In-depth comparison of the Berlekamp – Massey – Sakata and the Scalar-FGLM algorithms: the non adaptive variants

Jérémy Berthomieu, Jean-Charles Faugère

In-depth comparison of the Berlekamp – Massey – Sakata and the Scalar-FGLM algorithms: the non adaptive variants

Jérémy Berthomieu*, Jean-Charles Faugère

Sorbonne Universités, UPMC *Univ Paris 06,* CNRS*,* INRIA*,*
*Laboratoire d'Informatique de Paris 6 (*LIP6*), Équipe* PolSys*,*
4 place Jussieu, 75252 Paris Cedex 05, France

Abstract

We compare thoroughly the Berlekamp – Massey – Sakata algorithm and the Scalar-FGLM algorithm, which compute both the ideal of relations of a multi-dimensional linear recurrent sequence.

Suprisingly, their behaviors differ. We detail in which way they do and prove that it is not possible to tweak one of the algorithms in order to mimic exactly the behavior of the other.

Keywords: The BMS algorithm, the Scalar-FGLM algorithm, Gröbner basis computation, multidimensional linear recurrent sequence, algorithms comparison

Contents

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

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

1. Introduction

Computing the smallest linear recurrence relation satisfied by a sequence is a fundamental problem in Computer Science. It is the shortest linear feedback shift register (LFSR) which generates the sequence. The length of this relation estimates the linear complexity of the sequence.

In the 18th century, Gauß was interested in predicting the next term of a sequence. Given a discrete set $(u_i)_{i\in\mathbb{N}}$, find the best coefficients, in the least-squares sense, $(\alpha_i)_{1\leq i\leq d}$ that will approximate u_i by $-\sum_{k=1}^{d}\alpha_k\, u_{i-k}$. Least-square sense means that the solution minimizes the sum of the squares of the errors.

This problem has also been extensively used in Digital Signal Processing theory and applications. Numerically, Levinson – Durbin recursion method can be used to solve this problem. Hence, to some extent, the original Levinson – Durbin problem in Norbert Wiener's Ph.D. thesis, Levinson (1947); Wiener (1964), predates the Hankel interpretation of the Berlekamp – Massey algorithm, see for instance Jonckheere and Ma (1989).

The Berlekamp – Massey algorithm (BM, Berlekamp (1968); Massey (1969)) guesses a solution of this problem for sequences with one parameter, i.e. in the one-dimensional case. This algorithm has been tremendously studied and many variants

were designed. We refer the reader to Kaltofen and Pan (1991); Kaltofen and Yuhasz (2013a,b) for a very nice classification of the BM algorithms for solving this problem, and for its generalization to matrix sequences.

Classically, two designs of the BM algorithm are used.

The first one assumes that the coefficients of the sequence $(u_i)_{i\in\mathbb{N}}$ are given *online*, i.e. u_{i+1} is known only after u_i, and that a bound d is given such that u_{d-1} will be computed but not u_d. Then, the BM algorithm guesses a linear recurrence relation satisfied by the table $(u_0, \ldots, u_i)$, checks if this relation is satisfied by $(u_0, \ldots, u_{i+1})$ and updates the relation if it was not. The algorithm stops when reaching u_{d-1}.

The other one assumes that the table $(u_0, \ldots, u_{d-1})$ is known at once. Then, the algorithm finds the kernel of the Hankel matrix of size $\lceil d/2\rceil \times \lfloor d/2\rfloor$ associated with the sequence $(u_i)_{i\in\mathbb{N}}$. A complexity breakthrough is reached since this comes down to calling the extended Euclidean algorithm between x^d and $U(x) = \sum_{i=0}^{i-1} u_i\, x^{d-i-1}$ and stopping it prematurely when reaching a remainder of degree strictly less than $\lfloor d/2\rfloor$. The relation is then given by the Bézout coefficient of $U(x)$ associated with this remainder. See Blackburn (1997); Dornstetter (1987).

Sakata extended the BM algorithm to 2 dimensions in Sakata (1988) and then to n dimensions in Sakata (1990, 2009). The so-called Berlekamp – Massey – Sakata algorithm (BMS) guesses a Gröbner basis of the ideal of relations satisfied by the first terms of the input sequence, (Sakata, 1990, Lemma 5).

In a way, the BMS algorithm extends the first design of the BM algorithm, as when calling the BMS algorithm on a univariate sequence, it behaves exactly like the BM algorithm on this sequence.

The so-called Scalar-FGLM algorithm, presented in Berthomieu et al. (2015, 2016) guesses the reduced Gröbner basis of the ideal of relations of a sequence. It extends the second design of the BM algorithm through the computation of the kernel of a *multi-Hankel* matrix, the multivariate generalization of a Hankel matrix. However, no fast method is currently known for computing this kernel.

While the second design of the BM algorithm seems more efficient than the first one, mainly thanks to fast Euclidean algorithms, it is not clear how their multidimensional extensions compare. Surprisingly, the BMS and the Scalar-FGLM algorithm behave so differently that it is not possible to apply a small modification on either algorithm in order to simulate the behavior of the other.

1.1. Related works

Computing linear recurrence relations of multi-dimensional sequences finds applications in Coding Theory, Computer Algebra and Combinatorics.

Historically, the BM algorithm was designed to decode cyclic codes, like the BCH codes, Bose and Ray-Chaudhuri (1960); Hocquenghem (1959). Therefore,

decoding n-dimensional cyclic codes, a generalization of Reed Solomon codes, was Sakata's motivation for designing the BMS algorithm in Sakata (1991).

On the other hand, as the output of the BMS and the Scalar-FGLM algorithms is a Gröbner basis, a natural application in Computer Algebra is the computation of a Gröbner basis of an ideal for another order, typically from a total degree ordering to an elimination ordering. In fact the latest versions of the Sparse-FGLM algorithm rely heavily on the BM and BMS algorithms, see Faugère and Mou (2011, 2017).

Finally, computing linear recurrence relations with *polynomial* coefficients finds applications in Computer Algebra for computing properties of univariate and multivariate Special Functions. The Dynamic Dictionary of Mathematical Functions (DDMF, Benoit et al. (2010)) generates automatically web-pages on univariate special functions through the differential equations they satisfy. Equivalently, they could be generated through the linear recurrence relations satisfied by the sequence of coefficients of their Taylor series. Deciding whether 2D/3D-space walks are D-finite or not finds applications in Combinatorics, see Banderier and Flajolet (2002); Bostan et al. (2014); Bousquet-Mélou and Mishna (2010); Bousquet-Mélou and Petkovšek (2003). This motivated the authors to extend the Scalar-FGLM algorithm to handle relations with polynomial coefficients in Berthomieu and Faugère (2016).

1.2. Contributions

The main goal of this paper is to compare both the BMS and the Scalar-FGLM algorithms. As it is not possible to store the whole input sequence, both algorithms takes a bound as an input and only handle sequence terms up to this index bound.

We start by recalling some classical notation and definitions that shall be used in the proofs and the algorithms of the paper in Section 2.

Then, in order to be self-contained, we dedicate the next two sections to a presentation of each algorithm.

A lot of articles, such as Bras-Amorós and O'Sullivan (2006); Sakata (1988, 1990, 2009), or book chapters, such as (Cox et al., 2005, Chapter 10), present the BMS algorithm. Some of them deals with the very general case of an ordered domain. We specialize this description to the simpler case of a polynomial ring $\mathbb{K}[x_1, \ldots, x_n]$. In the BMS algorithm, the input bound is a monomial, so that the algorithm shall visit every monomial in increasing order up to the bound.

On the other hand, in Section 4, we describe the Scalar-FGLM algorithm with a point of view closer to the BMS algorithm. In the Scalar-FGLM algorithm, the input bound is a set of terms which contains the staircase of the computed Gröbner basis.

These presentations shall help us to first design a new algorithm in between both of them in Section 5.

Then, it will help us to compare them in Section 6, our main contribution of this paper. We detail exactly how both algorithms behave similarly and how, depending on the input, they can surprisingly differ.

A main likeness between both algorithms is that they determine which monomials are in the Gröbner basis staircase. However, they handle the leading terms outside of this staircase differently.

Theorem 1. *Let* $\mathbf{u} = (u_{i,j})_{(i,j)\in\mathbb{N}^2}$ *be a sequence, let* $\prec$ *be a degree monomial ordering.*

Assuming we call each algorithm on $\mathbf{u}$*,* $\prec$ *and a bound allowing us to find the same set* S *as the staircase, then*

- *for any monomial* m *on the border of* S*, the* BMS *algorithm returns a relation with leading term* m*. Therefore, the computed ideal of relations is zero-dimensional.*
- *the* Scalar-FGLM *algorithm returns relations with leading terms on the border of* S *but may fail to close the staircase. Therefore, the computed ideal of relations might be positive-dimensional.*

If $\mathbf{u}$ *is linear recurrent and the bound big enough, then both algorithms compute correctly the ideal of relations of* $\mathbf{u}$*.*

The last part of the theorem is important as in most applications $\mathbf{u}$ *is* linear recurrent. Therefore, both algorithms are able to retrieve the ideal of relations of $\mathbf{u}$.

We refer to Theorem 15 for a more precise and general version of this result.

By design, these algorithms return a set of relations, satisfied by the sequence terms, and their shifts, i.e. how far these relations have been tested. The following theorem proves that the outputs of the algorithms are quite different. This should convince the reader that the algorithms do not compute the same thing whenever the bound is too low or $\mathbf{u}$ is not linear recurrent. It is a specialization of Theorem 19 to the binomial sequence.

Theorem 2. *Let* $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$ *be the sequence of the binomial coefficients and let* $\prec$ *be a total degree monomial ordering.*

Assuming we call each algorithm on $\mathbf{b}$*,* $\prec$ *and a bound allowing us to retrieve the same relations* $xy - y - 1, y^d, (x-1)^d$*, with* $d > 2$*.*

- *Then, the* Scalar-FGLM *algorithm ensures that the shifts of the three relations are equal: they are still valid when multiplied by all the monomials of degree at most* $d - 1$*.*

- *The* BMS *algorithm ensures that the shifts of* y^d *and* $(x-1)^d$ *are less than the shift of* $xy-y-1$*: relations* y^d *and* $(x-1)^d$ *are still valid when multiplied by all the monomials of degree at most* $d-1$ *while relation* $xy-y-1$ *is still valid when multiplied by all the monomials of degree at most* $2d-3$*.*

In other words, the lesser the leading monomial of a relation computed by the BMS *algorithm, the greater its shift.*

We mention earlier that the Sparse-FGLM algorithm was a possible application of these algorithms. Although, they are not meant to be run with the lexicographical ordering, we prove the following result to illustrate the difference in behaviors of these algorithms. This result is extended to any dimension in Theorem 20.

Theorem 3. *Let* $\mathbf{u} = (u_{i,j})_{(i,j)\in\mathbb{N}^2}$ *be a linear recurrent sequence whose ideal of relations* $I = \langle g(y), x - f(y)\rangle$ *is in* shape position *for the* lex$(y \prec x)$ *ordering, with* $\deg f < \deg g = d$ *and* g *squarefree.*

Assuming we call each algorithm on $\mathbf{u}$*, the* lex$(y \prec x)$ *ordering, and a bound on the sequence terms.*

- *The* Scalar-FGLM *algorithm, with the set of terms* $T = \{1, y, \ldots, y^{d-1}\}$*, yields the ideal* I*.*
- *The* BMS *algorithm, visiting monomials* $1, y, \ldots, y^d$*, yields the ideal* $\langle g(y), x\rangle$*. This ideal is not* I *unless* $f = 0$*.*

In other words, the Scalar-FGLM *algorithm can retrieve an ideal of relations in shape position while, in general, the* BMS *algorithm cannot.*

Finally, in Section 7, we compare the algorithms based on the number of basic operations and the number of table queries they perform.

We show that the Scalar-FGLM algorithm performs in general more queries to the table than the BMS algorithm. Yet, in the best case scenario where the leading terms of the Gröbner basis of the ideal are all the monomials of a given degree, the Scalar-FGLM has a better behavior than the BMS algorithm.

1.3. Perspectives

We are now in a position where the BMS algorithm and the Scalar-FGLM algorithm are well understood and where we know that each algorithm has strengths and weaknesses.

As anticipated in the original paper, the naive linear algebra solver in the Scalar-FGLM algorithm is its main weakness. Therefore, a fast multi-Hankel solver could improve this algorithm. Moreover, although its presentation is of a

global algorithm, it can be turned into an iterative one using naive Gaussian elimination. Thus, a fast multi-Hankel arithmetic could also be useful for an iterative variant of the algorithm.

On the other hand, the BMS algorithm is a real iterative algorithm: if in addition of the relations, one outputs the set of failing relations (see Remark 10), then one could continue the computation up to a farther bound with no additional cost. Moreover, it is a faster algorithm since it uses a polynomial arithmetic instead of a linear algebra one.

A consequence of this paper could be the design of an hybrid algorithm taking advantage of both the BMS and the Scalar-FGLM algorithms. Another direction would be the study of adaptive variants of the algorithms. The Adaptive Scalar-FGLM (Berthomieu et al. (2015, 2016)) is a more efficient variant of the Scalar-FGLM algorithm trying not to test too far the computed relations in order to minimize the table queries and the complexity. Likewise, one could design an adaptive variant of the BMS algorithm based on this philosophy and study their complexities.

In summary, the goal would be to take a step further in the hybrid approach using the efficiency of the polynomial arithmetic in the BMS algorithm to compute the relations and the smaller number of queries performed by the Adaptive Scalar-FGLM algorithm.

2. Preliminaries

In this section, we present classical notation that shall be used all along the paper. We also present some definitions that will be useful for all the proofs and algorithms.

2.1. Sequences and relations

Let $n \geq 1$, we write $\mathbf{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$. Likewise, we denote $\mathbf{x} = (x_1, \ldots, x_n)$ and for $\mathbf{i} \in \mathbb{N}^n$, we write $\mathbf{x}^\mathbf{i} = x_1^{i_1} \cdots x_n^{i_n}$. Let $\mathbf{u} = (u_\mathbf{i})_{\mathbf{i} \in \mathbb{N}^n}$ be a n-dimensional sequence over the field $\mathbb{K}$. If there exists a finite set of indices $\mathcal{K} \subset \mathbb{N}^n$ and numbers $(\alpha_\mathbf{k})_{\mathbf{k} \in \mathcal{K}}$ in the field $\mathbb{K}$ such that

$$\forall \mathbf{i} \in \mathbb{N}^n, \sum_{\mathbf{k} \in \mathcal{K}} \alpha_\mathbf{k} \, u_{\mathbf{k}+\mathbf{i}} = 0, \tag{1}$$

then we say that $\mathbf{u}$ satisfies the linear recurrence relation (simply relation in the following) defined by $\boldsymbol{\alpha} = (\alpha_\mathbf{k})_{\mathbf{k} \in \mathcal{K}}$.

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

$$\forall (i,j) \in \mathbb{N}^2,\ \mathbf{b}_{i+1,j+1} - \mathbf{b}_{i,j+1} - \mathbf{b}_{i,j} = 0$$

is a linear recurrence relation for the sequence $\mathbf{b}$.

As we can only work with a finite number of terms of a sequence, in this paper, a *table* shall denote a finite subset of terms of a sequence: it is one of the input parameters of the algorithms.

Given a finite table extracted from the sequence $\mathbf{u}$, the main purpose of the BMS and the Scalar-FGLM algorithms is to, lousy speaking, determine a minimal set of relations that will allow us to generate this finite table using only the values of $\mathbf{u}$ on their supports.

In order to study the relations satisfied by the sequence $\mathbf{u}$, it will be useful to associate them with polynomials in $\mathbb{K}[\mathbf{x}]$.

Definition 1. *Let* $f = \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, \mathbf{x}^{\mathbf{k}} \in \mathbb{K}[\mathbf{x}]$. *We will denote by* $[f]_{\mathbf{u}}$, *or* $[f]$ *when no ambiguation arises, the linear combination* $\sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, u_{\mathbf{k}}$. *Moreover, if* $\boldsymbol{\alpha}$ *defines a relation for* $\mathbf{u}$, *that is 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 this relation.*

The main benefit of the [ ] notation resides in the immediate fact that for all index $\mathbf{i}$, $\left[\mathbf{x}^{\mathbf{i}}\, f\right] = \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, u_{\mathbf{k}+\mathbf{i}}$.

In the previous example, the Pascal's rule relation is associated with polynomial $P = x\,y - y - 1$, so that

$$\forall (i,j) \in \mathbb{N}^2,\ [x^i\, y^j\, P] = 0.$$

Definition 2 (Fitzpatrick and Norton (1990); Sakata (1988))**.** *Let* $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ *be a n-dimensional sequence with coefficients in* $\mathbb{K}$. *The sequence* $\mathbf{u}$ *is* linear recurrent *if from a nonzero finite number of initial terms* $\{u_{\mathbf{i}},\ \mathbf{i} \in S\}$, *and a finite number of linear recurrence relations, without any contradiction, one can compute any term of the sequence.*

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

2.2. Gröbner bases

We let $\mathcal{T}$ be the set of all monomials in $\mathbb{K}[\mathbf{x}]$, i.e. $\mathcal{T} = \{\mathbf{x}^{\mathbf{i}},\ \mathbf{i} \in \mathbb{N}^n\}$. 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 $\mathbb{K}[\mathbf{x}]$, the *leading monomial* of f, denoted $\mathrm{LM}(f)$, is the greatest monomial in the support of f for $\prec$. The *leading coefficient* of f, denoted $\mathrm{LC}(f)$, is the nonzero coefficient of $\mathrm{LM}(f)$. The *leading term* of f, $\mathrm{LT}(f)$, is defined as $\mathrm{LT}(f) = \mathrm{LC}(f)\ \mathrm{LM}(f)$. For an ideal I, we denote, classically, $\mathrm{LM}(I) = \{\mathrm{LM}(f),\ f \in I\}$.

