

# Polynomial-Division-Based Algorithms for Computing Linear Recurrence Relations

Jérémy Berthomieu, Jean-Charles Faugère

▶ **To cite this version:**

Jérémy Berthomieu, Jean-Charles Faugère. Polynomial-Division-Based Algorithms for Computing Linear Recurrence Relations. Journal of Symbolic Computation, 2022, 109, pp.1-30. 10.1016/j.jsc.2021.07.002 . hal-01935229v3

**HAL Id: hal-01935229**

**https://inria.hal.science/hal-01935229v3**

Submitted on 6 Jul 2021

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# Polynomial-Division-Based Algorithms for Computing Linear Recurrence Relations

Jérémy Berthomieu[a,*], Jean-Charles Faugère[b,c]

[a] *Sorbonne Université,* CNRS, LIP6, *F-75005, Paris, France*
[b] *CryptoNext Security*
[c] *Sorbonne Université,* CNRS, INRIA, LIP6, *F-75005, Paris, France*

**Abstract**

Sparse polynomial interpolation, sparse linear system solving or modular rational reconstruction are fundamental problems in Computer Algebra. They come down to computing linear recurrence relations of a sequence with the Berlekamp–Massey algorithm. Likewise, sparse multivariate polynomial interpolation and multidimensional cyclic code decoding require guessing linear recurrence relations of a multivariate sequence.

Several algorithms solve this problem. The so-called Berlekamp–Massey–Sakata algorithm (1988) uses polynomial additions and shifts by a monomial. The Scalar-FGLM algorithm (2015) relies on linear algebra operations on a multi-Hankel matrix, a multivariate generalization of a Hankel matrix. The Artinian Gorenstein border basis algorithm (2017) uses a Gram-Schmidt process.

We propose a new algorithm for computing the Gröbner basis of the ideal of relations of a sequence based solely on multivariate polynomial arithmetic. This algorithm allows us to both revisit the Berlekamp–Massey–Sakata algorithm through the use of polynomial divisions and to completely revise the Scalar-FGLM algorithm without linear algebra operations.

A key observation in the design of this algorithm is to work on the mirror of the truncated generating series allowing us to use polynomial arithmetic modulo a monomial ideal. It appears to have some similarities with Padé approximants of this mirror polynomial.

As an addition from the paper published at the ISSAC conference, we give an adaptive variant of this algorithm taking into account the shape of the final Gröbner basis gradually as it is discovered. The main advantage of this algorithm is that its complexity in terms of operations and sequence queries only depends on the output Gröbner basis.

All these algorithms have been implemented in Maple and we report on our comparisons.

*Keywords:* Gröbner bases; linear recursive sequences; Berlekamp–Massey–Sakata; extended Euclidean algorithm; Padé approximants

*Laboratoire d'Informatique de Paris 6, Sorbonne Université, boîte courrier 169, 4 place Jussieu, F-75252 Paris Cedex 05, France.

*Email addresses:* jeremy.berthomieu@lip6.fr (Jérémy Berthomieu), jcf@cryptonext-security.com, jean-charles.faugere@inria.fr (Jean-Charles Faugère)

## 1. Introduction

The Berlekamp–Massey algorithm (BM), introduced by Berlekamp in 1968 [2] and Massey in 1969 [24] is a fundamental algorithm in Coding Theory, [9, 20], and Computer Algebra. It allows one to perform efficiently sparse polynomial interpolation, sparse linear system solving or modular rational reconstruction.

In 1988, Sakata extended the BM algorithm to dimension $n$. This algorithm, known as the Berlekamp–Massey–Sakata algorithm (BMS), can be used to compute a Gröbner basis of the zero-dimensional ideal of the relations satisfied by a sequence, [27, 28, 29]. Analogously to dimension 1, the BMS algorithm allows one to decode cyclic codes in dimension $n > 1$, an extension of Reed–Solomon's codes. Furthermore, the latest versions of the Sparse-FGLM algorithm rely heavily on the efficiency of the BMS algorithm to compute the change of ordering of a Gröbner basis, [16, 17].

### *1.1. Related Work*

In dimension 1, it is well known that the BM algorithm can be seen in a matrix form requiring to solve a linear Hankel system of size $D$, the order of the recurrence, see [22], or the Levinson–Durbin method, [23, 30]. If we let $\mathsf{M}(D)$ be a cost function for multiplying two polynomials of degree $D$, for instance $\mathsf{M}(D) \in O(D \log D \log\log D)$, [12, 13], then solving a linear Hankel system of size $D$ comes down to performing a truncated extended Euclidean algorithm called on two polynomials of degree $D$, [8, 11, 15]. More precisely, it can be done in $O(\mathsf{M}(D) \log D)$ operations.

In [3, 4], the authors present the Scalar-FGLM algorithm, extending the matrix version of the BM algorithm for multidimensional sequences. It consists in computing the relations of the sequence through the computation of a maximal submatrix of full rank of a *multi-Hankel* matrix, a multivariate generalization of a Hankel matrix. Then, it returns the minimal Gröbner basis $\mathcal{G}$ of the ideal of relations satisfied by the sequence. These notions are recalled in Section 2. If we denote by $S$ the staircase defined by $\mathcal{G}$ and $T$ the input set of monomials containing $S \cup \mathrm{LM}(\mathcal{G})$, then the complexity of the Scalar-FGLM algorithm is $O((\#T)^\omega)$, where $2 \leq \omega \leq 3$ is the linear algebra exponent. However, we do not know how to exploit the multi-Hankel structure to improve this complexity.

The Artinian Gorenstein border bases algorithm (AGbb) was presented in [25] for computing a border basis $\mathcal{B}$ of the ideal of relations. It extends the algorithm of [3] using polynomial arithmetic allowing it to reach the better complexity $O((\#S + \#\mathcal{B}) \cdot \#S \cdot \#T)$ with the above notation.

Another viewpoint is that computing linear recurrence relations can be seen as computing Padé approximants of a truncation of the generating series $\sum_{i_1,\ldots,i_n \geq 0} w_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}$. In [18], the authors extend the extended Euclidean algorithm for computing multivariate Padé approximants. Given a polynomial $P$ and an ideal $B$, find polynomials $F$ and $C$ such that $P = \frac{F}{C} \bmod B$, where the leading monomials of $F$ and $C$ satisfy some constraints.

It is also worth noticing that we now know that both the BMS and the Scalar-FGLM algorithms are not equivalent, see [6], i.e. it is not possible to tweak one algorithm to mimic the behavior of the other. However, if the input sequence is linear recurrent and sufficiently many sequence terms are visited, then both algorithms compute a Gröbner basis of the zero-dimensional ideal of relations.

*1.2. Contributions*

In the whole paper, we assume that the input sets of the Scalar-FGLM algorithm are the sets of all the monomials less than a given monomial and that these sets are finite. In order to improve the complexity of the algorithm, we will use polynomial arithmetic in all the operations. Even though they are not equivalent, this reduces the gap between the BMS and the Scalar-FGLM algorithms and provides a unified presentation.

In Section 3, we present the BM, the BMS and the Scalar-FGLM algorithms in a unified polynomial viewpoint. Using the mirror of the truncated generating series is a key ingredient letting us perform the computations modulo a specific monomial ideal $B$: a vector in the kernel of a multi-Hankel matrix is a polynomial $C$ such that

$$\mathrm{LM}(P\,C \bmod B) \prec t_C, \tag{1}$$

where $P$ is the mirror of the truncated generating series, LM denotes the leading monomial and $t_C$ is a monomial associated to $C$.

One interpretation of this is the computation of multivariate Padé approximants $\frac{F}{C}$ of $P$ modulo $B$ with different constraints than in [18] since we require that $\mathrm{LM}(C)$ is in a given set of terms and $\mathrm{LM}(P\,C \bmod B)$ satisfies equation (1).

This polynomial point of view allows us to design the Polynomial Scalar-FGLM algorithm (Algorithm 1) in Section 4 based on multivariate polynomial divisions. It computes, in a sense, a generating set of polynomials whose product with $P$ modulo $B$ must satisfy equation (1). If they do not, by polynomial divisions, we make new ones until finding minimal polynomials satisfying this constraint. It is worth noticing that in dimension 1, we recover the truncated extended Euclidean algorithm applied to the mirror polynomial of the generating series of the input sequence, truncated in degree $D$, and $x^{D+1}$. All the examples are available on [7].

Our main result is Theorem 21, a simplified version of which is

**Theorem 1.** *Let* $\mathbf{w}$ *be a sequence,* $\prec$ *be a total degree monomial ordering and* $a$ *be a monomial. Let us assume that the reduced Gröbner basis* $\mathcal{G}$ *of the ideal of relations of* $\mathbf{w}$ *for* $\prec$ *and its staircase* $S$ *satisfy* $a \succeq \max(S \cup \mathrm{LM}(\mathcal{G}))$ *and for all* $g \preceq a$, $s = \max_{\sigma \preceq a}\{\sigma,\ \sigma\, g \preceq a\}$, *we have* $\max(S) \preceq s$. *Then, the* Polynomial Scalar-FGLM *algorithm applied to* $\mathbf{w}$, $\prec$ *and* $a$ *terminates and computes a minimal Gröbner basis of the ideal of relations of* $\mathbf{w}$ *for* $\prec$ *in* $O(\#S\,(\#S + \#\mathcal{G})\,\#\{\sigma, \sigma \preceq a\})$ *operations in the base field.*

Let us also remark that the complexity bound is based on naive multivariate polynomial arithmetic and that this algorithm can benefit from improvements made in this domain.

In applications such as Gröbner bases change of orderings through the Sparse-FGLM algorithm, sequence queries are costly, [17]. In [3], an adaptive variant of the Scalar-FGLM algorithm was designed aiming to minimize the number of sequence queries to recover the relations.

In Section 5, we show how we can transform the Adaptive Scalar-FGLM algorithm of [3] into an algorithm using polynomial arithmetic. This algorithm is output sensitive and probabilistic, like the Adaptive Scalar-FGLM algorithm is. That is, its main advantage is that its complexity only depends on the sizes of the computed staircase and Gröbner basis.

**Theorem 2** (see Theorem 26)**.** *Let* $\mathbf{w}$ *be a sequence,* $\prec$ *be a total degree monomial ordering.*

*Let us assume that calling the* Adaptive Polynomial Scalar-FGLM *algorithm on* $\mathbf{w}$ *and* $\prec$ *yields the Gröbner basis* $\mathcal{G}$ *and its staircase* $S$.

*Then, the* Adaptive Polynomial Scalar-FGLM *algorithm performs at most* $O((\#S + \#\mathcal{G})^2 \#2S)$ *operations in the base field and* $\#2(S \cup \mathrm{LM}(\mathcal{G}))$ *table queries to recover* $\mathcal{G}$*, where for a set* $T$*,* $2T = \{tt', t, t' \in T\}$.

Finally, in Section 6, we compare the Polynomial Scalar-FGLM algorithm with our implementations of the BMS, the Scalar-FGLM and the AGbb algorithms. Our algorithm performs always fewer arithmetic operations than the others starting from a certain size. Even for an example family favorable towards the BMS algorithm, our algorithm performs better.

Although we have compared the numbers of arithmetic operations, it would be beneficial to have an efficient implementation. This would be the first step into designing a similar efficient algorithm for computing linear recurrence relations with polynomial coefficients, extending the Beckermann–Labahn algorithm [1] for computing multivariate Hermite–Padé approximants.

Amongst the changes from the ISSAC version of the paper, [5], the main additions are a complete redesign of the Scalar-FGLM algorithm through polynomial arithmetic in Section 3.2.2 and a full description of the Adaptive Polynomial Scalar-FGLM algorithm, an adaptive variant of the Polynomial Scalar-FGLM algorithm using polynomial divisions as well, in Section 5.2. Generically, one could expect to make one relation with leading monomial $m\,x_i^2$ through a division of polynomials related to relations with leading monomials $m$ and $m\,x_i$. Yet, the naive approach given in [5, Section 5] could not do so as it does not perform any division. The Adaptive Polynomial Scalar-FGLM algorithm visits the monomials in the same order as the Adaptive Scalar-FGLM algorithm to recover the relations and replaces any linear algebra computations by polynomial ones, see [3]. We also give the complexity of this algorithm in terms both of the number of operations and the number of sequence queries.

Furthermore, one of the main obstructions to the design of this adaptive variant is that at each step, some polynomials are updated. This update process adds terms supposed to be small with respect to the ordering. Yet, their leading terms were not stable during this update process.

Lastly, in Section 3, we now more clearly define what $t_C$ should be in Equation 1. This is a key point in the Polynomial Scalar-FGLM algorithm and a more complete description is available in Proposition 13.

## 2. Notation

We give a brief description of classical notation used in the paper.

### *2.1. Sequences and relations*

For $n \geq 1$, we let $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$ and for $\mathbf{x} = (x_1, \ldots, x_n)$, we write $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_n^{i_n}$.

**Definition 3.** *Let* $\mathbb{K}$ *be a field,* $\mathcal{K} \subseteq \mathbb{N}^n$ *be finite,* $\mathbf{w} \in \mathbb{K}^{\mathbb{N}^n}$ *be a* $n$*-dimensional sequence with terms in* $\mathbb{K}$ *and* $f = \sum_{\mathbf{k} \in \mathcal{K}} \gamma_{\mathbf{k}}\, \mathbf{x}^{\mathbf{k}} \in \mathbb{K}[\mathbf{x}]$*. We let* $[f]_{\mathbf{w}}$*, or* $[f]$*, be the linear combination* $\sum_{\mathbf{k} \in \mathcal{K}} \gamma_{\mathbf{k}}\, w_{\mathbf{k}}$*. If for all* $\mathbf{i} \in \mathbb{N}^n$*,* $\left[\mathbf{x}^{\mathbf{i}} f\right] = 0$*, then we say that* $f$ *is the* polynomial of the relation induced by $\boldsymbol{\gamma} = (\gamma_{\mathbf{k}})_{\mathbf{k} \in \mathcal{K}} \in \mathbb{K}^{\#\mathcal{K}}$.

The main benefit of the [ ] notation resides in the immediate fact that for any index $\mathbf{i}$, its *shift by* $\mathbf{x}^{\mathbf{i}}$ is $\left[\mathbf{x}^{\mathbf{i}} f\right] = \sum_{\mathbf{k} \in \mathcal{K}} \gamma_{\mathbf{k}}\, w_{\mathbf{k}+\mathbf{i}}$.

**Example 4.** *Let* $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j) \in \mathbb{N}^2}$ *be the sequence of the binomial coefficients. Then,* $xy - y - 1$ *is the polynomial of Pascal's rule:*

$$\forall (i, j) \in \mathbb{N}^2,\ [x^i y^j (xy - y - 1)] = \mathbf{b}_{i+1,j+1} - \mathbf{b}_{i,j+1} - \mathbf{b}_{i,j} = 0.$$

**Definition 5** ([19, 27]). *Let* $\mathbf{w} = (w_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ *be an n-dimensional sequence with coefficients in* $\mathbb{K}$*. The sequence* $\mathbf{w}$ *is* linear recurrent *if from a nonzero finite number of initial terms* $\{w_{\mathbf{i}},\ \mathbf{i} \in S\}$*, and a finite number of relations, without any contradiction and without ambiguity, one can compute any term of the sequence.*

*Equivalently,* $\mathbf{w}$ *is linear recurrent if* $\{f \in \mathbb{K}[x],\ \forall\, m \in \mathbb{K}[\mathbf{x}], [m\, f]_{\mathbf{w}} = 0\} \subseteq \mathbb{K}[x]$*, its ideal of relations, is* zero-dimensional.

As the input parameters of the algorithms are the first terms of a sequence, a *table* shall denote a finite subset of terms of a sequence.

### *2.2. Gröbner bases*

Let $\mathcal{T} = \{\mathbf{x}^{\mathbf{i}},\ \mathbf{i} \in \mathbb{N}^n\}$ be the set of all monomials in $\mathbb{K}[\mathbf{x}]$. A monomial ordering $\prec$ on $\mathbb{K}[\mathbf{x}]$ is an order relation satisfying the following three classical properties:

1. for all $m \in \mathcal{T}$, $1 \preceq m$;
2. for all $m, m', s \in \mathcal{T}$, $m \prec m' \Rightarrow m\, s \prec m'\, s$;
3. every subset of $\mathcal{T}$ has a least element for $\prec$.

For a monomial ordering $\prec$ on $\mathbb{K}[\mathbf{x}]$ and $f \in \mathbb{K}[\mathbf{x}]$, $f \neq 0$, the *leading monomial* of $f$, denoted $\textsc{lm}(f)$, is the greatest monomial in the support of $f$ for $\prec$. The *leading coefficient* of $f$, denoted $\textsc{lc}(f)$, is the nonzero coefficient of $\textsc{lm}(f)$. The *leading term* of $f$, $\textsc{lt}(f)$, is defined as $\textsc{lt}(f) = \textsc{lc}(f)\ \textsc{lm}(f)$. For $f = 0$, to simplify the presentation, we shall define $\textsc{lm}(f) = \textsc{lc}(f) = \textsc{lt}(f) = 0$. For an ideal $I$, we denote $\textsc{lm}(I) = \{\textsc{lm}(f),\ f \in I\}$. Furthermore, we naturally extend $\prec$ to $\mathcal{T} \cup \{0\}$ with $0 \prec 1$.

We recall briefly the definition of a Gröbner basis and a staircase.

**Definition 6.** *Let* $I$ *be a nonzero ideal of* $\mathbb{K}[\mathbf{x}]$ *and let* $\prec$ *be a monomial ordering. A set* $\mathcal{G} \subseteq I$ *is a* Gröbner basis *of* $I$ *if for all* $f \in I$*, there exists* $g \in \mathcal{G}$ *such that* $\textsc{lm}(g) | \textsc{lm}(f)$.

*A Gröbner basis* $\mathcal{G}$ *of* $I$ *is* minimal *if for any* $g \in \mathcal{G}$, $\langle \mathcal{G} \setminus \{g\}\rangle \neq I$.

*Furthermore,* $\mathcal{G}$ *is* reduced *if for any* $g, g' \in \mathcal{G}$, $g \neq g'$ *and any monomial* $m \in \operatorname{supp} g'$, $\textsc{lm}(g) \nmid m$.

*The* staircase *of* $\mathcal{G}$ *is defined as* $S = \text{Staircase}(\mathcal{G}) = \{s \in \mathcal{T},\ \forall\, g \in \mathcal{G}, \textsc{lm}(g) \nmid s\}$*. It is also the canonical basis of* $\mathbb{K}[\mathbf{x}]/I$.

