ is a minimal $\preccurlyeq$-Gröbner basis of $\langle \boldsymbol{EP}\rangle$.

Proof. Since $\boldsymbol{P}$ is minimal, $\boldsymbol{\mu}_i \neq \boldsymbol{\mu}_\pi$ for all $i \neq \pi$; then Lemma 3.4 ensures that $\boldsymbol{EP}$ is a $\preccurlyeq$-Gröbner basis and Lemma 3.2 gives

$$\mathrm{lm}_\preccurlyeq(\boldsymbol{QP}) = (\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_{\pi-1}, X_{j_1}\boldsymbol{\mu}_\pi,\dots,X_{j_\ell}\boldsymbol{\mu}_\pi,\boldsymbol{\mu}_{\pi+1},\dots,\boldsymbol{\mu}_k).$$

By construction of $j_1,\dots,j_\ell$, one has $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{QP})\rangle = \langle \mathrm{lm}_\preccurlyeq(\boldsymbol{EP})\rangle$, which implies

$$\begin{aligned}\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP}\rangle)\rangle = \langle \mathrm{lm}_\preccurlyeq(\boldsymbol{EP})\rangle &= \langle \mathrm{lm}_\preccurlyeq(\boldsymbol{QP})\rangle \\ &\subset \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{QP}\rangle)\rangle \subset \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP}\rangle)\rangle.\end{aligned}$$

Hence $\langle \mathrm{lm}_\preccurlyeq(\boldsymbol{QP})\rangle = \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{QP}\rangle)\rangle$, and $\boldsymbol{QP}$ is a minimal $\preccurlyeq$-Gröbner basis. We conclude using [13, Lem. 15.5], which shows that $\langle \boldsymbol{QP}\rangle \subset \langle \boldsymbol{EP}\rangle$ and $\langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{QP}\rangle)\rangle = \langle \mathrm{lm}_\preccurlyeq(\langle \boldsymbol{EP}\rangle)\rangle$ imply $\langle \boldsymbol{QP}\rangle = \langle \boldsymbol{EP}\rangle$. □

Example 3.6. Consider the case $\mathcal{R} = \mathbb{K}[X,Y]$ and $m = 1$. Let $\boldsymbol{P} = \left[\begin{smallmatrix} X \\ Y+1 \end{smallmatrix}\right] \in \mathcal{R}^{2\times 1}$, which is the reduced $\preccurlyeq_1$-Gröbner basis of $\langle X, Y+1\rangle$ for any monomial order $\preccurlyeq_1$ on $\mathrm{Mon}(\mathcal{R})$. Let also $\boldsymbol{E} \in \mathcal{R}^{3\times 2}$ whose rows are $(X\boldsymbol{e}_1, Y\boldsymbol{e}_1, \boldsymbol{e}_2)$; according to Theorem 3.1, $\boldsymbol{E}$ is a reduced $\preccurlyeq_2$-Gröbner basis for any monomial order $\preccurlyeq_2$ on $\mathrm{Mon}(\mathcal{R}^2)$. Now, the product $\boldsymbol{EP} \in \mathcal{R}^{3\times 1}$ has entries X^2, XY, and $Y+1$. Thus, $\langle \mathrm{lm}_{\preccurlyeq_3}(\boldsymbol{EP})\rangle = \langle X^2, XY, Y\rangle = \langle X^2, Y\rangle$ for any monomial order $\preccurlyeq_3$ on $\mathrm{Mon}(\mathcal{R})$. On the other hand, $\langle \boldsymbol{EP}\rangle$ contains $X = X(Y+1) - XY$, hence $\langle \mathrm{lm}_{\preccurlyeq_3}(\boldsymbol{EP})\rangle \neq \langle \mathrm{lm}_{\preccurlyeq_3}(\langle \boldsymbol{EP}\rangle)\rangle$, which means that $\boldsymbol{EP}$ is not a $\preccurlyeq_3$-Gröbner basis.

3.3 Algorithm

We now describe Algorithm Syzygy_BaseCase, which will serve as the base case of the divide and conquer scheme.

Theorem 3.7. *Let $\mathcal{N} \subset \mathcal{R}^n$ be an $\mathcal{R}$-submodule, let $\boldsymbol{F} \in \mathcal{R}^{m\times n}$, and let $\boldsymbol{P} \in \mathcal{R}^{k\times m}$ be a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ for some monomial order $\preccurlyeq$ on $\mathcal{R}^m$. Assume that the input of Algorithm 1 is such that $\ker(\varphi) \cap \mathcal{N}$ is an $\mathcal{R}$-module, $\boldsymbol{G} = \boldsymbol{PF}$, and $\mathrm{lm}_\preccurlyeq(\boldsymbol{P}) = (\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_k)$. Then Algorithm 1 returns $(\boldsymbol{Q},\boldsymbol{L})$ such that $\boldsymbol{QP}$ is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$ and $\boldsymbol{L} = \mathrm{lm}_\preccurlyeq(\boldsymbol{QP})$.*

Proof. If $(\varphi(\boldsymbol{g}_1),\dots,\varphi(\boldsymbol{g}_k)) = (0,\dots,0)$, then Algorithm 1 stops at Line 2 and returns $\boldsymbol{Q} = \boldsymbol{I}_k$ and $\boldsymbol{K}$. Thus $\boldsymbol{QP} = \boldsymbol{P}$, hence by assumption $\boldsymbol{L} = \boldsymbol{K} = \mathrm{lm}_\preccurlyeq(\boldsymbol{P}) = \mathrm{lm}_\preccurlyeq(\boldsymbol{QP})$, and $\boldsymbol{QP}$ is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$; besides, the identity $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}) = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$ is easily deduced from $(\varphi(\boldsymbol{g}_1),\dots,\varphi(\boldsymbol{g}_k)) = (0,\dots,0)$.