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

Definition 3. *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 $\mathrm{LM}(g) | \mathrm{LM}(f)$.*

The set $\mathcal{G}$ is a minimal *Gröbner basis of I if for any $g \in \mathcal{G}$, $\mathcal{G} \setminus \{g\}$ does not span I.*

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

Let $\mathcal{G}$ be a reduced truncated Gröbner basis, the staircase *of $\mathcal{G}$ is*

$$S = \mathrm{Staircase}(\mathcal{G}) = \{s \in \mathcal{T},\ \forall\, g \in \mathcal{G}, \mathrm{LM}(g) \nmid s\}.$$

It is also the canonical basis of $\mathbb{K}[\mathbf{x}]/I$.

Remark 4. *By definition, a staircase is stable by division: that is, for any $s, s' \in \mathcal{T}$, if s is in the staircase of $\mathcal{G}$ and $s' | s$, then s' is also in the staircase of $\mathcal{G}$.*

In some instances, the goal will be to make the smallest Gröbner basis staircase from a monomial set S: this is done by adding all the divisors of the elements of S. We denote this by stabilizing S with the Stabilize(S) *command.*

We, now, present notation of Sakata (1988, 1990, 2009) and relate it to polynomials and polynomial ideals. This definition shall act like a dictionary between Sakata's notation in these paper and the polynomials algebra notation. We also refer to Guisse (2017), (Mora, 2009, Section 1) and (Sakata, 2009, Section 2) for this kind of dictionary.

Definition 4. *Given a set of polynomials $G \subseteq \mathbb{K}[\mathbf{x}]$.*

- $\Sigma(G) = \{\mathbf{x}^{\mathbf{i}},\ \exists\, g \in G,\ \mathrm{LM}(g) | \mathbf{x}^{\mathbf{i}}\}$.

  Whenever, G is a Gröbner basis of an ideal I, $\Sigma(G)$ is by definition $\mathrm{LM}(I)$.

- *As* $\Sigma(G)$ *satisfies* $\forall\, s \in \Sigma(G), m \in \mathcal{T}$*, if* $s|m$*, then* $m \in \Sigma(G)$*, it has minimal elements for the division. They form the set* $\sigma(G) = \min_{|}(\Sigma(G))$.

  Whenever, G is a minimal Gröbner basis of an ideal I, $\sigma(G)$ *is by definition* $\mathrm{LM}(G)$.

- $\Delta(G) = \mathcal{T} \setminus \Sigma(G)$.

  Whenever G is a Gröbner basis of an ideal I, $\Delta(G)$ *is its* staircase*, the canonical basis of* $\mathbb{K}[\mathbf{x}]/I$.

- *As* $\Delta(G)$ *satisfies* $\forall\, d \in \Delta(G), m \in \mathcal{T}$*, if* $m|d$*, then* $m \in \Delta(G)$*, it has maximal elements for the division. They form the set* $\delta(G) = \max_{|}(\Delta(G))$.

  Whenever, G is a Gröbner basis of an ideal I, $\delta(G)$ *is by definition the* corner set *of the staircase.*

Gröbner basis theory allows us to choose any monomial ordering $\prec$. Among all the monomial ordering, we will mainly use the

- $\mathrm{LEX}(x_n \prec \cdots \prec x_1)$ ordering which compares monomials as follows $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{i}'}$ 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 (Cox et al., 2015, Chapter 2, Definition 3);

- $\mathrm{DRL}(x_n \prec \cdots \prec x_1)$ order which compares monomials as follows $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{i}'}$ 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 $i_k > i'_k$. Equivalently, there exists k, $1 \leq k \leq n$ such that for all $\ell > k$, $i_1 + \cdots + i_\ell = i'_1 + \cdots + i'_\ell$ and $i_1 + \cdots + i_k < i'_1 + \cdots + i'_k$, see (Cox et al., 2015, 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 $\{m \prec M,\ m \in \mathcal{T}\}$ is finite. Such an ordering $\prec$ makes $(\mathbb{N}^n, \prec)$ isomorphic to $(\mathbb{N}, <)$, thus it makes sense to speak about the next monomial for $\prec$.

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. It is well known that any monomial ordering $\prec$ on $\mathcal{T}$ can be obtained from a matrix $A \in \mathbb{R}^{n\times n}$ through: $\mathbf{x}^{\mathbf{i}} \prec \mathbf{x}^{\mathbf{j}}$ if, and only if, $\mathbf{x}^{A\cdot\mathbf{i}} \prec_{\mathrm{LEX}} \mathbf{x}^{A\cdot\mathbf{j}}$, see Erdös (1956). Such a matrix $A \in \mathbb{R}^{n\times n}$ defines a monomial ordering if its first row is nonnegative. It defines a weight ordering if its first row is positive, see Robbiano (1986) and (Cox et al., 2015, Chapter 2, Exercises 4.10 and 4.11)

Definition 5. *Let I be a homogeneous ideal of* $\mathbb{K}[\mathbf{x}]$ *and let* $\prec$ *be a monomial ordering. A set* $\mathcal{G} \subseteq I$ *is a* d-truncated Gröbner basis*, or truncated Gröbner basis*

of I up to degree d, if for all $g \in \mathcal{G}$, $\deg g \leq d$ *and for for all $f \in I$, if* $\deg f \leq d$, *then there exists a $g \in \mathcal{G}$ such that* $\mathrm{LT}(g) | \mathrm{LT}(f)$.

This can be computed using any Gröbner basis algorithm by discarding critical pairs of degree greater than d.

For an affine ideal I, an analogous definition of d-truncated Gröbner basis exists. It is the output of a Gröbner basis algorithm discarding all critical pairs (f, f') with $\deg \mathrm{LT}(f) + \deg \mathrm{LT}(f') - \deg \mathrm{lcm}(\mathrm{LT}(f), \mathrm{LT}(f')) > d$, i.e. with degree higher than d. In this situation, a d-truncated Gröbner basis $\mathcal{G}$ will span the subspace of polynomials $\sum_{g \in \mathcal{G}} h_g\, g$ with $\deg h_g \leq d - \deg g$.

A truncated Gröbner basis $\mathcal{G}$ is *reduced* if for any $g, g' \in \mathcal{G}$ and any monomial $m \in \operatorname{supp} g$, $\mathrm{LM}(g') \nmid m$.

The following definition extends the definition of the staircase of a Gröbner basis to truncated Gröbner basis.

Definition 6. *Let $\mathcal{G}$ be a reduced truncated Gröbner basis, the* staircase *of $\mathcal{G}$ is*

$$S = \mathrm{Staircase}(\mathcal{G}) = \{s \in \mathcal{T},\ \forall\, g \in \mathcal{G}, \mathrm{LM}(g) \nmid s\}.$$

2.3. Gorenstein ideals

From any ideal $J \subseteq \mathbb{K}[\mathbf{x}]$, it is clear that one can construct a sequence $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i} \in \mathbb{N}^n}$ whose ideal of relations contains J: from a Gröbner basis $\mathcal{G}$ of J and staircase S, set the values of the sequence terms $u_{\mathbf{i}} = [\mathbf{x}^{\mathbf{i}}]$, for $\mathbf{x}^{\mathbf{i}} \in S$, as desired and then computes the terms $u_{\mathbf{j}} = [\mathbf{x}^{\mathbf{j}}]$, for $\mathbf{x}^{\mathbf{j}} \in \mathrm{LM}(I)$, using the relations given by $\mathcal{G}$.

However, Proposition 3.3 in Brachat et al. (2010) proves that there are nonzero ideals of $\mathbb{K}[\mathbf{x}]$ that cannot be the ideals of relations of linear recurrent sequences, whenever $n \geq 2$. Indeed, the ideal of relations is necessarily *Gorenstein*, Gorenstein (1952); Macaulay (1934), and problems occur only if J has a zero of multiplicity at least 2.

For instance, there is no bivariate sequence $\mathbf{u} = (u_{i,j})_{(i,j) \in \mathbb{N}^2}$ whose ideal of relations I is $J = \langle x^2, xy, y^2 \rangle$. That is, any sequence $\mathbf{u}$ satisfying $u_{2+i,j} = u_{1+i,1+j} = u_{i,2+j} = 0$, for all $(i, j) \in \mathbb{N}^2$, satisfies a relation induced by a degree-1 polynomial. Hence, I strictly contains J.

The following theorem can also be found in (Elkadi and Mourrain, 2007, Theorem 8.3).

Theorem 5. *Let $I \subseteq \mathbb{K}[\mathbf{x}]$ be a 0-dimensional ideal and let $R = \mathbb{K}[\mathbf{x}]/I$. The ideal I (resp. ring R) is* Gorenstein *if equivalently*

1. *R and its dual are isomorphic as R-modules;*

2. *there exists a* $\mathbb{K}$*-linear form* τ *on* R *such that the following bilinear form is non degenerate*

$$\begin{aligned} R \times R &\to \mathbb{K} \\ (a, b) &\mapsto \tau(a\, b). \end{aligned}$$

On the one hand, this result is important for the Sparse-FGLM application. If the input ideal is not Gorenstein, the output ideal will be bigger. However, this can be easily tested by comparing the degrees of the input and output ideals. On the other hand, this yields a probabilistic test for the Gorenstein property of an ideal J. Pick at random initial conditions, construct a sequence thanks to these initial conditions and J and then compute the ideal I of relations of the sequence. If $I = J$, then J is Gorenstein. We refer to Daleo and Hauenstein (2016) for another test on the Gorenstein property of an ideal.

2.4. Multi-Hankel matrices

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

In a multivariate setting, we can extend this Hankel matrices notion to *multi-Hankel* matrices. Indexing the rows and columns with monomials $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_n^{i_n}$ and $\mathbf{x}^{\mathbf{i}'} = x_1^{i'_1} \cdots x_n^{i'_n}$, the coefficient of H lying on the row labeled with $\mathbf{x}^{\mathbf{i}}$ and column labeled with $\mathbf{x}^{\mathbf{i}'}$ is $u_{\mathbf{i}+\mathbf{i}'}$. Given two sets of monomials U and T, we let $H_{U,T}$ be the multi-Hankel matrix with rows (resp. columns) indexed with monomials in U (resp. T).

Example 2. *Let* $\mathbf{u} = (u_{i,j})_{(i,j) \in \mathbb{N}^2}$ *be a sequence.*

1. *Let* $U = \{1, y, y^2, x, x\,y, x\,y^2, x^2, x^2\,y, x^2\,y^2\}$ *and* $T = \{1, y, x, x\,y, x^2, x^2\,y\}$*, then*

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

We can see that this matrix is a 3×3 block-Hankel *matrix with Hankel blocks of size* 3×2*.*

2. *Let* $T = \{1, y, x, y^2, xy, x^2\}$*, then the following matrix has a less obvious structure:*

$$H_{T,T} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ xy \\ x^2 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & y & x & y^2 & xy & x^2 \end{array} \\ \begin{pmatrix} u_{0,0} & u_{0,1} & u_{1,0} & u_{0,2} & u_{1,1} & u_{2,0} \\ u_{0,1} & u_{0,2} & u_{1,1} & u_{0,3} & u_{1,2} & u_{2,1} \\ u_{1,0} & u_{1,1} & u_{2,0} & u_{1,2} & u_{2,1} & u_{3,0} \\ u_{0,2} & u_{0,3} & u_{1,2} & u_{0,4} & u_{1,3} & u_{2,2} \\ u_{1,1} & u_{1,2} & u_{2,1} & u_{1,3} & u_{2,2} & u_{3,3} \\ u_{2,0} & u_{2,3} & u_{3,0} & u_{2,2} & u_{3,3} & u_{0,4} \end{pmatrix} \end{array}.$$

3. The BMS algorithm

As in Guisse (2017), we specialize to $\mathbb{K}[\mathbf{x}]$ the presentation of the BMS algorithm given in Bras-Amorós and O'Sullivan (2006), Cox et al. (2005) and Sakata (2009) in the more general case of ordered domains.

3.1. A Polynomial interpretation of the BMS *algorithm*

Given a table $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ and a weight ordering $\prec$ for $\mathbf{x}$. We let $\mathcal{T}_0 = \{0\} \cup \{\mathbf{x}^{\mathbf{i}},\ \mathbf{i} \in \mathbb{N}^n\}$ and extend $\prec$ (still denoted by $\prec$) to $\mathcal{T}_0$ with the convention that $0 \prec 1$.

The goal is to iterate on a monomial m, by only considering, at each step, the table $(u_{\mathbf{i}})_{\mathbf{i}\in\{\mathbf{k},\ \mathbf{x}^{\mathbf{k}}\preceq m\}}$. As we only know partially the table $\mathbf{u}$, we need to define some notions according to this partial knowledge at step m.

Definition 7. *Let* $m \in \mathcal{T}_0$*. Let* $f \in \mathbb{K}[\mathbf{x}]$*, we say that the relation* f *is* valid up to m*, whenever*

$$\forall t \in \mathcal{T}_0,\ \mathrm{LM}(t\,f) \preceq m \Rightarrow [t\,f] = 0.$$

We thus define the shift *of* f *as* $\mathrm{shift}(f) = \frac{m}{\mathrm{LM}(f)}$.

We say that the relation f fails *at* m *whenever*

$$\forall t \in \mathcal{T}_0,\ t\,f \prec m \Rightarrow [t\,f] = 0,$$
$$\left[\frac{m}{\mathrm{LM}(f)}\,f\right] \neq 0.$$

We define the fail *of* f *as* $\mathrm{fail}(f) = m$*. If the relation* f *never fails, that is for all* $t \in \mathcal{T}_0$*,* $[t\,f] = 0$*, then by convention* $\mathrm{fail}(f) = \mathrm{shift}(f) = +\infty$.

Proposition 6. *Let* $\mathbf{u}$ *be a table and* $f \in \mathbb{K}[x]$ *such that* $\mathrm{fail}(f) \succ m$*. For all* $g \in \mathbb{K}[\mathbf{x}]$*, if* $\mathrm{LM}(g\,f) \preceq m$*, then* $[g\,f] = 0$*.*

The following proposition show how to combine two failing relations with the same shift in order to obtain a new relation valid with a bigger shift.

Proposition 7. *Let f_1 and f_2 be two relations such that $v = \frac{\text{fail}(f_1)}{\text{LM}(f_1)} = \frac{\text{fail}(f_2)}{\text{LM}(f_2)}$ and $e_1 = [v\, f_1]$, $e_2 = [v\, f_2]$. Let f be the nonzero polynomial $f_1 - \frac{e_1}{e_2} f_2$. Then, for $i \in \{1, 2\}$, $\text{fail}(f) > \text{fail}(f_i)$, i.e. $\frac{\text{fail}(f)}{\text{LM}(f)} > v$.*

Proof. For any $c \in \mathbb{K}$ and any $\mu \in \mathbb{K}[\mathbf{x}]$ such that $\text{LM}(g) \prec v$, we have $[\mu\,(f_1 + c\, f_2)] = [\mu\, f_1] + c\,[\mu\, f_2] = 0$, hence $\text{fail}(f_1 + c\, f_2) \geq \text{fail}(f_i)$.

