Quasi-Linear Guessing of Minimal Lexicographic Gröbner Bases of Ideals of C-Relations of Random Bi-Indexed Sequences

Jérémy Berthomieu, Romain Lebreton, Kevin Tran

Quasi-Linear Guessing of Minimal Lexicographic Gröbner Bases of Ideals of C-Relations of Random Bi-Indexed Sequences

Jérémy Berthomieu
Sorbonne Université, CNRS, LIP6
Paris, France
jeremy.berthomieu@lip6.fr

Romain Lebreton
Université de Montpellier, CNRS, LIRMM
Montpellier, France
romain.lebreton@lirmm.fr

Kevin Tran
Sorbonne Université, CNRS, LIP6
Paris, France
kevin.tran@sorbonne-universite.fr

ABSTRACT

Computing recurrence relations for sequences is a central problem in computer algebra, with applications in error-correcting codes, Gröbner basis computation, and sparse interpolation. While uni-indexed C-recursive sequences benefit from quasi-linear algorithms leveraging the half-gcd method, the extension to multi-indexed sequences remains computationally challenging. Existing methods for bi-indexed sequences achieve quadratic complexity at best, limiting their practical use.

This paper presents a quasi-linear algorithm for computing lexicographic Gröbner bases of the ideal of C-relations associated to bi-indexed sequences. Our approach extends the half-gcd algorithm in $\mathbb{K}^{\mathbb{N}}[y]$ by integrating a pseudo-Euclidean division. This approach shows how to leverage the bi-Hankel structure of the matrix, significantly improving the efficiency of computing minimal C-relations closing the complexity gap between the uni- and bi-indexed cases. Our algorithm is restricted to bi-indexed sequences whose associated bi-Hankel matrix has generic row rank profile.

KEYWORDS

multi-indexed sequences, linear relation guessing, Hankel matrices, Gröbner bases, half-gcd algorithm, quasi-linear algorithm

1 INTRODUCTION

Context. Guessing the minimal linear recurrence relation with constant coefficients (C-relation) of order d of a sequence $(u_i)_{i\in\mathbb{N}}$ is a fundamental problem in computer algebra and error correcting codes. It is for instance one of the latter steps of the Wiedemann algorithm [23] for computing the minimal polynomial of a matrix or solving a sparse linear system. The multi-indexed analogue, that is with a sequence $(u_{i_1,\dots,i_n})_{(i_1,\dots,i_n)\in\mathbb{N}^n}$ is at the root of n-dimensional cyclic codes and also the Sparse-FGLM variant [10] of the FGLM algorithm [9] for Gröbner bases change of order.

Given the $D+1$ first terms $u_0,\dots,u_D$ of a uni-indexed sequence, the problem of computing the minimal C-relation can be modeled through a kernel computation of a *Hankel* matrix. It computes the correct relation as long as $D \geq 2d$. This Hankel structure leads to non-naive algorithms with complexity much better than $O(D^\omega)$, where $2 \leq \omega < 3$ is the matrix multiplication exponent, relying on the extended Euclidean algorithm called on polynomials x^{D+1} and $\sum_{i=0}^{D} u_i x^{D-i}$. The first instance of such a non-naive algorithm is due independently to Berlekamp [1] and Massey [14], both targeting an application to error correcting codes, and is now known as the Berlekamp–Massey algorithm. Thanks to quasi-linear algorithms for computing the extended Euclidean algorithm [7, 15], see also [22, Chap. 11], the complexity of computing such a minimal C-relation of order d is $\tilde{O}(D)$, as long as $D \geq 2d$.