In the rest of the proof, assume $(\varphi(\boldsymbol{g}_1),\dots,\varphi(\boldsymbol{g}_k)) \neq (0,\dots,0)$. Define $\boldsymbol{E} \in \mathcal{R}^{(k+r-1)\times k}$ as in Eq. (1) with π and λ_i as in Algorithm 1 and $\alpha_j = \varphi(X_j\boldsymbol{g}_\pi)/v_\pi$ for $1 \le j \le r$; in particular, $\boldsymbol{Q}$ computed at Line 8 is formed by a subset of the rows of $\boldsymbol{E}$.

First, $\boldsymbol{E}$ is a $\preccurlyeq_{\boldsymbol{K}}$-Gröbner basis according to Theorem 3.1, since by definition of π and λ_i one gets the implications $\boldsymbol{e}_i \preccurlyeq_{\boldsymbol{K}} \boldsymbol{e}_\pi \Rightarrow v_i = 0 \Rightarrow \lambda_i = 0$, for $i \neq \pi$.

Algorithm 1 Syzygy_BaseCase$(\varphi, \boldsymbol{G}, \preccurlyeq, \boldsymbol{L})$

Input:
- a linear functional $\varphi : \mathcal{R}^n \to \mathbb{K}$,
- a matrix $\boldsymbol{G}$ in $\mathcal{R}^{k\times n}$ with rows $\boldsymbol{g}_1,\dots,\boldsymbol{g}_k \in \mathcal{R}^n$,
- a monomial order $\preccurlyeq$ on $\mathcal{R}^m$,
- a list $\boldsymbol{K} = (\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_k)$ of elements of $\mathrm{Mon}(\mathcal{R}^m)$.

Output:
- a matrix $\boldsymbol{Q}$ in $\mathcal{R}^{(k+\ell-1)\times k}$ for some $\ell \in \{0,\dots,r\}$,
- a list $\boldsymbol{L}$ of $k+\ell-1$ elements of $\mathrm{Mon}(\mathcal{R}^k)$.

1: $(v_1,\dots,v_k) \leftarrow (\varphi(\boldsymbol{g}_1),\dots,\varphi(\boldsymbol{g}_k)) \in \mathbb{K}^k$
2: **if** $(v_1,\dots,v_k) = (0,\dots,0)$ **then return** $(\boldsymbol{I}_k, \boldsymbol{K})$
3: $\preccurlyeq_{\boldsymbol{K}} \leftarrow$ SchreyerOrder$(\preccurlyeq, \boldsymbol{K})$
4: $\pi \leftarrow \arg\min_{\preccurlyeq_{\boldsymbol{K}}} \{\boldsymbol{e}_i \mid 1 \le i \le k, v_i \neq 0\}$ ▷ *the index i such that $v_i \neq 0$ which minimizes $\boldsymbol{e}_i$ with respect to $\preccurlyeq_{\boldsymbol{K}}$*
5: $\{j_1 < \cdots < j_\ell\} \leftarrow \{j \in \{1,\dots,r\} \mid X_j\boldsymbol{\mu}_\pi \notin \langle \boldsymbol{\mu}_i, i \neq \pi\rangle\}$
6: $\alpha_{j_s} \leftarrow \varphi(X_{j_s}\boldsymbol{g}_\pi)/v_\pi$ for $1 \le s \le \ell$
7: $\lambda_i \leftarrow -v_i/v_\pi$ for $1 \le i < \pi$ and $\pi < i \le k$
8: $\boldsymbol{Q} \leftarrow$ matrix in $\mathcal{R}^{(k+\ell-1)\times k}$ as in Eq. (3)
9: $\boldsymbol{L} \leftarrow (\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_{\pi-1}, X_{j_1}\boldsymbol{\mu}_\pi,\dots,X_{j_\ell}\boldsymbol{\mu}_\pi,\boldsymbol{\mu}_{\pi+1},\dots,\boldsymbol{\mu}_k)$
10: **return** $(\boldsymbol{Q},\boldsymbol{L})$

Next, we claim that $\langle \boldsymbol{E}\rangle = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G})$. Indeed, the rows of $\boldsymbol{PF}$ are in $\mathcal{N}$, and thus so are those of $\boldsymbol{EG} = \boldsymbol{EPF}$. Moreover, by choice of π and λ_i the rows of $\boldsymbol{EG}$ are in $\ker(\varphi)$, since for $i \neq \pi$ one has $\varphi((\boldsymbol{p}_i + \lambda_i\boldsymbol{p}_\pi)\boldsymbol{F}) = \varphi(\boldsymbol{g}_i + \lambda_i\boldsymbol{g}_\pi) = v_i + \lambda_i v_\pi = 0$ and for $1 \le j \le r$ one has $\varphi((X_j - \alpha_j)\boldsymbol{p}_\pi\boldsymbol{F}) = \varphi((X_j - \alpha_j)\boldsymbol{g}_\pi) = \varphi(X_j\boldsymbol{g}_\pi) - \alpha_j v_\pi = 0$. Therefore the rows of $\boldsymbol{EG}$ are in $\ker(\varphi) \cap \mathcal{N}$, that is, $\langle \boldsymbol{E}\rangle \subset \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G})$. To prove the reverse inclusion, recall from Theorem 3.1 that $\langle \boldsymbol{E}\rangle$ has codimension 1 in $\mathcal{R}^k$ and hence $\mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G})$ is either $\langle \boldsymbol{E}\rangle$ or $\mathcal{R}^k$. Since

$$0 \neq v_\pi = \varphi(\boldsymbol{g}_\pi) = \varphi(\boldsymbol{p}_\pi\boldsymbol{F}) = \varphi(\boldsymbol{e}_\pi\boldsymbol{PF}) = \varphi(\boldsymbol{e}_\pi\boldsymbol{G})$$

one has that $\boldsymbol{e}_\pi \notin \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G})$, hence $\mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G}) = \langle \boldsymbol{E}\rangle$.