It remains to prove that for a good choice of c, we have a strict inequality: as, $[v\,(f_1 + c\, f_2)] = [v\, f_1] + c\,[v\, f_2] = e_1 + c\, e_2$, it is clear that $[v\, f] = [v\,(f_1 - \frac{e_1}{e_2} f_2)] = 0$, so that $\text{fail}(f) > v$ $\text{LM}(f) \geq \text{fail}(f_i)$. □

Definition 8. *Using the same notation as in Definition 6, we let*

$$I_m = \{f \in \mathbb{K}[\mathbf{x}],\ \text{fail}\,(f) > m\},$$

and $\mathcal{G}_m$ be the least elements for $\prec$ of I_m, it is a truncated Gröbner basis of I_m:

$$\mathcal{G}_m = \min_{\prec}\{g,\ g \in I_m\},$$
$$S_m = \text{Staircase}(\mathcal{G}_m).$$

Example 3. *Let us go back to Example 1 with sequence $\mathbf{b} = \left(\binom{i}{j}\right)_{(i,j)\in\mathbb{N}^2}$. Consider $\mathbb{K}[x, y]$ with the $\text{DRL}(y \prec x)$ ordering, and $m = x^2$.*

y^2	0		
y	0	1	
1	1	1	1
	1	x	x^2

From this table, on the one hand, we can deduce that

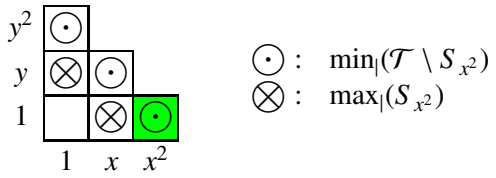
- *since it is not identically 0, there is no relation with leading monomial 1 valid up to x^2, hence $1 \in S_{x^2}$;*
- *since $[y + \alpha] = \alpha$ and $[x\,(y + \alpha)] = 1 + \alpha$, there is no relation with leading monomial y valid up to $x\,y$ and thus x^2, hence $y \in S_{x^2}$;*
- *since $[y\,(x + \beta\, y + \alpha)] = 1$, there is no relation with leading monomial x valid up to $x\,y$ and thus x^2, hence $x \in S_{x^2}$.*

On the other hand, we can check that

- *since $[y^2] = 0$, relation y^2 is valid up to y^2 and thus x^2, hence $y^2 \in \mathcal{T} \setminus S_{x^2}$;*

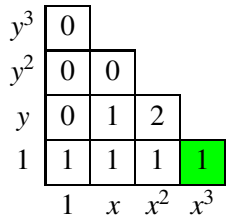
- *since* $[x\,y - 1] = 0$*, relation* $x\,y - 1$ *is valid up to* $x\,y$ *and thus* x^2*, hence* $x\,y \in \mathcal{T} \setminus S_{x^2}$*;*
- *since* $[x^2 - x] = 0$*, relation* $x^2 - x$ *is valid up to* x^2*, hence* $x^2 \in \mathcal{T} \setminus S_{x^2}$*.*

Therefore, $S_{x^2} = \{1, y, x\}$*,* $\max_{|}(S_{x^2}) = \{y, x\}$ *and* $\min_{|}(\mathcal{T} \setminus S_{x^2}) = \{y^2, x\,y, x^2\}$*. This is summed up in the following diagram.*



Let us notice that many relations with respective leading monomials $y^2, x\,y, x^2$ *suit actually. These would be* $y^2 - \alpha_1\,x + \alpha_y\,y + \alpha_1, x\,y - (1 + \alpha_1)\,x + \alpha_y\,y + \alpha_1$ *and* $x^2 - (1 + \alpha_1)\,x + \alpha_y\,y + \alpha_1$*. Furthermore,* I_{x^2} *is not stable by addition:* $(x^2 - x), (x^2 - 2\,x + 1) \in I_{x^2}$ *but* $x^2 - x - (x^2 - 2\,x + 1) = (x - 1) \notin I_{x^2}$ *since* $\mathrm{fail}\,(x - 1) = x\,y$*. Hence,* I_{x^2} *is not an ideal of* $\mathbb{K}[x, y]$*.*

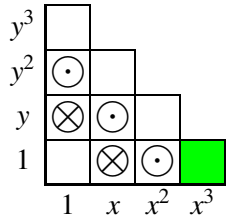
For $m = x^3$*, with the following table, we find that*



- *since* $[y^2] = [y\,y^2] = [x\,y^2] = 0$*, then* y^2 *is valid up to* $x\,y^2$ *and thus* x^3*;*
- *since* $[x\,y - 1] = [y\,(x\,y - 1)] = 0$ *and* $[x\,(x\,y - y)] = 1$*, then* $x\,y - 1$ *fails at* $x^2\,y$*. Yet, since* $[y] = [y\,y] = 0$ *and* $[x\,y] = 1$*, then by Proposition 7,* $[x\,y - y - 1] = [y\,(x\,y - y - 1)] = 0$ *and* $[x\,(x\,y - y - 1)]$ *vanishes as well. Hence,* $x\,y - y - 1$ *is valid up to* $x^2\,y$ *and thus* x^3*;*
- *since* $[x^2 - x] = 0$ *and* $[y\,(x^2 - x)] = 1$*, then* $x^2 - x$ *fails at* $x^2\,y$*. Likewise, since* $[x - 1] = 0$ *and* $[y\,(x - 1)] = 1$*, then* $[x^2 - 2\,x + 1] = 0$ *and* $[y\,(x^2 - 2\,x + 1)] = 0$*. Furthermore,* $[x\,(x^2 - 2\,x + 1)] = 0$*, so that* $x^2 - 2\,x + 1$ *is valid up to* x^3*.*

Therefore, $S_{x^3} = \{1, y, x\}$*,* $\max_{|}(S_{x^3}) = \{y, x\}$ *and* $\min_{|}(\mathcal{T} \setminus S_{x^3}) = \{y^2, x\,y, x^2\}$*. We can also check that these relations span the only valid relations with support in*

$S_{x^3} \cup \{y^2, xy, x^2\}$.



Although I_m is not an ideal in general, we have the following results:

Proposition 8. *Using the notation of Definitions 7 and 8,*

1. *I_m is closed under multiplication by elements of $\mathbb{K}[\mathbf{x}]$,*
2. *for all monomials t, t' such that $t|t'$,*
   (a) *if $t' \in S_m$, then $t \in S_m$.*
   (b) *if $t \in \mathcal{T} \setminus S_m$, then $t' \in \mathcal{T} \setminus S_m$,*

Moreover, it is clear that the sequence $(I_m)_{m\in\mathcal{T}_0}$ is decreasing and that if $\mathbf{u}$ is linear recurrent then $I = \bigcap_{m\in\mathcal{T}_0} I_m$. Therefore, $(S_m)_{m\in\mathcal{T}_0}$ is increasing and its limit is S the finite target staircase. Hence, for m big enough, S_m will be the target staircase. We will give an upper bound in Proposition 11.

The following result gives an intrinsic characterization of S_m that is key in the iteration of the BMS algorithm.

Proposition 9. *For all monomial $m \in \mathcal{T}_0$, $S_m = \left\{\frac{\mathrm{fail}(f)}{\mathrm{LM}(f)},\ f \notin I_m\right\}$.*

Furthermore, let m^+ be the successor of m. Let s be a monomial in the staircase S_{m^+}. Then, s was added at step m^+, i.e. $s \notin S_m$, if, and only if, $s|m^+$ and $\frac{m^+}{s} \in S_{m^+} \setminus S_m$.

Proof. We shall prove the first assertion by double inclusion. If $s = \frac{\mathrm{fail}(f)}{\mathrm{LM}(f)}$ then for all $g \in \mathbb{K}[\mathbf{x}]$ such that $\mathrm{LM}(g) = s$, $\mathrm{fail}(g) \preceq m$, hence $s \notin \mathrm{LM}(I_m)$, $s \in S_m$.

The reverse inclusion is proved by induction on m. For $m = 0$, $S_m = \emptyset$ and there is nothing to do. Let us assume the inclusion is satisfied for a monomial m.

Let $s \in S_{m^+}$. On the one hand, if $s \in S_m$, then there exists $f \in \mathbb{K}[\mathbf{x}] \setminus I_m \subseteq \mathbb{K}[\mathbf{x}] \setminus I_{m^+}$ such that $s = \frac{\mathrm{fail}(f)}{\mathrm{LM}(f)}$.

If, on the other hand, $s \in S_{m^+} \setminus S_m$, then there exists a relation $f \in \mathbb{K}[\mathbf{x}]$ such that $\mathrm{LM}(f) = s$, and $m \prec \mathrm{fail}(f) \preceq m^+$, hence $\mathrm{fail}(f) = m^+$ and s divides m^+.

Let us assume that for all $g \in \mathbb{K}[\mathbf{x}]$ with $\mathrm{LM}(g) = \frac{m^+}{s}$, we have $\mathrm{fail}(g) \preceq m \prec m^+$. Therefore, $\frac{m^+}{s} \in S_m$ and there exists $h \notin I_m$ such that $\frac{\mathrm{fail}(h)}{\mathrm{LM}(h)} = \frac{m^+}{s}$. By Proposition 7, there is $\alpha \in \mathbb{K}$ such that $\mathrm{fail}(f - \alpha h) \succ m^+$. Since $\mathrm{fail}(h) \preceq m \prec m^+$, then $\mathrm{LM}(h) \preceq s$ and $\mathrm{LM}(f - \alpha h) = s$, hence $\frac{\mathrm{fail}(f-\alpha h)}{\mathrm{LM}(f-\alpha h)} \succ \frac{m^+}{s}$. This contradicts the fact that $\frac{m^+}{s} \in S_m$. Thus there exists a $g \in \mathbb{K}[\mathbf{x}]$ with $\mathrm{LM}(g) = \frac{m^+}{s}$ and $\mathrm{fail}(g) \succeq m^+$.

Let g be such a relation, since $\text{fail}(f) = m^+$, then $[g\, f] \neq 0$ and $\text{fail}(g) = m^+$. Therefore, $\frac{\text{fail}(g)}{\text{LM}(g)} = \frac{m^+}{m^+/s} = s$ so that $s \in \left\{\frac{\text{fail}(f)}{\text{LM}(f)},\ f \notin I_{m^+}\right\}$.

Now, we proved that $s \in S_{m^+} \setminus S_m$ implies $s|m^+$ and $\frac{m^+}{s} \in S_{m^+} \setminus S_m$. This implication is clearly an equivalence. □

From this proposition it follows that if $m \in \mathcal{T}_0$, and if m^+ is its successor:

$$\max_{|}(S_{m^+}) = \max_{|}\left(\max_{|}(S_m) \cup \left\{\frac{m^+}{s},\ s \in \min_{|}(\mathcal{T} \setminus S_m) \cap S_{m^+}\right\}\right) \tag{2}$$

Relation 2 allows us to construct, iterating on the monomial m, the set of relations G_m representing the truncated Gröbner basis of I_m. Relations $g \in G_m$ are indexed by their leading monomials, describing $\mathcal{T} \setminus S_m$.

Remark 10. *We can also construct another set, describing the edge of S_m, still denoted S_m, as there is a one-to-one correspondence between a staircase and its edge. The relations $h \in S_m$ are indexed by their ratio $\frac{\text{fail}(h)}{\text{LM}(h)}$ between their fail and their leading monomial, describing the full staircase of I_m.*

When two relations h and h' in S_m are such that $\frac{\text{fail}(h)}{\text{LM}(h)} = \frac{\text{fail}(h')}{\text{LM}(h')}$, then we only need to keep one. Since the goal is to combine a relation of S_m with a relation failing at m^+ to make a new one with a bigger shift, as in Proposition 7, it is best to handle smaller polynomials.

This yields Algorithm 1.

We saw that for m big enough, S_m will be the target staircase. We now give an upper bound.

Proposition 11. *Let* $\mathbf{u}$ *be a linear recurrent sequence and I be its ideal of relations.*

Let S be the staircase of I for $\prec$. Let $s_{\max}$ be the largest monomial in S. Then, for $m \geq (s_{\max})^2$, $S_m = S$.

Let $\mathcal{G}$ be a minimal Gröbner basis of I for $\prec$ and let $g_{\max}$ be the largest leading monomial of $\mathcal{G}$. Then, for $m \geq s_{\max} \cdot \max_{\prec}(g_{\max}, s_{\max})$, the BMS *algorithm returns a minimal Gröbner basis of I for $\prec$.*

Example 4. *For the* DRL$(y \prec x)$ *ordering, $I = \langle x^p, y^q\rangle$ and $q > p \geq 1$, we have, $s_{\max} = x^{p-1}\, y^{q-1}$ and $g_{\max} = y^q$. Therefore, the right staircase is found at most at step $m = x^{2\,p-2}\, y^{2\,q-2}$, while the Gröbner basis is found at most at step $x^{p-1}\, y^{q-1}\ \max_{\prec}(x^{p-1}\, y^{q-1}, x^q)$, i.e. $y^{2\,q-1}$ if $p = 1$ and $x^{2\,p-2}\, y^{2\,q-2}$ otherwise.*

From Propositions 9 and 11, we can deduce that $S = \left\{\frac{\text{fail}(f)}{\text{LM}(f)},\ f \notin I\right\}$.

Algorithm 1: The BMS algorithm.

Input: A table $\mathbf{u} = (u_\mathbf{i})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$ and a monomial M as the stopping condition.

Output: A set G of relations generating I_M.

$T := \{m \in \mathbb{K}[\mathbf{x}],\ m \preceq M\}$. `// ordered for` $\prec$

$G := \{1\}$. `// the future Gröbner basis`

$S := \emptyset$. `// staircase edge, elements will be` $[h, \mathrm{fail}(h)/\,\mathrm{LM}(h)]$

For all $m \in T$ **do**

  $S' := S$.

  For $g \in G$ **do**

    If $\mathrm{LM}(g) | m$ **then**

      $e := \left\lfloor \frac{m}{\mathrm{LM}(g)}\, g \right\rfloor_\mathbf{u}$.

      If $e \neq 0$ **then**

        $S' := S' \cup \left\{ \left[\frac{g}{e}, \frac{m}{\mathrm{LM}(g)} \right] \right\}$.

  $S' := \min_|\{[h, \mathrm{fail}(h)/\,\mathrm{LM}(h)]\}$. `// see Remark 10`

  $G' := \mathrm{Border}(S')$.

  For $g' \in G'$ **do**

    Let $g \in G$ such that $\mathrm{LM}(g) | \mathrm{LM}(g')$.

    If $\mathrm{LM}(g) \nmid m$ **then**

      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\, g$. `// translates the relation`

    Else if $\exists\, h \in S, \frac{m}{\mathrm{LM}(g')} | \mathrm{fail}(h)$ **then**

      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\, g - \left\lfloor \frac{m}{\mathrm{LM}(h)}\, h \right\rfloor_\mathbf{u} \frac{\mathrm{LM}(g')\ \mathrm{fail}(h)}{m}\, h$. `// see Proposition 7`

    Else $g' := g$.

  $G := G'$.

  $S := S'$.

Return G.

Example 5. *We give the trace of the algorithm called on the binomial sequence* $\mathbf{b}$ *for the* DRL$(y \prec x)$ *ordering up to monomial* x^3 *(hence visiting all the monomials of degree at most* 3*).*

To simplify the reading, whenever a relation succeeds in m or cannot be tested in m, we skip the updating part as this relation remains the same.

We start with the empty staircase S *and the relation* $G = \{1\}$.

For the monomial 1

The relation $g_1 = 1$ *fails since* $[\mathbf{b}_{0,0}] = 1$. *Thus* $S' = \{[1, 1]\}$.
S' *is updated to* $\{[1, 1]\}$ *and* $G' = \{y, x\}$.
For the relation $g'_1 = y$, $y \nmid 1$ *thus* $g'_1 = y$.
For the relation $g'_2 = x$, $x \nmid 1$ *thus* $g'_2 = x$.
We update $G := G' = \{y, x\}$ *and* $S := S' = \{[1, 1]\}$.

For the monomial y

The relation $g_1 = y$ *succeeds since* $[\mathbf{b}_{0,1}] = 0$.
Nothing must be done for the relation $g_2 = x$.
S' *is set to* $\{[1, 1]\}$ *and* $G' = \{y, x\}$.
We set $g'_1 = y$ *and* $g'_2 = x$.
We update $G := G' = \{y, x\}$ *and* $S := S' = \{[1, 1]\}$.

For the monomial x

Nothing must be done for the relation $g_1 = y$.
The relation $g_2 = x$ *fails since* $[\mathbf{b}_{1,0}] = 1$. *Thus* $S' = \{[1, 1], [x, 1]\}$.
S' *is set to* $\{[1, 1]\}$ *and* $G' = \{y, x\}$.
We set $g'_1 = y$.
For the relation $g'_2 = x$, $x|x$ *and* $\frac{x}{x}|\,\mathrm{fail}(1)$, *hence* $g'_2 = x - 1$.
We update $G := G' = \{y, x - 1\}$ *and* $S := S' = \{[1, 1]\}$.

For the monomial y^2

The relation $g_1 = y$ *succeeds since* $[\mathbf{b}_{0,2}] = 0$.
Nothing must be done for the relation $g_2 = x - 1$.
S' *is set to* $\{[1, 1]\}$ *and* $G' = \{y, x\}$.
We set $g'_1 = y$ *and* $g'_2 = x - 1$.
We update $G := G' = \{y, x - 1\}$ *and* $S := S' = \{[1, 1]\}$.

For the monomial $x\,y$

The relation $g_1 = y$ *fails since* $[\mathbf{b}_{1,1}] = 1$. *Thus* $S' = \{[1, 1], [y, x]\}$.
The relation $g_2 = x - 1$ *fails since* $[\mathbf{b}_{1,1} - \mathbf{b}_{0,1}] = 1$. *Thus* $S' = \{[1, 1], [y, x], [x - 1, y]\}$.
S' *is set to* $\{[y, x], [x - 1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.
For the relation $g'_1 = y^2$, $y^2 \nmid x\,y$ *thus* $g'_1 = y^2$.
For the relation $g'_2 = x\,y$, $x\,y|x\,y$ *and* $\frac{x\,y}{x\,y}|\,\mathrm{fail}(y)$, *hence* $g'_2 = x\,y - 1$.
For the relation $g'_3 = x^2$, $x^2 \nmid x\,y$ *thus* $g'_3 = x^2 - x$.

We update $G := G' = \{y^2, x\,y-1, x^2-x\}$ *and* $S := S' = \{[y, x], [x-1, y]\}$.

For the monomial x^2

Nothing must be done for the relation $g_1 = y^2$.

Nothing must be done for the relation $g_2 = x\,y - 1$.

The relation $g_3 = x^2 - x$ *succeeds since* $[\mathbf{b}_{2,0} - \mathbf{b}_{1,0}] = 0$.

S' *is set to* $\{[y, x], [x - 1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.

We set $g'_1 = y^2$, $g'_2 = x\,y - 1$ *and* $g'_3 = x^2 - x$.

We update $G := G' = \{y^2, x\,y-1, x^2-x\}$ *and* $S := S' = \{[y, x], [x-1, y]\}$.

For the monomial y^3

The relation $g_1 = y^2$ *succeeds since* $[\mathbf{b}_{0,3}] = 0$.

Nothing must be done for the relation $g_2 = x\,y - 1$.

Nothing must be done for the relation $g_3 = x^2 - x$.

S' *is set to* $\{[y, x], [x - 1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.

We set $g'_1 = y^2$, $g'_2 = x\,y - 1$ *and* $g_3 = x^2 - x$.