Gröbner basis theory allows us to choose any monomial ordering, among which, we mainly use the

$\textsc{lex}(x_n \prec \cdots \prec x_1)$ **ordering** which satisfies $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{i}'}$ if, and only if, there exists $k$, $1 \leq k \leq n$, such that for all $\ell < k$, $i_\ell = i'_\ell$ and $i_k < i'_k$, see [14, Chapter 2, Definition 3];

$\textsc{drl}(x_n \prec \cdots \prec x_1)$ **ordering** which satisfies $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{i}'}$ if, and only if, $i_1 + \cdots + i_n < i'_1 + \cdots + i'_n$ or $i_1 + \cdots + i_n = i'_1 + \cdots + i'_n$ and there exists $k$, $2 \leq k \leq n$, such that for all $\ell > k$, $i_\ell = i'_\ell$ and $i_k > i'_k$, see [14, Chapter 2, Definition 6].

However, in the BMS algorithm, we need to be able to enumerate all the monomials up to a bound monomial. This forces the user to take an ordering $\prec$ such that for all $M \in \mathcal{T}$, the set $\mathcal{T}_{\preceq a} = \{m \preceq a,\ m \in \mathcal{T}\}$ is finite. Such an ordering $\prec$ makes $(\mathbb{N}^n, \prec)$ isomorphic to $(\mathbb{N}, <)$ as an ordered set. Hence, for a monomial $m$, it makes sense to speak about the previous (resp. next) monomial $m^-$ (resp. $m^+$) for $\prec$. The DRL ordering is an example for an ordering on which every term other than 1 has an immediate predecessor.

This request excludes for instance the LEX ordering, and more generally any elimination ordering. In other words, only weighted degree ordering, or *weight ordering*, should be used.

Now that a monomial ordering is defined, we can say that a relation given by a polynomial $f \in \mathbb{K}[\mathbf{x}]$ *fails when shifted by* $s$ if for all monomials $\sigma \prec s$, $[\sigma f] = 0$ but $[s f] \neq 0$, see also [28, 29].

### *2.3. Multi-Hankel matrices*

A matrix $H \in \mathbb{K}^{m \times n}$ is *Hankel*, if there exists a sequence $\mathbf{w} = (w_i)_{i \in \mathbb{N}}$ such that for all $(i, i') \in \{1, \ldots, m\} \times \{1, \ldots, n\}$, the coefficient $h_{i,i'}$ lying on the $i$th row and $i'$th column of $H$ satisfies $h_{i,i'} = w_{i+i'}$.

In a multivariate setting, we can extend this notion to *multi-Hankel* matrices. For two sets of monomials $U$ and $T$, we let $H_{U,T}$ be the multi-Hankel matrix with rows (resp. columns) indexed with $U$ (resp. $T$) so that the coefficient of $H_{U,T}$ lying on the row labeled with $\mathbf{x}^{\mathbf{i}} \in U$ and column labeled with $\mathbf{x}^{\mathbf{i}'} \in T$ is $w_{\mathbf{i}+\mathbf{i}'}$.

**Example 7.** *Let* $\mathbf{w} = (w_{i,j,k})_{(i,j,k) \in \mathbb{N}^3}$ *be a sequence.*

1. *For* $U = \{1, z, z^2, y, yz, yz^2\} = \{1, z, z^2\} \cup y\{1, z, z^2\}$ *and* $T = \{1, z, y, yz, y^2, y^2 z\} = \{1, z\} \cup y\{1, z\} \cup y^2\{1, z\}$*, ordered for* LEX$(z \prec y \prec x)$*,*

$$H_{U,T} = \begin{array}{c} \\ 1 \\ z \\ z^2 \\ y \\ yz \\ yz^2 \end{array} \begin{array}{c} \begin{array}{cc|cc|cc} 1 & z & y & yz & y^2 & y^2 z \end{array} \\ \left(\begin{array}{cc|cc|cc} w_{0,0,0} & w_{0,0,1} & w_{0,1,0} & w_{0,1,1} & w_{0,2,0} & w_{0,2,1} \\ w_{0,0,1} & w_{0,0,2} & w_{0,1,1} & w_{0,1,2} & w_{0,2,1} & w_{0,2,2} \\ w_{0,0,2} & w_{0,0,3} & w_{0,1,2} & w_{0,1,3} & w_{0,2,2} & w_{0,2,3} \\ \hline w_{0,1,0} & w_{0,1,1} & w_{0,2,0} & w_{0,2,1} & w_{0,3,0} & w_{0,3,1} \\ w_{0,1,1} & w_{0,1,2} & w_{0,2,1} & w_{0,2,2} & w_{0,3,1} & w_{0,3,2} \\ w_{0,1,2} & w_{0,1,3} & w_{0,2,2} & w_{0,2,3} & w_{0,3,2} & w_{0,3,3} \end{array}\right) \end{array}$$

   *is a* $2 \times 3$*-block-Hankel matrix with* $3 \times 2$*-Hankel blocks.*

2. *For* $\tilde{U} = U \cup xU \cup x^2 U \cup x^3 U$ *and* $\tilde{T} = T \cup xT \cup x^2 T \cup x^3 T \cup x^4 T$*, also ordered for* LEX$(z \prec y \prec x)$*,*

$$H_{\tilde{U},\tilde{T}} = \begin{array}{c} \\ U \\ xU \\ x^2 U \\ x^3 U \end{array} \begin{array}{c} \begin{array}{ccccc} T & xT & x^2 T & x^3 T & x^4 T \end{array} \\ \left(\begin{array}{ccccc} H_{U,T} & H_{U,xT} & H_{U,x^2 T} & H_{U,x^3 T} & H_{U,x^4 T} \\ \hline H_{xU,T} & H_{xU,xT} & H_{xU,x^2 T} & H_{xU,x^3 T} & H_{xU,x^4 T} \\ \hline H_{x^2 U,T} & H_{x^2 U,xT} & H_{x^2 U,x^2 T} & H_{x^2 U,x^3 T} & H_{x^2 U,x^4 T} \\ \hline H_{x^3 U,T} & H_{x^3 U,xT} & H_{x^3 U,x^2 T} & H_{x^3 U,x^3 T} & H_{x^3 U,x^4 T} \end{array}\right) \end{array},$$

   *where* $H_{x^i U,x^{i'} T} = H_{x^{i+i'} U,T}$ *for any* $i, i'$ *since* $H_{x^i U,x^{i'} T}$ *is the same matrix as* $H_{U,T}$ *where each coefficient* $w_{0,j,k}$ *has been replaced by* $w_{i+i',j,k}$*. Therefore,* $H_{\tilde{U},\tilde{T}}$ *is a* $4 \times 5$-block-Hankel *matrix with* $6 \times 6$*-multi-Hankel blocks like* $H_{U,T}$*.*

3. *For* $T = \{1, y, x, y^2, xy, x^2\}$*, ordered for* DRL$(z \prec y \prec x)$*,* $H_{T,T}$ *is a multi-Hankel matrix whose structure is less clear. It can be considered as a block-Hankel matrix with blocks of*

*different sizes, noticing that* $T = \{1\} \cup y\left\{1, \frac{x}{y}\right\} \cup y^2\left\{1, \frac{x}{y}, \frac{x^2}{y^2}\right\}$,

$$H_{T,T} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ xy \\ x^2 \end{array} \begin{array}{c} \begin{array}{ccc|cc|c} 1 & y & x & y^2 & xy & x^2 \end{array} \\ \left(\begin{array}{ccc|cc|c} w_{0,0,0} & w_{0,1,0} & w_{1,0,0} & w_{0,2,0} & w_{1,1,0} & w_{2,0,0} \\ \hline w_{0,1,0} & w_{0,2,0} & w_{1,1,0} & w_{0,3,0} & w_{1,2,0} & w_{2,1,0} \\ w_{1,0,0} & w_{1,1,0} & w_{2,0,0} & w_{1,2,0} & w_{2,1,0} & w_{3,0,0} \\ \hline w_{0,2,0} & w_{0,3,0} & w_{1,2,0} & w_{0,4,0} & w_{1,3,0} & w_{2,2,0} \\ w_{1,1,0} & w_{1,2,0} & w_{2,1,0} & w_{1,3,0} & w_{2,2,0} & w_{3,1,0} \\ w_{2,0,0} & w_{2,1,0} & w_{3,0,0} & w_{2,2,0} & w_{3,1,0} & w_{4,0,0} \end{array}\right) \end{array}.$$

4. *For* $U = \{1, z, y, x, z^2, yz, xz, y^2, xy, x^2\} = \{1\} \cup z\left\{1, \frac{y}{z}, \frac{x}{z}\right\} \cup z^2\left\{1, \frac{y}{z}, \frac{x}{z}, \frac{y^2}{z^2}, \frac{xy}{z^2}, \frac{x^2}{z^2}\right\}$, *also ordered for* DRL$(z \prec y \prec x)$, *the matrix* $H_{U,U}$ *can be seen as a block-matrix like* $H_{T,T}$ *except each block is a multi-Hankel matrix in two variables. In fact, the bottom-right block would be the same as* $H_{T,T}$ *where each coefficient* $w_{i,j,0}$ *is replaced by* $w_{i,j,4-i-j}$.

### *2.4. Polynomials associated to multi-Hankel matrices*

For two sets of terms $T$ and $U$, we let $T + U$ denote their Minkowski sum, i.e. $T + U = \{t\,u,\ t \in T, u \in U\}$, and $2\,T = T + T$.

For a set of terms $T$, we let $M = \text{LCM}(T)$. We let $P_T$ be the mirror polynomial of the truncated generating series of a sequence $\mathbf{w}$, i.e.

$$P_T = \sum_{t \in T} [t]\,\frac{M}{t}.$$

**Example 8.** *Let* $\mathbf{w} = (w_{i,j,k})_{(i,j,k)\in\mathbb{N}^3}$ *be a sequence and* $T = \{1, z, y, x, z^2, yz\}$, *then* $M = xyz^2$ *and*

$$\begin{aligned} P_T &= [1]\,xyz^2 + [z]\,xyz + [y]\,xz^2 + [x]\,yz^2 + [z^2]\,xy + [yz]\,xz \\ &= w_{0,0,0}\,xyz^2 + w_{0,0,1}\,xyz + w_{0,1,0}\,xz^2 + w_{1,0,0}\,yz^2 + w_{0,0,2}\,xy + w_{0,1,1}\,xz. \end{aligned}$$

In this paper, we will mostly deal with polynomials $P_{T+U}$ as there is a strong connection between $H_{U,T}$ and $P_{T+U}$.

Finally, letting $M = \text{LCM}(T+U) = x_1^{D_1} \cdots x_n^{D_n}$ and $B$ be the monomial ideal $(x_1^{D_1+1}, \ldots, x_n^{D_n+1})$, we will use pairs of multivariate polynomials $R_m = [F_m, C_m]$. If $m \in B$, then we set $F_m = m$ and $C_m = 0$. Otherwise, $\text{LM}(C_m) = m$ and $F_m = P_{T+U}\,C_m \bmod B$.

## 3. From matrices to polynomials

Before detailing the unified polynomial viewpoint, we recall the linear algebra viewpoint of the BM, the BMS and the Scalar-FGLM algorithms.

### *3.1. The* BM *algorithm*

Let $\mathbf{w} = (w_i)_{i\in\mathbb{N}}$ be a one-dimensional table. Classically, when calling the BM algorithm, one does not know in advance the order of the output relation. Therefore, from a matrix viewpoint,

one wants to compute the greatest collection of vectors

$$\begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{x^{d-1}} \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \gamma_1 \\ \vdots \\ \gamma_{x^{d-1}} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ \gamma_1 \\ \vdots \\ \gamma_{x^{d-1}} \\ 1 \end{pmatrix}$$

in the kernel of $H_{\{1\},\{1,\ldots,x^D\}} = \begin{matrix} 1 & \cdots & x^D \end{matrix} \begin{pmatrix} w_0 & \cdots & w_D \end{pmatrix}$, that is $\gamma_1, \ldots, \gamma_{x^{d-1}} \in \mathbb{K}$ such that the relation $[C_{x^d}] = w_d + \sum_{k=0}^{d-1} \gamma_{x^k} w_k$ and its shifts, $[x\, C_{x^d}], \ldots, [x^{D-d}\, C_{x^d}]$, are all 0. Equivalently, we look for the least $d$ such that $H_{\mathcal{T}_{\leq x^{D-d}}, \mathcal{T}_{\leq x^d}} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{x^{d-1}} \\ 1 \end{pmatrix} = 0$.

This Hankel matrix-vector product can be extended into

$$\begin{pmatrix} w_0 & \cdots & w_{d-1} & w_d \\ w_1 & \cdots & w_d & w_{d+1} \\ \vdots & & \vdots & \vdots \\ w_{D-d} & \cdots & w_{D-1} & w_D \\ w_{D-d+1} & \cdots & w_D & 0 \\ \vdots & \iddots & \iddots & \vdots \\ w_D & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{x^{d-1}} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ f_{x^{d-1}} \\ \vdots \\ f_1 \end{pmatrix}, \tag{2}$$

representing the product of polynomials $P_{\mathcal{T}_{\leq x^D}} = \sum_{i=0}^{D} w_i\, x^{D-i}$ and $C_{x^d} = x^d + \sum_{k=0}^{d-1} \gamma_{x^k}\, x^k$ modulo $B = x^{D+1}$. The requirement for $C_{x^d}$ to encode a valid relation is now that $\mathrm{LM}(F_{x^d}) \prec x^d$ with $F_{x^d} = P_{\mathcal{T}_{\leq x^D}}\, C_{x^d} \bmod B$.

This viewpoint gives rise to the following version of the BM algorithm: Start with $R_B = [F_B, C_B] = [B, 0]$ and $B = x^{D+1}$, and $R_1 = [F_1, C_1] = [P_{\mathcal{T}_{\leq x^D}}, 1]$. Compute the quotient $Q$ of the Euclidean division of $F_B = B$ by $F_1$ and then compute $R_{\mathrm{LM}(Q)} = R_B - Q\, R_1 = [F_B - Q\, F_1, C_B - Q\, C_1] = [F_{\mathrm{LM}(Q)}, C_{\mathrm{LM}(Q)}]$. Repeat with $R_1$ and $R_{\mathrm{LM}(Q)}$ until reaching a pair $R_{x^d} = [P_{\mathcal{T}_{\leq x^D}}\, C_{x^d} \bmod B, C_{x^d}] = [F_{x^d}, C_{x^d}]$ with $\mathrm{LM}(C_{x^d}) = x^d$ and $\mathrm{LM}(F_{x^d}) \prec x^d$. This is in fact the extended Euclidean algorithm called on $B = x^{D+1}$ and $F_1$ without any computation of the Bézout's cofactors of $x^{D+1}$.

**Example 9.** *Let us consider the Fibonacci table* $\mathbf{F} = (F_i)_{i \in \mathbb{N}}$ *with* $F_0 = F_1 = 1$ *and assume* $D = 5$. *On the one hand, although the kernel of*

$$H_{\{1\},\{1,x,x^2,x^3,x^4,x^5\}} = \begin{matrix} 1 & x & x^2 & x^3 & x^4 & x^5 \end{matrix} \begin{pmatrix} 1 & 1 & 2 & 3 & 5 & 8 \end{pmatrix}$$

*has dimension* 5 *and* $\begin{pmatrix} -1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *is in this kernel, it corresponds to* $[x - 1] = 0$, *its shifted vectors* $\begin{pmatrix} 0 \\ -1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ 1 \end{pmatrix}$ *are not, as they correspond to* $[x^i\,(x-1)] \neq 0$, *for* $1 \leq i \leq 4$. *However,*

*these vectors*

$$\begin{pmatrix}-1\\-1\\1\\0\\0\\0\end{pmatrix},\begin{pmatrix}0\\-1\\-1\\1\\0\\0\end{pmatrix},\begin{pmatrix}0\\0\\-1\\-1\\1\\0\end{pmatrix},\begin{pmatrix}0\\0\\0\\-1\\-1\\1\end{pmatrix}$$

*are in the kernel and form the greatest collection of shifted vectors as such. They correspond to* $[x^i\,(x^2 - x - 1)] = 0$*, for* $0 \le i \le 3$*. Finally, we have*

$$\begin{pmatrix}1&1&2\\1&2&3\\2&3&5\\3&5&8\\5&8&0\\8&0&0\end{pmatrix}\begin{pmatrix}-1\\-1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\\-13\\-8\end{pmatrix},$$

*where the gray zeroes (*0*) are due to the matrix extension and not the sequence itself.*

*On the other hand,* $B = x^6$*,* $R_B = [B, 0]$ *and* $R_1 = [x^5 + x^4 + 2\,x^3 + 3\,x^2 + 5\,x + 8, 1]$*. As we can see* $R_1 = [F_1, C_1]$ *with* $\text{LM}(C_1) = 1$ *and* $\text{LM}(F_1) = x^5 \ge 1$*.*

*The first step of the extended Euclidean algorithm yields* $R_x = [x^4 + x^3 + 2\,x^2 + 3\,x - 8, x - 1] = [F_x, C_x]$ *with* $\text{LM}(C_x) = x$ *and* $\text{LM}(F_x) = x^4 \ge x$*.*

*Then, the second step yields* $R_{x^2} = [-13\,x - 8, x^2 - x - 1] = [F_{x^2}, C_{x^2}]$ *with* $\text{LM}(C_{x^2}) = x^2$ *and* $\text{LM}(F_{x^2}) = x \prec x^2$ *so* $C_{x^2}$ *is a valid relation. We return* $C_{x^2}$*.*

**Remark 10.** *The* BM *algorithm always returns a non-zero relation. If no pair* $R_{x^\delta} = [F_{x^\delta}, C_{x^\delta}]$ *satisfies the requirements, then it will return a pair* $R_{x^d}$ *with* $\text{LM}(C_{x^d}) \succ x^D$*. From a matrix viewpoint, it returns an element of the kernel of the empty matrix* $H_{\emptyset,\mathcal{T}_{\preceq x^d}}$*.*

### *3.2. Multidimensional extension*

In this section, we show how to extend Section 3.1 to multidimensional sequences. Subsection 3.2.1 corresponds to the BMS algorithm. We shall see that this extension is the closest to the BM algorithm. Then, Subsection 3.2.2 corresponds to the Scalar-FGLM, which, in some way, is more general.