It follows that $\langle \boldsymbol{EP}\rangle = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$. Indeed, the rows of $\boldsymbol{EPF}$ are in $\ker(\varphi)\cap\mathcal{N}$ as noted above, and thus $\langle \boldsymbol{EP}\rangle \subset \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$. Now let $\boldsymbol{p} \in \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$; thus in particular $\boldsymbol{p} \in \mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$, and $\boldsymbol{p} = \boldsymbol{qP}$ for some $\boldsymbol{q} \in \mathcal{R}^k$. Then $\boldsymbol{pF} = \boldsymbol{qPF} = \boldsymbol{qG} \in \ker(\varphi)\cap\mathcal{N}$, hence $\boldsymbol{q} \in \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{G}) = \langle \boldsymbol{E}\rangle$, and therefore $\boldsymbol{p} \in \langle \boldsymbol{EP}\rangle$.

Now, $\varphi(\boldsymbol{p}_\pi\boldsymbol{F}) \neq 0$ implies $\boldsymbol{p}_\pi \notin \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F}) = \langle \boldsymbol{EP}\rangle$. Thus Lemma 3.3 ensures $\langle \boldsymbol{EP}\rangle \neq \langle \boldsymbol{P}\rangle$, and finally Corollary 3.5 states that $\boldsymbol{QP}$ is a minimal $\preccurlyeq$-Gröbner basis of $\langle \boldsymbol{EP}\rangle = \mathrm{Syz}_{\ker(\varphi)\cap\mathcal{N}}(\boldsymbol{F})$. Besides Lemma 3.2 yields $\mathrm{lm}_\preccurlyeq(\boldsymbol{QP}) = \mathrm{lm}_{\preccurlyeq_{\boldsymbol{K}}}(\boldsymbol{Q})\boldsymbol{K} = \boldsymbol{L}$. □

4 DIVIDE AND CONQUER ALGORITHM

Repeating the basic procedure described in Section 3.3 iteratively, we obtain an algorithm for syzygy basis computation when $\mathcal{N}$ is an intersection of kernels of linear functionals with a specific property (see Eq. (4)). This algorithm is similar to [25, Algo. 2] and [30, Algo. 3.2], apart from differences in the input description. Here, the input consists of linear functionals $\varphi_1,\dots,\varphi_D : \mathcal{R}^n \to \mathbb{K}$, with the assumption that

$$\mathcal{N}_i = \cap_{1\le j\le i} \ker(\varphi_j) \text{ is an } \mathcal{R}\text{-module for } 1 \le i \le D. \tag{4}$$

Then we consider the $\mathcal{R}$-module $\mathcal{N} = \mathcal{N}_D = \cap_{1\le j\le D}\ker(\varphi_j)$, which is such that $\mathcal{R}^n/\mathcal{N}$ has dimension at most D as a $\mathbb{K}$-vector

space. For F in $\mathcal{R}^{m\times n}$, the following algorithm computes a minimal $\preccurlyeq$-Gröbner basis of the syzygy module $\mathrm{Syz}_{\mathcal{N}}(F)$. Note that we do not specify the representation of F since it may depend on the specific functionals φ_i; typically, one considers F to be known modulo $\mathcal{N}$, via the images of its rows by the functionals φ_i.

Algorithm 2 Syzygy_Iter($\varphi_1, \ldots, \varphi_D, F, \preccurlyeq$)

Input:
- linear functionals $\varphi_1, \ldots, \varphi_D : \mathcal{R}^n \to \mathbb{K}$ such that Eq. (4),
- a matrix F in $\mathcal{R}^{m\times n}$,
- a monomial order $\preccurlyeq$ on $\mathcal{R}^m$.

Output:
- a minimal $\preccurlyeq$-Gröbner basis $P \in \mathcal{R}^{k\times m}$ of $\mathrm{Syz}_{\mathcal{N}}(F)$.

1: $P \leftarrow I_m \in \mathcal{R}^{m\times m}$; $G \leftarrow F$; $L \leftarrow (e_1, \ldots, e_m) = \mathrm{lm}_{\preccurlyeq}(P)$
2: **for** $i = 1, \ldots, D$ **do**
3: $\quad (Q, L) \leftarrow$ Syzygy_BaseCase($\varphi_i, G, \preccurlyeq, L$)
4: $\quad P \leftarrow QP$; $G \leftarrow QG$
5: **return** P

Corollary 4.1. *At the end of the ith iteration of Algorithm 2, P is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}_i}(F)$, and one has $G = PF$ as well as $L = \mathrm{lm}_{\preccurlyeq}(P)$. In particular, Algorithm 2 is correct.*

Proof. Note that at Line 1 of Algorithm 2, $P = I_m$ is the reduced $\preccurlyeq$-Gröbner basis of $\mathcal{R}^m = \mathrm{Syz}_{\mathcal{N}_0}(F)$ with $\mathcal{N}_0 = \mathcal{R}^n$, and both $G = PF = F$ and $L = (e_1, \ldots, e_m) = \mathrm{lm}_{\preccurlyeq}(P)$ hold. We conclude that if $D = 0$, Algorithm 2 is correct.

The rest of the proof is by induction on D. We claim that the properties in the statement are preserved across the D iterations. Precisely, we assume that at the beginning of the ith iteration, P is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}_i}(F)$, $G = PF$, and $L = \mathrm{lm}_{\preccurlyeq}(P)$.

Since $\mathcal{N}_{i+1} = \ker(\varphi_{i+1}) \cap \mathcal{N}_i$ is an $\mathcal{R}$-module, applying Theorem 3.7 shows that (Q, L) computed during the iteration are such that $L = \mathrm{lm}_{\preccurlyeq}(QP)$ and that QP is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}_{i+1}}(F)$. □

This allows us to deduce bounds on the size of a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(F)$.