Related work. The case of an n-indexed sequence, $n \geq 2$, $\boldsymbol{u} = (u_{i_1,\dots,i_n})_{(i_1,\dots,i_n)\in\mathbb{N}^n}$ is more involved. The set of relations of $\boldsymbol{u}$ forms an ideal, denoted $I(\boldsymbol{u})$, which is 0-dimensional whenever $\boldsymbol{u}$ is C-recursive. Guessing consists in computing a representation of this ideal, that is a $\prec$-Gröbner basis for a given monomial order $\prec$ in the context of this paper. Denoting $\mathcal{S}_{\boldsymbol{u}}$ the $\prec$-*staircase* of $I(\boldsymbol{u})$, *i.e.* the monomials that are not $\prec$-leading monomials of $I(\boldsymbol{u})$, and $\mathcal{G}_{\boldsymbol{u}}$ the $\prec$-reduced Gröbner basis of $I(\boldsymbol{u})$, the complexity of the problem must depend on the number of given terms of $\boldsymbol{u}$, and on $|\mathcal{G}_{\boldsymbol{u}}|$ and $|\mathcal{S}_{\boldsymbol{u}}|$, in order to encode the output in the monomial basis. The first algorithm to guess such a Gröbner basis is due to Sakata and extends the Berlekamp–Massey algorithm, leading the author to calling it the Berlekamp–Massey–Sakata algorithm [18–20]. More recent algorithms were proposed based on linear algebra, *i.e.* computing the kernel of a *multi-Hankel* matrix [2, 3] or using a Gram-Schmidt process [16]. Another approach is based on multivariate polynomial arithmetic, especially division of polynomials such as [4, 5], or specifically for the bivariate case [11] using an approach similar to the uni-indexed case as they work on the polynomial $\sum_{j=0}^{D_y} (u_{i,j})_{i\in\mathbb{N}} y^{D_y-j} \in \mathbb{K}^{\mathbb{N}}[y]$. Finally, let us mention a bivariate Padé approximation method [17].

The complexity analysis of all these algorithms is not an easy task. Restricting ourselves to the case where the number of known terms of $\boldsymbol{u}$ is minimal to ensure the correctness of the output allows us to express their complexities more easily. In the uni-indexed case, this would imply $D = \Theta(d)$, so that the complexity is $\tilde{O}(d)$.

In [20], the complexity of the Berlekamp–Massey–Sakata algorithm is $O(|\mathcal{S}_{\boldsymbol{u}}|^2 \cdot |\mathcal{G}_{\boldsymbol{u}}|)$, though the output need not be a reduced Gröbner basis. The complexity of the algorithm of [2, 3] is $O((|\mathcal{S}_{\boldsymbol{u}}|^\omega + |\mathcal{S}_{\boldsymbol{u}}|^2 \cdot |\mathcal{G}_{\boldsymbol{u}}|)$ and the output is reduced. The algorithm of [16] has complexity $O(|\mathcal{S}_{\boldsymbol{u}}|^2 \cdot (|\mathcal{S}_{\boldsymbol{u}}| + |\mathcal{B}_{\boldsymbol{u}}|))$, where $\mathcal{B}_{\boldsymbol{u}}$ is a *border basis*, and thus has larger size than $\mathcal{G}_{\boldsymbol{u}}$, while the algorithm [4, 5] has a similar complexity $O(|\mathcal{S}_{\boldsymbol{u}}|^2 \cdot (|\mathcal{S}_{\boldsymbol{u}} + |\mathcal{G}_{\boldsymbol{u}}|))$. Furthermore, they all need the sequence terms $u_{i_1,\dots,i_n}$ where $x_1^{i_1}\cdots x_n^{i_n}$ is in the Minkowski sum of $\mathcal{S}_{\boldsymbol{u}}$ with itself, denoted $2\mathcal{S}_{\boldsymbol{u}}$. If we simplify further to the bi-indexed case and we denote d_x (resp. d_y) the maximal degree in x (resp. y) of $\mathcal{G}_{\boldsymbol{u}}$, these complexity upper bounds become at least $O(\max(d_x, d_y)^2 |\mathcal{G}_{\boldsymbol{u}}|)$ using the fact that $|\mathcal{S}_{\boldsymbol{u}}| \geq d_x + d_y - 1$. Now, on the one hand, all the monomials $x^i y^j$ for $0 \leq i < d_x$ and $0 \leq j < d_y$ are in $2\mathcal{S}_{\boldsymbol{u}}$ and, on the other hand, all monomials in $2\mathcal{S}_{\boldsymbol{u}}$ have degree in x (resp. y) at most $2d_x - 2$ (resp. $2d_y - 2$). Hence, all these algorithms need exactly $\Theta(d_x d_y)$ terms. Finally, using also $\Theta(d_x d_y)$ terms of $\boldsymbol{u}$, the algorithm of [11] computes a Gröbner basis of $I(\boldsymbol{u})$ in $\tilde{O}(d_x^{\omega+1} d_y)$ operations, while [17] requires $\tilde{O}(\min(d_x, d_y)^\omega d_x d_y)$ operations.