We update $G := G' = \{y^2, x\,y-1, x^2-x\}$ *and* $S := S' = \{[y, x], [x-1, y]\}$.

For the monomial $x\,y^2$

The relation $g_1 = y^2$ *succeeds since* $[\mathbf{b}_{1,2}] = 0$.

The relation $g_2 = x\,y - 1$ *succeeds since* $[\mathbf{b}_{1,2} - \mathbf{b}_{0,1}] = 0$.

Nothing must be done for the relation $g_3 = x^2 - x$.

S' *is set to* $\{[y, x], [x - 1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.

We set $g'_1 = y^2$, $g'_2 = x\,y - 1$ *and* $g_3 = x^2 - x$.

We update $G := G' = \{y^2, x\,y-1, x^2-x\}$ *and* $S := S' = \{[x, y], [y, x-1]\}$.

For the monomial $x^2\,y$

Nothing must be done for the relation $g_1 = y^2$.

The relation $g_2 = x\,y - 1$ *fails since* $[\mathbf{b}_{2,1} - \mathbf{b}_{1,0}] = 1$. *Thus* $S' = \{[y, x], [x - 1, y], [x\,y - 1, x]\}$.

The relation $g_3 = x^2 - x$ *fails since* $[\mathbf{b}_{2,1} - \mathbf{b}_{1,1}] = 1$. *Thus* $S' = \{[y, x], [x - 1, y], [x\,y - 1, x], [x^2 - x, y]\}$.

S' *is set to* $\{[y, x], [x - 1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.

We set $g'_1 = y^2$.

For the relation $g'_2 = x\,y$, $x\,y | x^2\,y$ *and* $\frac{x^2\,y}{x\,y} | \,\mathrm{fail}(y)$, *hence* $g'_3 = x\,y - y - 1$.

For the relation $g'_3 = x^2$, $x^2 | x^2\,y$ *and* $\frac{x^2\,y}{x^2} | \,\mathrm{fail}(x - 1)$, *hence* $g'_3 = x^2 - 2\,x + 1$.

We update $G := G' = \{y^2, x\,y - y - 1, x^2 - 2\,x + 1\}$ *and* $S := S' = \{[y, x], [x - 1, y]\}$.

For the monomial x^3

Nothing must be done for the relation $g_1 = y^2$.

Nothing must be done for the relation $g_2 = x\,y - y - 1$.

The relation $g_3 = x^2 - 2\,x + 1$ *succeeds since* $[\mathbf{b}_{3,0} - 2\,\mathbf{b}_{2,0} + \mathbf{b}_{1,0}] = 0$.

S' is set to $\{[y, x], [x-1, y]\}$ *and* $G' = \{y^2, x\,y, x^2\}$.
We set $g'_1 = y^2$, $g'_2 = x\,y - y - 1$ *and* $g_3 = x^2 - 2\,x + 1$.
We update $G := G' = \{y^2, x\,y - y - 1, x^2 - 2\,x + 1\}$ *and* $S := S' = \{[y, x], [x-1, y]\}$.

The algorithm returns relations $y^2, x\,y - y - 1, x^2 - 2\,x + 1$*, all three with a shift* x.

3.2. A Linear Algebra interpretation of the BMS *algorithm*

In order to make the presentation of the BMS algorithm closer to that of the Scalar-FGLM algorithm, we propose to replace every evaluation using the [ ] operator with a matrix-vector product.

As stated above, given a monic relation $f = \text{LM}(f) + \sum_{s\in S} \alpha_s\, s$, testing the shift of this relation by a monomial m is done with the bracket operator, i.e. testing whether $[m\, f] = 0$ or not. Denoting $\vec{f}$, the vector

$$\vec{f} = \begin{matrix} \\ \vdots \\ s\in S \\ \vdots \\ \text{LM}(f) \end{matrix} \begin{matrix} 1 \\ \begin{pmatrix} \vdots \\ \alpha_s \\ \vdots \\ 1 \end{pmatrix} \end{matrix},$$

this can also be done through testing if the following matrix-vector product

$$H_{m,S\cup\{\text{LM}(f)\}}\,\vec{f} = \begin{matrix} m \end{matrix} \begin{matrix} \cdots & s\in S & \cdots & \text{LM}(f) \\ \begin{pmatrix} \cdots & [m\, s] & \cdots & [m\ \text{LM}(f)] \end{pmatrix} \end{matrix} \begin{pmatrix} \vdots \\ \alpha_s \\ \vdots \\ 1 \end{pmatrix} = 0$$

or not. In this setting, the definitions of the *shift* and the *fail* of a relation, i.e. Definition 7, become as follows.

Definition 9. *Let* $f = \text{LT}(f) + \sum_{s\in S} \alpha_s\, s$ *be a polynomial.*
The monomial m *is a* shift *of* f *if*

$$H_{\{1,\ldots,m\},S\cup\{\text{LM}(f)\}}\,\vec{f} = \begin{matrix} 1 \\ \vdots \\ m \end{matrix} \begin{matrix} \cdots & s\in S & \cdots & \text{LM}(f) \\ \begin{pmatrix} \cdots & [s] & \cdots & [\text{LM}(f)] \\ & \vdots & & \vdots \\ \cdots & [m\, s] & \cdots & [m\ \text{LM}(f)] \end{pmatrix} \end{matrix} \begin{pmatrix} \vdots \\ \alpha_s \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Let m^+ be the successor of m, m^+ $\mathrm{LM}(f)$ is the fail of f *if*

$$H_{\{1,\ldots,m,m^+\},S\cup\{\mathrm{LM}(f)\}}\,\vec{f} = \begin{array}{c} \\ 1 \\ \vdots \\ m \\ m^+ \end{array}\!\!\begin{array}{c} \begin{array}{cccc} \cdots & s\in S & \cdots & \mathrm{LM}(f) \end{array} \\ \begin{pmatrix} \cdots & [s] & \cdots & [\mathrm{LM}(f)] \\ & \vdots & & \vdots \\ \cdots & [m\,s] & \cdots & [m\ \mathrm{LM}(f)] \\ \cdots & [m^+\,s] & \cdots & [m^+\ \mathrm{LM}(f)] \end{pmatrix} \end{array} \begin{pmatrix} \vdots \\ \alpha_s \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ e \end{pmatrix},$$

with $e \neq 0$.

We can also write another proof of Proposition 7 with a matrix viewpoint.

Proof of Proposition 7. Let $f_1 = \mathrm{LM}(f_1) + \sum_{s\in S} \alpha_s\, s$ and $f_2 = \mathrm{LM}(f_2) + \sum_{s\in S'} \beta_s\, s$ be monic. Let v^- be the predecessor of v. Let $\tilde{S} = S \cup S' \setminus \{\mathrm{LM}(f_2), \mathrm{LM}(f_1)\}$, assuming $\mathrm{LM}(f_2) \neq \mathrm{LM}(f_1)$, then we have

$$H_{\{1,\ldots,v^-,v\},\tilde{S}\cup\{\mathrm{LM}(f_2),\mathrm{LM}(f_1)\}}\,(\vec{f_1} + c\,\vec{f_2}) = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ e_1 + c\,e_2 \end{pmatrix}$$

$$\begin{array}{c} \\ 1 \\ \vdots \\ v^- \\ v \end{array}\!\!\begin{array}{c} \begin{array}{ccccc} \cdots & s\in\tilde{S} & \cdots & \mathrm{LM}(f_2) & \mathrm{LM}(f_1) \end{array} \\ \begin{pmatrix} \cdots & [s] & \cdots & [\mathrm{LM}(f_2)] & [\mathrm{LM}(f_1)] \\ & \vdots & & \vdots & \vdots \\ \cdots & [v^-\,s] & \cdots & [v^-\ \mathrm{LM}(f_2)] & [v^-\ \mathrm{LM}(f_1)] \\ \cdots & [v\,s] & \cdots & [v\ \mathrm{LM}(f_2)] & [v\ \mathrm{LM}(f_1)] \end{pmatrix} \end{array} \begin{pmatrix} \vdots \\ \alpha_s + c\beta_s \\ \vdots \\ c \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ e_1 + c\,e_2 \end{pmatrix}.$$

It is now clear that vector $\vec{f_1} - \frac{e_1}{e_2}\,\vec{f_2}$ is in the kernel of this matrix. That is, polynomial $f_1 - \frac{e_1}{e_2}\,f_2$ has a shift v. □

Changing every evaluation into a matrix-vector product in the BMS algorithm yields the following presentation of the BMS algorithm, namely Algorithm 2.

Algorithm 2: Linear Algebra variant of the BMS algorithm.

Input: A table $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$ and a monomial M as the stopping condition.

Output: A set G of relations generating I_M.

$T := \{m \in \mathbb{K}[\mathbf{x}], m \preceq M\}$. `// ordered for` $\prec$

$G := \{1\}$. `// the future Gröbner basis`

$S := \emptyset$. `// staircase edge, elements will be` $[h, \mathrm{fail}(h)/\,\mathrm{LM}(h)]$

For all $m \in T$ **do**

  $S' := S$.

  For $g \in G$ **do**

    If $\mathrm{LM}(g) | m$ **then**

      $e := H_{\left\{\frac{m}{\mathrm{LM}(g)}\right\},\mathrm{supp}(g)}\,\vec{g}$.

      If $e \neq 0$ **then**

        $S' := S' \cup \left\{\left[\frac{g}{e}, \frac{m}{\mathrm{LM}(g)}\right]\right\}$.

  $S' := \min_{\mathrm{fail}(h)\in S'} \{[h, \mathrm{fail}(h)/\,\mathrm{LM}(h)]\}$. `// see Remark 10`

  $G' := \mathrm{Border}(S')$.

  For $g' \in G'$ **do**

    Let $g \in G$ such that $\mathrm{LM}(g) | \mathrm{LM}(g')$.

    If $\mathrm{LM}(g) \nmid m$ **then**

      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\, g$. `// shifts the relation`

    Else if $\exists\, h \in S, \frac{m}{\mathrm{LM}(g')} | \,\mathrm{fail}(h)$ **then**

      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\, g - \left(H_{\left\{\frac{m}{\mathrm{LM}(h)}\right\},\mathrm{supp}(h)}\,\vec{h}\right) \frac{\mathrm{LM}(g')\ \mathrm{fail}(h)}{m}\, h$. `// see Prop. 7`

    Else $g' := g$.

  $G := G'$

  $S := S'$

Return G.

4. The Scalar-FGLM algorithm

This section is devoted to the description of the Scalar-FGLM algorithm introduced in Berthomieu et al. (2015, 2016).

The Scalar-FGLM algorithm aims at computing linear recurrence relations of a multidimensional sequence with a matrix viewpoint and an approach close to the FGLM algorithm, see Faugère et al. (1993).

The main idea is to shift the linear recurrence relations in order to determine their coefficients. As we can only know a finite number of the sequence terms, we need the following definition.

Definition 10. *Let $f \in \mathbb{K}[\mathbf{x}]$ and T be a set of monomials in $\mathbf{x}$, we say that f has a shift T if*

$$\forall m \in T,\ [m\, f] = 0. \tag{3}$$

Remark 12. *We would like to emphasize that this definition is close to Definition 7 of the shift for the* BMS *algorithm.*

Whenever T is a set of monomials $T_M = \{m,\ m \preceq M\}$, f has a shift T_M if, and only if, f has a shift M, i.e. $\mathrm{fail}(f) \succ \mathrm{LM}(f)\, M$.

Unless stated otherwise, we will now always assume that the set T is stable by division.

From the relations $\left[\mathbf{x}^{\mathbf{i}+\mathbf{d}} + \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, \mathbf{x}^{\mathbf{i}+\mathbf{k}}\right] = 0$, valid for all $\mathbf{x}^{\mathbf{i}} \in T$, one can deduce that the polynomial $P = \mathbf{x}^{\mathbf{d}} + \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, \mathbf{x}^{\mathbf{k}}$ satisfies $[m\, P] = 0$ for all $m \in T$. In other words, P has a shift T.

To determine P with a shift T_M, it suffices to solve the linear system

$$\begin{cases} \left[\mathbf{x}^{\mathbf{d}} + \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, \mathbf{x}^{\mathbf{k}}\right] & = 0 \\ \quad\vdots & \quad\vdots \\ \left[m\, x^{\mathbf{d}} + \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, m\, \mathbf{x}^{\mathbf{k}}\right] & = 0 \\ \quad\vdots & \quad\vdots \\ \left[M\, x^{\mathbf{d}} + \sum_{\mathbf{k}\in\mathcal{K}} \alpha_{\mathbf{k}}\, M\, \mathbf{x}^{\mathbf{k}}\right] & = 0. \end{cases}$$

Before determining the coefficients of the relations, one needs to determine their support.

Definition 11. *Let T be a finite subset of terms. We say that a finite set $S \subset T$ is a* useful staircase *with respect to $\mathbf{u}$, T and $\prec$ if*

$$\sum_{t\in S} \beta_t\, [m\, t] = 0,\quad \forall\, m \in S$$

implies that $\beta_t = 0$ for all $t \in S$, S is maximal for the inclusion and minimal for $\prec$. We compare two ordered sets for $\prec$ by seeing them as tuples of their elements and then comparing them lexicographically.

We recall that for two sets of terms U and T, the multi-Hankel matrix associated with U and T is

$$H_{U,T} = \begin{array}{c} \\ \vdots \\ m' \in U \\ \vdots \end{array} \begin{array}{c} \begin{array}{ccc} \cdots & m \in T & \cdots \end{array} \\ \begin{pmatrix} \ddots & \vdots & \iddots \\ \cdots & [m\,m'] & \cdots \\ \iddots & \vdots & \ddots \end{pmatrix} \end{array}.$$

Whenever $U = \{1, x, \ldots, x^{k-1}\}$ and $T = \{1, x, \ldots, x^{\ell-1}\}$ then $H_{U,T}$ is a classical Hankel matrix of size $k \times \ell$.

Definition 11 can be rewritten in term of a matrix rank.

Definition 12. *Let T be a finite subset of terms.*

We say that a finite set $S \subset T$ is a useful staircase *with respect to* $\mathbf{u}$*, T and $\prec$ if the matrix $H_{S,S}$ has full rank equal to $\#S$ and to* $\operatorname{rank} H_{T,T}$*, S is minimal for the inclusion and for $\prec$.*

We compare two ordered sets for $\prec$ by seeing them as tuples of their elements and then comparing them lexicographically.

In other words, S is the column rank profile of matrix $H_{T,T}$.

As noted by the authors, it is important to notice that useful staircases need not be Gröbner bases staircases as proven by the following example. Though, if the set of terms T contains the true staircase of the ideal of relations of I with respect to $\prec$, then the useful staircase will be this staircase, as expected.

Example 6. *We consider the bivariate sequence* $\mathbf{u} = (\mathbb{1}_{i=j=1})_{(i,j)\in\mathbb{N}^2} = \begin{pmatrix} 0&0&0&0&\cdots \\ 0&1&0&0&\cdots \\ 0&0&0&0&\cdots \\ 0&0&0&0&\cdots \\ \vdots&\vdots&\vdots&\vdots&\ddots \end{pmatrix}$ *whose ideal of relations is $\langle y^2, x^2\rangle$. The useful staircase with respect to* $\mathbf{u}$*, $T = \{1, y, x, y^2\}$ and* $\textsc{drl}(y \prec x)$ *is $S = \{y, x\}$, as the columns labeled with* 1 *and y^2 of the matrix*

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

are zero. However, for a bigger set $T' = \{1, y, x, y^2, xy, x^2\}$*, the useful staircase of the matrix*

$$H_{T',T'} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ xy \\ x^2 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & y & x & y^2 & xy & x^2 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \end{array}$$

is the true staircase $\{1, y, x, xy\}$*, which is stable by division.*

Proposition 13. *If* S *is the useful staircase with respect to the finite subset* T *and* $\prec$*, then for all* $m \in T \setminus S$*, there exists a relation with support in* $S \cup \{m\}$*, but not in* S*, with a shift* T*.*

In particular, we can always pick m *in the border of* S*.*

Proof. If $m \in T \setminus S$, then $S \cup \{m\}$ is bigger than S. As the rank of $H_{T,S\cup\{m\}}$ cannot be $\#S \cup \{m\} = \#S + 1 = \operatorname{rank} H_{T,S} + 1$, then it must be $\#S$. Therefore, the last column of $H_{T,S\cup\{m\}}$, labeled with m, is a linear combination of the previous ones, i.e. there is a relation with support in $S \cup \{m\}$ but not in S. □

Finding this relation is straightforward, as it suffices to solve the nondegenerate linear system $H_{T,S}\,\boldsymbol{\alpha} + H_{T,\{m\}} = 0$ which is equivalent to solving $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{m\}} = 0$.

It is worth noticing that nothing can be concluded on the existence of a relation with support in $S \cup \{m\}$ with a shift T, whenever $m \notin T$, though.

In the Scalar-FGLM algorithm presented in Berthomieu et al. (2015, 2016), a relation was returned for every m in the border of S, whether m was in T or not by solving the linear system $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\cup\{m\}} = 0$. This would mean that some relations could be returned without even being tested with a shift T, see also Example 10. Therefore, it seems preferable to only return relations with support in T, to ensure the shift T.

This yields the Algorithm 3 that differs thus a little bit from the one in the aforementioned articles.

Example 7. *We give the trace of the algorithm called on two sequences: the sequence* $\mathbf{u} = (2^i\,3^j\,(i+1))_{(i,j)\in\mathbb{N}^2}$ *and the the binomial sequence* $\mathbf{b}$ *with the* $\text{DRL}(y \prec x)$ *ordering, and on the set* $T = \{1, y, x, y^2, xy, x^2\}$ *of all the monomials of degree at most* $d = 2$*.*

Algorithm 3: The Scalar-FGLM algorithm.