Lemma 4.2. *Let $P \in \mathcal{R}^{k\times m}$ be the output of Algorithm 2. Then, $m \le k \le m + (r-1)D$, and thus the same holds for any minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(F)$. Furthermore, at the end of the iteration i of Algorithm 2, the basis Q has at most $k + D - i$ elements.*

Proof. Remark that all minimal $\preccurlyeq$-Gröbner bases of the same module have the same number of rows. Before the first iteration, the basis is I_m which has m rows, and each iteration of the for loop adds $\ell - 1$ rows to the basis for some ℓ in $\{0, \ldots, r\}$. Therefore $k \le m + (r-1)D$, and the last claim follows from $\ell - 1 \ge -1$. The lower bound $m \le k$ comes from the fact that $\mathcal{R}^m/\mathrm{Syz}_{\mathcal{N}}(F)$ has finite dimension as a $\mathbb{K}$-vector space. □

This iterative algorithm can be turned into a divide and conquer one (Algorithm 3), by reorganizing how the products are performed. It computes a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(F)$, if one takes as input $G = F$ and $K = (e_1, \ldots, e_m)$.

Algorithm 3 Syzygy_DaC($\varphi_1, \ldots, \varphi_D, G, \preccurlyeq, K$)

Input:
- linear functionals $\varphi_1, \ldots, \varphi_D : \mathcal{R}^n \to \mathbb{K}$,
- a matrix G in $\mathcal{R}^{k\times n}$,
- a monomial order $\preccurlyeq$ on $\mathcal{R}^m$,
- a list $K = (\mu_1, \ldots, \mu_k)$ of elements of $\mathrm{Mon}(\mathcal{R}^m)$.

Output:
- a matrix Q in $\mathcal{R}^{\ell\times m}$ for some $\ell \ge 0$,
- a list L of ℓ elements of $\mathrm{Mon}(\mathcal{R}^m)$.

1: **if** $D = 1$ **then return** Syzygy_BaseCase($\varphi_i, G, \preccurlyeq, K$)
2: $(Q_1, L_1) \leftarrow$ Syzygy_DaC($\varphi_1, \ldots, \varphi_{\lfloor D/2 \rfloor}, G, \preccurlyeq, K$)
3: $(Q_2, L_2) \leftarrow$ Syzygy_DaC($\varphi_{\lfloor D/2 \rfloor + 1}, \ldots, \varphi_D, Q_1 G, \preccurlyeq, L_1$)
4: **return** $(Q_2 Q_1, L_2)$

Theorem 4.3. *Let $\mathcal{N} \subset \mathcal{R}^n$ be an $\mathcal{R}$-submodule, let $F \in \mathcal{R}^{m\times n}$, and let $P \in \mathcal{R}^{k\times m}$ be a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(F)$ for some monomial order $\preccurlyeq$ on $\mathcal{R}^m$. Assume that the input of Algorithm 3 is such that $G = PF$, and $\mathrm{lm}_{\preccurlyeq}(P) = (\mu_1, \ldots, \mu_k)$, and*

$$\mathcal{N}_i \cap \mathcal{N} \text{ is an } \mathcal{R}\text{-module for } 1 \le i \le D, \tag{5}$$

where $\mathcal{N}_i = \cap_{1\le j\le i} \ker(\varphi_j)$. Then Algorithm 3 outputs (Q, L) such that QP is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}_D \cap \mathcal{N}}(F)$ and $L = \mathrm{lm}_{\preccurlyeq}(QP)$.

Proof. If $D = 1$ the output returned by Algorithm 1 is correct, since by Theorem 3.7, QP is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\ker(\varphi_1)\cap\mathcal{N}}(F)$ and $L = \mathrm{lm}_{\preccurlyeq}(QP)$. We assume by induction hypothesis that Algorithm 3 returns the output foreseen by Theorem 4.3 when the number of input linear functionals is $< D$, and when the assumptions of the theorem are satisfied.

By such a hypothesis, since $G = PF$ and $K = \mathrm{lm}_{\preccurlyeq}(P)$, one deduces that (Q_1, L_1) are such that $Q_1 P$ is a $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{M}}(F)$, with $\mathcal{M} = \mathcal{N}_{\lfloor D/2 \rfloor} \cap \mathcal{N}$, and $L_1 = \mathrm{lm}_{\preccurlyeq}(Q_1 P)$.

Let $\mathcal{K}_i = \cap_{\lfloor D/2 \rfloor + 1 \le j \le i} \ker(\varphi_j)$, for each $i = \lfloor D/2 \rfloor + 1, \ldots, D$. By hypothesis $\mathcal{K}_i \cap \mathcal{M} = \mathcal{N}_i \cap \mathcal{N}$ is a module, for $i = \lfloor D/2 \rfloor + 1, \ldots, i = D$. Since $Q_1 G = Q_1 PF$ and $Q_1 P$ is a $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{M}}(F)$, and $L_1 = \mathrm{lm}_{\preccurlyeq}(Q_1 P)$, we can apply again the induction hypothesis, and conclude that (Q_2, L_2) is such that $Q_2 Q_1 P$ is a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{K}_D\cap\mathcal{M}}(F) = \mathrm{Syz}_{\mathcal{N}_D\cap\mathcal{N}}(F)$, and $L_2 = \mathrm{lm}_{\preccurlyeq}(Q_2 Q_1 P)$. We conclude that the global output $(Q_2 Q_1, L_2)$ satisfies the claimed properties. □

5 MULTIVARIATE PADÉ APPROXIMATION

The algorithm in the previous section gives a general framework, which can be refined when applied to a particular context. Here, we consider the context of multivariate Padé approximation, where

$$\mathcal{N} = \langle X_1^{d_1}, \ldots, X_r^{d_r} \rangle \times \cdots \times \langle X_1^{d_1}, \ldots, X_r^{d_r} \rangle \subseteq \mathcal{R}^n, \tag{6}$$

for some $d_1, \ldots, d_r \in \mathbb{Z}_{>0}$. We begin with some remarks on the degrees and sizes of Gröbner bases of syzygy modules $\mathrm{Syz}_{\mathcal{N}}(F)$.