#### *3.2.1. The* BMS *algorithm*

For a multidimensional table $\mathbf{w} = (w_\mathbf{i})_{\mathbf{i}\in\mathbb{N}^n}$, the BMS algorithm extends the BM algorithm by computing vectors in the kernel of a multi-Hankel matrix

$$H_{\{1\},\mathcal{T}_{\preceq a}} = \begin{array}{c} \begin{matrix}1 & \cdots & a^- & a\end{matrix}\\ \begin{pmatrix}[1] & \cdots & [a^-] & [a]\end{pmatrix}\end{array}$$

corresponding to having relations $[C_g] = 0$, with $\text{LM}(C_g) = g$ minimal for the division and for all $t$ such that $t\,g \preceq a$, $[t\,C_g] = 0$ as well. This also comes down to finding the least (for the partial order $|$) monomials $g_1, \ldots, g_r \preceq a$ such that $\dim\ker H_{\mathcal{T}_{\preceq s_k},\mathcal{T}_{\preceq g_k}} > 0$ with $s_k$ the greatest monomial such that $s_k\,g_k \preceq a$ for all $k$, $1 \le k \le r$. Then, each multi-Hankel matrix-vector product can be

extended further as in equation (2), taking the multi-Hankel matrix $H_{\mathcal{T}_{\preceq a},\mathcal{T}_{\preceq g_k}}$ and setting to zero any sequence term $[t\,u]$ with $t\,u \notin \mathcal{T}_{\preceq a}$.

$$\begin{pmatrix} [1] & \cdots & [g_k^-] & [g_k] \\ [1^+] & \cdots & [1^+\,g_k^-] & [1^+\,g_k] \\ \vdots & & \vdots & \vdots \\ [s_k] & \cdots & [s_k\,g_k^-] & [s_k\,g_k] \\ [s_k^+] & \cdots & [s_k^+\,g_k^-] & 0 \\ \vdots & & \iddots & \vdots \\ [a] & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{g_k^-} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ f_{M/s_k^+} \\ \vdots \\ f_{M/a} \end{pmatrix}, \tag{3}$$

where $M = \text{LCM}(\mathcal{T}_{\preceq a}) = x_1^{D_1} \cdots x_n^{D_n}$. It then represents the product of polynomials $P_{\mathcal{T}_{\preceq a}} = \sum_{t \preceq a} [t]\,\frac{M}{t}$ and $C_{g_k} = g_k + \sum_{t \prec g_k} \gamma_t\,t$ modulo $B = (x_1^{D_1+1}, \ldots, x_n^{D_n+1})$. The requirement for $C_{g_k}$ to encode a valid relation is now that $\text{LM}(F_{g_k}) \prec \frac{M}{s_k}$ with $F_{g_k} = P_{\mathcal{T}_{\preceq a}}\,C_{g_k} \bmod B$.

Let us notice that $[s_k^+\,g_k^-]$ can also be a 0 if $s_k^+\,g_k^- \succ a$ and that, more generally, the gray zeroes need not be diagonally aligned like they are in the univariate case. This is illustrated by the following example.

**Example 11.** *Let us consider the binomial table* $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$ *with* $\text{DRL}(y \prec x)$ *and assume* $a = x^2\,y$. *The kernel of*

$$H_{\{1\},\mathcal{T}_{\preceq x^2 y}} = \begin{array}{c} \begin{matrix} 1 & y & x & y^2 & x\,y & x^2 & y^3 & x\,y^2 & x^2\,y \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 2 \end{pmatrix} \end{array}$$

*has clearly dimension* 8. *Two vectors in the kernel,* $\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *and* $\begin{pmatrix} -1 \\ \alpha \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, *with* $\alpha$ *any number in* $\mathbb{K}$, *correspond to the independent relations* $[y] = 0$ *and* $[x + \alpha\,y - 1] = 0$. *However, not all their shifts belong to the kernel. For the former,* $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, *corresponding to* $[y^2] = 0$, *belongs to the kernel but* $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *does not, as* $[x\,y] \neq 0$. *For the latter,* $\begin{pmatrix} 0 \\ -1 \\ 0 \\ \alpha \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ *does not belong to the kernel, as* $[x\,y + \alpha\,y^2 - y] \neq 0$, *whatever* $\alpha$ *is.*

*Therefore, the vectors in the kernel that we seek must correspond to relations* $[C_g] = 0$ *with* $g \in \{y^2, x\,y, x^2, \ldots, x^2\,y\}$.

*In fact, as* $[m\,y^2] = 0$ *for* $1 \preceq m \preceq x$, *the vectors* $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$, *are in the kernel and fulfill*

*the requirements. We can indeed notice that*

$$H_{\mathcal{T}_{\leq x},\mathcal{T}_{\leq y^2}} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{matrix} \\ 1 \\ y \\ x \end{matrix} \begin{matrix} \begin{matrix} 1 & y & x & y^2 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix} \end{matrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{matrix} \\ 1 \\ y \\ x \\ y^2 \\ xy \\ x^2 \\ y^3 \\ xy^2 \\ x^2y \end{matrix} \begin{matrix} \begin{matrix} 1 & y & x & y^2 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 \end{pmatrix} \end{matrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix},$$

*where the gray zeroes (0) are due to the matrix extension and not the binomial sequence itself. From the polynomial point of view,*

$$\begin{aligned} F_{y^2} &= P_{\mathcal{T}_{\leq x^2 y}} C_{y^2} \bmod B \\ &= (x^2 y^3 + x y^3 + x y^2 + y^3 + 2 y^2)\, y^2 \bmod (x^3, y^4) \\ &= 0. \end{aligned}$$

*Likewise, the vectors* $\begin{pmatrix} -(1+\alpha) \\ \beta \\ \alpha \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -(1+\alpha) \\ 0 \\ \beta \\ \alpha \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ -(1+\alpha) \\ 0 \\ \beta \\ \alpha \\ 0 \\ 0 \\ 1 \end{pmatrix}$*, are in the kernel for* $\alpha = 0$ *and* $\beta = -1$*, as they correspond to* $[m\,(x\,y + \alpha\,x + \beta\,y - (1+\alpha))] = [m\,(x\,y - y - 1)] = 0$*, for* $1 \preceq m \preceq x$*. Furthermore,*

$$\begin{matrix} \\ 1 \\ y \\ x \\ y^2 \\ xy \\ x^2 \\ y^3 \\ xy^2 \\ x^2y \end{matrix} \begin{matrix} \begin{matrix} 1 & y & x & y^2 & xy \end{matrix} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \end{pmatrix} \end{matrix} \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ -1 \\ -3 \\ 0 \\ 0 \\ -2 \end{pmatrix},$$

*From the polynomial point of view,* $F_{xy} = P_{\mathcal{T}_{\leq x^2 y}}\,(x\,y - y - 1) \bmod (x^3, y^4) = -x\,y^2 - 3\,y^3 - 2\,y^2$*.*

*Finally, the vectors* $\begin{pmatrix} -(1+\alpha) \\ \beta \\ \alpha \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -(1+\alpha) \\ 0 \\ \beta \\ \alpha \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$*, are in the kernel for* $\alpha = -2$ *and* $\beta = 0$*, as they*

*correspond to* $[m\,(x^2+\alpha\,x+\beta\,y-(1+\alpha))] = [m\,(x^2-2\,x+1)] = 0$*, for* $1 \preceq m \preceq y$*. Furthermore,*

$$\begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ x\,y \\ x^2 \\ y^3 \\ x\,y^2 \\ x^2\,y \end{array}\!\!\begin{array}{c} \begin{array}{cccccc} 1 & y & x & y^2 & x\,y & x^2 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 2 \\ 1 & 1 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array} \begin{pmatrix} 1 \\ 0 \\ -2 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -1 \\ 0 \\ -3 \\ 1 \\ 0 \\ 0 \\ 2 \end{pmatrix}.$$

*From the polynomial point of view,* $F_{x^2} = P_{\mathcal{T}_{\preceq x^2\,y}}\,(x^2-2\,x+1) \bmod (x^3, y^4) = -x\,y^3 - 3\,x\,y^2 + y^3 + 2\,y^2$.

*The* BMS *algorithm will return the three relations* $C_{y^2} = y^2$, $C_{x\,y} = x\,y - y - 1$ *and* $C_{x^2} = x^2 - 2\,x + 1$.

**Remark 12.** *As for the* BM *algorithm, the* BMS *algorithm will always return a relation* $C_g$ *with* $\text{LM}(C_g) = g$ *a pure power in each variable. Therefore, it can return* $C_g$ *with* $g \succ a$*, corresponding to a vector in the kernel of the empty matrix* $H_{\emptyset,\mathcal{T}_{\preceq g}}$.

### *3.2.2. The* Scalar-FGLM *algorithm*

The Scalar-FGLM algorithm aims to compute vectors in the kernel of a more general multi-Hankel matrix $H_{U,T}$, with $T$ and $U$ two ordered sets of monomials. The kernel vectors that we wish to compute are those corresponding to relations $[uC_g] = 0$ with $\text{LM}(C_g) = g$ and $u \in U$, such that for all $t \in \mathcal{T}$, if $t\,g \in T$, then $[u\,t\,C_g] = 0$. In other words, if the vector corresponding to $C_g$ is in the kernel, then for all $t$ with $t\,g \in T$, so is the vector corresponding to $t\,C_g$.

Let us assume that both sets of terms $T$ and $U$ satisfy $T = \mathcal{T}_{\preceq a}$ and $U = \mathcal{T}_{\preceq b}$. This allows us to encompass both the BMS algorithm and the Scalar-FGLM algorithm.

The goal is to extend the multi-Hankel matrix-vector product

$$\begin{array}{c} \\ 1 \\ \vdots \\ b^- \\ b \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 1 & \cdots & a^- & a \end{array} \\ \begin{pmatrix} [1] & \cdots & [a^-] & [a] \\ \vdots & & \vdots & \vdots \\ [b^-] & \cdots & [a^-\,b^-] & [a\,b^-] \\ [b] & \cdots & [a^-\,b] & [a\,b] \end{pmatrix} \end{array} \begin{pmatrix} \gamma_1 \\ \vdots \\ \gamma_{g^-} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \tag{4}$$

in a similar fashion as in equations (2) and (3) with as many rows as possible and setting any table term $[t\,u]$ to zero whenever $t\,u \succ a\,b$.

For $C_g$ a relation, we want to build a multi-Hankel matrix $H_{U,T}$ whose kernel contains the vector corresponding to $C_g$ if, and only if, the vectors corresponding to $t\,C_g$ are in the kernel of $H_{\mathcal{T}_{\preceq b},\mathcal{T}_{\preceq a}}$. This is achieved by choosing $T = \mathcal{T}_{\preceq g} = \{1, \ldots, g\}$ and picking, for each $t$, the rows labeled with $\{t, \ldots, b\,t\} = \mathcal{T}_{\preceq b} + \{t\}$. Thus, the set of all rows is $U = \mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$ where $s$ is the largest monomial such that $s\,g \preceq a$.

Now, we can expand this matrix by adding rows up to $a\,b$ and setting table terms $[t\,u]$ to 0 whenever $t\,u \succ a\,b$. Yet, since the first rows are in $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$ and the set of rows should be stable by division, we remove from $\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b}$ any multiple of a monomial in $\mathcal{T}_{\preceq b\,s} \setminus (\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s})$.

It remains to make the link between this matrix-vector product and the product of the two polynomials $P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}$ and $C_g$ modulo $B = (x_1^{D_1+1}, \ldots, x_n^{D_n+1})$. Note that since $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} \subseteq \mathcal{T}_{\preceq b\,s}$ but may not be equal to $\mathcal{T}_{\preceq b\,s}$, the leading monomial of $F_g = P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}\,C_g \bmod B$ is $\frac{M}{u}$ with $u$ a multiple of a monomial that may not be in $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$. We let $\tilde{F}_g$ be the same polynomial as $F_g$ where we set to zero any monomial $\frac{M}{u}$ in $F_g$ with $u$ a multiple of a monomial in $\mathcal{T}_{\preceq b\,s} \setminus (\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s})$. Since the monomials $\frac{M}{u}$ with $u \in \mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$ are now the largest possible monomials in $\tilde{F}_g$, $C_g$ is a valid relation if, and only if, $\textsc{lm}(\tilde{F}_g) \prec \frac{M}{b\,s}$.

**Proposition 13.** *Let $T = \mathcal{T}_{\preceq a}$ and $U = \mathcal{T}_{\preceq b}$ be finite sets of monomials in $\mathbb{K}[\mathbf{x}]$, let $M = \textsc{lcm}(T + U) = x_1^{D_1} \cdots x_n^{D_n}$ and $B = (x_1^{D_1+1}, \ldots, x_n^{D_n+1})$.*

*Let $C_g$ be a polynomial with support in $T$ and with leading monomial $g$ and let $s$ be the greatest monomial such that $s\,g \preceq a$.*

*Let $\mathcal{G}_s$ be a minimal set of monomials generating the sets of monomials less than $b\,s$ but not in $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$, i.e. $\mathcal{G}_s$ is a reduced Gröbner basis of the monomial ideal generated by $\mathcal{T}_{\preceq b\,s} \setminus (\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s})$.*

*Let $\tilde{F}_g$ be the polynomial obtained by setting to zero all the coefficients of monomials $\frac{M}{u}$ of $F_g = P_{T+U}\,C_g \bmod B = \sum_{\tau\in(T+U)} f_{g,\tau}\,\frac{M}{\tau}$, with $u \in \langle \mathcal{G}_s \rangle$. That is, $\tilde{F}_g = \sum_{\tau\in(T+U)} \tilde{f}_{g,\tau}\,\frac{M}{\tau}$, where $\text{NormalForm}\left(\sum_{\tau\in(T+U)} f_{g,\tau}\,\tau, \mathcal{G}_s\right) = \sum_{\tau\in(T+U)} \tilde{f}_{g,\tau}\,\tau$.*

*Then, $[u\,t\,C_g] = 0$ for all $u \in U$ and all $t \in \mathcal{T}_{\preceq s}$ if, and only if, $\textsc{lm}(\tilde{F}_g) \prec \frac{M}{b\,s}$.*

**Example 14.** *We still consider the binomial table* **b** *with* $\textsc{drl}(y \prec x)$. *We let $a = b = x\,y^2$ so that $T = U = \mathcal{T}_{\preceq x\,y^2}$*

$$H_{U,T} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ x\,y \\ x^2 \\ y^3 \\ x\,y^2 \end{array} \begin{array}{c} \begin{array}{cccccccc} 1 & y & x & y^2 & x\,y & x^2 & y^3 & x\,y^2 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & 0 & 0 \\ 1 & 1 & 1 & 0 & 2 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 2 & 0 & 1 & 3 & 0 & 0 \\ 1 & 2 & 1 & 1 & 3 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 3 & 0 & 0 \end{pmatrix} \end{array}.$$

*The computation of the kernel of this matrix yields the vectors* $\begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ -1 \\ 0 \\ -1 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ *corresponding to* $[u\,(x\,y - y - 1)] = [u\,y\,(x\,y - y - 1)] = 0$ *for all $u \in U$ and the vector* $\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$ *corresponding to* $[u\,y^3] = 0$ *for all $u \in U$.*

*For $g = x\,y$, since $g\,y = x\,y^2 = a$, we have $s = y$. Then, $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x\,y^2} + \mathcal{T}_{\preceq y} = \mathcal{T}_{\preceq x\,y^3} \setminus \{x^3\}$. Thus, we do not add any row with label multiple of $x^3$ in the extended matrix-vector product. That*

*is, the set of rows of the extended matrix is* $(\mathcal{T}_{\leq xy^2} + \mathcal{T}_{\leq xy^2}) \setminus \{x^3, x^3\,y, x^4, x^3\,y^2\}$*:*

$$
\begin{array}{c}
\\
1 \\ y \\ x \\ y^2 \\ x\,y \\ x^2 \\ y^3 \\ x\,y^2 \\ x^2\,y \\ x^3 \\ y^4 \\ x\,y^3 \\ x^2\,y^2 \\ x^3\,y \\ x^4 \\ y^5 \\ x\,y^4 \\ x^2\,y^3 \\ x^3\,y^2 \\ y^6 \\ x\,y^5 \\ x^2\,y^4
\end{array}
\begin{array}{c}
\begin{array}{ccccc} 1 & y & x & y^2 & x\,y \end{array} \\
\begin{pmatrix}
1 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 0 & 2 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 2 & 0 & 1 \\
1 & 2 & 1 & 1 & 3 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 \\
2 & 1 & 3 & 0 & 3 \\
1 & 3 & 1 & 3 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
1 & 0 & 3 & 0 & 0 \\
3 & 3 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0
\end{pmatrix}
\end{array}
\begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}
=
\begin{pmatrix}
0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ -4 \\ 0 \\ 0 \\ -1 \\ -6 \\ -1 \\ 0 \\ 0 \\ 0 \\ 3 \\ 0 \\ 0 \\ 0
\end{pmatrix}.
$$

*From the polynomial viewpoint,* $F_{xy} = P_{T+U}\,(x\,y - y - 1) \bmod (x^5, y^7) = -4\,x\,y^6 - x^2\,y^4 - 6\,x\,y^5 - y^6 - 3\,x\,y^4$ *so that* $\tilde{F}_{xy} = -x^2\,y^4 = \sum_{\tau\in(T+U)} \tilde{f}_{g,\tau}\,\frac{M}{\tau}$*. The vector* $\begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$ *being in the kernel of* $H_{\mathcal{T}_{\leq xy^2}+\mathcal{T}_{\leq y},\mathcal{T}_{\leq xy}}$ *is then equivalent to asking that* $\textsc{lm}(\tilde{F}_{xy}) \prec \frac{M}{b\,s} = \frac{x^4\,y^6}{x\,y^3} = x^3\,y^3$*. Notice that this condition is not satisfied by* $F_{xy}$ *since* $\textsc{lm}(F_{xy}) = x\,y^6$*.*

*For* $g = y^3$*, since* $a = x\,y^2$*, we have* $s = 1$*. Then,* $\mathcal{T}_{\leq g} + \mathcal{T}_{\leq s} = \mathcal{T}_{\leq y^3} + \mathcal{T}_{\leq 1} = \mathcal{T}_{\leq y^3}$*, thus we add*

*all the rows from* $\mathcal{T}_{\preceq x y^2} + \mathcal{T}_{\preceq x y^2}$.

$$
\begin{array}{c}
 \\
1 \\
y \\
x \\
y^2 \\
x\,y \\
x^2 \\
y^3 \\
x\,y^2 \\
x^2\,y \\
x^3 \\
y^4 \\
x\,y^3 \\
x^2\,y^2 \\
x^3\,y \\
x^4 \\
y^5 \\
x\,y^4 \\
x^2\,y^3 \\
x^3\,y^2 \\
y^6 \\
x\,y^5 \\
x^2\,y^4
\end{array}
\begin{array}{c}
\begin{array}{ccccccc} 1 & y & x & y^2 & x\,y & x^2 & y^3 \end{array} \\
\begin{pmatrix}
1 & 0 & 1 & 0 & 1 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 2 & 0 \\
1 & 1 & 1 & 0 & 2 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 2 & 0 & 1 & 3 & 0 \\
1 & 2 & 1 & 1 & 3 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 3 & 0 \\
2 & 1 & 3 & 0 & 3 & 0 & 0 \\
1 & 3 & 1 & 3 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 3 & 0 & 0 & 0 & 0 \\
3 & 3 & 0 & 0 & 0 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
3 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix}
\end{array}
\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}
=
\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.
$$

*The polynomial* $F_{y^3} = P_{T+U}\, y^3 \bmod (x^5, y^7) = 0$*, so that* $\tilde{F}_{y^3} = 0$*. Trivially,* $\textsc{lm}(\tilde{F}_{y^3})$ *satisfies any constraint on its leading monomial, in particular* $\textsc{lm}(\tilde{F}_{y^3}) \prec \frac{M}{b\,s} = \frac{x^4 y^6}{x y^2} = x^2\, y^4$.