Contribution. The main contribution of this paper is Guessing-Bivar, an algorithm that takes as an input the $(D_x+1)(D_y+1)$

sequence terms $u_{i,j}$ for $0 \le i \le D_x$ and $0 \le j \le D_y$ and returns a minimal lexicographic Gröbner basis of $I(\boldsymbol{u})$, with support in $\{x^i y^j \mid 0 \le i \le d_x, 0 \le j \le d_y\}$ for $\boldsymbol{u} = (u_{i,j})_{(i,j)\in\mathbb{N}^2}$ using $\tilde{O}(D_x D_y + d_x d_y |\mathcal{G}_{\boldsymbol{u}}|)$ operations. This algorithm works under the assumption that the multi-Hankel matrix $(u_{i+k,j+\ell})_{x^i y^j, x^k y^\ell \in \mathcal{S}_{\boldsymbol{u}}}$ has a LU decomposition without pivoting. This condition is experimentally always satisfied whenever the terms $(u_{i,j})_{x^i y^j \in \mathcal{S}_{\boldsymbol{u}}}$ are picked at random. As a consequence, this closes the complexity gap between the uni-indexed case and the bi-indexed one.

Organization of the paper. In §2, we recall the polynomial representation of C-relations, and also how to relate their guessing to linear algebra and univariate gcd computation. In §3, we extend this viewpoint to bi-indexed sequences under the aforementioned assumption on the associated multi-Hankel matrix. In §4, we design a half-gcd-like algorithm on bivariate polynomials and how it can be used as a subroutine of GuessingBivar for guessing. Finally, our benchmarks in §5 confirm the efficiency of our algorithm.

2 PRELIMINARIES

In this section, we recall all basic definitions and results on matrices, C-recursive multi-indexed sequences, polynomials and Gröbner bases. We consider $\mathbb{N}$ as the set of all natural numbers including 0, also consider that $\deg(0) = -\infty$. We note $\boldsymbol{x} = (x_1, \ldots, x_n)$ the variables used for polynomials and $\boldsymbol{i} = (i_1, \ldots, i_n) \in \mathbb{N}^n$. We note $\boldsymbol{x}^{\boldsymbol{i}} = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. If there is no ambiguity on the number of variables or indices we denote $\mathbb{K}[\boldsymbol{x}] = \mathbb{K}[x_1, \ldots, x_n]$ and $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$.

2.1 Uni-indexed sequences

For uni-indexed sequences, C-recursive sequences are the ones satisfying linear recurrences with constant coefficients.

Definition 2.1.1. *A sequence $(u_i)_{i\in\mathbb{N}}$ is* C-recursive *if there exist $g_0, \ldots, g_{d-1} \in \mathbb{K}$ such that for $i \in \mathbb{N}$, $u_{i+d} = g_{d-1}u_{i+d-1} + \ldots + g_0 u_i$.*

Such a combination is called *C-relation* and can be represented as a polynomial $g = x^d - \sum_{i=0}^{d-1} g_i x^i \in \mathbb{K}[x]$. Computing a C-relation can be reduced to a linear system solving problem.

The *Hankel matrix of size d* associated to the sequence $\boldsymbol{u} = (u_i)_{i\in\mathbb{N}}$ is $\mathcal{H} = (u_{i+j})_{0\le i,j<d} \in \mathbb{K}^{d\times d}$. Moreover, one can compute the C-relation $g = x^d - \sum_{i=0}^{d-1} g_i x^i$ by solving the linear system $\begin{bmatrix} g_0 & g_1 & \ldots & g_{d-1}\end{bmatrix} \mathcal{H} = \begin{bmatrix} u_d & \ldots & u_{2d-1}\end{bmatrix}$.