To express this context in the framework of Section 4, we take for the D linear functionals φ_i the dual basis of the canonical monomial basis of $\mathcal{R}^n/\mathcal{N}$. Precisely, the linear functionals are $\varphi_{\mu,j} : \mathcal{R}^n \to \mathbb{K}$ for $1 \le j \le n$ and all monomials $\mu \in \mathrm{Mon}(\mathcal{R})$ with $\deg_{X_i}(\mu) < d_i$ for $1 \le i \le r$, defined as follows: for $f = (f_1, \ldots, f_n) \in \mathcal{R}^n$, $\varphi_{\mu,j}(f)$ is the coefficient of the monomial μ in f_j. These linear functionals

can be ordered in several ways to ensure that Eq. (4) is satisfied. Here we design our algorithm by ordering the functionals $\varphi_{\mu,j}$ according to the term-over-position lexicographic order on the monomials $\mu \boldsymbol{e}_j \in \mathrm{Mon}(\mathcal{R}^n)$.

Example 5.1. Consider the case of $r = 2$ variables X, Y with $d_1 = 2$, $d_2 = 4$, and $n = 2$. Then the functionals are

$$\varphi_{1,1},\ \varphi_{1,2},\ \varphi_{Y,1},\ \varphi_{Y,2},\ \varphi_{Y^2,1},\ \varphi_{Y^2,2},\ \varphi_{Y^3,1},\ \varphi_{Y^3,2},$$
$$\varphi_{X,1},\ \varphi_{X,2},\ \varphi_{XY,1},\ \varphi_{XY,2},\ \varphi_{XY^2,1},\ \varphi_{XY^2,2},\ \varphi_{XY^3,1},\ \varphi_{XY^3,2},$$

in this specific order.

Lemma 5.2. *Let $\mathcal{N}$ be as in Eq. (6), let $\boldsymbol{F} \in \mathcal{R}^{m\times n}$, and let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$. Then, for $1 \le i \le r$, each polynomial in the reduced $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ either has degree in X_i less than d_i or has the form $X_i^{d_i}\boldsymbol{e}_j$ for some $1 \le j \le m$.*

Proof. Let $\boldsymbol{P}$ be the reduced $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ and let $i \in \{1,\dots,r\}$. Since $\mathcal{R}^m/\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ has finite dimension as a $\mathbb{K}$-vector space, for each $j \in \{1,\dots,n\}$ there is a polynomial in $\boldsymbol{P}$ whose $\preccurlyeq$-leading monomial has the form $X_i^d\boldsymbol{e}_j$ for some $d \ge 0$. Since $\boldsymbol{P}$ is reduced, any other $(p_1,\dots,p_m)$ in $\boldsymbol{P}$ whose $\preccurlyeq$-leading monomial has support j is such that $\deg_{X_i}(p_j) < d \le d_i$; the last inequality follows from the fact that the monomial $X_i^{d_i}\boldsymbol{e}_j$ is in $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ and thus is a multiple of $X_i^d\boldsymbol{e}_j$. It follows that all polynomials in $\boldsymbol{P}$ whose $\preccurlyeq$-leading monomial is not among $\{X_i^{d_i}\boldsymbol{e}_j, 1 \le j \le n\}$ must have degree in X_i less than d_i. On the other hand, any polynomial in $\boldsymbol{P}$ whose $\preccurlyeq$-leading monomial is $X_i^{d_i}\boldsymbol{e}_j$ for some j must be equal to this monomial, since it belongs to $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ and $\boldsymbol{P}$ is reduced. □

In the context of Algorithm 3, Lemma 5.2 allows us to truncate the product $\boldsymbol{Q}_2\boldsymbol{Q}_1$ while preserving a $\preccurlyeq$-Gröbner basis.

Corollary 5.3. *Let $\mathcal{N}$ be as in Eq. (6), let $\boldsymbol{F} \in \mathcal{R}^{m\times n}$, let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$, and let $\boldsymbol{P} \in \mathcal{R}^{k\times m}$ be a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$. If $\boldsymbol{P}$ is modified by truncating each of its polynomials modulo $\langle X_1^{d_1+1},\dots,X_r^{d_r+1}\rangle$, then $\boldsymbol{P}$ is still a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$.*

Proof. On the first hand, this modification of $\boldsymbol{P}$ does not affect the $\preccurlyeq$-leading terms since they all have X_i-degree less than $d_i + 1$ according to Lemma 5.2, hence after modification we still have $\langle \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P})\rangle = \langle \mathrm{lm}_{\preccurlyeq}(\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F}))\rangle$. On the other hand, after this modification we also have $\langle \boldsymbol{P}\rangle \subseteq \mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ since we started from a basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ and added to each of its elements some multiples of $\langle X_1^{d_1+1},\dots,X_r^{d_r+1}\rangle$, which are contained in $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$. Then [13, Lem. 15.5] yields $\langle \boldsymbol{P}\rangle = \mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$, hence the conclusion. □

Then, the divide and conquer approach can be refined as described in Algorithm 4. The correctness of this algorithm can be shown by following the proof of Theorem 4.3 and with the following considerations. By induction hypothesis, $\boldsymbol{Q}_1$ is such that each component of the rows of $\boldsymbol{Q}_1\boldsymbol{G}$ is an element of

$$\langle X_1^{d_1},\dots,X_{j-1}^{d_{j-1}},X_j^{\lfloor d_j/2\rfloor},X_{j+1},\dots,X_r\rangle,$$

hence its truncation modulo

$$\langle X_1^{d_1},\dots,X_j^{d_j},X_{j+1},\dots,X_r\rangle$$

Algorithm 4 Padé$(d_1,\dots,d_r,\boldsymbol{G},\preccurlyeq,\boldsymbol{K})$

Input:
- integers $d_1,\dots,d_r \in \mathbb{Z}_{>0}$,
- a matrix $\boldsymbol{G}$ in $\mathcal{R}^{k\times n}$,
- a monomial order $\preccurlyeq$ on $\mathcal{R}^m$,
- a list $\boldsymbol{K} = (\boldsymbol{\mu}_1,\dots,\boldsymbol{\mu}_k)$ of elements of $\mathrm{Mon}(\mathcal{R}^m)$.