## 4. A division-based algorithm

The goal is now to design an algorithm based on polynomial division to determine all the $C_g$ for $|$-minimal $g$ such that $\textsc{lm}(\tilde{F}_g)$ is small enough, where $F_g = P_{T+U}\, C_g \bmod B$ and $\tilde{F}_g$ is obtained from $F_g$ as in Proposition 13.

We start with two sets of terms $T = \mathcal{T}_{\preceq a}$ and $U = \mathcal{T}_{\preceq b}$ so that $M = x_1^{D_1} \cdots x_n^{D_n} = \textsc{lcm}(T + U)$. We initialize $B = (B_1, \ldots, B_n) = (x_1^{D_1+1}, \ldots, x_n^{D_n+1})$, $R_{B_1} = [B_1, 0], \ldots, R_{B_n} = [B_n, 0]$ and $R_1 = [P_{T+U}, 1]$.

For any monomial $g$ not in the ideal spanned by $B$ and $R_g = [F_g, C_g] = [P_{T+U}\, C_g \bmod B, C_g]$, by Proposition 13, $C_g$ is a valid relation if $g \in T$ and $\textsc{lm}(\tilde{F}_g) \prec \frac{M}{b\,s}$ with $s = \max\{\sigma,\ \sigma\, g \preceq a\}$. To go along with the fact that the BMS algorithm always returns a relation $C_g$ with $g = \textsc{lm}(C_g)$ a pure power of a variable, if $g \notin T$, then $C_g$ will automatically be considered a valid relation as well.

From a failing relation $C_m$, we get that $m$ is in the staircase of the Gröbner basis of relations. Thus, each time a built relation is not valid, we update the staircase of the ideal of relations. At each step, we know a staircase $S$ which is a subset of the output and target staircase. Equivalently, we know the set $\mathcal{H} = \min_{|}\{h \in \mathcal{T} \setminus S\}$ which are the leading terms of the candidate relations.

The algorithm uses the following subroutines

NormalForm($R_{m'}, [R_m, R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_r}]$)**,** for computing the *normal form* of $[F_{m'}, C_{m'}]$ wrt. the list $R_m, R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_r}$ with $\text{LM}(F_{t_1}) \succ \cdots \succ \text{LM}(F_{t_r})$. To do so, it computes first $Q_m, Q_{B_1}, \ldots, Q_{B_n}, Q_{t_1}, \ldots, Q_{t_r}$ the quotients of the division of $F_{m'}$ by the list of polynomials $[F_m, B_1, \ldots, B_n, F_{t_1}, \ldots, F_{t_r}]$ and then return $R_h = R_{m'} - Q_m R_m - Q_{B_1} R_{B_1} - \cdots - Q_{B_n} R_{B_n} - Q_{t_1} R_{t_1} - \cdots - Q_{t_r} R_{t_r}$.

Stabilize($S$)**,** for computing the true staircase containing $S$, i.e. all the divisors of terms in $S$.

Border($S$)**,** for computing the least terms for $|$ outside of $S$.

For $h \in \mathcal{H}$, we now want to build $R_h$ with the least $\text{LM}(\tilde{F}_h)$.

**Instruction 15.** *Pick a failing pair $R_m = [F_m, C_m]$ with $h = q\,m$ and $m$ the largest for $\prec$,*

1. *if there exists another failing pair $R_{m'} = [F_{m'}, C_{m'}]$ such that $\text{LM}(F_{m'}) = q\ \text{LM}(F_m)$, then compute $R_h$ as the* NormalForm($R_{m'}, [R_m, R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_n}]$) *where $C_{t_1}, \ldots, C_{t_r}$ are failing relations and $\text{LM}(F_{t_1}) \succ \cdots \succ \text{LM}(F_{t_r})$.*
2. *otherwise, compute $R_h$ as* NormalForm($q\,R_m, [R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_n}]$).

**Remark 16.** *If $q\ \text{LM}(F_m)$ is in the ideal spanned by B, then case 2 of Instruction 15 is equivalent to computing the normal form of $[q\ \text{LM}(F_m), 0]$ wrt. $[R_m, R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_r}]$. In fact, unless the table is 0, at the start, $R_1 = [P_{T+U}, 1]$ must fail when shifted by a monomial $s = x_1^{i_1} \cdots x_n^{i_n}$ and we have to make new pairs $R_{x_1^{i_1+1}}, \ldots, R_{x_n^{i_n+1}}$. Since $\text{LM}(P_{T+U}) = \frac{M}{s}$, then these pairs can be computed as the normal forms of $[x_k^{i_k+1}\,\frac{M}{s}, 0] = [B_k, 0]\,M'$, with $M' \in \mathcal{T}$, wrt. the ordered list $[R_1, R_{B_1}, \ldots, R_{B_n}]$. In dimension 1, this comes down to reducing $[x_1^{D_1+1}, 0] = [B_1, 0] = R_{B_1}$ wrt. $[R_1, R_{B_1}]$, and thus $R_1$ only. This is indeed the first step of the extended Euclidean algorithm called on $B_1$ and $F_1$ as described in Section 3.1.*

**Example 17** (See [7])**.** *Let $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$ be the binomial table, $\prec$ be the $\text{DRL}(y \prec x)$ monomial ordering and $T = \mathcal{T}_{\preceq x^3}$ and $U = \{1\}$ be sets of terms. We have $a = x^3$, $b = 1$, $T = T + U$ and $M = \text{LCM}(T) = x^3\,y^3$ so that $P_T = x^3\,y^3 + x^2\,y^3 + x^2\,y^2 + x\,y^3 + 2\,x\,y^2 + y^3$, $R_1 = [P_T, 1] = [F_1, C_1]$ and $R_{B_1} = [x^4, 0]$, $R_{B_2} = [y^4, 0]$.*

- *$m = 1$, thus $s = x^3$ and as $\text{LM}(F_1) = \text{LM}(P_T) = x^3\,y^3 = \frac{M}{1}$, then the relation $C_1$ fails when shifting by 1 so that 1 is in the staircase. Thus $\mathcal{H} = \{y, x\}$. We create $R_y$ by computing the normal form of $[y\ \text{LM}(F_1), 0] = [x^3\,y^4, 0]$ wrt. $[R_1, R_{B_1}, R_{B_2}]$ and get $R_y = [F_y, C_y] = [x^2\,y^3 + 2\,x\,y^3, y]$. Likewise $R_x = [F_x, C_x] = [x^3\,y^2 + x^2\,y^2 - 2\,x\,y^2 - y^3, x - 1]$.*
- *$m = y$, thus $s = x^2$ and as $\text{LM}(F_y) = x^2\,y^3 = \frac{M}{x}$, then the relation $C_y$ fails when shifting by $x$ so that $y$ is in the staircase. Thus $\mathcal{H} = \{x, y^2\}$. We create*
  - *$R_{y^2} = [0, y^2]$ by computing the normal form of $[y\ \text{LM}(F_y), 0] = [x^2\,y^4, 0]$ wrt. $[R_y, R_{B_1}, R_{B_2}, R_1, R_x]$.*
- *$m = x$, thus $s = x^2$ and as $\text{LM}(F_x) = x^3\,y^2 = \frac{M}{y}$, then the relation $C_x$ fails when shifting by $y$ so that $x$ is in the staircase. Thus $\mathcal{H} = \{y^2, x\,y, x^2\}$. We create*
  - *$R_{x\,y} = [-x^2\,y^2 - 3\,x\,y^3 - 2\,x\,y^2 - y^3, x\,y - y - 1]$ by computing the normal form of $R_1$ wrt. $[R_y, R_{B_1}, R_{B_2}, R_x]$;*

**Algorithm 1:** Polynomial Scalar-FGLM

**Input:** A table $\mathbf{w} = (w_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$ and two monomials $a$ and $b$.

**Output:** A Gröbner basis $G$ of the ideal of relations of $\mathbf{w}$ for $\prec$.

$T \coloneqq \{t \in \mathcal{T},\ t \preceq a\}$, $U \coloneqq \{u \in \mathcal{T},\ u \preceq b\}$.

$M \coloneqq \text{LCM}(T)\,\text{LCM}(U)$.

**For** $i$ **from** 1 **to** $n$ **do** $R_{B_i} \coloneqq \left[x_i^{1+\deg_{x_i} M}, 0\right]$. // pairs on the edge

$P \coloneqq \sum_{\tau\in(T+U)} [\tau]\,\frac{M}{\tau}$. // the mirror of the truncated generating series

$R \coloneqq \{[P, 1]\}$. // set of pairs $[F_m, C_m] = [P \cdot C_m \bmod B, C_m]$ to be tested

$R' \coloneqq \emptyset$. // set of failing pairs

$G \coloneqq \emptyset$, $S \coloneqq \emptyset$. // the future Gröbner basis and staircase

**While** $R \neq \emptyset$ **do**

  $R_m = [F_m, C_m] \coloneqq$ first element of $R$ and remove it from $R$.

  **If** $m \notin T$ *or* $\text{LM}(\tilde{F}_m) \prec \frac{M}{b\,s}$ **then** // good relation, see Proposition 13

    $G \coloneqq G \cup \{C_m\}$.

  **Else** // bad relation

    $R' \coloneqq R' \cup \{R_m\}$.

    **For all** $r \in R$ **do** // reduce next pairs with it

      $r \coloneqq \text{NormalForm}(r, [R_{B_1}, \ldots, R_{B_r}, R_m])$.

    $S \coloneqq \text{Stabilize}(S \cup \{m\})$.

    $H \coloneqq \text{Border}(S)$.

    **For all** $h \in H$ **do** // compute new pairs

      **If** *there is no relation* $C_h \in G$ *or no pair* $R_h \in R$ **then**

        Make a new pair $R_h = [F_h, C_h]$ following Instruction 15 and add it to $R$.

**Return** $G$.

  - $R_{x^2} = [-3\,x^2\,y^2 - x\,y^3 + 2\,x\,y^2 + y^3, x^2 - 2\,x + 1]$ *by computing the normal form of* $[x \cdot \mathrm{LM}(F_x), 0] = [x^4\,y^2, 0]$ *wrt.* $[R_x, R_{B_1}, R_{B_2}, R_1, R_y]$.

- $m = y^2$*, thus* $s = x$ *and as* $F_{y^2} = 0$*, then the relation is necessarily valid.*

- $m = x\,y$*, thus* $s = x$ *and as* $\mathrm{LM}(F_{x\,y}) = x^2\,y^2 = \frac{M}{x\,y}$*, then the relation* $C_{x\,y}$ *is valid.*

- $m = x^2$*, thus* $s = x$ *and, likewise, as* $\mathrm{LM}(F_{x^2}) = x^2\,y^2 = \frac{M}{x\,y}$*, then the relation* $C_{x^2}$ *is valid.*

*We return* $C_{y^2} = y^2$, $C_{x\,y} = x\,y - y - 1$ *and* $C_{x^2} = x^2 - 2\,x + 1$.

**Example 18** (See [7] and Example 14)**.** *We keep* $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$*, the binomial table, and* $\prec$ *set as* $\mathrm{DRL}(y \prec x)$*. We let however* $T = U = \mathcal{T}_{\preceq x\,y^2}$ *so that* $a = b = x\,y^2$, $2\,T = T + T$ *and* $M = \mathrm{LCM}(2\,T) = x^4\,y^6$*. Thus,* $P_{2\,T} = x^4\,y^6 + x^3\,y^6 + x^3\,y^5 + x^2\,y^6 + 2\,x^2\,y^5 + x\,y^6 + x^2\,y^4 + 3\,x\,y^5 + y^6 + 3\,x\,y^4$, $R_1 = [P_{2\,T}, 1] = [F_1, C_1]$ *and* $R_{B_1} = [x^5, 0]$, $R_{B_2} = [y^7, 0]$.

- $m = 1$*, thus* $s = x\,y^2$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x^2\,y^4} \setminus \{x^4\,y, x^5\}$*, with* $x^5$ *not dividing* $M$*. Therefore,* $\tilde{F}_1$ *is obtained from* $F_1$ *by removing monomial* $\frac{M}{x^4\,y} = y^5$*. As* $\mathrm{LM}(F_1) = \mathrm{LM}(P_{2\,T}) = x^4\,y^6 \succeq \frac{M}{b\,s} = x^2\,y^2$*, then the relation* $C_1$ *fails and* $1$ *is in the staircase. Thus* $\mathcal{H} = \{y, x\}$*. We create* $R_y$ *by computing the normal form of* $[y \cdot \mathrm{LM}(F_1), 0] = [x^3\,y^4, 0]$ *wrt.* $[R_1, R_{B_1}, R_{B_2}]$ *and get* $R_y = [F_y, C_y] = [x^3\,y^6 + 2\,x^2\,y^6 + x^2\,y^5 + 3\,x\,y^6 + 3\,x\,y^5, y]$*. Likewise* $R_x = [F_x, C_x] = [x^4\,y^5 + x^3\,y^5 + x^3\,y^4 + x^2\,y^5 + 2\,x^2\,y^4 + 3\,x\,y^5 + y^6 + 3\,x\,y^4, x - 1]$.

- $m = y$*, thus* $s = x\,y$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x\,y^4} \setminus \{x^4\}$*. Therefore,* $\tilde{F}_y$ *is obtained from* $F_y$ *by removing monomial* $\frac{M}{x^4} = y^6$*. As* $\mathrm{LM}(F_y) = x^3\,y^6 \succeq \frac{M}{b\,s} = x^2\,y^3$*, then the relation* $C_y$ *fails and* $y$ *is in the staircase. Thus* $\mathcal{H} = \{x, y^2\}$*. We create*

  - $R_{y^2} = [x^2\,y^6 + 3\,x\,y^6, y^2]$ *by computing the normal form of* $[y \cdot \mathrm{LM}(F_y), 0] = [x^3\,y^7, 0]$ *wrt.* $[R_y, R_{B_1}, R_{B_2}, R_1, R_x]$.

- $m = x$*, thus* $s = y^2$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x\,y^4} \setminus \{x^3\,y, x^4\}$*. Therefore,* $\tilde{F}_x$ *is obtained from* $F_x$ *by removing monomials* $\frac{M}{x^3\,y} = x\,y^5$ *and* $\frac{M}{x^4} = y^6$*. As* $\mathrm{LM}(F_x) = x^4\,y^5 \succeq \frac{M}{b\,s} = x^3\,y^2$*, then the relation* $C_x$ *fails and* $x$ *is in the staircase. Thus* $\mathcal{H} = \{y^2, x\,y, x^2\}$*. We create*

  - $R_{x\,y} = [-4\,x\,y^6 - x^2\,y^4 - 6\,x\,y^5 - y^6 - 3\,x\,y^4, x\,y - y - 1]$ *by computing the normal form of* $R_1$ *wrt.* $[R_y, R_{B_1}, R_{B_2}, R_x]$*;*
  - $R_{x^2} = [x^4\,y^4 + x^3\,y^4 - 4\,x^2\,y^5 - x\,y^6 - 5\,x^2\,y^4 + 3\,x\,y^5 + y^6 + 3\,x\,y^4, x^2 - 2\,x + 1]$ *by computing the normal form of* $[x \cdot \mathrm{LM}(F_x), 0] = [x^5\,y^5, 0]$ *wrt.* $[R_x, R_{B_1}, R_{B_2}, R_1, R_y]$.

- $m = y^2$*, thus* $s = x$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x^2\,y^2}$*. As* $\mathrm{LM}(F_{y^2}) = x^4\,y^6 \succeq \frac{M}{b\,s} = x^2\,y^4$*, then the relation* $C_{y^2}$ *fails and* $y^2$ *is in the staircase. Thus* $\mathcal{H} = \{x\,y, x^2, y^3\}$*. We create*

  - $R_{y^3} = [0, y^3]$ *by computing the normal form of* $[y \cdot \mathrm{LM}(F_{y^2}), 0] = [x^2\,y^7, 0]$ *wrt.* $[R_{y^2}, R_{B_1}, R_{B_2}, R_1, R_x, R_y, R_{x^2}]$.

- $m = x\,y$*, thus* $s = y$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x\,y^3} \setminus \{x^3\}$*. Therefore,* $\tilde{F}_{x\,y}$ *is obtained from* $F_{x\,y}$ *by removing monomial* $\frac{M}{x^3} = x\,y^6$*. As* $\mathrm{LM}(\tilde{F}_{x\,y}) = x^2\,y^4 \prec \frac{M}{b\,s} = x^3\,y^3$*,* $C_{x\,y}$ *is valid.*

- $m = x^2$*, thus* $s = 1$ *and* $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s} = \mathcal{T}_{\preceq x\,y^2}$*. As* $\mathrm{LM}(F_{x^2}) = x^4\,y^4 \succeq \frac{M}{b\,s} = x^3\,y^4$*, then the relation* $C_{x^2}$ *fails and* $x^2$ *is in the staircase. Thus* $\mathcal{H} = \{x\,y, y^3, x^3\}$*. We create*

– $R_{x^3} = [-4\,x^3\,y^5 - 6\,x^3\,y^4 + 7\,x^2\,y^5 + 5\,x\,y^6 + 8\,x^2\,y^4 - 3\,x\,y^5 - y^6 - 3\,x\,y^4, x^3 - 3\,x^2 + y^2 + 3\,x - 1]$ *by computing the normal form of* $[x \operatorname{LM}(F_{x^2}), 0] = [x^5\,y^4, 0]$ *wrt.* $[R_{x^2}, R_{B_1}, R_{B_2}, R_1, R_x, R_y, R_{y^2}]$.