For a polynomial $g = x^d - \sum_{i=0}^{d-1} g_i x^i \in \mathbb{K}[x]$, we define $\hat{g} = x^d g(1/x) \in \mathbb{K}[x]$ as the mirror of g. Another approach is done using generating series $S = \sum_{i\in\mathbb{N}} u_i x^i \in \mathbb{K}[[x]]$. The generating series of a C-recursive sequence admits a finite representation. Indeed, for such series S there exists $p, q \in \mathbb{K}[x]$ such that $qS = p$ with $\deg(p) < d$ and $q = \hat{g}$. From the degree constraint on p and q, one can recover p and q from the relation $qS = p \bmod x^{D+1}$ with $D \ge 2d$. This modular equation can be rewritten as a Bézout's identity $qS + rx^{D+1} = p$ with $r \in \mathbb{K}[x]$ and computing $q = \hat{g}$ comes down to computing a Truncated Extended Euclidean algorithm. A fast computation of this relation can be done through a call to the half-gcd algorithm [12, 15, 21]. The half-gcd algorithm is based on a fast reduction algorithm.

Lemma 2.1.2. *Let $a, b \in \mathbb{K}[x]$ with $\deg(a) = D$ and $\deg(b) = d$ such that $D \ge d$. Computing $q, r \in \mathbb{K}[x]$ satisfying $a = qb + r$ with $\deg(r) < d$ can be done in $\tilde{O}(D)$ operations in $\mathbb{K}$.*

The transpose of this operation called the extension is computed in the same complexity by the Tellegen's principle [6]. This operation corresponds to the extension of C-recursive sequences $(u_i)_{i\in\mathbb{N}}$ by the C-relation $g = x^d - \sum_{i=0}^{d-1} g_i x^i$, for $S = \sum_{i=0}^{d-1} u_i x^i$, it computes $\tilde{S} = \sum_{i=0}^{D} u_i x^i$ using $u_{i+d} = g_{d-1}u_{i+d-1} + \ldots g_0 u_i$ for $i \ge 0$.

Recall that $\tilde{O}(\cdot)$ means that polylogarithmic factors are omitted.

Theorem 2.1.3. *Computing the C-relation $g \in \mathbb{K}[x]$ on $(u_i)_{i\in\mathbb{N}}$ of degree d, knowing the $D+1$ initial terms of $(u_i)_{i\in\mathbb{N}}$ with $D \ge 2d$, can be done in $\tilde{O}(D)$ operations in $\mathbb{K}$.*

The half-gcd algorithm can also be derived to a Hankel system solving of size $d-1$ (see [7]) and can be done in $\tilde{O}(d)$ operations.

2.2 Multivariate polynomial rings

For multi-indexed sequences, we use multivariate polynomials to represent the C-relations. For a polynomial $f \in \mathbb{K}[\boldsymbol{x}]$ and $\boldsymbol{\alpha} \in \mathbb{N}^n$, we note $f_{\boldsymbol{\alpha}}$ the coefficient of f associated to the monomial $\boldsymbol{x}^{\boldsymbol{\alpha}}$, the support of f is the monomial set $\operatorname{supp}(f) = \{\boldsymbol{x}^{\boldsymbol{\alpha}} \mid f_{\boldsymbol{\alpha}} \ne 0\}$.

We define the box monomial set of parameter $\boldsymbol{d} \in \mathbb{N}^n$ as $\boldsymbol{d}$-box $:= \{\boldsymbol{x}^{\boldsymbol{\alpha}} \mid 0 \le \alpha_j \le d_j \text{ for all } 1 \le j \le n\}$. Also, we denote by $\mathbb{K}[\boldsymbol{x}]_{\le \boldsymbol{d}}$ the set of polynomials with support in $\boldsymbol{d}$-box.

For polynomials $f, g \in \mathbb{K}[\boldsymbol{x}]_{\le \boldsymbol{d}}$, the addition of $f + g$ can be computed using $O(\prod_{i=1}^n d_i)$ operations in $\mathbb{K}$ and the multiplication fg can be computed using $\tilde{O}(\prod_{i=1}^n (2d_i))$ operations.