Input: A table $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, $\prec$ a monomial ordering and T a set of terms in $\mathbf{x}$ stable by division.

Output: A reduced truncated Gröbner basis with respect to $\prec$ of the ideal of relations of $\mathbf{u}$ with staircase included in T.

Build the matrix $H_{T,T}$.
Compute the useful staircase (column rank profile) S of $H_{T,T}$ such that $\operatorname{rank} H_{T,T} = \operatorname{rank} H_{S,S}$.
$S' := \text{Stabilize}(S)$. `// the staircase (stable under division)`
$L := T \backslash S'$. `// the set of next terms to study`
$G := \emptyset$. `// the future Gröbner basis`
While $L \neq \emptyset$ **do**
  $t := \min_{\prec}(L)$.
  Find $\boldsymbol{\alpha}$ such that $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{t\}} = 0$.
  $G := G \cup \{t + \sum_{s\in S} \alpha_s\, s\}$.
  Remove multiples of t in L and sort L by increasing order (with respect to $\prec$).
Return G.

1. *We build the matrix*

$$H_{T,T} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \\ x\,y \\ x^2 \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & y & x & y^2 & x\,y & x^2 \end{array} \\ \begin{pmatrix} 1 & 3 & 4 & 9 & 12 & 12 \\ 3 & 9 & 12 & 27 & 36 & 36 \\ 4 & 12 & 12 & 36 & 36 & 32 \\ 9 & 27 & 36 & 81 & 108 & 108 \\ 12 & 36 & 36 & 108 & 108 & 96 \\ 12 & 36 & 32 & 108 & 96 & 80 \end{pmatrix} \end{array}.$$

The useful staircase of this matrix is $S = \{1, x\}$.
It is stable by division so $S' = S$.
We set $L = \{1, y, x, y^2, x\,y, x^2\} \setminus \{1, x\} = \{y, y^2, x\,y, x^2, y^3, x\,y^2, x^2\,y, x^3\}$ *and* $G = \emptyset$.
We take $t = y$ *and solve* $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{y\}} = 0$ *which yields relation* $y - 3$, *so* $G = \{y - 3\}$ *and* L *is updated to* $\{x^2, x^3\}$.
We take $t = x^2$ *and solve* $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{x^2\}} = 0$ *which yields relation* $x^2 - 4\,x + 4$, *so* $G = \{y - 3, x^2 - 4\,x + 4\}$ *and* L *is updated to* $\emptyset$.
We return $G = \{y - 3, x^2 - 4\,x + 4\}$.
Furthermore, the relations $g \in G$ *satisfy* $[m\,g] = 0$, *for all* $m \in T = \{1, y, x, y^2, x\,y, x^2\}$, *i.e. have a shift* T.

2. *We build the matrix*

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

The useful staircase of this matrix is $S = \{1, y, x, y^2, x^2\}$.
It is stable by division so $S' = S$.
We set $L = \{1, y, x, y^2, xy, x^2\} \setminus \{1, y, x, y^2, x^2\} = \{xy, xy^2, x^2y\}$ *and* $G = \emptyset$.
We take $t = xy$ *and solve* $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{xy\}} = 0$ *which yields relation* $xy - y - 1$, *so* $G = \{xy - y - 1\}$ *and* L *is updated to* $\emptyset$.
We return $G = \{xy - y - 1\}$.
Furthermore, this relation $g \in G$ *satisfies* $[m\,g] = 0$, *for all* $m \in T = \{1, y, x, y^2, xy, x^2\}$, *i.e. has a shift* T.

5. Another linear algebra solver inspired by the BMS algorithm

In this section, we design an algorithm for computing the ideal of relations of a sequence that is close to both the BMS algorithm and to the Scalar-FGLM algorithm. The main idea will be to increase the number of rows and columns of several multi-Hankel matrices and to check whether the ranks of these matrices are increasing.

Proposition 14. *Let* S *be a staircase and* g *be a relation on sequence* $\mathbf{u}$ *such that* $\mathrm{LM}(g)$ *lies on the border of* S *and* $\mathrm{supp}(g) \subseteq S \cup \{\mathrm{LM}(g)\}$. *Assume furthermore that* g *has a shift* m, *that is* $[g\,\mu] = 0$ *for all* $\mu \preceq m$.

Let m^+ *be the successor of* m. *If* $[m^+\,g] \neq 0$, *then the linear system*

$$\begin{cases} \sum_{s\in S} \alpha_s\,[s] + [\mathrm{LM}(g)] & = 0 \\ & \vdots \\ \sum_{s\in S} \alpha_s\,[m\,s] + [m\ \mathrm{LM}(g)] & = 0 \\ \sum_{s\in S} \alpha_s\,[m^+\,s] + [m^+\ \mathrm{LM}(g)] & = 0 \end{cases}$$

has no solution and there is no nonzero valid relation with support in Stabilize $(S \cup \{m^+\})$.

Proof. This is a consequence of Proposition 9. □

Example 8. 1. *Let us consider the binomial sequence* $\mathbf{b}$ *and relations* y *and* $x-1$*. We know that the relation* y *has a shift* y*, i.e.* $[y] = [y^2] = 0$*, and we want to check if a relation with leading monomial* y *has a shift* x*. Therefore, we need to solve*

$$\begin{cases} \alpha_1\,[1] + [y] & = 0 \\ \alpha_1\,[y] + [y^2] & = 0 \\ \alpha_1\,[x] + [x\,y] & = 0 \end{cases} \iff \begin{cases} \alpha_1 & = 0 \\ 0 & = 0 \\ \alpha_1 + 1 & = 0 \end{cases}$$

which has no solution. Hence x *is in the staircase. Thanks to Proposition 9, since relation* $[y]$ *fails in* $x\,y$ *for* $[x\,y] = 1$*, we can also determine that* x *is in the staircase.*
Likewise, we know that the relation $x-1$ *has a shift* 1*, i.e.* $[x-1] = 0$*, and we want to check if a relation with leading monomial* x *has a shift* y*. Therefore, we need to solve*

$$\begin{cases} \alpha_1\,[1] + [x] & = 0 \\ \alpha_1\,[y] + [x\,y] & = 0 \end{cases} \iff \begin{cases} \alpha_1 + 1 & = 0 \\ 1 & = 0 \end{cases}$$

which has no solution. Hence y *is in the staircase.*

2. *We still consider the binomial sequence* $\mathbf{b}$ *but with relations* $y^2, x\,y - 1$ *and* $x^2 - x$*. We know that the relation* $x^2 - x$ *has a shift* 1*, i.e.* $[x^2 - x] = 0$*, and we want to check if a relation with leading monomial* x^2 *has a shift* y*. Therefore, we need to solve*

$$\begin{cases} \alpha_1\,[1] + \alpha_y\,[y] + \alpha_x\,[x] + [x^2] & = 0 \\ \alpha_1\,[y] + \alpha_y\,[y^2] + \alpha_x\,[x\,y] + [x^2\,y] & = 0 \end{cases} \iff \begin{cases} \alpha_1 + \alpha_x + 1 & = 0 \\ \alpha_x + 2 & = 0 \end{cases}$$

whose solution is $\alpha_x = -2, \alpha_1 = 1$ *and* α_y *is any. Hence, although the relation* $x^2 - x$ *fails at* $x^2\,y$ *for* $[x^2\,y - x\,y] = 1$*, the relation* $x^2 - 2\,x + 1$ *does not and has a shift* y*.*

This yields Algorithm 4.

Example 9. *We detail how Algorithm 4 behaves on the binomial sequence* $\mathbf{b}$ *up to monomial* x^2*. We start with the empty staircase* S *and the relation* 1*, with* $V_1 = \emptyset$*.*

For the monomial 1*, the matrix* $H_{\{1\},\emptyset}$ *has rank* 0 *while the matrix* $H_{\{1\},\{1\}} = (\,1\,)$ *has rank* 1*, hence* S *is updated to* $\{1\}$ *and the relations are now* y*, with* $V_y = \emptyset$*, and* x*, with* $V_x = \emptyset$*.*
For the monomial y*,*

Algorithm 4: Linear Algebra solver.

Input: A table $\mathbf{u} = (u_\mathbf{i})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$ and a monomial M as the stopping condition.

Output: A set G of relations generating I_M.

$T := \{m \in \mathbb{K}[\mathbf{x}],\ m \preceq M\}$. `// ordered for` $\prec$

$G := \{[1, \emptyset]\}$. `// the future Gb, elements will be` $[g, V_g]$

$S := \emptyset$. `// the staircase`

For all $m \in T$ **do**

  $S' := S$

  For $g \in G$ **do**

    If $\mathrm{LM}(g) | m$ **then**

      If $\operatorname{rank} H_{V_g \cup \left\{\frac{m}{\mathrm{LM}(g)}\right\}, S} < \operatorname{rank} H_{V_g \cup \left\{\frac{m}{\mathrm{LM}(g)}\right\}, S \cup \{\mathrm{LM}(g)\}}$ **then**

        $S' := S' \cup \left\{\frac{m}{\mathrm{LM}(g)}\right\}$.

      Else

        $V_g := V_g \cup \left\{\frac{m}{\mathrm{LM}(g)}\right\}$.

  $S :=$ Stabilize(S').

  $G :=$ Border(S).

  For $g \in G$ **do**

    $V_g := \{\mu \in \mathbb{K}[\mathbf{x}], \mu\ \mathrm{LM}(g) \preceq m\}$

For $g \in G$ **do**

  Find $\boldsymbol{\alpha}$ such that $H_{V_g, S}\ \boldsymbol{\alpha} + H_{V_g, \{\mathrm{LM}(g)\}} = 0$.

  $g := g + \sum_{s\in S} \alpha_s\, s$.

Return G.

both matrices $H_{\{1\},\{1\}} = \begin{pmatrix} 1 \end{pmatrix}$ *and* $H_{\{1\},\{1,y\}} = \begin{pmatrix} 1 & 0 \end{pmatrix}$ *have rank* 1*, hence* V_y *is updated to* $\{1\}$*;*
as x does not divide y, nothing is done.

For the monomial x,

as y does not divide x, nothing is done;
both matrices $H_{\{1\},\{1\}} = \begin{pmatrix} 1 \end{pmatrix}$ *and* $H_{\{1\},\{1,x\}} = \begin{pmatrix} 1 & 1 \end{pmatrix}$ *have rank* 1*, hence* V_x *is updated to* $\{1\}$*.*

For the monomial y^2*,*

both matrices $H_{\{1,y\},\{1\}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *and* $H_{\{1,y\},\{1,y\}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ *have rank* 1*, hence* V_y *is updated to* $\{1, y\}$*;*
as x does not divide y, nothing is done.

For the monomial $x\,y$*,*

the matrix $H_{\{1,y,x\},\{1\}} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ *has rank* 1 *while the matrix* $H_{\{1,y,x\},\{1,y\}} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 1 \end{pmatrix}$ *has rank* 2*, hence* S *is updated to* $\{1, y\}$*.*
the matrix $H_{\{1,y\},\{1\}} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *has rank* 1 *while the matrix* $H_{\{1,y\},\{1,x\}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ *has rank* 2*, hence* S *is updated to* $\{1, y, x\}$ *and the relations are now* y^2*, with* $V_{y^2} = \{1\}$*,* $x\,y$*, with* $V_{x\,y} = \{1\}$*, and* x^2*, with* $V_{x^2} = \emptyset$*.*

For the monomial x^2*,*

as y^2 *does not divide* x^2*, nothing is done;*
as $x\,y$ *does not divide* x^2*, nothing is done;*
both matrices $H_{\{1\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}$ *and* $H_{\{1\},\{1,y,x,x^2\}} = \begin{pmatrix} 1 & 0 & 1 & 1 \end{pmatrix}$ *have rank* 1*, hence* V_{x^2} *is updated to* $\{1\}$*.*

For the monomial y^3*,*

both matrices $H_{\{1,y\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ *and* $H_{\{1,y\},\{1,y,x,y^2\}} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ *have rank* 2*, hence* V_{y^2} *is updated to* $\{1, y\}$*.*
as $x\,y$ *does not divide* y^3*, nothing is done;*
as x^2 *does not divide* y^3*, nothing is done.*

For the monomial $x\,y^2$*,*

both matrices $H_{\{1,y,x\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ *and* $H_{\{1,y,x\},\{1,y,x,y^2\}} = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{pmatrix}$ *have rank* 3*, hence* V_{y^2} *is updated to* $\{1, y, x\}$*.*
both matrices $H_{\{1,y\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ *and* $H_{\{1,y\},\{1,y,x,x\,y\}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ *have rank* 2*, hence* $V_{x\,y}$ *is updated to* $\{1, y\}$*.*
as x^2 *does not divide* $x\,y^2$*, nothing is done.*

For the monomial $x^2\,y$*,*

as y^2 *does not divide* $x^2\,y$*, nothing is done;*
both matrices $H_{\{1,y,x\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ *and* $H_{\{1,y,x\},\{1,y,x,x\,y\}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 2 \end{pmatrix}$ *have rank* 2*, hence* $V_{x\,y}$ *is updated to* $\{1, y, x\}$*.*

both matrices $H_{\{1,y\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ *and* $H_{\{1,y\},\{1,y,x,x^2\}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$ *have rank* 2*, hence* V_{x^2} *is updated to* $\{1, y\}$.

For the monomial x^3*,*

as y^2 *does not divide* x^3*, nothing is done;*

as $x\,y$ *does not divide* x^3*, nothing is done;*

both matrices $H_{\{1,y,x\},\{1,y,x\}} = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}$ *and* $H_{\{1,y,x\},\{1,y,x,x^2\}} = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 2 \\ 1 & 1 & 1 & 1 \end{pmatrix}$ *have rank* 3*, hence* V_{x^2} *is updated to* $\{1, y, x\}$.

Solving the linear systems yields relations y^2*, with a shift* x*,* $x\,y - y - 1$*, with a shift* x*, and* $x^2 - 2\,x + 1$*, with a shift* x*.*

6. Analogies and differences

In this section, we present a list of similarities and differences of behaviors and output for the BMS and the Scalar-FGLM algorithms. This should convince the reader that these algorithms are not the same and that it is not possible to tweak one of them to mimic the behavior of the other.

6.1. Closed staircase

Although both algorithms compute first a set of elements in the staircase, one of the main differences between the BMS and the Scalar-FGLM algorithms is how they handle the leading terms outside of this staircase.

Theorem 15. *Let* $\mathbf{u}$ *be a sequence and* $\prec$ *be a monomial ordering.*

Calling the BMS *algorithm on* $\mathbf{u}$*,* $\prec$ *and a stopping monomial* M *yields a truncated Gröbner basis of a zero-dimensional ideal.*

Calling the Scalar-FGLM *algorithms on* $\mathbf{u}$*,* $\prec$ *and a set of terms* T *stable by division yields a truncated Gröbner basis of an ideal, with leading monomials in* T*, which is not necessarily a zero-dimensional ideal.*

Furthermore, if the BMS *and the* Scalar-FGLM *algorithms compute the ideal of relations of* $\mathbf{u}$*, then the ideal computed by the* BMS *algorithm is included in the ideal computed by the* Scalar-FGLM *algorithm. These ideals are equal if, and only if,* $\mathbf{u}$ *is linear recurrent.*

Proof. The proof of the first part comes directly from the line $G' := \text{Border}(S')$ in the description of the BMS algorithm and then to the manipulations done to $g' \in G'$.

The proof of the second part comes from the fact that the potential leading terms in the Scalar-FGLM algorithm are taken in the intersection of the border of the staircase and the input set of terms. Nothing may ensure that this set has a pure power of every variable. See also Example 10. □

This is illustrated in the following examples.

Example 10. 1. *We let* $\mathbf{u} = \left(i^2 + j + \mathbb{1}_{3\,i+2\,j>9}\right)_{(i,j)\in\mathbb{N}^2}$ *be a sequence and consider the* DRL$(y \prec x)$ *ordering.*
The BMS *algorithm called on* $\mathbf{u}$ *and the stopping monomial* y^3 *returns the ideal of relations* $\langle x - y, y^2 - 2\,y\rangle$.
The Scalar-FGLM *algorithm called on* $\mathbf{u}$ *and the set of terms* $T = \{1, y, x, y^2\}$ *returns the ideal of relations* $\langle y^2 - 2\,y + 1\rangle$.

2. *We consider now the binomial sequence* $\mathbf{b}$ *and the* DRL$(y \prec x)$ *ordering.*
The BMS *algorithm called on* $\mathbf{b}$ *and the stopping monomial* x^5 *returns* $\langle x\,y - y - 1, y^3, (x-1)^3\rangle$.
The Scalar-FGLM *algorithm called on* $\mathbf{b}$ *and the set of terms* T *of all the monomials of degree at most* 3 *returns* $\langle x\,y - y - 1\rangle$.
The first ideal is obviously included in the second which is the true ideal of relations of the binomial sequence.

Remark 16. *It is possible to tweak the* Scalar-FGLM *algorithm so that it* tries *to close the staircase. The idea is to pick the potential leading terms in the border of the staircase. Then, for* t *such a potential leading term, if* t *is not in the input set of terms* T*, one tries to solve* $H_{T,S}\,\boldsymbol{\alpha} + H_{T,\{t\}} = 0$ *instead of only* $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{t\}} = 0$*, so that relation* $t + \sum_{s\in S}\alpha_s\,s$ *has a shift* T*. See Algorithm 5.*

Algorithm 5: Tweaked Scalar-FGLM algorithm.