- $m = y^3$, *thus* $s = 1$ *and* $\mathcal{T}_{\leq b} + \mathcal{T}_{\leq s} = \mathcal{T}_{\leq x\,y^2}$. *As* $\operatorname{LM}(\tilde{F}_{y^3}) = 0 \prec \frac{M}{b\,s} = x^3\,y^4$, $C_{y^3}$ *is valid.*
- $m = x^3$, *thus* $s = 0$ *and* $C_{x^3}$ *is trivially valid.*

  *Notice that any relation in* $x^3$ *would trivially be valid. Though, this is the one yielding the smallest leading monomial for* $F_{x^3}$, *i.e.* $x^3\,y^5$.

*We return* $C_{x\,y} = x\,y - y - 1$, $C_{y^3} = y^2$ *and* $C_{x^3} = x^3 - 3\,x^2 + y^2 + 3\,x - 1$.

**Remark 19.** *Like the* BMS *algorithm, this algorithm creates new potential relations by making polynomial combinations of failing relations. As a consequence, at each step of the main loop, the potential relations, i.e. elements of R, are not necessarily interreduced. Either we can interreduce the final Gröbner basis before returning it at the last line of the algorithm, or when* $C_g$ *is added to the set G we can update all the current relations by removing multiples of* $[F_g, C_g]$ *and likewise, reduce by* $[F_g, C_g]$, *any subsequent pair* $[F_m, C_m]$.

**Example 20** (See [7])**.** *We give the trace of the* Polynomial Scalar-FGLM *algorithm with the slight modification above called on the table* $\mathbf{w} = ((2\,i+1) + (2\,j-1)\,(-1)^{i+j})_{(i,j)\in\mathbb{N}^2}$, *the stopping monomials* $a = y^5$ *and* $b = 1$ *and the monomial ordering* $\operatorname{DRL}(y \prec x)$.

*We set* $T := \mathcal{T}_{\leq y^5}$, $U := \{1\}$, $M := x^4\,y^5$ *and* $P = 4\,x^3\,y^5 + 4\,x^4\,y^3 + 4\,x^3\,y^4 + 4\,x^2\,y^5 - 4\,x^4\,y^2 + 4\,x^2\,y^4 + 8\,x\,y^5 + 8\,x^4\,y + 8\,x^3\,y^2 + 8\,x^2\,y^3 + 8\,x\,y^4 + 8\,y^5 - 8\,x^4$, $R_{B_1} := [x^5, 0], R_{B_2} := [y^6, 0]$, $R = [[P, 1]]$.

**Pair** $R_1 = [F_1, C_1] = [P, 1]$, $R := \emptyset$ *and since* $1 \in T$ *but* $\operatorname{LM}(F_1) = x^3\,y^5 \geq \frac{M}{s} = x^4$, *then*

- $R' := \{R_1\}$, $S := \{1, x\}$ *and* $H := \{y, x^2\}$.
- *We make new pairs added to R:*
  - $R_y = [F_y, C_y] :=$ NormalForm$([y \operatorname{LM}(F_1), 0], [R_1, R_{B_1}, R_{B_2}])$ *which can be normalized into* $R_y, = [4\,x^4\,y^4 - \cdots, y - 1]$;
  - $R_{x^2} = [F_{x^2}, C_{x^2}] :=$ NormalForm$([x^2 \operatorname{LM}(F_1), 0], [R_1, R_{B_1}, R_{B_2}])$ *which can be normalized into* $R_{x^2} = [4\,x^4\,y^3 - \cdots, x^2 - x - 1]$.

**Pair** $R_y = [F_y, C_y]$, $R := \{R_{x^2}\}$ *and since* $y \in T$ *but* $\operatorname{LM}(F_y) = x^4\,y^4 \geq \frac{M}{s} = x^4\,y$, *then*

- $R' := \{R_1, R_y\}$, $S := \{1, y, x\}$ *and* $H := \{y^2, x\,y, x^2\}$.
- *We make new pairs added to R:*
  - *As* $y \operatorname{LM}(F_y) = x^4\,y^5 \notin \langle x^5, y^6\rangle$ *and* $\operatorname{LM}(F_1) \neq y \operatorname{LM}(F_y)$, *we can only set* $R_{y^2} = [F_{y^2}, C_{y^2}] :=$ NormalForm$(y\,R_y, [R_{B_1}, R_{B_2}, R_1, R_y])$ *which can be normalized into* $R_{y^2} = [-4\,x^4\,y^3 - \cdots, y^2 - x + 2\,y - 1]$;
  - $R_{x\,y} = [F_{x\,y}, C_{x\,y}] :=$ NormalForm$([x \operatorname{LM}(F_y), 0], [R_y, R_{B_1}, R_{B_2}, R_1])$ *which can be normalized into* $R_{x\,y} = [4\,x^4\,y^2 - \cdots, x\,y - x + y - 1]$.
  - *Nothing is done for* $x^2$ *since* $R_{x^2}$ *already exists.*

**Pair** $R_{y^2} = [F_{y^2}, C_{y^2}]$, $R := \{R_{x\,y}, R_{x^2}\}$ *and since* $y^2 \in T$ *but* $\operatorname{LM}(F_{y^2}) = x^4\,y^3 \geq \frac{M}{s} = x^4\,y^2$, *then*

- *As* $\text{LM}(F_{x^2}) \geq \text{LM}(F_{y^2})$*, we reduce it and obtain* $R_{x^2} \coloneqq [-8\,x^2\,y^4 - \cdots, x^2 + y^2 - 2\,x + 2\,y - 2]$.
- $R' \coloneqq \{R_1, R_y, R_{y^2}\}$, $S \coloneqq \{1, y, x, y^2\}$ *and* $H \coloneqq \{x\,y, x^2, y^3\}$.
- *We make new pairs added to* $R$*:*
  - $R_{x\,y}$ *and* $R_{x^2}$ *already exist so we do nothing for them.*
  - *Since* $\text{LM}(F_y) = y\ \text{LM}(F_{y^2})$*, we can set* $R_{y^3} = [F_{y^3}, C_{y^3}] \coloneqq \text{NormalForm}(R_y, [R_{y^2}, R_{B_1}, R_{B_2}, R_y, R_1])$ *which can be normalized into* $R_{y^3} = [4\,x^3\,y^4 - \cdots, y^3 - x\,y + y^2 + x - 2\,y]$.

**Pair** $R_{x\,y} = [F_{x\,y}, C_{x\,y}]$, $R \coloneqq \{R_{x^2}, R_{y^3}\}$ *and since* $x\,y \in T$ *and* $\text{LM}(F_{x\,y}) = x^4\,y^2 \prec \frac{M}{s} = x^2\,y^5$*, then*

- $G \coloneqq \{x\,y - x + y - 1\}$.
- *As* $C_{y^3} = y^3 - x\,y + y^2 + x - 2\,y$ *has a term in* $x\,y$*, we update* $R_{y^3} \coloneqq R_{y^3} + R_{x\,y} = [4\,x^3\,y^4 - \cdots, y^3 + y^2 - y - 1]$.

**Pair** $R_{x^2} = [F_{x^2}, C_{x^2}]$, $R \coloneqq \{R_{y^3}\}$ *and since* $x^2 \in T$ *and* $\text{LM}(F_{x^2}) = x^2\,y^4 \prec \frac{M}{s} = x^2\,y^5$*, then*

- $G \coloneqq \{x\,y - x + y - 1, x^2 + y^2 - 2\,x + 2\,y - 2\}$.

**Pair** $R_{y^3} = [F_{y^3}, C_{y^3}]$, $R \coloneqq \emptyset$ *and since* $y^3 \in T$ *and* $\text{LM}(F_{y^3}) = x^3\,y^4 \prec \frac{M}{s} = x^4\,y^3$*, then*

- $G \coloneqq \{x\,y - x + y - 1, x^2 + y^2 - 2\,x + 2\,y - 2, y^3 + y^2 - y - 1\}$.

*We return* $G$.

**Theorem 21.** *Let a table* $\mathbf{w}$*, a monomial ordering* $\prec$ *and two monomials* $a$ *and* $b$ *be the input of the* Polynomial Scalar-FGLM *algorithm. Let us assume that the reduced Gröbner basis* $\mathcal{G}$ *of the ideal of relations of* $\mathbf{w}$ *for* $\prec$ *and its staircase* $S$ *satisfy* $a \geq \max(S \cup \text{LM}(\mathcal{G}))$ *and for all* $g \preceq a$*,* $s = \max\{\sigma \in \mathcal{T},\ \sigma\,g \preceq a\}$*, we have* $\max(S) \preceq s$.

*Then, the* Polynomial Scalar-FGLM *algorithm terminates and computes a minimal Gröbner basis of the ideal of relations of* $\mathbf{w}$ *for* $\prec$ *in* $O(\#S\,(\#S + \#\mathcal{G})\,\#(\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b}))$ *operations in the base field.*

*Proof.* The proof is mainly based on the termination and validity of the BMS algorithm. For any monomial $m \in \mathcal{T}_{\preceq a}$, we denote by $C^\star_m$ the last (and therefore one with the largest fail) relation made by the BMS algorithm starting with $m$, if there is any.

Starting with $R_1 = [F_1, C_1] = [P_{\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b}}, 1]$, $\text{LM}(F_1)$ yields exactly the fail of relation $C_1 = C^\star_1$ so that, as in the BMS algorithm, we know the leading monomials of the potential next relations.

Let us assume now that for any monomial $\mu \prec h$, the pair $R_\mu = [F_\mu, C_\mu]$ made by the Polynomial Scalar-FGLM algorithm is equivalent to $C^\star_\mu$, that is either both $C_\mu$ and $C^\star_\mu$ fail when shifting by exactly the same monomial or they both succeed on $\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b}$.

Since $C_\mu$ and $C^\star_\mu$ are equivalent, the current discovered staircase by the BMS and the Polynomial Scalar-FGLM algorithms are the same. Thus either $h$ is a leading monomial of a relation to be built by both algorithms or it is not. Without loss of generality, we can assume it is. There exists a monomial $m$ such that $m|h$ and $R_m = [F_m, C_m]$ and $C^\star_m$ have been made. In the BMS algorithm, the relation $C^\star_h$ is obtained as $\frac{h}{m}\,C^\star_m - \sum_{\mu<h} q^\star_\mu\,C^\star_\mu$ while in the Polynomial Scalar-FGLM algorithm, $C_h$ is made as $\frac{h}{m}\,C_m - \sum_{\mu<h} q_\mu\,C_\mu$. In each computation, $q^\star_\mu$ and $q_\mu$ are chosen so that $C^\star_m$ and $C_m$ have the largest fail (or equivalently $\tilde{F}_m$ has the least leading monomial), hence $C^\star_m$ and $C_m$ are equivalent. For $h \in S$, the potential relation $C_h$ made by the algorithm must fail when

shifted by a monomial in $S$. Thus, there exist $\sigma_1, \sigma_2$ such that $\sigma_1\,\sigma_2 \in S$, $\sigma_1\,h \preceq a$, $\sigma_2 \preceq b$ and the column labeled with $\sigma_1\,h$ of the matrix $H_{\mathcal{T}_{\preceq b},\mathcal{T}_{\preceq a}}$ is independent from the previous ones. For $g \in \text{LM}(\mathcal{G})$, by Section 3.2, the relation $C_g$ has been tested shifted by all the monomials in $\mathcal{T}_{\preceq b} + \mathcal{T}_{\preceq s}$, with $s = \max\{\sigma \in \mathcal{T},\ \sigma\,g \preceq a\}$. The theorem hypothesis is exactly that the full staircase is included in the set of tested shifts, hence we can ensure that $C_g$ corresponds to a kernel vector of $H_{S,S\cup\{g\}}$ with the last coordinate equal to 1.

Furthermore, as in the proof of the BMS algorithm, the failures of relations $C_m$ ensure that the returned relations $C_h$ are all such that their leading monomials are minimal for the division. That is, the returned Gröbner basis is minimal.

Concerning the complexity of the algorithm. Since $\mathcal{T}_{\preceq a}$ and $\mathcal{T}_{\preceq b}$ are stable by division, so is $\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}$. Let us recall that the support of $P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}$ is $\{\frac{M}{\tau},\ \tau \in (\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b})\}$, $M = \text{LCM}(\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b})$. Since each $F_m$ satisfies $F_m = P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}\,C_m \bmod B$, then the monomials in the support of $F_m$ are multiples of the monomials in the support of $P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}$ and thus are included in the support of $P_{\mathcal{T}_{\preceq a}+\mathcal{T}_{\preceq b}}$. Each pair $R_m = [F_m, C_m]$ for $m \in S \cup \text{LM}(\mathcal{G})$ must be reduced by all the previous ones lying in the staircase in at most $\#S\,\#(\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b})$ operations. Reducing the relations to obtain a minimal Gröbner basis can be done in $O(\#S\,\#\mathcal{G}\,\#(\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq b}))$ operations, hence this part is not the bottleneck of the algorithm. □

**Remark 22.** *Using the same notation, the* AGbb *algorithm computes a border basis $\mathcal{B}$ of the ideal of relations using $O(\#S\,(\#S + \#\mathcal{B})\,\#(\mathcal{T}_{\preceq a} + \mathcal{T}_{\preceq a}))$ operations in the base field [25]. Thus, in theory, the* AGbb *and the* Polynomial Scalar-FGLM *algorithms share the same complexity estimates, whenever $a = b$.*

*However, the given complexity bound is based on naive multivariate polynomial arithmetic. Thus the goal would be to investigate how to exploit fast polynomial multiplication to speed up the* NormalForm *procedure computations in the* Polynomial Scalar-FGLM *algorithm.*

*Let us recall that in the univariate case, complexity improvements are made thanks to fast Euclidean algorithm through a divide-and-conquer approach and using fast polynomial division and multiplication.*

*In this multivariate setting, a divide-and-conquer approach has already been investigated in [26] relying on fast polynomial matrix arithmetic. Likewise, some improvements were made regarding the reduction of a bivariate polynomial by the reduced Gröbner basis of the ideal spanned by two polynomials for* drl *in [21]. This is a first step in this direction.*

*A further step would be to determine the quotients fastly using, like in the univariate case, fast multiplication. Usually the reduction of a polynomial by several polynomials might be intricate. Yet, in our experiments, we observed that the call $R_h = \text{NormalForm}(R_{m'}, [R_m, R_{B_1}, \ldots, R_{B_n}, R_{t_1}, \ldots, R_{t_r}])$ can actually be done in several simpler steps.*

1. *A call to $R_h = \text{NormalForm}(R_{m'}, R_m)$ to reduce $F_m$ wrt. $F_{m'}$.*
2. *A cleaning step to remove some high-degree monomials in $F_h$, corresponding to $R_h = \text{NormalForm}(R_h, [R_{B_1}, \ldots, R_{B_n}])$. Note that the quotients, here, need not be stored.*
3. *A Gaussian elimination-like step to find the linear combination of $F_h, F_{t_1}, \ldots, F_{t_r}$ with the smallest leading monomial. This corresponds to a call $R_h = \text{NormalForm}(R_h, [R_{t_1}, \ldots, R_{t_r}])$.*

*Hence, one might only need to compute the first quotient, associated to $F_m$, fastly.*

*Finally, the computation of $C_h$ is done through polynomial multiplications and thus benefit from any improvement thereof.*

*We shall see in Section 6, that the* Polynomial Scalar-FGLM *algorithm seems to perform better thanks to the multivariate polynomial arithmetic.*

## 5. An adaptive variant

In some applications, the actual size of the staircase, or at least an upper bound thereof, is known. While it provides an early termination criterion for the BMS, Scalar-FGLM and Polynomial Scalar-FGLM algorithms, this might fail to drastically reduce the number of table queries. Indeed, for the $\text{DRL}(x_n \prec \cdots \prec x_1)$ ordering, whether the set of leading monomials of the Gröbner basis is $\{x_n, \ldots, x_2, x_1^d\}$ or all the monomials of degree $d$: $\{x_n^d, x_{n-1}\, x_n^{d-1}, \ldots, x_1\, x_n^{d-1}, \ldots, x_1^d\}$, the BMS algorithm requires to visit all the monomials up to $x_1^{2\,d-1}$. Therefore, it needs to visit $\binom{n+2\,d-1}{n}$ table terms to compute a Gröbner basis of size $n$ with a staircase of size $d$ in the former case and a Gröbner basis of size $\binom{n+d-1}{n-1}$ with a staircase of size $\binom{n+d-1}{n}$ in the latter. Furthermore, in some applications, like the Sparse-FGLM algorithm one, computing a single table term can be very costly. Thus, requiring as few table terms as possible to retrieve the correct ideal of relations is critical.

The Adaptive Scalar-FGLM algorithm [3] was designed to minimize the number of table queries by taking into account the shape of the Gröbner basis gradually as it is discovered. The algorithm starts with $S = \emptyset$. At each step, $S$ is a staircase containing only monomials that we know are in the target staircase, this means that the matrix $H_{S,S}$ must be full rank. Likewise, $L$ is a set of monomials on the border of $S$. For $m$ the smallest monomial in $L$, we check if $H_{S\cup\{m\},S\cup\{m\}}$, with $S \cup \{m\}$ has a greater rank than $H_{S,S}$ or not. If it does not, then the last column, labeled with $m$, must be linearly dependent from the previous one. That is, a relation $C_m$ is found and any multiple of $m$ is removed from $L$. Otherwise, no relation $C_m$ with $\text{LM}(C_m) = m$ must exist. Thus, $m$ is added to the staircase $S$, removed from $L$ and monomials $m\, x_i$ are added to $L$.