Output:
- a matrix $\boldsymbol{Q}$ in $\mathcal{R}^{\ell\times m}$ for some $\ell \ge 0$,
- a list $\boldsymbol{L}$ of ℓ elements of $\mathrm{Mon}(\mathcal{R}^m)$.

1: **if** $d_1 = \cdots = d_r = 1$ **then**
2: $\quad\boldsymbol{Q} \in \mathcal{R}^{k\times k} \leftarrow \boldsymbol{I}_k$; $\boldsymbol{H} \leftarrow \boldsymbol{G} \bmod X_1,\dots,X_r$; $\boldsymbol{L} \leftarrow \boldsymbol{K}$
3: $\quad$**for** $i = 1,\dots,n$ **do**
4: $\quad\quad\varphi \leftarrow$ linear functional $\mathcal{R}^n \to \mathbb{K}$ defined by $\varphi(\boldsymbol{f}) = f_i(\boldsymbol{0})$
5: $\quad\quad(\boldsymbol{Q}_i,\boldsymbol{L}) \leftarrow$ Syzygy_BaseCase$(\varphi,\boldsymbol{H},\preccurlyeq,\boldsymbol{L})$
6: $\quad\quad\boldsymbol{Q} \leftarrow \boldsymbol{Q}_i\boldsymbol{Q} \bmod X_1^2,\dots,X_r^2$
7: $\quad\quad\boldsymbol{H} \leftarrow \boldsymbol{Q}_i\boldsymbol{H} \bmod X_1,\dots,X_r$
8: $\quad$**return** $(\boldsymbol{Q},\boldsymbol{L})$
9: $j \leftarrow \max\{i \in \{1,\dots,r\} \mid d_i > 1\}$
10: $(\boldsymbol{Q}_1,\boldsymbol{L}_1) \leftarrow$ Padé$(d_1,\dots,d_{j-1},\lfloor d_j/2\rfloor,1,\dots,1,\boldsymbol{G},\preccurlyeq,\boldsymbol{K})$
11: $\boldsymbol{G}_2 \leftarrow X_j^{-\lfloor d_j/2\rfloor}(\boldsymbol{Q}_1\boldsymbol{G} \bmod X_1^{d_1},\dots,X_j^{d_j},X_{j+1},\dots,X_r)$
12: $(\boldsymbol{Q}_2,\boldsymbol{L}_2) \leftarrow$ Padé$(d_1,\dots,d_{j-1},\lceil d_j/2\rceil,1,\dots,1,\boldsymbol{G}_2,\preccurlyeq,\boldsymbol{L}_1)$
13: $\boldsymbol{Q} \leftarrow \boldsymbol{Q}_2\boldsymbol{Q}_1 \bmod X_1^{d_1+1},\dots,X_r^{d_r+1}$
14: **return** $(\boldsymbol{Q},\boldsymbol{L}_2)$

is an $\mathcal{R}$-multiple of $X_j^{\lfloor d_j/2\rfloor}$. It follows that on Line 11, $\boldsymbol{G}_2$ is well defined. Moreover, for $\boldsymbol{p} \in \mathcal{R}^m$ the next equations are equivalent:

$$\boldsymbol{p}\boldsymbol{Q}_1\boldsymbol{G} = 0 \mod X_1^{d_1},\dots,X_{j-1}^{d_{j-1}},X_j^{d_j}$$
$$\boldsymbol{p}\boldsymbol{G}_2 = \boldsymbol{p}X_j^{-\lfloor d_j/2\rfloor}\boldsymbol{Q}_1\boldsymbol{G} = 0 \mod X_1^{d_1},\dots,X_{j-1}^{d_{j-1}},X_j^{\lceil d_j/2\rceil}$$

This justifies the division by $X_j^{\lfloor d_j/2\rfloor}$ at Line 11 and the fact that the second call is done with $\lceil d_j/2\rceil$ instead of d_j at Line 12.

For the complexity analysis, we use Lemma 5.2 to give a bound on the size of the computed Gröbner bases, which differs from the general bound in Lemma 4.2.

Corollary 5.4 (of Lemma 5.2). *Let $\mathcal{N}$ be as in Eq. (6), let $\boldsymbol{F} \in \mathcal{R}^{m\times n}$, let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$, and let $\boldsymbol{P} \in \mathcal{R}^{k\times m}$ be a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$. Then,*

$$k \le md_1\cdots d_r/(\max_{1\le i\le r} d_i).$$

Proof. Let $\boldsymbol{L} = \mathrm{lm}_{\preccurlyeq}(\boldsymbol{P}) \in \mathcal{R}^{k\times m}$ and let $\bar{\imath}$ be such that $d_{\bar{\imath}} = \max_{1\le i\le r} d_i$. It is enough to prove that $\boldsymbol{L}$ has at most $d_1\cdots d_r/d_{\bar{\imath}}$ rows of the form $\mu\boldsymbol{e}_j$ for each $j \in \{1,\dots,m\}$; by Lemma 5.2, the monomial $\mu \in \mathrm{Mon}(\mathcal{R})$ has X_i-degree at most d_i for $1 \le i \le r$. Now, for each monomial $\nu = X_1^{e_1}\cdots X_{\bar{\imath}-1}^{e_{\bar{\imath}-1}}X_{\bar{\imath}+1}^{e_{\bar{\imath}+1}}\cdots X_r^{e_r}$ with $e_i \le d_i$ for all $i \ne \bar{\imath}$, there is at most one row $\mu\boldsymbol{e}_j$ in $\boldsymbol{L}$ such that $\mu = \nu X_{\bar{\imath}}^e$ for some $e \ge 0$: otherwise, one of two such rows would divide the other, which would contradict the minimality of $\boldsymbol{P}$. The number of such monomials ν is precisely $d_1\cdots d_r/d_{\bar{\imath}}$. □

Here we have $D = nd_1\cdots d_r$, hence the above bound on the cardinality of minimal $\preccurlyeq$-Gröbner bases refines the bound in Lemma 4.2 as soon as $m \le n(r-1)(\max_{1\le i\le r} d_i)$.