For multivariate polynomials, we have to define a total order on the monomial set. In our study, we are only interested on the lexicographic order, we refer to [8] for more general consideration. We note $\prec$ the lexicographic order on $\mathbb{K}[x_1, \ldots, x_n]$ with $x_1 \prec \ldots \prec x_n$ and such that $\boldsymbol{x}^{\boldsymbol{\alpha}} \prec \boldsymbol{x}^{\boldsymbol{\beta}}$ if there exists $1 \le k \le n$ such that for any $j < k, \alpha_j = \beta_j$ and $\alpha_k < \beta_k$. For a nonzero polynomial $f \in \mathbb{K}[\boldsymbol{x}]$, the leading monomial of f w.r.t. $\prec$ is noted $\operatorname{lm}(f)$ and corresponds to the maximum monomial of f ordered by $\prec$. The leading coefficient of f w.r.t. $\prec$ is noted $\operatorname{lc}(f) \in \mathbb{K}$ is the coefficient associated to $\operatorname{lm}(f)$. The leading term of f w.r.t. $\prec$ is noted $\operatorname{lt}(f) = \operatorname{lc}(f)\operatorname{lm}(f)$.

An ideal of $\mathbb{K}[\boldsymbol{x}]$ can be generated by a finite set of polynomials. Gröbner bases are particular sets of generators with interesting computational properties. For an ideal $I \subseteq \mathbb{K}[\boldsymbol{x}]$, a Gröbner basis $\mathcal{G}$ of I for the lexicographic order is a finite generating set of I such that $\langle \operatorname{lm}(\mathcal{G})\rangle = \langle \operatorname{lm}(I)\rangle$, *i.e.* it spans $\operatorname{lm}(I)$ as a monomial set. A minimal Gröbner basis $\mathcal{G}$ is a Gröbner basis such that no $\operatorname{lm}(g) \in \operatorname{lm}(\mathcal{G})$ is divisible by an element in $\operatorname{lm}(\mathcal{G}\backslash\{g\})$. The (unique) reduced Gröbner basis $\mathcal{G}$ is a minimal Gröbner basis such that for all $g \in \mathcal{G}$, the monomials $m \in \operatorname{supp}(g)$ are not divisible by any $\operatorname{lm}(\mathcal{G}\backslash\{g\})$.

The staircase $\mathcal{S}$ associated to an ideal I is $\mathcal{S} := \{\boldsymbol{x}^{\boldsymbol{\alpha}} \mid \boldsymbol{x}^{\boldsymbol{\alpha}} \notin \operatorname{lm}(I)\}$. It forms a $\mathbb{K}$-vector space basis of the quotient ring $\mathbb{K}[\boldsymbol{x}]/I$. The polynomial division with remainder by a Gröbner basis (defined in [8, Chapter 2.7]) gives a unique polynomial r with support in the staircase $\mathcal{S}$. For $f \in \mathbb{K}[\boldsymbol{x}]$, we denote by $r = f \operatorname{rem}(\mathcal{G}) \in \mathbb{K}[\boldsymbol{x}]$ with $\operatorname{supp}(r) \subset \mathcal{S}$ the unique remainder of f by a Gröbner basis $\mathcal{G}$. The polynomial division with remainder of $f \in \mathbb{K}[\boldsymbol{x}]$ by a Gröbner basis $\mathcal{G}$, as defined in [8, Chapter 2.7], yields a unique polynomial denoted $r = f \operatorname{rem}(\mathcal{G}) \in \mathbb{K}[\boldsymbol{x}]$ with support in the staircase $\mathcal{S}$.

We recall the notion of colon ideal by one polynomial. A more general description can be found in [8, Chapter 4.4]. Let I be an ideal of $\mathbb{K}[\boldsymbol{x}]$ and let $f \in \mathbb{K}[\boldsymbol{x}]$, the colon ideal of I by f is $I : \langle f\rangle = \{g \in \mathbb{K}[\boldsymbol{x}] \mid gf \in I\}$.