**Example 23.** *Let us consider the sequence* $\mathbf{w} = (p_{i_0+1})_{\mathbf{i}\in\mathbb{N}^n}$ *where* $p_{i_0+1}$ *stands for the* $(i_0+1)$*st prime number if* $i_0 < d$ *and* 0 *otherwise. For* DRL*, or even* LEX*, the* Adaptive Scalar-FGLM *algorithm computes the rank of the following matrices*

- $H_{\{1\},\{1\}} = \begin{pmatrix} 2 \end{pmatrix}$. *Its rank is* 1*, the dimension of the matrix, so* $1 \in S$*;*
- $H_{\{1,x_n\},\{1,x_n\}} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$. *Its rank is* 1 *which is not the dimension of the matrix so a relation* $C_{x_n}$ *is found. This is* $C_{x_n} = x_n - 1$.
- $H_{\{1,x_{n-1}\},\{1,x_{n-1}\}} = \cdots = H_{\{1,x_2\},\{1,x_2\}} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$. *Their ranks are also* 1 *which are not the dimensions of the matrices so the relations* $C_{x_{n-1}} = x_{n-1} - 1, \ldots, C_{x_2} = x_2 - 1$ *are found.*
- $H_{\{1,x_1\},\{1,x_1\}} = \begin{pmatrix} 2 & 3 \\ 3 & 5 \end{pmatrix}$. *Its rank is* 2*, the dimension of the matrix. Thus,* $x_1 \in S$.
- $H_{\{1,x_1,x_1^2\},\{1,x_1,x_1^2\}} = \begin{pmatrix} 2 & 3 & 5 \\ 3 & 5 & 7 \\ 5 & 7 & 11 \end{pmatrix}$. *Its rank is* 3*, the dimension of the matrix. Therefore,* $x_1^2 \in S$.
- $\ldots$*;*
- $H_{\{1,x_1,\ldots,x_1^{d-1}\},\{1,x_1,\ldots,x_1^{d-1}\}} = \begin{pmatrix} 2 & 3 & 5 & \cdots & p_d \\ 3 & 5 & 7 & \cdots & 0 \\ 5 & 7 & 11 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_d & 0 & 0 & \cdots & 0 \end{pmatrix}$. *Its rank is d, the dimension of the matrix, so* $x_1^d \in S$.
- $H_{\{1,x_1,\ldots,x_1^d\},\{1,x_1,\ldots,x_1^d\}} = \begin{pmatrix} 2 & 3 & 5 & \cdots & p_d & 0 \\ 3 & 5 & 7 & \cdots & 0 & 0 \\ 5 & 7 & 11 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ p_d & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}$. *Its rank is also d, which is not the dimension of the matrix. Thus, the relation* $C_{x_1^d} = x_1^d$ *is found.*

*It thus requires merely* $2\,(n+d)-1$ *table terms instead of* $\binom{n+2\,d-1}{n}$.

As described in Sections 3 and 4, the Polynomial Scalar-FGLM algorithm is based on polynomials from matrices with columns set $\mathcal{T}_{\preceq a}$ and rows set $\mathcal{T}_{\preceq b}$. However, here, we need matrices with more general sets of monomials for the rows and columns. Therefore, the main tool of the adaptive variant of the Polynomial Scalar-FGLM algorithm is new basic routines so that we can perform polynomial divisions while also ensuring that our polynomials are related to multi-Hankel matrices with these columns and rows sets of monomials. Since at each step, $S$ is a staircase and $m$ is a monomial lying on its border so that $S \cup \{m\}$ is also a staircase, then the corresponding matrices would be $H_{S,S}$ and $H_{S\cup\{m\},S\cup\{m\}}$. Therefore, any instance of $T + U$ from the previous sections will be replaced by $2\,S \coloneqq S + S$, the Minkowski sum of $S$ with itself, or likewise by $2\,(S \cup \{m\})$.

At each step, we have the polynomial $P_{2\,S}$, associated to matrix $H_{S,S}$, a monomial ideal $B_{2\,S}$, determined as in Section 3.2, and pairs $R_{2\,S,t} = [F_{2\,S,t}, C_t] = [P_{2\,S}\; C_t \bmod B_{2\,S}, C_t]$. At the next step, we compute $P_{2\,(S\cup\{m\})}$ from $P_{2\,S}$ by shifting it by $\frac{\text{LCM}(S\cup\{m\})^2}{\text{LCM}(S)^2}$ and adding the missing terms, update $B_{2\,S}$ into $B_{2\,(S\cup\{m\})}$ and likewise update each $R_{2\,(S\cup\{m\}),t}$ by shifting $F_{2\,S,t}$ and adding the missing terms to make $F_{2\,(S\cup\{m\}),t}$. It remains to compute $R_{2\,(S\cup\{m\}),m}$ such that $\operatorname{supp} C_m \subseteq S \cup \{m\}$ and $F_{2\,(S\cup\{m\})}$ is sufficiently "small" to ensure that $C_m$ is a valid relation or not. This is where two approaches are possible. The first one is the naive one; it was proposed in [5] and is recalled in Section 5.1. It is based on polynomial arithmetic, yet does not use as many polynomial divisions as the Polynomial Scalar-FGLM does. The other one is presented in Section 5.2 and fully uses polynomial divisions to perform the computations. In particular, we design some new basic routines to do so. This yields the Adaptive Polynomial Scalar-FGLM algorithm, or Algorithm 2.

### *5.1. A naive approach*

In this naive approach, the only remaining things are the initialization and reduction of $R_{2\,(S\cup\{m\}),m}$ and then testing if $C_m$ is valid.

The pair $R_{2\,(S\cup\{m\}),m}$ is initialized as $m\,R_{2\,(S\cup\{m\}),1}$ and then reduced, as in Section 4, by $R_{2\,(S\cup\{m\}),B_1}$, $\ldots, R_{2\,(S\cup\{m\}),B_n}$, where $B_1, \ldots, B_n \in B_{2\,S}$. Then, we can reduce it incrementally by all the other $R_{2\,(S\cup\{m\}),t}$, which comes down to just subtracting a constant multiple of them.

Finally, when a valid relation $C_g$ is found, any multiple of $g$ is removed from the set of potential monomials to add to $S$. Moreover, we can further reduce a future relation $R_{2\,(S\cup\{m\}),m} = [F_{2\,(S\cup\{m\}),m}, C_m]$ with any pair $\left[\frac{M}{\mu\,g}, 0\right]$, $m \succeq \mu\,g$ to clean the support of $F_{2\,(S\cup\{m\})}$. As $\frac{M}{\mu\,g}$ is a single monomial, this can be done easily, not unlike the reductions by $R_{2\,(S\cup\{m\}),B_1}, \ldots, R_{2\,(S\cup\{m\}),B_n}$.

### *5.2. A division-based adaptive variant*

In [5], we did not go further in the design of an adaptive variant of the Polynomial Scalar-FGLM. In particular, that version could not initialize a pair $R_{2\,(S\cup\{m\}),m}$ as the quotient of two pairs of polynomials. In the following part of this section, we show how to initialize a new pair as the quotient of two previously computed pairs of polynomials.

The algorithm uses some new procedures that are not needed in Polynomial Scalar-FGLM. Indeed, at step $m$, when computing $R_{2\,S',m} = [F_{2\,S',m}, C_m]$, with $S' = S \cup \{m\}$, we can at first only ensure that $\operatorname{supp} C_m \subseteq \mathcal{T}_{\preceq m}$. Yet, we need to have $\operatorname{supp} C_m \subseteq S' = \mathcal{T}_{\preceq m} \setminus \langle \text{LM}(C_g), g \in G\rangle$. Thus, we need to reduce $C_m$ by all the already computed $C_g$'s.

NormalFormRightSide($R_{2\,S,m}, [R_{2\,S,g_1}, \ldots, R_{2\,S,g_r}]$) that computes the quotients $Q_{g_1}, \ldots, Q_{g_r}$ of the division of $C_m$ by $C_{g_1}, \ldots, C_{g_r}$, with $R_{2\,S,g_1}, \ldots, R_{2\,S,g_r} \in G$ and then returns $R_{2\,S,m} - Q_{g_1}\,R_{2\,S,g_1} - \cdots - Q_{g_r}\,R_{2\,S,g_r}$.

NormalFormHigherPart($R_{2S,m}, [R_{2S,s_1}, \ldots, R_{2S,s_q}]$) that behaves like NormalForm, except only the higher part $\tilde{F}_{2S',t}$ of a polynomial $F_{2S',t}$ is used. For $t = B_i$, $\tilde{F}_{2S',t} = F_{2S',t} = B_i$, otherwise $\tilde{F}_{2S',t}$ is obtained from $F_{2S',t}$ by removing any monomial dividing $\frac{\text{LCM}(S')^2}{g}$ with $g \in \text{LM}(\mathcal{G})$. Then NormalFormHigherPart($R_{2S',m}, [R_{2S',s_1}, \ldots, R_{2S',s_q}]$) computes the normal form of $\tilde{F}_{2S',m}$ with respect to $[\tilde{F}_{2S',s_1}, \ldots, \tilde{F}_{2S',s_q}]$ and the corresponding quotients $Q_1, \ldots, Q_q$. It then returns $R_{2S',m} - Q_1 R_{2S',s_1} - \cdots - Q_q R_{2S',s_q}$.

The definition of $\tilde{F}_{2S',m}$ extends the one used in Section 3.2.2. The rationale is the same: using the leading monomial of $F_{2S',m}$ to check whether $C_m$ is a valid relation or not is not the same as checking if the last column of $H_{S',S'}$ linearly depends from the previous ones. Indeed, the leading monomial might correspond to a row that is not present in $H_{S',S'}$. Since $S'$ does not contain any monomial that is a multiple of $g$ with $R_g \in G$, then it makes sense to remove any monomial dividing $\frac{\text{LCM}(S')^2}{g}$, with $R_g$ still in $G$.

**Algorithm 2:** Adaptive Polynomial Scalar-FGLM

**Input:** A table $\mathbf{w} = (w_\mathbf{i})_{\mathbf{i} \in \mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$.
**Output:** A Gröbner basis $G$ of the ideal of relations of $\mathbf{w}$ for $\prec$.

$L := \{1\}$.
$G := \emptyset, S := \emptyset$. // the future Gröbner basis and staircase
$B := \{B_1, \ldots, B_n\} = \{x_1^0, \ldots, x_n^0\}$.
$R_{2S,B_1} := [B_1, 0], \ldots, R_{2S,B_n} := [B_n, 0]$.
**While** $L \neq \emptyset$ **do**
  $m :=$ first element of $L$ and remove it from $L$.
  $S' := S \cup \{m\}$.
  Update $B$ and all pairs $R_{2S,t}$ into $R_{2S',t}$ for $t \in S \cup G \cup B$.
  **If** $m = 1$ **then** $R_1 := [w_{0,\ldots,0}, 1]$.
  **Else if** $m = \mu\, x_i^2$ *with* $\mu, \mu\, x_i \in S$ **then**
    $R_{2S',m} :=$ NormalFormHigherPart($R_{2S',\mu}, [R_{2S',\mu x_i}, R_{2S',B_1}, \ldots, R_{2S',B_n}]$).
  **Else** // $m = \mu\, x_i$ with $\mu \in S$
    $R_{2S',m} :=$ NormalForm($x_i\, R_{2S',\mu}, [R_{2S',B_1}, \ldots, R_{2S',B_n}]$).
  $R_{2S',m} :=$ NormalFormRightSide($R_{2S',m}, [R_{2S',g_1}, \ldots, R_{2S',g_r}]$). // $g_1, \ldots, g_r \in G$
  $R_{2S',m} :=$ NormalForm($R_{2S',m}, [R_{2S',B_1}, \ldots, R_{2S',B_n}]$).
  $R_{2S',m} :=$ NormalFormHigherPart($R_{2S',m}, [R_{2S',s_1}, \ldots, R_{2S',s_q}]$). // $s_1, \ldots, s_q \in S$
  $R_{2S',m} = [F_{2S',m}, C_m]$.
  **If** $\text{LM}(\tilde{F}_{2S',m}) \prec \frac{\text{LCM}(S')^2}{m}$ **then** // Relation succeeds
    Update $R_{2S',m}$ into $R_{2S,m}$.
    $G := G \cup \{R_{2S,m}\}$.
    Remove multiples of $m$ in $L$.
  **Else** // Relation fails
    Delete every pair $R_{2S,t}$ for $t \in S \cup G \cup B$.
    $S := S'$.
    $L := L \cup \{x_1\, m, \ldots, x_n\, m\}$, remove any multiples of $\text{LM}(G)$ and sort it by increasing order.
**return** $G$.

**Remark 24.** *To simplify the presentation, we did not consider the case where some sequence terms might not be available. This can happen for instance in the error correcting code application. Likewise, if the sequence is not linear recurrent, then an infinite loop might happen. Both situations require an easy modification of the algorithm.*

For the correctness of the algorithm, we need to prove the following lemma.

**Lemma 25.** *Let $S$ be the current computed staircase and let $\mathcal{G}$ be the current computed Gröbner basis. Let $m$ be the least monomial not in $S$ and not divisible by $\operatorname{LM}(\mathcal{G})$ and let $S' = S \cup \{m\}$. Then, for all $t$, $\operatorname{LM}(\tilde{F}_{2S',t}) = \frac{\operatorname{LCM}(S')^2}{\operatorname{LCM}(S)^2} \operatorname{LM}(\tilde{F}_{2S,t})$ and $\operatorname{LM}(\tilde{F}_{2S',m}) \preceq \frac{\operatorname{LCM}(S')^2}{m}$. Furthermore, this weak inequality is an equality if, and only if, $C_m$ is not a valid relation.*

*Proof.* If $\mathcal{G} = \emptyset$, then the result is clear as $\tilde{F}_{2S',m} = F_{2S',m}$. Otherwise, the leading monomial of $\tilde{F}_{2S',m}$ is less than $\frac{\operatorname{LCM}(S')}{t}$ with $t \in S$ and cannot be a divisor of $\frac{\operatorname{LCM}(S')}{g}$ with $g \in \operatorname{LM}(\mathcal{G})$. Hence it must be at most $\frac{\operatorname{LCM}(S')}{m}$.

Furthermore, for $S = \{1, \dots, s_q\}$, the coefficient of $\frac{\operatorname{LCM}(S')}{m}$ can be read as the last coefficient of this product

$$\begin{array}{c} \\ 1 \\ \vdots \\ s_q \\ m \end{array} \begin{array}{c} \begin{array}{cccc} 1 & \cdots & s_q & m \end{array} \\ \begin{pmatrix} [1] & \cdots & [s_q] & [m] \\ \vdots & & \vdots & \vdots \\ [s_q] & \cdots & [s_q^2] & [m\, s_q] \\ [m] & \cdots & [m\, s_q] & [m^2] \end{pmatrix} \end{array} \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_{s_q} \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ f_{2S',m} \end{pmatrix}.$$

Hence, the relation is valid if, and only if, this coefficient is zero. □

The leading monomial of the higher part of $F_{2S',m}$ tells us whether $C_m$ is a valid relation or not.

**Theorem 26.** *Assuming the* Adaptive Polynomial Scalar-FGLM *algorithm called on table* **w** *returns a Gröbner basis $\mathcal{G}$ with staircase $S$, then the algorithm does not need more that $\#\,2\,(S \cup \operatorname{LM}(\mathcal{G}))$ table queries to recover $\mathcal{G}$.*

*Furthermore, it performs at most $O((\#\,S + \#\,\mathcal{G})^2\,\#\,2\,S)$ operations to recover $\mathcal{G}$.*

*Proof.* Since $\tilde{F}_{2S,t}$ is obtained from $F_{2S,t}$ by removing all the monomials dividing $\frac{\operatorname{LCM}(S)^2}{g}$, $g \in \operatorname{LM}(\mathcal{G})$, then $\tilde{F}_{2S,t}$ is actually the polynomial obtained from the product of the extended matrix $H_{T,S}$ and the vector representing $C_t$, where $T = 2\,S \setminus \{g\,\tau, g \in \operatorname{LM}(\mathcal{G}), \tau \in \mathcal{T}\}$. Hence, updating from $\tilde{F}_{2S,t}$ to $\tilde{F}_{2S',t}$ is equivalent to updating $H_{T,S}$ to $H_{T',S'}$, with $T' = 2\,S' \setminus \{g\,\tau, g \in \operatorname{LM}(\mathcal{G}), \tau \in \mathcal{T}\}$ in this matrix-vector product. Yet, the first nonzero coefficient of this product remains the same through this updating process.

At step $m$, $F_{2S',t} = P_{2S'}\,C_t \bmod B_{2S'}$ for any $t \in S \cup \operatorname{LM}(\mathcal{G})$. As in the end of the step, $m$ is either found to be a member of the final $S$ or the final $\operatorname{LM}(\mathcal{G})$, then $S' \subseteq (S \cup \operatorname{LM}(\mathcal{G}))$ and thus $2\,S' \subseteq 2\,(S \cup \operatorname{LM}(\mathcal{G}))$.

At step $m$, a pair $R_{2S,t} = [F_{2S,t}, C_t]$ is updated into $R_{2\,(S\cup\{m\}),t}$ by adding terms with support in $2\,(S \cup \{m\})$, so in the last step, all the polynomials have support in a set of size $\#\,2\,(S \cup \{g\})$ where $g \in \operatorname{LM}(\mathcal{G})$.

Furthermore, for each monomial $t \in S \cup \operatorname{LM}(\mathcal{G})$, the pair $R_{2S',t}$ is reduced by all the previous ones lying in the staircase or the Gröbner basis in at most $(\#\,S + \#\,\mathcal{G})\,\#\,2\,S$ operations. Hence, at most $O((\#\,S + \#\,\mathcal{G})^2\,\#\,2\,S)$ operations are needed. □

**Example 27.** *We consider the following sequence* $\mathbf{w} = (w_{i,j})_{(i,j)\in\mathbb{N}^2}$

$$\mathbf{w} = \begin{pmatrix} 6 & 9 & 5 & 1 & 10 & -6 & -9 & \cdots \\ 3 & 12 & 2 & 4 & 7 & -3 & -12 & \cdots \\ 6 & 9 & 5 & 1 & 10 & -6 & -9 & \cdots \\ 3 & 12 & 2 & 4 & 7 & -3 & -12 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

*For a pair* $R_{2\,S,t} = [F_{2\,S,t}, C_t]$*, we let* $\tilde{R}_{2\,S,t} = [\tilde{F}_{2\,S,t}, C_t]$.