Proposition 5.5. *For $\mathcal{R} = \mathbb{K}[X, Y]$, let*

$$\mathcal{N} = \langle X^d, Y^e \rangle \times \cdots \times \langle X^d, Y^e \rangle \subset \mathcal{R}^n,$$

let $\boldsymbol{F} \in \mathcal{R}^{m \times n}$ with $\deg_X(\boldsymbol{F}) < d$ and $\deg_Y(\boldsymbol{F}) < e$, and let $\preccurlyeq$ be a monomial order on $\mathcal{R}^m$. Algorithm 4 computes a minimal $\preccurlyeq$-Gröbner basis of $\mathrm{Syz}_{\mathcal{N}}(\boldsymbol{F})$ using $\tilde{O}((M^{\omega-1} + Mn)(M+n)de)$ operations in $\mathbb{K}$, where $M = m \min(d, e)$.

Proof. According to Corollary 5.4, the number of rows of the matrices $\boldsymbol{Q}$ computed in Algorithm 4 is at most $M = m \min(d, e)$. It follows that all matrices $\boldsymbol{Q}_i, \boldsymbol{Q}_1, \boldsymbol{Q}_2, \boldsymbol{Q}$ in the algorithm have at most M rows and at most M columns, and that the matrices $\boldsymbol{G}, \boldsymbol{H}, \boldsymbol{G}_1, \boldsymbol{G}_2$ have at most M rows and exactly n columns. Besides, by Kronecker substitution [7, Chap. 1 Sec. 8], multiplying two bivariate matrices of dimensions $M \times M$ (resp. $M \times n$) and bidegree at most (d, e) costs $\tilde{O}(M^\omega de)$ (resp. $\tilde{O}(M^\omega(1 + n/M)de)$) operations in $\mathbb{K}$.

Let $C(m, n, d, e)$ denote the number of field operations used by Algorithm 4; we have $C(m, n, d, e) \leq C(M, n, d, e)$. First, for $e > 1$, $C(M, n, d, e)$ is bounded by $C(M, n, d, \lfloor e/2 \rfloor) + C(M, n, d, \lceil e/2 \rceil) + \tilde{O}(M^\omega(1 + n/M)de)$. Indeed, there are two recursive calls with parameters $(d, \lfloor e/2 \rfloor)$ and $(d, \lceil e/2 \rceil)$, and two matrix products $\boldsymbol{Q}_1\boldsymbol{G}$ and $\boldsymbol{Q}_2\boldsymbol{Q}_1$ to perform; as noted above, the latter products cost $\tilde{O}(M^\omega(1 + n/M)de)$ operations in $\mathbb{K}$. The same analysis for $d > 1$ and $e = 1$ shows that $C(M, n, d, 1)$ is bounded by $C(M, n, \lfloor d/2 \rfloor, 1) + C(M, n, \lceil d/2 \rceil, 1) + \tilde{O}(M^\omega(1 + n/M)d)$.

Finally, for $d = e = 1$, we show that $C(M, n, 1, 1) \in O(M(M+n)n)$. In this case, there are n iterations of the loop. Each of them makes one call to Syzygy_BaseCase, which uses $O(M)$ field operations for computing the λ_i's at Line 7; note that the α_j's are zero in the present context where the linear functional φ corresponds to the constant coefficient. The computed basis $\boldsymbol{Q}_i$ has a single nontrivial column (it has the form in Eq. (3)), so that computing $\boldsymbol{Q}_i\boldsymbol{Q}$ mod $\langle X_1^2, \ldots, X_r^2 \rangle$ (resp. $\boldsymbol{Q}_i\boldsymbol{H}$ mod $\langle X_1, \ldots, X_r \rangle$) can be done naively at a cost of $O(M^2)$ (resp. $O(M(M+n))$) operations in $\mathbb{K}$.

Based on the previous inequalities, unrolling the recursion by following the divide-and-conquer scheme leads to the announced complexity bound. □

ACKNOWLEDGMENTS

Acknowledgements. The first author acknowledges support from the Fondation Mathématique Jacques Hadamard through the Programme PGMO, project number 2018-0061H.

REFERENCES

[1] M.E. Alonso, M.G. Marinari, and T. Mora. 2003. The Big Mother of all Dualities: Möller Algorithm. *Communications in Algebra* 31, 2 (2003), 783–818. https://doi.org/10.1081/AGB-120017343

[2] B. Beckermann. 1992. A reliable method for computing M-Padé approximants on arbitrary staircases. *J. Comput. Appl. Math.* 40, 1 (1992), 19–42. https://doi.org/10.1016/0377-0427(92)90039-Z

[3] B. Beckermann and G. Labahn. 1994. A Uniform Approach for the Fast Computation of Matrix-Type Padé Approximants. *SIAM J. Matrix Anal. Appl.* 15, 3 (1994), 804–823. https://doi.org/10.1137/S0895479892230031

[4] B. Beckermann and G. Labahn. 1997. Recursiveness in matrix rational interpolation problems. *J. Comput. Appl. Math.* 77, 1 (1997), 5–34. https://doi.org/10.1016/S0377-0427(96)00120-3

[5] C. Berkesch and F.-O. Schreyer. 2015. Syzygies, finite length modules, and random curves. In *Commutative Algebra and Noncommutative Algebraic Geometry*. Mathematical Sciences Research Institute Publications (Vol. 67), pp. 25–52.

[6] J. Berthomieu and J.-C. Faugère. 2018. A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations. In *Proceedings ISSAC 2018*. 79–86. https://doi.org/10.1145/3208976.3209017

[7] D. Bini and V. Y. Pan. 1994. *Polynomial and Matrix Computations (Vol. 1): Fundamental Algorithms*. Birkhauser Verlag.

[8] M. Ceria and T. Mora. 2018. Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game. *Preprint arXiv:1805.09165*.