Input: A table $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, $\prec$ a monomial ordering and T a set of terms in $\mathbf{x}$ stable by division.

Output: A reduced truncated Gröbner basis with respect to $\prec$ of the ideal of relations of $\mathbf{u}$ with staircase included in T.

Build the matrix $H_{T,T}$.
Compute the useful staircase (column rank profile) S of $H_{T,T}$ such that $\operatorname{rank} H_{T,T} = \operatorname{rank} H_{S,S}$.
$S' :=$ Stabilize(S).
$L := \left(T \cup \bigcup_{i=1}^{n} x_i\,S'\right)\setminus S'$.
$G := \emptyset$.
While $L \neq \emptyset$ **do**
  $t := \min_{\prec}(L)$.
  Find $\boldsymbol{\alpha}$ such that $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{t\}} = 0$.
  If $t \in T$ *or* $H_{T\setminus S,S}\,\boldsymbol{\alpha} + H_{T\setminus S,\{t\}} = 0$ **then** `// has a shift T!`
    $G := G \cup \{t + \sum_{s\in S}\alpha_s\,s\}$.
  Remove multiples of t in L and sort L by increasing order (with respect to $\prec$).
Return G.

Let us notice that this tweaked version of the Scalar-FGLM still can fail to close the staircase.

Example 11. *We call Algorithm 5 on sequence* $\mathbf{u} = \left(i^2 + j + \mathbb{1}_{3\,i+2\,j>9}\right)_{(i,j)\in\mathbb{N}^2}$*, the set* $T = \{1, y, x, y^2\}$ *and the* DRL$(y \prec x)$ *ordering as in Example 10.*

We build the matrix

$$H_{T,T} = \begin{array}{c} \\ 1 \\ y \\ x \\ y^2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & x & y^2 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 3 & 4 \end{pmatrix} \end{array}.$$

The useful staircase of this matrix is $S = \{1, y, x\}$.
It is stable by division so $S' = S$.
We set $L = \{1, y, x, y^2, x\,y, x^2\} \setminus \{1, y, x\} = \{y^2, x\,y, x^2\}$ *and* $G = \emptyset$.
We take $t = y^2$ *and solve* $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{y^2\}} = 0$ *which yields relation* $y^2 - 2\,y + 1$*, so* $G = \{y^2 - 2\,y + 1\}$ *and* L *is updated to* $\{x\,y, x^2\}$.
We take $t = x\,y$ *and solve*

$$H_{S,S\cup\{x\,y\}} \begin{pmatrix} \alpha_1 \\ \alpha_y \\ \alpha_x \\ 1 \end{pmatrix} = \begin{array}{c} \\ 1 \\ y \\ x \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & x & x\,y \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 4 & 5 \end{pmatrix} \end{array} \begin{pmatrix} \alpha_1 \\ \alpha_y \\ \alpha_x \\ 1 \end{pmatrix} = 0,$$

which yields relation $x\,y - x - y + 1$*. We check that*

$$H_{T\setminus S,S\cup\{x\,y\}} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = \begin{array}{c} \\ y^2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & x & x^2 \end{array} \\ \begin{pmatrix} 2 & 3 & 3 & 4 \end{pmatrix} \end{array} \begin{pmatrix} 1 \\ -1 \\ -1 \\ 1 \end{pmatrix} = 0,$$

set $G = \{y^2 - 2\,y + 1, x\,y - x - y + 1\}$ *and update* L *to* $\{x^2\}$.
We take $t = x^2$ *and solve*

$$H_{S,S\cup\{x\,y\}} \begin{pmatrix} \alpha_1 \\ \alpha_y \\ \alpha_x \\ 1 \end{pmatrix} = \begin{array}{c} \\ 1 \\ y \\ x \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & x & x\,y \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 2 \\ 1 & 2 & 2 & 3 \\ 1 & 2 & 4 & 5 \end{pmatrix} \end{array} \begin{pmatrix} \alpha_1 \\ \alpha_y \\ \alpha_x \\ 1 \end{pmatrix} = 0,$$

which yields relation $x^2 - 2\,x^2 - 2\,x + 3$*. However,*

$$H_{T\setminus S,S\cup\{x^2\}} \begin{pmatrix} 3 \\ -2 \\ -2 \\ 1 \end{pmatrix} = \begin{array}{c} \\ y^2 \end{array} \begin{array}{c} \begin{array}{cccc} 1 & y & x & x^2 \end{array} \\ \begin{pmatrix} 2 & 3 & 3 & 7 \end{pmatrix} \end{array} \begin{pmatrix} 3 \\ -2 \\ -2 \\ 1 \end{pmatrix} = 1,$$

so the relation is not valid when shifted by y^2. Hence, we let $G = \{y^2 - 2y + 1, xy - x - y + 1\}$ and update L to $\emptyset$.
We return $G = \{y^2 - 2y + 1, xy - x - y + 1\}$.
Furthermore, each relation $g \in G$ satisfies $[m\,g] = 0$, for all $m \in T = \{1, y, x, y^2\}$, i.e. has a shift T.

6.2. Reduction of relations

Even though the BMS and the Scalar-FGLM algorithms may compute the same ideal of relations for a given sequence, the Gröbner bases they compute may differ. However, it is possible to tweak the BMS algorithm so that it returns the same Gröbner basis of the ideal as the Scalar-FGLM algorithm.

Theorem 17. *Let $\mathbf{u}$ be a sequence and $\prec$ be a monomial ordering.*

Calling the Scalar-FGLM *algorithms on $\mathbf{u}$, $\prec$ and a set of terms T stable by division yields a truncated minimal reduced Gröbner basis of an ideal.*

Calling the BMS *algorithm on $\mathbf{u}$, $\prec$ and a stopping monomial M yields a truncated minimal Gröbner basis of an ideal, which is not necessarily reduced.*

Furthermore, even if $\mathbf{u}$ is linear recurrent and the Scalar-FGLM *algorithm computes the ideal of relations of $\mathbf{u}$, then there is no reason for the output of the* BMS *algorithm to be reduced.*

Proof. When updating a relation g thanks to a failing relation h in the BMS algorithm, nothing ensures that g has support in $S \cup \{\mathrm{LM}(g)\}$, where S is the current staircase, as $\operatorname{supp} h$ may not be included in S. This prevents the returned Gröbner basis to be reduced, see also Example 12.

As the Scalar-FGLM algorithm computes a staircase S, the monomials on the border of S and then solves a multi-Hankel linear system indexed by S and one of the monomial on this border, it is clear that the output truncated Gröbner basis is reduced. □

The following example show which Gröbner bases are returned by the BMS and the Scalar-FGLM algorithms for a same sequence.

Example 12. *We let $\mathbf{u} = \left(i^2 + j^2 - 1\right)_{(i,j)\in\mathbb{N}^2}$ be a sequence and consider the* DRL*$(y \prec x)$ ordering. The ideal of relations of $\mathbf{u}$ is $I = \langle xy - x - y + 1, x^2 - y^2 - 2x + 2y, y^3 - 3y^2 + 3y - 1\rangle$.*

The BMS *algorithm called on $\mathbf{u}$ and the stopping monomial y^5 returns $g_1 = xy - x - y + 1$, with shift x^2, $g_2 = x^2 - \frac{1}{3}xy - y^2 - \frac{5}{3}x + \frac{7}{3}y - \frac{1}{3}$, with shift x^2 and $g_3 = y^3 - \frac{1}{2}xy - 3y^2 + \frac{1}{2}x + \frac{7}{2}y - \frac{3}{2}$, with shift y^2. We can notice that $\{g_1, g_2, g_3\}$ is a minimal Gröbner basis but not a reduced Gröbner basis of I.*

The Scalar-FGLM *algorithm called on* $\mathbf{u}$ *and the set of all the monomials of degree at most* 3 *yields relations* $g'_1 = x\,y - x - y + 1, g'_2 = x^2 - y^2 - 2\,x + 2\,y, g'_3 = y^3 - 3\,y^2 + 3\,y - 1$. *We can notice that* $\{g'_1, g'_2, g'_3\} = \{g_1, g_2 + \frac{1}{3}\,g_1, g_3 + \frac{1}{2}\,g_1\}$ *is a minimal reduced Gröbner basis of* I.

Remark 18. *Let* g'_1, g'_2 *be two computed relations by the* BMS *algorithm and let* μ *be a monomial. Assume* $\mu\ \mathrm{LM}(g'_1) \preceq \mathrm{LM}(g'_2)$, *then* $\mathrm{shift}(\mu\ \mathrm{LM}(g'_1)) \succeq \mathrm{LM}(g'_2) = v$. *Therefore* $g'_2 - c\,\mu\,g'_1$ *has still shift* v *for any scalar* c: *hence one can replace* g'_2 *by* $g'_2 - c\,\mu\,g'_1$, *i.e. one can reduce* g'_2 *by* g'_1 *into* g_2 *and replace* g'_2 *by* g_2. *Let us notice that we can tweak the* BMS *algorithm so that, at each step, the set of relations is a truncated reduced Gröbner basis. It suffices to perform an inter-reductions of the computed relations at the end of each step of the* ***For*** *loop, see Algorithm 6.*

Algorithm 6: Tweaked BMS algorithm

Input: A table $\mathbf{u} = (u_\mathbf{i})_{\mathbf{i}\in\mathbb{N}^n}$ with coefficients in $\mathbb{K}$, a monomial ordering $\prec$ and a monomial M as the stopping condition.

Output: A set G of relations generating I_M.

$T := \{m \in \mathbb{K}[\mathbf{x}],\ m \preceq M\}$.
$G := \{1\}$.
$S := \emptyset$.
For all $m \in T$ **do**
  $S' := S$
  For $g \in G$ **do**
    If $\mathrm{LM}(g) | m$ **then**
      $e := \left[\frac{m}{\mathrm{LM}(g)}\,g\right]_\mathbf{u}$
      If $e \neq 0$ **then**
        $S' := S' \cup \left\{\left[\frac{g}{e}, \frac{m}{\mathrm{LM}(g)}\right]\right\}$.
    $S' := \min_{\mathrm{fail}(h)\in S'} \{[h, \mathrm{fail}(h)/\ \mathrm{LM}(h)]\}$.
    $G' := \mathrm{Border}(S')$.
  For $g' \in G'$ **do**
    Let $g \in G$ such that $\mathrm{LM}(g) | \mathrm{LM}(g')$.
    If $\mathrm{LM}(g) \nmid m$ **then**
      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\,g$.
    Else if $\exists\, h \in S, \frac{m}{\mathrm{LM}(g')} | \mathrm{fail}(h)$ **then**
      $g' := \frac{\mathrm{LM}(g')}{\mathrm{LM}(g)}\,g - \left[\frac{m}{\mathrm{LM}(h)}\,h\right]_\mathbf{u}\ \frac{\mathrm{LM}(g')\ \mathrm{fail}(h)}{m}\,h$.
    Else $g' := g$.
  $G := \mathrm{InterReduce}(G')$
  $S := S'$
Return G.

6.3. Validity of relations

We compare the relationship between relations and shifts as they are computed by the BMS and the Scalar-FGLM algorithms.

Theorem 19. *Let* $\mathbf{u}$ *be a sequence and* $\prec$ *be a monomial ordering.*

Calling the BMS *algorithm on* $\mathbf{u}$*,* $\prec$ *and a stopping monomial* M *yields relations* $g_1, \ldots, g_r$ *and shifts* $v_1, \ldots, v_r$ *such that*

$$\forall\, i, 1 \leq i \leq r, \quad v_i \ \mathrm{LM}(g_i) \leq M$$

and g_i *is valid with a shift* v_i*, potentially* 0*.*

Calling the Scalar-FGLM *algorithm on* $\mathbf{u}$*,* $\prec$ *and a set of terms* $T_M = \{m,\ m \leq M\}$ *yields relations* $g'_1, \ldots, g'_{r'}$ *such that*

$$\forall\, i, 1 \leq i \leq r', \quad \mathrm{LM}(g'_i) \leq M$$

and g'_i *has a shift* T_M*, i.e. is valid with a shift* M*.*

Proof. The BMS algorithm tests its relations up to M, i.e. it shifts them up to M. In the worst case, the leading term of a relation is greater than M, but then it has a shift 0.

The Scalar-FGLM algorithm returns relations $g = \mathrm{LT}(g) + \sum_{s \in S} \alpha_s\, s$ such that $H_{T,S}\, \boldsymbol{\alpha} + H_{T,\{\mathrm{LM}(g)\}} = 0$, i.e. they are valid when shifted by any monomial in T. □

We illustrate this with the following example.

Example 13. *We let* $\mathbf{b}$ *be the binomial sequence and consider the* $\mathrm{DRL}(y \prec x)$ *ordering.*

The BMS *algorithm called on* $\mathbf{b}$ *and the stopping monomial* x^7 *returns* $x\,y - y - 1$*, with a shift* x^5*;* y^4*, with a shift* x^3*; and* $(x-1)^4$*, with a shift* x^3*.*

With the matrix viewpoint, one has

$$21 \text{ rows} \begin{cases} & \begin{matrix} 1 & y & x & xy \end{matrix} \\ \begin{matrix} 1 \\ y \\ x \\ \vdots \\ x^3 \\ \vdots \\ x^5 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 3 & 1 & 4 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 5 & 1 & 6 \end{pmatrix} \end{cases} \begin{pmatrix} -1 \\ -1 \\ 0 \\ 1 \end{pmatrix} = 0,$$

$$10 \text{ rows} \begin{cases} & \begin{matrix} 1 & y & x & \cdots & y^4 \end{matrix} \\ \begin{matrix} 1 \\ y \\ x \\ \vdots \\ x^3 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 3 & 1 & \cdots & 0 \end{pmatrix} \end{cases} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = 0, \quad \begin{matrix} & \begin{matrix} 1 & y & x & \cdots & x^4 \end{matrix} \\ \begin{matrix} 1 \\ y \\ x \\ \vdots \\ x^3 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 4 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 1 & 1 & \cdots & 1 \end{pmatrix} \end{matrix} \begin{pmatrix} 1 \\ 0 \\ -4 \\ \vdots \\ 1 \end{pmatrix} = 0.$$

We can notice that the first matrix has many more rows than the other two.

The Scalar-FGLM *algorithm called on* $\mathbf{b}$ *and the set* T *of all the monomials of degree at most* 3 *returns* $xy - y - 1$ *with a shift* x^3*. With the matrix viewpoint, one has*

$$10 \text{ rows} \begin{cases} & \begin{matrix} 1 & y & x & xy \end{matrix} \\ \begin{matrix} 1 \\ y \\ x \\ \vdots \\ x^3 \end{matrix} & \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 2 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 3 & 1 & 4 \end{pmatrix} \end{cases} \begin{pmatrix} -1 \\ -1 \\ 0 \\ 1 \end{pmatrix} = 0.$$

Likewise, calling Algorithm 5 on the same input returns $xy - y - 1, y^4, x^4$*, all*

three valid up to x^3. With the matrix viewpoint, we also have this matrix equality:

$$10 \text{ rows} \left\{ \begin{array}{c} \\ 1 \\ y \\ x \\ \vdots \\ x^3 \end{array} \right. \begin{array}{c} \begin{array}{ccccc} 1 & y & x & \cdots & y^4 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 1 & 1 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 3 & 1 & \cdots & 0 \end{pmatrix} \end{array} \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \begin{array}{c} 1 \\ y \\ x \\ \vdots \\ x^3 \end{array} \begin{array}{c} \begin{array}{ccccc} 1 & y & x & \cdots & x^4 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 4 \\ 1 & 1 & 1 & \cdots & 1 \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & 3 & 1 & \cdots & 1 \end{pmatrix} \end{array} \begin{pmatrix} 1 \\ 0 \\ -4 \\ \vdots \\ 1 \end{pmatrix} = 0.$$

We can see that the last two matrices have as many rows as the first one.

That being said, for a monomial $m = \mu \operatorname{LM}(g) \in T$, the column labeled with m in $H_{T,T}$ is also linearly dependent from the previous ones. In particular, it allows us to verify that the relation $\mu\, g$ is valid with a shift T, i.e. g is valid with a shift $T \cup \mu\, T$.

Example 14. *Resuming Example 13, the columns labeled with $x\,y^2$, $x^2\,y$, $x\,y^3$, $x^2\,y^2$ and $x^3\,y$ are linearly dependent from the previous ones. For instance, the column labeled with $x\,y^2$ is the sum of the columns labeled with y^2 and y. Thus, Pascal's rule $x\,y - y - 1$ is also valid with shifts $y\,T$, $x\,T$, $y^2\,T$, $x\,y\,T$ and $x^2\,T$. Since T is the set of the monomials of degree at most* 3, $\bigcup_{\mu \in \{1,y,x,y^2,x\,y,x^2\}} \mu\, T$ *is the set of all the monomials of degree* 5.

All in all, like for the BMS *algorithm, we find that the Pascal's rule is valid with a shift x^5.*

6.4. Monomial ordering and Set of Terms

Given a linear recurrent sequence $\mathbf{u}$ with ideal of relation defined by a Gröbner basis $\mathcal{G}$ for a monomial ordering $\prec$, the BMS and the Scalar-FGLM algorithms can return $\mathcal{G}$ only if the input set of terms contains the staircase defined by $\mathcal{G}$. That is why, it is preferable to run both of them with an ordering $\prec$ such that for all monomial $M \in \mathbb{K}[\mathbf{x}]$, $T_M = \{m,\ m \preceq M\}$ is finite. In particular, the lex ordering does not satisfy such a property.