*We start with* $L = \{1\}$*,* $G = S = \emptyset$*,* $B = (1,1)$ *and* $R_{2\,S,B_1} = [1,0]$*,* $R_{2\,S,B_2} = [1,0]$*.*

1. *We set* $m = 1$*,* $S' = \{1\}$*,* $R_{2\,S',B_1} = [1,0]$*,* $R_{2\,S',B_2} = [y,0]$ *and initialize* $R_{2\,S',1} = [6,1]$*.*
   *As* $\tilde{F}_{2\,S',1} = F_{2\,S',1} = 1$ *and* $\mathrm{LM}(\tilde{F}_{2\,S',1}) = 1 = \frac{\mathrm{LCM}(S')^2}{1}$ *the relation fails.*
   *L is updated to* $\{y, x\}$*.*
2. *We set* $m = y$*,* $S' = \{1, y\}$*,* $R_{2\,S',B_1} = [x,0]$*,* $R_{2\,S',B_2} = [y^3,0]$ *and* $R_{2\,S',1} = [6\,y^2+9\,y+5,1] = \tilde{R}_{2\,S',1}$*.*
   *We initialize* $R_{2\,S',y} = [9\,y^2 + 5\,y, y]$ *using* NormalForm *on* $y\,R_{2\,S',1}$ *and then reduce it to* $[-\frac{17}{2}\,y - \frac{15}{2}, y - \frac{3}{2}]$*.*
   *As* $\tilde{F}_{2\,S',y} = F_{2\,S',y}$ *and* $\mathrm{LM}(\tilde{F}_{2\,S',y}) = \frac{\mathrm{LCM}(S')^2}{y}$ *the relation fails.*
   *L is updated to* $\{x, y^2\}$*.*
3. *We set* $m = x$*,* $S' = \{1, y, x\}$*,* $R_{2\,S',B_1} = [x^3,0]$*,* $R_{2\,S',B_2} = [y^3,0]$*,*
   - $R_{2\,S',1} = [6\,x^2\,y^2 + 9\,x^2\,y + 3\,x\,y^2 + 5\,x^2 + 12\,x\,y + 6\,y^2, 1] = \tilde{R}_{2\,S',1}$*,*
   - $R_{2\,S',y} = [-\frac{17}{2}\,x^2\,y + \frac{15}{2}\,x\,y^2 - \frac{15}{2}\,x^2 - 18\,x\,y - 9\,y^2, y - \frac{3}{2}] = \tilde{R}_{2\,S',y}$*.*

   *We initialize* $R_{2\,S',x} = [3\,x^2\,y^2 + 12\,x^2\,y + 6\,x\,y^2, x]$ *using* NormalForm *on* $x\,R_{2\,S',1}$ *and then reduce it to* $[\frac{189}{17}\,x\,y^2 - \frac{155}{17}\,x^2 - \frac{372}{17}\,x\,y - \frac{186}{17}\,y^2, x + \frac{15}{17}\,y - \frac{31}{17}]$*.*
   *As* $\tilde{F}_{2\,S',x} = F_{2\,S',x}$ *and* $\mathrm{LM}(\tilde{F}_{2\,S',x}) = \frac{\mathrm{LCM}(S')^2}{x}$ *the relation fails.*
   *L is updated to* $\{y^2, x\,y, x^2\}$*.*
4. *We set* $m = y^2$*,* $S' = \{1, y, x, y^2\}$*,* $R_{2\,S',B_1} = [x^3,0]$*,* $R_{2\,S',B_2} = [y^5,0]$*,*
   - $R_{2\,S',1} = [6\,x^2\,y^4 + \cdots, 1] = \tilde{R}_{2\,S',1}$*,*
   - $R_{2\,S',y} = [-\frac{17}{2}\,x^2\,y^3 + \cdots, y - \frac{3}{2}] = \tilde{R}_{2\,S',y}$*,*
   - $R_{2\,S',x} = [\frac{189}{17}\,x\,y^4 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}] = \tilde{R}_{2\,S',x}$*.*

   *We initialize* $R_{2\,S',y^2} = [-\frac{106}{17}\,x\,y^4 + \cdots, y^2 - \frac{13}{17}\,y + \frac{16}{51}]$ *using* NormalFormHigherPart *on* $R_{2\,S',1}$ *and* $R_{2\,S',y}$ *and then reduce it to* $[\frac{1381}{189}\,x^2\,y^2 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$*.*
   *As* $\tilde{F}_{2\,S',y^2} = F_{2\,S',y^2}$ *and* $\mathrm{LM}(\tilde{F}_{2\,S',y^2}) = \frac{\mathrm{LCM}(S')^2}{y^2}$ *the relation fails.*
   *L is updated to* $\{x\,y, x^2, y^3\}$*.*
5. *We set* $m = x\,y$*,* $S' = \{1, y, x, y^2, x\,y\}$*,* $R_{2\,S',B_1} = [x^3,0]$*,* $R_{2\,S',B_2} = [y^5,0]$*,*
   - $R_{2\,S',1} = [6\,x^2\,y^4 + \cdots, 1] = \tilde{R}_{2\,S',1}$*,*
   - $R_{2\,S',y} = [-\frac{17}{2}\,x^2\,y^3 + \cdots, y - \frac{3}{2}] = \tilde{R}_{2\,S',y}$*,*
   - $R_{2\,S',x} = [\frac{189}{17}\,x\,y^4 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}] = \tilde{R}_{2\,S',x}$*,*
   - $R_{2\,S',y^2} = [\frac{1381}{189}\,x^2\,y^2 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}] = \tilde{R}_{2\,S',y^2}$*.*

*We initialize* $R_{2S',xy} = [-\frac{15}{2}\,x^2\,y^4 + \cdots, x\,y - \frac{3}{2}\,x]$ *using* NormalForm *on* $x\,R_{2S',y}$ *and then reduce it to* $[-15\,y^4 - 7\,x^2\,y - x\,y^2 - 14\,y^3 - 10\,x^2 - 4\,x\,y - 5\,y^2, x\,y + x - y - 1]$.
*As* $\tilde{F}_{2S',xy} = F_{2S',xy}$ *and* $\text{LM}(\tilde{F}_{2S',xy}) = y^4 \prec \frac{\text{LCM}(S')^2}{x\,y}$ *the relation succeeds!*
*We update* $R_{2S,xy} = [-9\,x\,y^4 + \cdots, x\,y + x - y - 1]$ *and put it in* $G$.

6. *We set* $m = x^2$, $S' = \{1, y, x, y^2, x^2\}$, $R_{2S',B_1} = [x^5, 0]$, $R_{2S',B_2} = [y^5, 0]$
   - $R_{2S',1} = [6\,x^4\,y^4 + \cdots, 1]$, $\tilde{R}_{2S',1} = [6\,x^4\,y^4 + \cdots, 1]$,
   - $R_{2S',y} = [-\frac{17}{2}\,x^4\,y^3 - + \cdots, y - \frac{3}{2}]$, $\tilde{R}_{2S',y} = [-\frac{17}{2}\,x^4\,y^3 - + \cdots, y - \frac{3}{2}]$,
   - $R_{2S',x} = [\frac{189}{17}\,x^3\,y^4 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$, $\tilde{R}_{2S',x} = [\frac{189}{17}\,x^3\,y^4 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$,
   - $R_{2S',y^2} = [\frac{1381}{189}\,x^4\,y^2 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$, $\tilde{R}_{2S',y^2} = [\frac{1381}{189}\,x^4\,y^2 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$,
   - $R_{2S',xy} = [-4\,x^4\,y^2 + \cdots, x\,y + x - y - 1]$.

   *We initialize* $R_{2S',x^2} = [-\frac{945}{34}\,x^4\,y^3 - x^4\,y^3 + \cdots, x^2 + \frac{15}{17}\,x\,y - \frac{45}{34}\,x + \frac{15}{34}\,y - \frac{47}{17}]$ *using* NormalFormHigherPart *on* $\tilde{R}_{2S',1}$ *and* $\tilde{R}_{2S',x}$ *and notice that the support of* $C_{x^2}$ *contains* $x\,y$ *which is not in* $S'$.
   *We then reduce it to* $[-12\,x^3\,y^3 + \cdots, x^2 - 1]$ *by computing first the reduction of the right part by* $x\,y + x - y - 1$ *and then by computing the reduction of the left parts without taking into account any monomials* $\frac{\text{LCM}(S')^2}{x\,y\,t} = \frac{x^3\,y^3}{t}$.
   *As* $\tilde{F}_{2S',x^2} = -x^4\,y^3 + \cdots \neq F_{2S',x^2}$ *and* $\text{LM}(\tilde{F}_{2S',x^2}) = x^4\,y^3 \prec \frac{\text{LCM}(S')^2}{x^2}$ *the relation succeeds!*
   *We update* $R_{2S,x^2} = [-9\,x^2\,y^3 + \cdots, x^2 - 1]$ *and put it in* $G$.

7. *We set* $m = y^3$, $S' = \{1, y, x, y^2, y^3\}$, $R_{2S',B_1} = [x^3, 0]$, $R_{2S',B_2} = [y^7, 0]$,
   - $R_{2S',1} = [6\,x^2\,y^6 + \cdots, 1]$, $\tilde{R}_{2S',1} = [6\,x^2\,y^6 + \cdots, 1]$,
   - $R_{2S',y} = [-\frac{17}{2}\,x^2\,y^5 - + \cdots, y - \frac{3}{2}]$, $\tilde{R}_{2S',y} = [-\frac{17}{2}\,x^2\,y^5 - + \cdots, y - \frac{3}{2}]$,
   - $R_{2S',x} = [\frac{189}{17}\,x\,y^6 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$, $\tilde{R}_{2S',x} = [\frac{189}{17}\,x\,y^6 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$,
   - $R_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^4 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$, $\tilde{R}_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^4 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$,
   - $R_{2S',xy} = [-9\,x\,y^6 + \cdots, x\,y + x - y - 1]$,
   - $R_{2S',x^2} = [-9\,x^2\,y^5 + \cdots, x^2 - 1]$.

   *We initialize* $R_{2S',y^3} = [-\frac{4204}{1381}\,x\,y^5 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$ *using* NormalFormHigherPart *on* $R_{2S',y}$ *and* $R_{2S',y^2}$.
   *We then reduce it to* $[-\frac{4204}{1381}\,x\,y^5 - \frac{4620}{1381}\,y^6 - \frac{25651}{1381}\,x^2\,y^3 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$ *by computing the reduction of the left parts without taking into account any monomials* $\frac{\text{LCM}(S')^2}{x\,y\,t} = \frac{x\,y^5}{t}$, $\frac{\text{LCM}(S')^2}{x^2\,t} = \frac{y^6}{t}$.
   *As* $\tilde{F}_{2S',y^3} = -\frac{25651}{1381}\,x^2\,y^3 + \cdots \neq F_{2S',y^3}$ *and* $\text{LM}(\tilde{F}_{2S',y^3}) = x^2\,y^3 = \frac{\text{LCM}(S')^2}{y^3}$ *the relation fails!*
   *L is updated to* $\{y^4\}$.

8. *We set* $m = y^4$, $S' = \{1, y, x, y^2, y^3, y^4\}$, $R_{2S',B_1} = [x^3, 0]$, $R_{2S',B_2} = [y^9, 0]$,
   - $R_{2S',1} = [6\,x^2\,y^8 + \cdots, 1]$, $\tilde{R}_{2S',1} = [6\,x^2\,y^8 + \cdots, 1]$,
   - $R_{2S',y} = [-\frac{17}{2}\,x^2\,y^7 - + \cdots, y - \frac{3}{2}]$, $\tilde{R}_{2S',y} = [-\frac{17}{2}\,x^2\,y^7 - + \cdots, y - \frac{3}{2}]$,
   - $R_{2S',x} = [\frac{189}{17}\,x\,y^8 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$, $\tilde{R}_{2S',x} = [\frac{189}{17}\,x\,y^8 + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$,

- $R_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^6 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$, $\tilde{R}_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^6 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$,
- $R_{2S',y^3} = [\frac{5463}{1381}\,x\,y^7 - \frac{4620}{1381}\,y^8 - \frac{25651}{1381}\,x^2\,y^5 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$, $\tilde{R}_{2S',y^3} = [-\frac{25651}{1381}\,x^2\,y^5 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$,
- $R_{2S',xy} = [-9\,x\,y^8 + \cdots, x\,y + x - y - 1]$,
- $R_{2S',x^2} = [-9\,x^2\,y^7 + \cdots, x^2 - 1]$.

*We initialize* $R_{2S',y^4}$ *using* NormalFormHigherPart *on* $R_{2S',y^2}$ *and* $R_{2S',y^3}$ *and then reduce it to* $[-\frac{571416}{25651}\,x\,y^7 + \cdots + \frac{504287}{25651}\,x^2\,y^4 + \cdots, y^4 - \frac{29900}{25651}\,y^3 + \frac{7703}{25651}\,y^2 + \frac{72041}{25651}\,x - \frac{35598}{25651}\,y - \frac{26811}{25651}]$ *by computing the reduction of the left parts without taking into account any monomials* $\frac{\text{LCM}(S')^2}{x\,y\,t} = \frac{x\,y^7}{t}$, $\frac{\text{LCM}(S')^2}{x^2\,t} = \frac{y^8}{t}$.

*As* $\tilde{F}_{2S',y^4} = \frac{504287}{25651}\,x^2\,y^4 + \cdots \neq F_{2S',y^3}$ *and* $\text{LM}(\tilde{F}_{2S',y^4}) = x^2\,y^4 = \frac{\text{LCM}(S')^2}{y^4}$ *the relation fails! L is updated to* $\{y^5\}$.

9. *We set* $m = y^5$, $S' = \{1, y, x, y^2, y^3, y^4, y^5\}$, $R_{2S',B_1} = [x^3, 0]$, $R_{2S',B_2} = [y^{11}, 0]$,
   - $R_{2S',1} = [6\,x^2\,y^{10} + \cdots, 1]$, $\tilde{R}_{2S',1} = [6\,x^2\,y^{10} + \cdots, 1]$,
   - $R_{2S',y} = [-\frac{17}{2}\,x^2\,y^9 - + \cdots, y - \frac{3}{2}]$, $\tilde{R}_{2S',y} = [-\frac{17}{2}\,x^2\,y^9 - + \cdots, y - \frac{3}{2}]$,
   - $R_{2S',x} = [\frac{189}{17}\,x\,y^{10} + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$, $\tilde{R}_{2S',x} = [\frac{189}{17}\,x\,y^{10} + \cdots, x + \frac{15}{17}\,y - \frac{31}{17}]$,
   - $R_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^8 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$, $\tilde{R}_{2S',y^2} = [\frac{1381}{189}\,x^2\,y^8 + \cdots, y^2 + \frac{106}{189}\,x - \frac{17}{63}\,y - \frac{134}{189}]$,
   - $R_{2S',y^3} = [\frac{5463}{1381}\,x\,y^9 - \frac{4620}{1381}\,y^{10} - \frac{25651}{1381}\,x^2\,y^7 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$, $\tilde{R}_{2S',y^3} = [-\frac{25651}{1381}\,x^2\,y^7 + \cdots, y^3 + \frac{1354}{1381}\,y^2 - \frac{607}{1381}\,x - \frac{190}{1381}\,y - \frac{770}{1381}]$,
   - $R_{2S',y^4} = [-\frac{648369}{25651}\,x\,y^9 + \cdots + \frac{504287}{25651}\,x^2\,y^6 + \cdots, y^4 - \frac{29900}{25651}\,y^3 + \frac{7703}{25651}\,y^2 + \frac{72041}{25651}\,x - \frac{35598}{25651}\,y - \frac{26811}{25651}]$, $\tilde{R}_{2S',y^4} = [\frac{504287}{25651}\,x^2\,y^6 + \cdots, y^4 - \frac{29900}{25651}\,y^3 + \frac{7703}{25651}\,y^2 + \frac{72041}{25651}\,x - \frac{35598}{25651}\,y - \frac{26811}{25651}]$,
   - $R_{2S',xy} = [-9\,x\,y^{10} + \cdots, x\,y + x - y - 1]$,
   - $R_{2S',x^2} = [-9\,x^2\,y^9 + \cdots, x^2 - 1]$.

   *We initialize* $R_{2S',y^5}$ *using* NormalFormHigherPart *on* $R_{2S',y^3}$ *and* $R_{2S',y^4}$ *and then reduce it to* $[12\,x\,y^9 + 6\,y^{10} + 2\,x\,y^8 + 4\,x\,y^7 + 7\,x\,y^6 - 9\,x^2\,y^4 - 3\,x\,y^5 - 5\,x^2\,y^3 - x^2\,y^2 - 10\,x^2\,y + 6\,x^2, y^5 + 1]$ *by computing the reduction of the left parts without taking into account any monomials* $\frac{\text{LCM}(S')^2}{x\,y\,t} = \frac{x\,y^9}{t}$, $\frac{\text{LCM}(S')^2}{x^2\,t} = \frac{y^{10}}{t}$.

   *As* $\tilde{F}_{2S',y^5} = -9\,x^2\,y^4 + \cdots \neq F_{2S',y^3}$ *and* $\text{LM}(\tilde{F}_{2S',y^5}) = x^2\,y^4 \prec \frac{\text{LCM}(S')^2}{y^5}$ *the relation succeeds! We update* $R_{2S,y^5} = [3\,x\,y^8 + \cdots, y^5 + 1]$ *and put it in G.*

*The algorithms returns G, in particular the second part of each pair:* $[x\,y + x - y - 1, x^2 - 1, y^5 + 1]$.

**Remark 28.** *At step* $y^4$*, updating* $R_{2S,y^3}$ *into* $R_{2S',y^3}$ *makes the leading monomial of* $F_{2S',y^3}$, $\frac{5463}{1381}\,\frac{\text{LCM}(S')^2}{x\,y}$*, totally different from this of* $F_{2S,y^3}$, $-\frac{4204}{1381}\,\frac{\text{LCM}(S)^2}{x\,y}$*. However, this is not the case when considering the leading monomials of* $\tilde{F}_{2S',y^3}$ *and* $\tilde{F}_{2S,y^3}$*, as* $\text{LM}(\tilde{F}_{2S',y^3}) = -\frac{25651}{1381}\,\frac{\text{LCM}(S')^2}{y^3} = \text{LM}(\tilde{F}_{2S,y^3})\,\frac{\text{LCM}(S')^2}{\text{LCM}(S)^2}$.

## 6. Experiments

In this section, we report on the number of counted arithmetic operations performed by the different algorithms for computing the Gröbner basis of the ideal of relations of some table families. They are counted using naive multiplications. To do so, we have a counter that is incremented by 1 each time a product in the base field is performed. For advanced functions that were not recoded, we use a formula. For instance, after a call to NormalForm($F_m$, $[F_1, \ldots, F_r]$), assuming the associated quotients are $Q_1, \ldots, Q_r$, then we use the following formula to increment the counter

$$\#\operatorname{supp} Q_1 \#\operatorname{supp} F_1 + \cdots + \#\operatorname{supp} Q_r \#\operatorname{supp} F_r.$$

Our implementation is available at `https://www-polsys.lip6.fr/~berthomieu/Guessing.mpl`.

For the Scalar-FGLM algorithm, this corresponds to the number of multiplications in the Gaussian elimination step to determine the staircase and the number of multiplications to solve the triangular systems, for each polynomial in the output Gröbner basis, to compute its coefficients.

For the BMS algorithm, this corresponds to the number of multiplications for testing each relation at a monomial and then updating the set of relations by correcting some of them or building new ones.

For the AGbb algorithm, this corresponds to the number of multiplications for computing the modified Gram-Schmidt orthogonalization process and the evaluation of polynomials on the table.