[9] L. Cerlienco and M. Mureddu. 1995. From algebraic sets to monomial linear bases by means of combinatorial algorithms. *Discrete Mathematics* 139, 1-3 (1995), 73–87. https://doi.org/10.1016/0012-365X(94)00126-4

[10] D. Coppersmith and S. Winograd. 1990. Matrix multiplication via arithmetic progressions. *J. Symb. Comput.* 9, 3 (1990), 251–280. https://doi.org/10.1016/S0747-7171(08)80013-2

[11] D. A. Cox, J. Little, and D. O'Shea. 2005. *Using Algebraic Geometry (second edition)*. Springer-Verlag New-York, New York, NY. https://doi.org/10.1007/b138611

[12] D. A. Cox, J. Little, and D. O'Shea. 2007. *Ideals, Varieties, and Algorithms (third edition)*. Springer-Verlag New-York, New York, NY. https://doi.org/10.1007/978-0-387-35651-8

[13] D. Eisenbud. 1995. *Commutative Algebra: with a View Toward Algebraic Geometry*. Springer, New York, Berlin, Heildelberg. https://doi.org/10.1007/978-1-4612-5350-1

[14] J.B. Farr and S. Gao. 2006. Computing Gröbner bases for vanishing ideals of finite sets of points. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*. Springer, 118–127.

[15] B. Felszeghy, B. Ráth, and L. Rónyai. 2006. The lex game and some applications. *J. Symb. Comput.* 41, 6 (2006), 663–681. https://doi.org/10.1016/j.jsc.2005.11.003

[16] P. Fitzpatrick. 1997. Solving a Multivariable Congruence by Change of Term Order. *J. Symb. Comput.* 24, 5 (1997), 575–589. https://doi.org/10.1006/jsco.1997.0153

[17] P. Fitzpatrick and J. Flynn. 1992. A Gröbner basis technique for Padé approximation. *J. Symb. Comput.* 13, 2 (1992), 133–138. https://doi.org/10.1016/S0747-7171(08)80087-9

[18] K. O. Geddes. 1973. *Algorithms for Analytic Approximation (to a Formal Power-series)*. Ph.D. Dissertation. University of Toronto, Canada.

[19] P. Giorgi, C.-P. Jeannerod, and G. Villard. 2003. On the complexity of polynomial matrix computations. In *ISSAC'03* (Philadelphia, PA, USA). ACM, 135–142. https://doi.org/10.1145/860854.860889

[20] M. Janet. 1920. Sur les systèmes d'équations aux dérivées partielles. *J. Math. Pures Appl.* 170 (1920), 65–152.

[21] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. 2016. Fast computation of minimal interpolation bases in Popov form for arbitrary shifts. In *ISSAC'16* (Waterloo, ON, Canada). ACM, 295–302. https://doi.org/10.1145/2930889.2930928

[22] C.-P. Jeannerod, V. Neiger, É. Schost, and G. Villard. 2017. Computing minimal interpolation bases. *J. Symb. Comput.* 83 (2017), 272–314. https://doi.org/10.1016/j.jsc.2016.11.015

[23] C.-P. Jeannerod, V. Neiger, and G. Villard. 2020. Fast computation of approximant bases in canonical form. *J. Symb. Comput.* 98 (2020), 192–224. https://doi.org/10.1016/j.jsc.2019.07.011

[24] F. Le Gall. 2014. Powers of Tensors and Fast Matrix Multiplication. In *ISSAC'14* (Kobe, Japan). ACM, 296–303. https://doi.org/10.1145/2608628.2608664

[25] M. G. Marinari, H. M. Möller, and T. Mora. 1993. Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Appl. Algebra Engrg. Comm. Comput.* 4, 2 (1993), 103–145. https://doi.org/10.1007/BF01386834

[26] H. M. Möller and B. Buchberger. 1982. The Construction of Multivariate Polynomials with Preassigned Zeros. In *EUROCAM'82 (LNCS)*, Vol. 144. Springer, 24–31. https://doi.org/10.1007/3-540-11607-9_3

[27] T. Mora. 2009. The FGLM Problem and Möller's Algorithm on Zero-dimensional Ideals. In *Gröbner Bases, Coding, and Cryptography*, M. Sala, S. Sakata, T. Mora, C. Traverso, and L. Perret (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 27–45. https://doi.org/10.1007/978-3-540-93806-4_3

[28] V. Neiger. 2016. *Bases of relations in one or several variables: fast algorithms and applications*. Ph.D. Dissertation. École Normale Supérieure de Lyon. https://tel.archives-ouvertes.fr/tel-01431413/

[29] V. Neiger and É. Schost. 2019. Computing syzygies in finite dimension using fast linear algebra. *Preprint arXiv:1912.01848*.

[30] H. O'Keeffe and P. Fitzpatrick. 2002. Gröbner basis solutions of constrained interpolation problems. *Linear Algebra Appl.* 351 (2002), 533–551. https://doi.org/10.1016/S0024-3795(01)00509-2

[31] F-O. Schreyer. 1980. *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstraßschen Divisionssatz*. Ph.D. Dissertation. Master's thesis, Fakultät für Mathematik, Universität Hamburg.

[32] A. Storjohann. 2006. Notes on computing minimal approximant bases. In *Challenges in Symbolic Computation Software (Dagstuhl Seminar Proceedings)*. http://drops.dagstuhl.de/opus/volltexte/2006/776

[33] M. Van Barel and A. Bultheel. 1992. A general module theoretic framework for vector M-Padé and matrix rational interpolation. *Numer. Algorithms* 3 (1992), 451–462. https://doi.org/10.1007/BF02141952

[34] P. Wynn. 1960. The Rational Approximation of Functions which are Formally Defined by a Power Series Expansion. *Math. Comp.* 14, 70 (1960), 147–186.

[35] W. Zhou and G. Labahn. 2012. Efficient Algorithms for Order Basis Computation. *J. Symb. Comput.* 47, 7 (2012), 793–819. https://doi.org/10.1016/j.jsc.2011.12.009