However, we can try to see how they behave when calling them with the lex monomial ordering. We relate this to the randomized reduction to the BM algorithm presented in (Berthomieu et al., 2015, 2016, Section 3) where the authors perform a randomized linear change of variables so that, generically, the ideal of relations is in shape position. We also relate this to the Sparse-FGLM algorithm application where the input is a sequence made from a Gröbner basis, typically for the drl ordering, and the output is the ideal of relations of this sequence for another ordering, typically lex, see Faugère and Mou (2011, 2017).

Theorem 20. *Let* $\mathbf{u}$ *be a linear recurrent sequence whose ideal of relation* I *is in shape position for the* $\text{LEX}(x_n \prec \cdots \prec x_2 \prec x_1)$ *ordering, i.e. there exist* g_n *squarefree and* $f_{n-1}, \ldots, f_1 \in \mathbb{K}[x_n]$ *with* $\deg g_n = d, \deg f_i < d$ *such that* $I = \langle g_n(x_n), x_{n-1} - f_{n-1}(x_n), \ldots, x_1 - f_1(x_n)\rangle$.

Calling the Scalar-FGLM *algorithm as designed in Berthomieu et al. (2015, 2016) or its tweaked version Algorithm 5 on* $\mathbf{u}$*,* T *containing at least* $\{1, x_n, \ldots, x_n^{d-1}\}$ *and* $\text{LEX}(x_n \prec \cdots \prec x_2 \prec x_1)$ *allows one to retrieve* I.

Calling the BMS *algorithm on* $\mathbf{u}$*, with the stopping monomial* x_n^e *and* $\text{LEX}(x_n \prec \cdots \prec x_2 \prec x_1)$ *yields* $\langle g(x_n), x_{n-1}, \ldots, x_1\rangle$*. This ideal is not equal to* I*, unless* $f_1 = \cdots = f_{n-1} = 0$.

In other words, the Scalar-FGLM *algorithm can retrieve an ideal of relations in shape position while, in general, the* BMS *algorithm cannot.*

Proof. When calling the Scalar-FGLM algorithm on $\mathbf{u}$ with the $\text{LEX}(x_n \prec \cdots \prec x_2 \prec x_1)$ ordering and with the set of terms T containing $\{1, x_n, \ldots, x_n^{d-1}\}$, the algorithm shall determine that the useful staircase $S = \{1, x_n, \ldots, x_n^{d-1}\}$. Then, the set of potential leading monomials is $\{x_n^d, x_{n-1}, \ldots, x_1\}$. For x_n^d, it solves $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{x_n^d\}} = 0$ and finds relation $g_n(x_n)$ while for any k, $1 \le k \le n-1$, it solves $H_{S,S}\,\boldsymbol{\alpha} + H_{S,\{x_k\}} = 0$ and finds relation $x_k - f_k(x_n)$. Then it tests that these relations have a shift T, and since they are the true relations of $\mathbf{u}$, they do.

When calling the BMS algorithm with the $\text{LEX}(x_n \prec \cdots \prec x_2 \prec x_1)$ ordering and with the stopping monomial $M = x_n^e$, the algorithm behaves *mutatis mutandis* like the BM algorithm except that as soon as 1 is detected to be in the staircase, the BMS algorithms adds polynomials $x_1, \ldots, x_{n-1}$ in the truncated Gröbner basis. As these relations cannot be tested further, the output shall always be $\mathcal{G} = \langle g(x_n), x_{n-1}, \ldots, x_1\rangle$. See also Example 15 below. □

We illustrate the behavior of the Scalar-FGLM algorithm with an example.

Example 15. *We let* $\mathbf{u} = (F_{4\,i+k})_{(i,j,k)\in\mathbb{N}^3}$ *be a sequence, where* $(F_i)_{i\in\mathbb{N}}$ *is the Fibonacci sequence, and consider the* $\text{DRL}(z \prec y \prec x)$ *ordering. The ideal of relations of* $\mathbf{u}$ *is* $I = \langle z^2 - z - 1, y - 1, x - 3\,z - 2\rangle$.

The Scalar-FGLM *algorithm called on* $\mathbf{u}$ *and the set of terms* $\{1, z, \ldots, z^{d+2}\}$ *yields* $\langle g_3, g_2, g_1\rangle$*, which is indeed the ideal of relations of the sequence. In detail:*

It creates the matrix

$$H_{T,T} = \begin{array}{c} \\ 1 \\ z \\ \vdots \\ z^{d+2} \end{array} \begin{array}{c} \begin{array}{cccc} 1 & z & \cdots & z^{d+2} \end{array} \\ \begin{pmatrix} 0 & 1 & \cdots & F_{d+2} \\ 1 & 1 & \cdots & F_{d+3} \\ \vdots & \vdots & & \vdots \\ F_{d+2} & F_{d+3} & \cdots & F_{2\,d+4} \end{pmatrix} \end{array}$$

and finds it has rank 2 *with useful staircase* $S = \{1, z\}$.
It solves

$$H_{S,S\cup\{z^2\}}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = \begin{matrix}1\\ z\end{matrix}\ \begin{matrix}\begin{matrix}1 & z & z^2\end{matrix}\\ \begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 2\end{pmatrix}\end{matrix}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = 0$$

and finds relation $z^2 - z - 1$.
Then, it solves

$$H_{S,S\cup\{y\}}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = \begin{matrix}1\\ z\end{matrix}\ \begin{matrix}\begin{matrix}1 & z & y\end{matrix}\\ \begin{pmatrix}0 & 1 & 1\\ 1 & 1 & 1\end{pmatrix}\end{matrix}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = H_{S,S\cup\{x\}}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = \begin{matrix}1\\ z\end{matrix}\ \begin{matrix}\begin{matrix}1 & z & x\end{matrix}\\ \begin{pmatrix}0 & 1 & 3\\ 1 & 1 & 5\end{pmatrix}\end{matrix}\begin{pmatrix}\alpha_1\\ \alpha_z\\ 1\end{pmatrix} = 0.$$

and finds the relations $g_2 = y - 1$ *and* $g_1 = x - 3z - 2$. *It also checks that the last two have a shift* T *with*

$$H_{T\setminus S,S\cup\{y\}}\begin{pmatrix}-1\\ 0\\ 1\end{pmatrix} = \begin{matrix}z^2\\ \vdots\\ z^{d+2}\end{matrix}\ \begin{matrix}\begin{matrix}1 & z & y\end{matrix}\\ \begin{pmatrix}1 & 2 & 1\\ \vdots & \vdots & \vdots\\ F_{d+2} & F_{d+3} & F_{d+2}\end{pmatrix}\end{matrix}\begin{pmatrix}-1\\ 0\\ 1\end{pmatrix} = 0,$$

$$H_{T\setminus S,S\cup\{x\}}\begin{pmatrix}-2\\ -3\\ 1\end{pmatrix} = \begin{matrix}z^2\\ \vdots\\ z^{d+2}\end{matrix}\ \begin{matrix}\begin{matrix}1 & z & x\end{matrix}\\ \begin{pmatrix}1 & 2 & 8\\ \vdots & \vdots & \vdots\\ F_{d+2} & F_{d+3} & F_{d+6}\end{pmatrix}\end{matrix}\begin{pmatrix}-2\\ -3\\ 1\end{pmatrix} = 0.$$

Finally, it returns g_3, g_2, g_1.

The BMS *algorithm called on* $\mathbf{u}$ *and the stopping monomial* z^{d+2} *returns* $\langle g_3, y, x\rangle$, *which is not the ideal of relations of the sequence, as neither* y *nor* x *are in* I. *In detail:*

The algorithms tests the relation $g = 1$ *in* $u_{0,0,0} = F_0 = 0$ *where it succeeds.*
It tests g *in* $u_{0,0,1} = F_1 = 1$ *where it fails. It has now relations* $g_1 = x, g_2 = y$ *and* $g_3 = z^2$, *all three with a shift* 0.
Going on testing z^2 *in* $u_{0,0,2} = F_2 = 1$, $u_{0,0,3} = F_3$ *and so on, it is able to update* g_3 *into* $z^2 - z - 1$ *but is never able to test either* g_1 *or* g_2.
Finally, it returns g_3 *with a shift* z^d *and* g_1, g_2 *with a shift* 0.

Although g_3 *is in the ideal of relations,* g_1 *and* g_2 *are not.*

Remark 21. *Let us notice though that, whenever the user knows the degree d of the ideal of relations of a linear recurrent sequence, we can tweak both algorithms to be able to recover fully the ideal of relations.*

On the one hand, it suffices to call the Scalar-FGLM *algorithm with the set of monomials $T = \{m,\ \deg m \leq d\}$ and the* lex$(x_n \prec \cdots \prec x_2 \prec x_1)$ *ordering.*

On the other hand, it suffices to change a little bit how we enumerate the monomials less than the stopping monomial M in the BMS *algorithm. In most implementation, monomials less than or equal to M are given by the ordered set of terms $T_M = \{m,\ m \preceq M\}$. If one knows in advance the degree d of the ideal, then it suffices to enumerate the monomials in $\{m,\ \deg m \leq 2\,d - 1, m \preceq M\}$ and to call the* BMS *algorithm with the* lex$(x_n \prec \cdots \prec x_2 \prec x_1)$ *ordering. This tweaked version of the* BMS *algorithm was implemented for the* Sparse-FGLM *application in Faugère and Mou (2011, 2017).*

7. Complexity and Benchmarks

In this section, we present some benchmarks to compare the behaviors of the BMS and the Scalar-FGLM algorithms. We relate them with the announced complexity of each algorithm.

Three families of ideals of relations are used to make the sequences.

- In the first family, the leading monomials of the ideal of relations are $\langle y^{\lfloor d/2 \rfloor}, x^d \rangle$. Thus, its staircase is a rectangle of size around $d^2/2$. In three variables, the leading monomials are $\langle z^{\lceil d/3 \rceil}, y^{\lfloor d/2 \rfloor}, x^d \rangle$, so that the staircase is a rectangular cuboid of size around $d^3/6$. This family will be called *Rectangle*.

- In the second family, the leading monomials of the ideal of relations are $\langle x\,y, y^d, x^d \rangle$. Thus, its staircase looks like a L and has size $2\,d - 1$. In three variables, the leading monomials are $\langle y\,z, x\,z, x\,y, z^d, y^d, x^d \rangle$, so that the staircase has size $3\,d - 2$. This family will be called L *shape*. It was considered as the worst case in Berthomieu et al. (2015, 2016) for the Adaptive Scalar-FGLM algorithm, a variant of the Scalar-FGLM algorithm, for the number of queries. It should also be a worst case for the BMS algorithm.

- In the last family, the leading monomials of the ideal of relations are all the monomials of degree d. Thus, its staircase is a simplex and has size $\binom{d+1}{2} = \frac{d\,(d+1)}{2}$ in two variables. In three variables, the staircase has size $\binom{d+2}{3} = \frac{d\,(d+1)\,(d+2)}{6}$. This family will be called *Simplex*. It should be the best case for both the Scalar-FGLM and the BMS algorithms.

For all these families, we called the algorithms with the $\text{DRL}(y \prec x)$ ordering.

For the BMS algorithm, we used Proposition 11 to estimate sharply the stopping monomial. For the Scalar-FGLM algorithm, we took all the monomials of the largest degree appearing in the staircase and the minimal Gröbner basis.

7.1. Counting the number of table queries

Thanks to the Proposition 11 giving a monomial M such that at step M, the BMS algorithm recovers a Gröbner basis of the ideal of relations of the input sequence, we can deduce the following proposition.

Proposition 22. *Let* $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ *be a sequence and* $\mathcal{G}$ *be a minimal Gröbner basis of its ideal of relations for a total degree ordering.*

Let d_S *be the greatest degree of the elements in the staircase of* $\mathcal{G}$, $d_{\mathcal{G}}$ *be the greatest degree of the elements in* $\mathcal{G}$ *and* $d_{\max} = \max(d_S, d_{\mathcal{G}})$.

Let $\mathcal{S}(d)$ *be the simplex of all monomials of degree* d.

Then, the BMS *algorithm needs to perform at least* $\#\mathcal{S}(d_S + d_{\max} - 1) = \binom{n+d_S+d_{\max}-1}{n}$ *and at most* $\#\mathcal{S}(d_S + d_{\max}) = \binom{n+d_S+d_{\max}}{n}$ *queries to* $\mathbf{u}$.

The Scalar-FGLM *algorithm called on* $T = \mathcal{S}(d_{\max})$ *the set of all of monomials of degree at most* $d_{\max}$ *needs to perform* $\#\mathcal{S}(2\,d_{\max}) = \binom{n+2\,d_{\max}}{n}$ *queries to* $\mathbf{u}$.

For n *fixed, these numbers grow as* $O(d_{\max}^n)$.

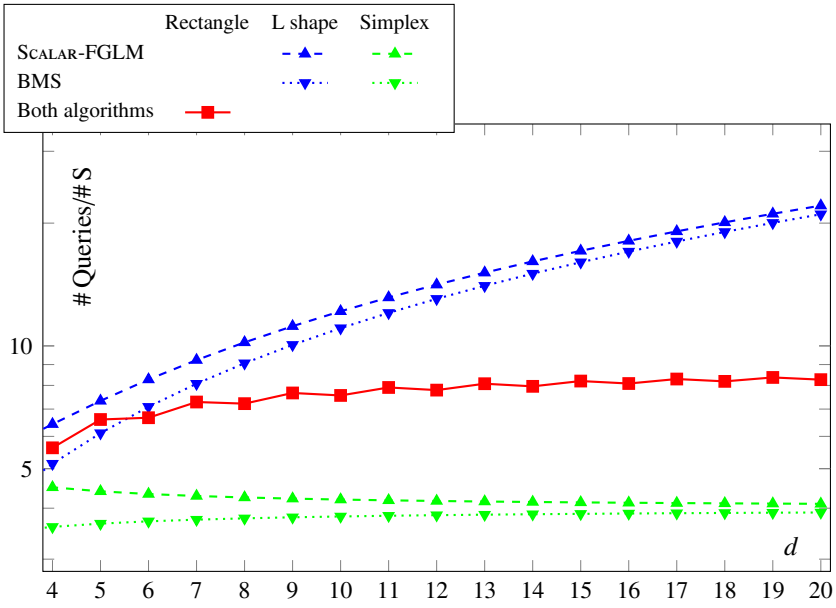


Figure 1: Number of table queries (2D)

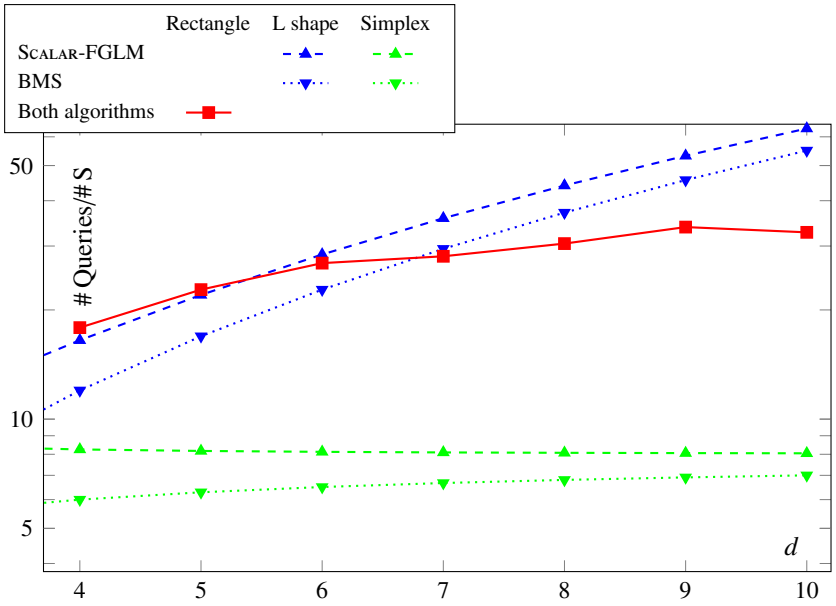


Figure 2: Number of table queries (3D)

In the experiments of Figures 1 and 2, we report on the ratio between the numbers of queries and the size of the staircase for the three families of polynomials.

Not surprisingly, the Scalar-FGLM algorithm always performs the most queries. This is due to the fact that in Proposition 22, either $d_{\mathcal{G}} = d_S + 1$ or $d_S \geq d_{\mathcal{G}}$, hence $d_{\max} \in \{d_S - 1, d_S\}$ and $d_S + d_{\max} \in \{2\,d_{\max} - 1, 2\,d_{\max}\}$.

Though, we can see that for the Rectangle family, each algorithm performs exactly as many queries as the other.

For the Rectangle and Simplex families, the size of the staircase and the number of queries grow like $O(d^n)$, where $n = 2, 3$, the dimension. This is why the ratio seems rather constant.

However, for the L shape family, the size of the staircase only grows as $O(d)$ while the number of queries grows as $O(d^n)$. This is also confirmed by our experiments, where the ratio between the number of queries and the size of the staircase grows much faster in dimension 3 than in dimension 2.

In fact, each algorithm performs as many queries for the L shape family as for the Simplex family. Thus, we can see that neither is able to take profit from the size of the staircase.

7.2. Counting the number of basic operations

The complexity of the BMS algorithm has been studied in Sakata (2009).

Proposition 23. *Let* $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ *be a sequence,* $\mathcal{G}$ *be a minimal Gröbner basis of its ideal of relations for a total degree ordering and* S *be the staircase of* $\mathcal{G}$.