For the Polynomial Scalar-FGLM algorithm, this corresponds to the number of multiplications to obtain the partial quotients in the normal forms computations and the polynomials $R_m$'s.

Three families in dimension 2 (Figure 1) and dimension 3 (Figure 2) are tested. For each of them we use the $\text{DRL}(z \prec y \prec x)$ ordering and denote by $S$ the staircase and $\text{LM}(\mathcal{G})$ the set of the leading monomials of the Gröbner basis of relations.

**Rectangle tables:** $\text{LM}(\mathcal{G}) = \{y^{\lfloor d/2 \rfloor}, x^d\}$ in dimension 2 and $\text{LM}(\mathcal{G}) = \{z^{\lceil d/3 \rceil}, y^{\lfloor d/2 \rfloor}, x^d\}$ dimension 3. This case is the best for the size of the Gröbner basis compared to the size of the staircase.

**L-shape tables:** $\text{LM}(\mathcal{G}) = \{x\,y, y^d, x^d\}$ in dimension 2 and $\text{LM}(\mathcal{G}) = \{y\,z, x\,z, x\,y, z^d, y^d, x^d\}$ in dimension 3. This case is the worst for the number of table queries compared to the sizes of the staircase and the Gröbner basis.

**Simplex tables:** $\text{LM}(\mathcal{G}) = \{y^d, x\,y^{d-1}, \ldots, x^d\}$ in dimension 2 and $\text{LM}(\mathcal{G}) = \{z^d, y\,z^{d-1}, x\,z^{d-1}, \ldots, y^d, x\,y^{d-1}, \ldots, x^d\}$ in dimension 3, i.e. all the monomials of degree $d$. This case is the best for the number of table queries and the worst for the size of the Gröbner basis, both compared to the size of the staircase.

Let $a = \max(S \cup \text{LM}(\mathcal{G}))$. Generically, a relation $C_m$ fails when shifted by $m$. From [10, Prop. 10], we know that the BMS algorithm recover all the relations when called up to monomial $\max(S)\,\max(S \cup \text{LM}(\mathcal{G}))$. Yet, if $\max(\text{LM}(\mathcal{G})) > \max(S)$, then for $g \in \text{LM}(\mathcal{G})$, the relation $C_g$ is not necessarily shifted by $g$, so we called it with $a^2$. So was the AGbb algorithm. The Scalar-FGLM algorithm was called on $U = T = \mathcal{T}_{\preceq a}$. The Polynomial Scalar-FGLM algorithm was called on $U = \{1\}, T = \mathcal{T}_{\preceq a^2}$ and $U = T = \mathcal{T}_{\preceq a}$ and we report the lower number of operations.

The Polynomial Scalar-FGLM algorithm performs fewer arithmetic operations than the others, for large $d$. More precisely, its number of operations appears to be linear in $(\#S)^2 = O(\#S\,(\#S + \#\mathcal{G}))$ in fixed dimension.

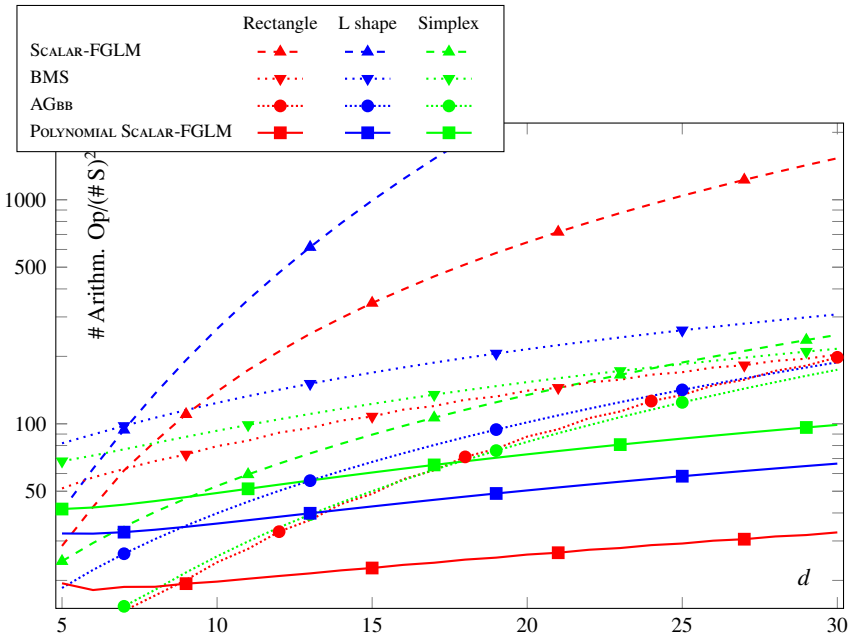



Figure 1: Number of arithmetic operations (2D)

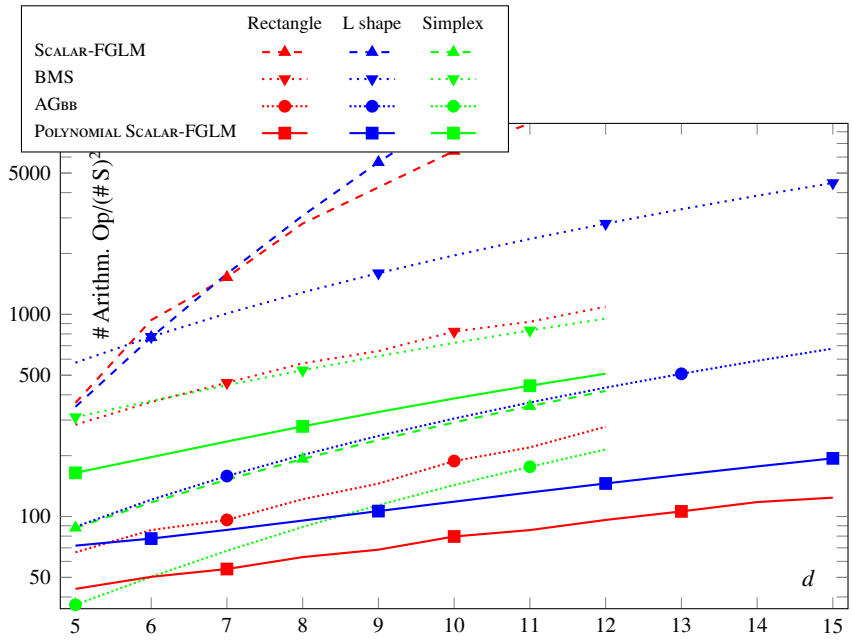



Figure 2: Number of arithmetic operations (3D)

**Simplex tables:** While it seems the AGbb and Scalar-FGLM algorithms are the fastest in Figure 2, we can expect that it will not be the case in higher degrees where the Polynomial Scalar-FGLM will be the fastest. This phenomenon is already observed in Figure 1 in low degree. This would confirm the observed speedup in dimension 2 to also dimension 3.

**L-shape tables:** Although the obtained speedups are not negligible, the adaptive variant should allow us to perform even fewer operations. See Section 5.

**Rectangle tables:** While this family has the best behavior for the BMS algorithm, the Polynomial Scalar-FGLM algorithm has an even greater speedup than in the Simplex case.

In the following Figures 3 and 4, we compare the number of operations performed by the Polynomial Scalar-FGLM, the Adaptive Scalar-FGLM and the Adaptive Polynomial Scalar-FGLM algorithms on these three families. First, as we can expect, the Adaptive Polynomial Scalar-FGLM algorithms always performs fewer operations than the Polynomial Scalar-FGLM algorithm. This happens even when giving the sharper sets of monomials $\mathcal{T}_{\leq a}$ and $\mathcal{T}_{\leq b}$ for the Polynomial Scalar-FGLM algorithm. Furthermore, like in the non-adaptive case, the polynomial arithmetic seems to be faster than the linear algebra ones. Though, it would be interesting to compare with a less naive implementation of the Adaptive Scalar-FGLM algorithm.

That being said, in three variables, the Adaptive Scalar-FGLM algorithm is the better one for the L-shape family in small size, until the Adaptive Polynomial Scalar-FGLM becomes the better one for bigger sizes. As the crossing happens later in 3D than in 2D, it is possible that the more variables, the bigger the degrees need to be for the Adaptive Polynomial Scalar-FGLM algorithm to be better than the Adaptive Scalar-FGLM algorithm, for this family. This makes the Adaptive Scalar-FGLM algorithm still a suited algorithm in this context.

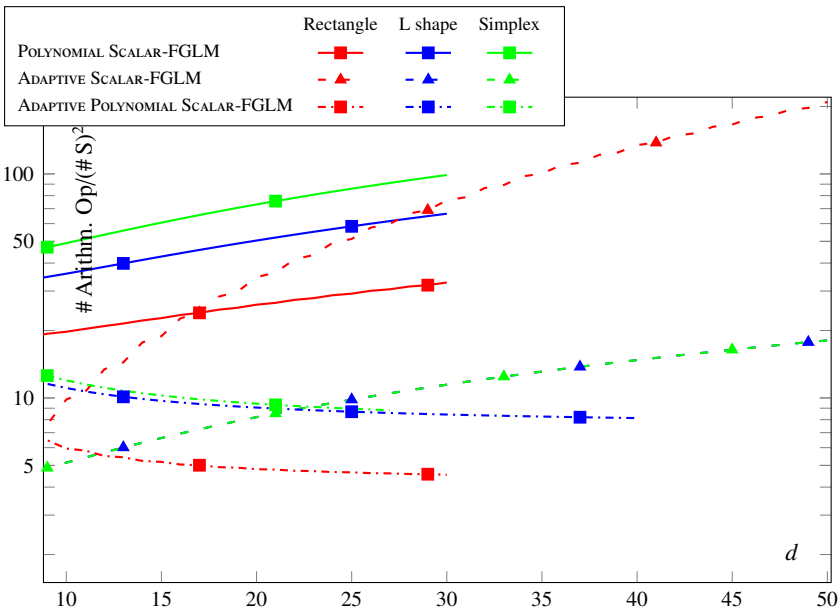



Figure 3: Number of arithmetic operations, for the adaptive variants, compared with the Polynomial Scalar-FGLM algorithm (2D)

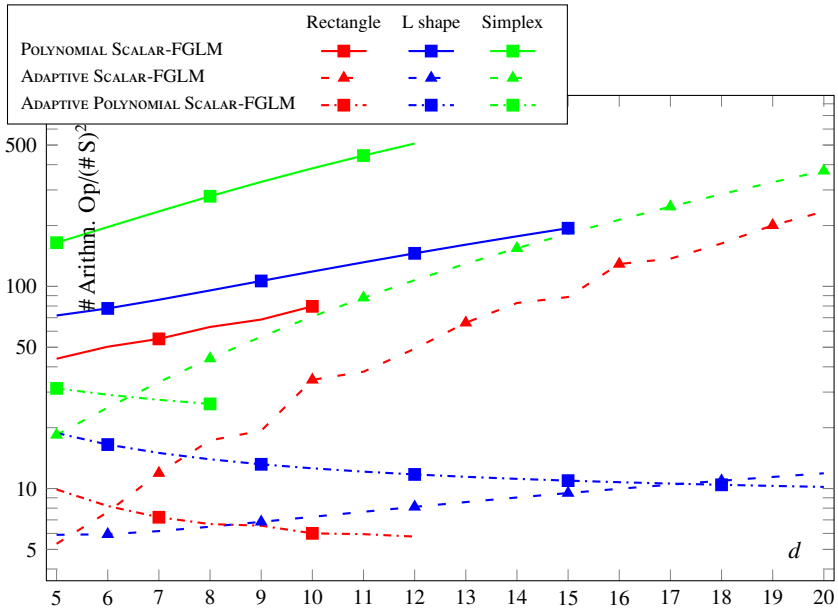



Figure 4: Number of arithmetic operations, for the adaptive variants, compared with the Polynomial Scalar-FGLM algorithm (3D)


## Acknowledgments

We thank the anonymous referees for their careful reading and their helpful comments to improve this paper. The authors are supported by the joint ANR-FWF ANR-19-CE48-0015 ECARP project, the ANR grants ANR-18-CE33-0011 Sesame and ANR-19-CE40-0018 De Rerum Natura projects, the PGMO grant CAMiSAdo and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement N. 813211 (POEMA).


## References


[1] Beckermann, B., Labahn, G., 1994. A uniform approach for the fast computation of matrix-type pade approximants. SIAM J. Matrix Anal. Appl. 15, 804–823. doi:10.1137/S0895479892230031.

[2] Berlekamp, E., 1968. Nonbinary BCH decoding. IEEE Trans. Inform. Theory 14, 242–242. doi:10.1109/TIT.1968.1054109.

[3] Berthomieu, J., Boyer, B., Faugère, J.Ch., 2015. Linear algebra for computing gröbner bases of linear recursive multidimensional sequences, in: Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation, ACM, New York, NY, USA. pp. 61–68. doi:10.1145/2755996.2756673.

[4] Berthomieu, J., Boyer, B., Faugère, J.Ch., 2017. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. Journal of Symbolic Computation 83, 36–67. doi:10.1016/j.jsc.2016.11.005. special issue on the conference ISSAC 2015: Symbolic computation and computer algebra.

[5] Berthomieu, J., Faugère, J.Ch., 2018. A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations, in: Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation, ACM, New York, NY, USA. pp. 79–86. doi:10.1145/3208976.3209017.

[6] Berthomieu, J., Faugère, J.Ch., 2020. In-depth comparison of the berlekamp–massey–sakata and the scalar-fglm algorithms: The adaptive variants. Journal of Symbolic Computation 101, 270–303. doi:10.1016/j.jsc.2019.09.001.

[7] Berthomieu, J., Faugère, J.Ch., 2021. Experiments. URL: http://www-polsys.lip6.fr/~berthomieu/JSC2021.html.
[8] Blackburn, S.R., 2006. Fast rational interpolation, reed-solomon decoding, and the linear complexity profiles of sequences. IEEE Trans. Inf. Theor. 43, 537–548. doi:10.1109/18.556111.
[9] Bose, R., Ray-Chaudhuri, D., 1960. On a class of error correcting binary group codes. Information and Control 3, 68 – 79. doi:10.1016/S0019-9958(60)90287-4.
[10] Bras-Amorós, M., O'Sullivan, M.E., 2006. The correction capability of the Berlekamp–Massey–Sakata algorithm with majority voting. Applicable Algebra in Engineering, Communication and Computing 17, 315–335. doi:10.1007/s00200-006-0015-8.
[11] Brent, R.P., Gustavson, F.G., Yun, D.Y., 1980. Fast solution of Toeplitz systems of equations and computation of Padé approximants. Journal of Algorithms 1, 259 – 295. doi:10.1016/0196-6774(80)90013-9.
[12] Cantor, D.G., Kaltofen, E., 1991. On fast multiplication of polynomials over arbitrary algebras. Acta Informatica 28, 693–701. doi:10.1007/BF01178683.
[13] Cooley, J.W., Tukey, J.W., 1965. An algorithm for the machine calculation of complex fourier series. Mathematics of Computation 19, 297–301. URL: http://www.jstor.org/stable/2003354, doi:10.2307/2003354.
[14] Cox, D., Little, J., O'Shea, D., 2015. Ideals, Varieties, and Algorithms. Undergraduate Texts in Mathematics. fourth ed., Springer, New York. An introduction to computational algebraic geometry and commutative algebra.
[15] Dornstetter, J., 1987. On the equivalence between Berlekamp's and Euclid's algorithms (corresp.). IEEE Transactions on Information Theory 33, 428–431. doi:10.1109/TIT.1987.1057299.
[16] Faugère, J.Ch., Mou, C., 2011. Fast algorithm for change of ordering of zero-dimensional gröbner bases with sparse multiplication matrices, in: Proceedings of the 36th International Symposium on Symbolic and Algebraic Computation, ACM, New York, NY, USA. pp. 115–122. doi:10.1145/1993886.1993908.
[17] Faugère, J.Ch., Mou, C., 2017. Sparse FGLM algorithms. Journal of Symbolic Computation 80, 538 – 569. doi:10.1016/j.jsc.2016.07.025.
[18] Fitzpatrick, P., Flynn, J., 1992. A gröbner basis technique for padé approximation. J. Symbolic Comput. 13, 133 – 138. doi:10.1016/S0747-7171(08)80087-9.
[19] Fitzpatrick, P., Norton, G., 1990. Finding a basis for the characteristic ideal of an $n$-dimensional linear recurring sequence. IEEE Trans. Inform. Theory 36, 1480–1487. doi:10.1109/18.59953.
[20] Hocquenghem, A., 1959. Codes correcteurs d'erreurs. Chiffres 2, 147 – 156.
[21] Hoeven, J.v.d., Larrieu, R., 2019. Fast Gröbner basis computation and polynomial reduction for generic bivariate ideals. AAECC 30, 509–539. doi:10.1007/s00200-019-00389-9.
[22] Jonckheere, E., Ma, C., 1989. A simple Hankel interpretation of the Berlekamp-Massey algorithm. Linear Algebra Appl. 125, 65 – 76. doi:10.1016/0024-3795(89)90032-3.
[23] Levinson, N., 1947. The Wiener RMS (Root-Mean-Square) error criterion in the filter design and prediction. J. Math. Phys. 25, 261–278. doi:10.1002/sapm1946251261.
[24] Massey, J.L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127. doi:10.1109/TIT.1969.1054260.
[25] Mourrain, B., 2017. Fast algorithm for border bases of artinian gorenstein algebras, in: Proceedings of the 2017 ACM on International Symposium on Symbolic and Algebraic Computation, ACM, New York, NY, USA. pp. 333–340. doi:10.1145/3087604.3087632.
[26] Naldi, S., Neiger, V., 2020. A divide-and-conquer algorithm for computing gröbner bases of syzygies in finite dimension, in: Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery, New York, NY, USA. p. 380–387. doi:10.1145/3373207.3404059.
[27] Sakata, S., 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. Symbolic Comput. 5, 321–337. doi:10.1016/S0747-7171(88)80033-6.
[28] Sakata, S., 1990. Extension of the Berlekamp-Massey algorithm to $N$ Dimensions. Inform. and Comput. 84, 207–239. doi:10.1016/0890-5401(90)90039-K.
[29] Sakata, S., 2009. The bms algorithm, in: Sala, M., Sakata, S., Mora, T., Traverso, C., Perret, L. (Eds.), Gröbner Bases, Coding, and Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 143–163. doi:10.1007/978-3-540-93806-4_9.
[30] Wiener, N., 1964. Extrapolation, Interpolation, and Smoothing of Stationary Time Series. The MIT Press, Cambridge, MA.