Then, the BMS *algorithm performs at most* $O\left((\#S)^2\ \text{LM}(\mathcal{G})\right)$ *operations to recover the ideal of relations of* $\mathbf{u}$.

The Scalar-FGLM computes the column rank profile of a matrix of size $\#\mathcal{S}(d_{\max})$. Then, it solves as many linear systems with the submatrix of size $\#S$ as there are polynomials in the Gröbner basis. All in all, we have the following result.

Proposition 24. *Let* $\mathbf{u} = (u_{\mathbf{i}})_{\mathbf{i}\in\mathbb{N}^n}$ *be a sequence,* $\mathcal{G}$ *be a reduced Gröbner basis of its ideal of relations for a total degree ordering and* S *be the staircase of* $\mathcal{G}$. *Let* $d_{\max}$ *be the maximal degree of the elements of* S *and* $\mathcal{G}$.

Then, the number of operations performed by the Scalar-FGLM *algorithm to recover the ideal of relations of* $\mathbf{u}$ *is at most* $O\left((\#\mathcal{S}(d_{\max}))^3 + (\#S)^2\,\#\ \text{LM}(\mathcal{G})\right)$.

In the following Figures 3 and 4, we report on the ratio between the number of basic operations and the cube of the size of the staircase.

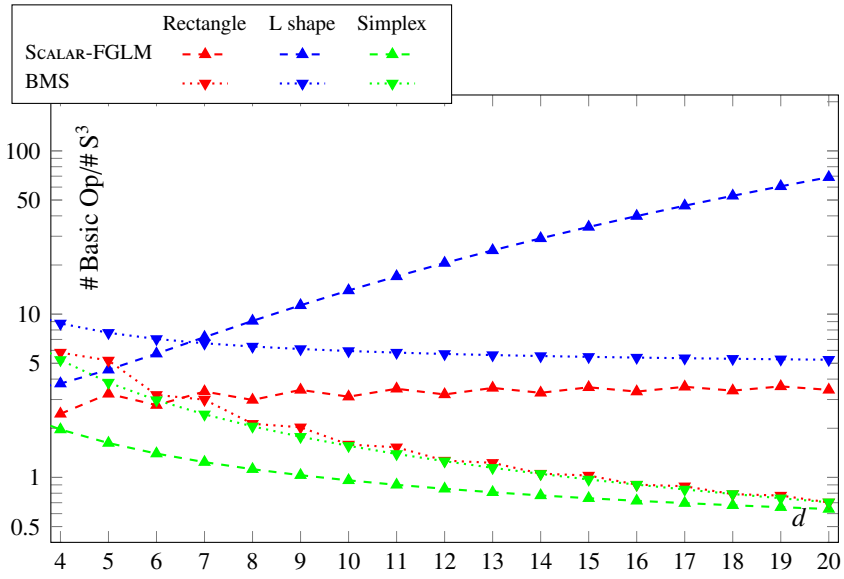


Figure 3: Number of basic operations (2D)

For the Rectangle family, we have $\#S \in O(d^n)$, $\#\mathcal{S}(d_{\max}) \in O(d^n)$ and $\text{LM}(\mathcal{G}) = 3$ so that $(\#S)^2\,\#\ \text{LM}(\mathcal{G}) \in O(d^{2n})$. This is why, we can see, first, a constant ratio between the number of basic operations done by the Scalar-FGLM algorithm and the size of the staircase and, then, a decreasing ratio for the BMS algorithm. An analogous analysis explains why, for the L shape family, the ratio is increasing for the Scalar-FGLM algorithm and quite constant for the BMS algorithm.

Unexpectedly, the Scalar-FGLM algorithm performs fewer basic operations than the BMS algorithm for the Simplex family. This is mainly due to the fact that, for this family, the term $(\#S)^2 \,\#\, \mathrm{LM}(\mathcal{G})$ is in fact larger than $(\#\mathcal{S}(d_{\max}))^3$.

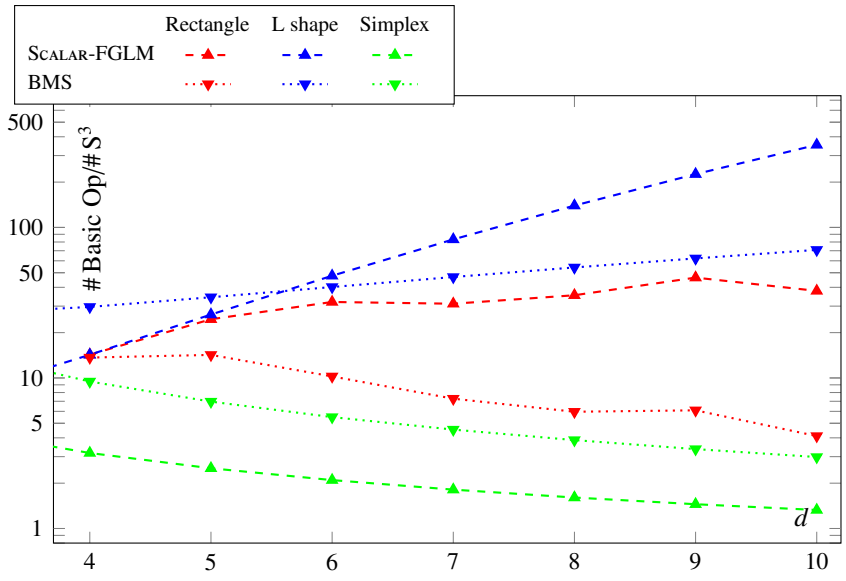


Figure 4: Number of basic operations (3D)

We now compare the ratio between the number of basic operations and the number of queries made by each algorithm in Figures 5 and 6.

As we can see, beside for the Simplex family where the Scalar-FGLM performed fewer operations but more queries than the BMS algorithm, the polynomial arithmetic of the BMS algorithm allows it to have a much better behavior than the Scalar-FGLM algorithm.

This reinforces the conviction that an hybrid approach between the BMS and the Scalar-FGLM algorithm or a fast multi-Hankel solver should be investigated.

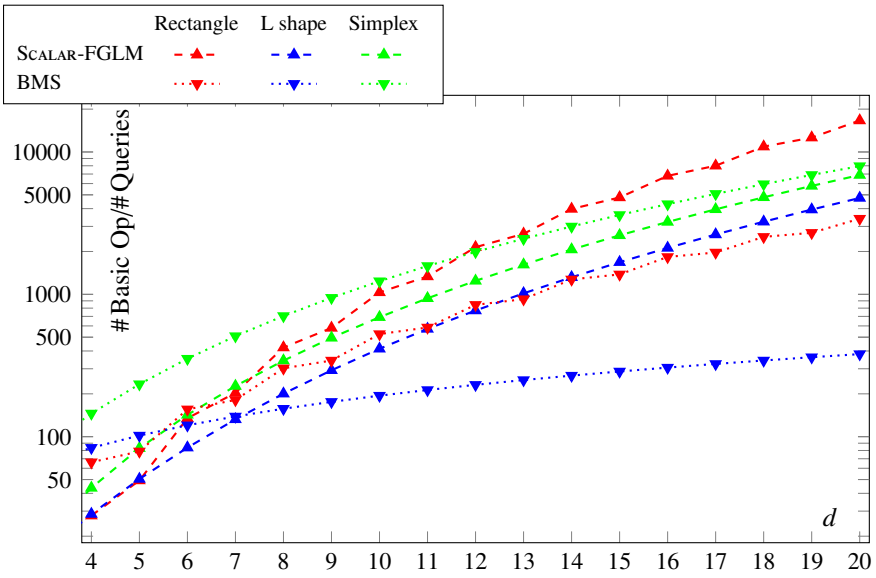


Figure 5: Number of basic operations by queries (2D)

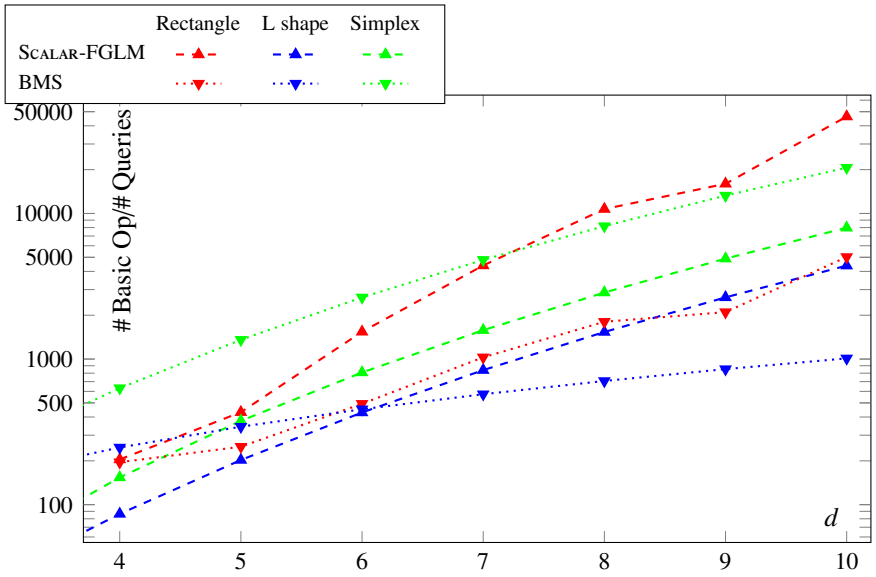


Figure 6: Number of basic operations by queries (3D)

References

Banderier, C., Flajolet, P., 2002. Basic analytic combinatorics of directed lattice paths. Theoret. Comput. Sci. 281 (1–2), 37–80, selected Papers in honour of Maurice Nivat.
URL http://www.sciencedirect.com/science/article/pii/S0304397502000075

Benoit, A., Chyzak, F., Darrasse, A., Gerhold, S., Mezzarobba, M., Salvy, B., 2010. The Dynamic Dictionary of Mathematical Functions (DDMF). In: Fukuda, K., Hoeven, J. v. d., Joswig, M., Takayama, N. (Eds.), Mathematical Software – ICMS 2010. Springer, Berlin, Heidelberg, pp. 35–41.
URL http://dx.doi.org/10.1007/978-3-642-15582-6_7

Berlekamp, E., 1968. Nonbinary BCH decoding. IEEE Trans. Inform. Theory 14 (2), 242–242.

Berthomieu, J., Boyer, B., Faugère, J.-Ch., 2015. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. In: 40th International Symposium on Symbolic and Algebraic Computation. Proceedings of the 40th International Symposium on Symbolic and Algebraic Computation. Bath, United Kingdom, pp. 61–68.

Berthomieu, J., Boyer, B., Faugère, J.-Ch., 2016. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. Journal of Symbolic Computation, 48.

Berthomieu, J., Faugère, J.-Ch., 2016. Guessing Linear Recurrence Relations of Sequence Tuples and P-recursive Sequences with Linear Algebra. In: 41st International Symposium on Symbolic and Algebraic Computation. Waterloo, ON, Canada, pp. 95–102.

Blackburn, S. R., 1997. Fast rational interpolation, reed-solomon decoding, and the linear complexity profiles of sequences. IEEE Transactions on Information Theory 43 (2), 537–548.

Bose, R., Ray-Chaudhuri, D., 1960. On a class of error correcting binary group codes. Information and Control 3 (1), 68 – 79.
URL http://www.sciencedirect.com/science/article/pii/S0019995860902874

Bostan, A., Bousquet-Mélou, M., Kauers, M., Melczer, S., 2014. On 3-dimensional lattice walks confined to the positive octant, to appear in Annals of Combinatorics.

Bousquet-Mélou, M., Mishna, M., 2010. Walks with small steps in the quarter plane. In: Algorithmic probability and combinatorics. Vol. 520 of Contemp. Math. Amer. Math. Soc., Providence, RI, pp. 1–39.
URL http://dx.doi.org/10.1090/conm/520/10252

Bousquet-Mélou, M., Petkovšek, M., 2003. Walks confined in a quadrant are not always d-finite. Theoret. Comput. Sci. 307 (2), 257–276, random Generation of Combinatorial Objects and Bijective Combinatorics.
URL http://www.sciencedirect.com/science/article/pii/S0304397503002196

Brachat, J., Comon, P., Mourrain, B., Tsigaridas, E. P. P., 2010. Symmetric tensor decomposition. Linear Algebra Appl. 433 (11-12), 1851–1872.

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 (5), 315–335.
URL http://dx.doi.org/10.1007/s00200-006-0015-8

Cox, D., Little, J., O'Shea, D., 2015. Ideals, Varieties, and Algorithms, 4th Edition. Undergraduate Texts in Mathematics. Springer, New York, an introduction to computational algebraic geometry and commutative algebra.

Cox, D. A., Little, J., O'Shea, D., 2005. Using Algebraic Geometry, 2nd Edition. Vol. 185 of Graduate Texts in Mathematics. Springer, New York.

Daleo, N. S., Hauenstein, J. D., 2016. Numerically testing generically reduced projective schemes for the arithmetic gorenstein property. In: Kotsireas, I. S., Rump, S. M., Yap, C. K. (Eds.), Mathematical Aspects of Computer and Information Sciences: 6th International Conference, MACIS 2015, Berlin, Germany, November 11-13, 2015, Revised Selected Papers. Springer International Publishing, Cham, pp. 137–142.
URL http://dx.doi.org/10.1007/978-3-319-32859-1_11

Dornstetter, J., 1987. On the equivalence between Berlekamp's and Euclid's algorithms (corresp.). IEEE Transactions on Information Theory 33 (3), 428–431.

Elkadi, M., Mourrain, B., 2007. Introduction à la résolution des systèmes polynomiaux. Vol. 59 of Mathématiques et Applications. Springer.

Erdös, J., 1956. On the structure of ordered real vector spaces. Publ. Math. Debrecen 4, 334–343.

Faugère, J.-Ch., Gianni, P., Lazard, D., Mora, T., 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symbolic Comput. 16 (4), 329–344.

Faugère, J.-Ch., Mou, C., 2011. Fast Algorithm for Change of Ordering of Zero-dimensional Gröbner Bases with Sparse Multiplication Matrices. In: Proc. of the 36th ISSAC. ACM, pp. 115–122.

Faugère, J.-Ch., Mou, C., 2017. Sparse FGLM algorithms. Journal of Symbolic Computation 80 (3), 538 – 569.

Fitzpatrick, P., Norton, G., 1990. Finding a basis for the characteristic ideal of an n-dimensional linear recurring sequence. IEEE Trans. Inform. Theory 36 (6), 1480–1487.

Gorenstein, D., 1952. An arithmetic theory of adjoint plane curves. Trans. Amer. Math. Soc. 72, 414–436.

Guisse, V., Sep. 2017. Algèbre linéaire dédiée pour les algorithmes Scalar-FGLM et Berlekamp-Massey-Sakata. Master's thesis, Université Paris Diderot (Paris 7). URL `https://hal.inria.fr/hal-01516249`

Hocquenghem, A., 1959. Codes correcteurs d'erreurs. Chiffres 2, 147 – 156.

Jonckheere, E., Ma, C., 1989. A simple Hankel interpretation of the Berlekamp-Massey algorithm. Linear Algebra Appl. 125 (0), 65 – 76.
URL `http://www.sciencedirect.com/science/article/pii/0024379589900323`

Kaltofen, E., Pan, V., 1991. Processor efficient parallel solution of linear systems over an abstract field. In: SPAA '91. ACM Press, New York, N.Y., pp. 180–191.

Kaltofen, E., Yuhasz, G., 2013a. A fraction free Matrix Berlekamp/Massey algorithm. Linear Algebra Appl. 439 (9), 2515–2526.

Kaltofen, E., Yuhasz, G., 2013b. On the Matrix Berlekamp-Massey Algorithm. ACM Trans. Algorithms 9 (4), 33:1–33:24.
URL `http://doi.acm.org/10.1145/2500122`

Levinson, N., 1947. The Wiener RMS (Root-Mean-Square) error criterion in the filter design and prediction. J. Math. Phys. 25, 261–278.

Macaulay, F. S., 1934. Modern algebra and polynomial ideals. Mathematical Proceedings of the Cambridge Philosophical Society 30, 27–46.
URL `http://journals.cambridge.org/article_S0305004100012354`

Massey, J. L., 1969. Shift-register synthesis and BCH decoding. IEEE Trans. Inform. Theory IT-15, 122–127.

Mora, T., 2009. Gröbner technology. In: Sala, M., Sakata, S., Mora, T., Traverso, C., Perret, L. (Eds.), Gröbner Bases, Coding, and Cryptography. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 11–25.
URL http://dx.doi.org/10.1007/978-3-540-93806-4_2

Robbiano, L., 1986. On the theory of graded structures. Journal of Symbolic Computation 2 (2), 139 – 170.
URL http://www.sciencedirect.com/science/article/pii/S0747717186800190

Sakata, S., 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. J. Symbolic Comput. 5 (3), 321–337.
URL http://www.sciencedirect.com/science/article/pii/S0747717188800336

Sakata, S., 1990. Extension of the Berlekamp-Massey algorithm to N Dimensions. Inform. and Comput. 84 (2), 207–239.
URL http://dx.doi.org/10.1016/0890-5401(90)90039-K

Sakata, S., 1991. Decoding binary 2-D cyclic codes by the 2-D Berlekamp-Massey algorithm. IEEE Trans. Inform. Theory 37 (4), 1200–1203.
URL http://dx.doi.org/10.1109/18.86974

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.
URL http://dx.doi.org/10.1007/978-3-540-93806-4_9

Wiener, N., 1964. Extrapolation, Interpolation, and Smoothing of Stationary Time Series. The MIT Press.