2.3 Multi-indexed C-recursive sequences

For $n > 0$, the set $\mathbb{K}^{\mathbb{N}^n}$ corresponds to the set of n-indexed sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$ with terms in $\mathbb{K}$. We denote the zero sequence by $\boldsymbol{0} = (0)_{\boldsymbol{i}\in\mathbb{N}^n}$. For C-recursive sequences, we allow two types of operations: index shifts and scalar multiplications on sequences. These operations can be described by the action $\star$ of $\mathbb{K}[\boldsymbol{x}]$ in $\mathbb{K}^{\mathbb{N}^n}$ such that $x_j^d \star \boldsymbol{u} = (u_{i_1,\ldots,i_j+d,\ldots,i_n})_{(i_1,\ldots,i_n)\in\mathbb{N}^n}$ for $1 \le j \le n$ and $d \in \mathbb{N}$, and extended by linearity to $\mathbb{K}[\boldsymbol{x}]$.

For a sequence $\boldsymbol{u} = (u_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathbb{N}^n}$, a C-relation g on $\boldsymbol{u}$ is a polynomial $g \in \mathbb{K}[\boldsymbol{x}]$ that satisfies $g \star \boldsymbol{u} = \boldsymbol{0}$. We note by $I(\boldsymbol{u}) = \{g \in \mathbb{K}[\boldsymbol{x}] \mid g \star \boldsymbol{u} = \boldsymbol{0}\}$ the ideal of relations of $\boldsymbol{u}$. A sequence $\boldsymbol{u}$ is C-recursive if the ideal of relations $I(\boldsymbol{u})$ is 0-dimensional *i.e.* $\dim_{\mathbb{K}}(\mathbb{K}[\boldsymbol{x}]/I(\boldsymbol{u})) < \infty$.

For a sequence $\boldsymbol{u}$, we denote by $\mathcal{G}_{\boldsymbol{u}}$ the reduced Gröbner basis w.r.t. $\prec$ of the ideal of relations $I(\boldsymbol{u})$, and $\mathcal{S}_{\boldsymbol{u}}$ the staircase w.r.t. $\prec$ of $I(\boldsymbol{u})$ also we note $\mathcal{S}_{\boldsymbol{u},\prec m} = \{\boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathcal{S}_{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{\alpha}} \prec m\}$. We note the exponents set of $\mathcal{S}_{\boldsymbol{u}}$ by $\mathcal{E}_{\boldsymbol{u}} = \{\boldsymbol{\alpha} \in \mathbb{N}^n \mid \boldsymbol{x}^{\boldsymbol{\alpha}} \in \mathcal{S}_{\boldsymbol{u}}\}$ and $\mathcal{E}_{\boldsymbol{u},\prec e} = \{\boldsymbol{\alpha} \in \mathcal{E}_{\boldsymbol{u}} \mid \boldsymbol{x}^{\boldsymbol{\alpha}} \prec \boldsymbol{x}^e\}$.

For $\boldsymbol{u}$ a C-recursive sequence and $\mathcal{G}$ a Gröbner basis of $I(\boldsymbol{u})$, any term of $\boldsymbol{u}$ can be computed from the relations in $\mathcal{G}$ and the initial terms in $\mathcal{S}_{\boldsymbol{u}}$ [19]. A C-recursive sequence is uniquely determined by the terms associated to the exponents from the staircase $\mathcal{S}_{\boldsymbol{u}}$, as the other terms are linear combinations of the ones in the staircase.

Lemma 2.3.1 ([20, §2]). *Fix $I(\boldsymbol{u})$ and $\mathcal{G}$ a Gröbner basis of $I(\boldsymbol{u})$ w.r.t. the order $\prec$. Then $I(\boldsymbol{u}) \subset I(\boldsymbol{v})$ iff for all $\boldsymbol{\beta} \in \operatorname{lm}(I(\boldsymbol{u}))$, we have $v_{\boldsymbol{\beta}} = \sum_{\boldsymbol{\alpha}\in\mathcal{E}_{\boldsymbol{u}}} c_{\boldsymbol{\alpha}} v_{\boldsymbol{\alpha}}$ with $\boldsymbol{x}^{\boldsymbol{\beta}} \operatorname{rem}(\mathcal{G}) = \sum_{\boldsymbol{\alpha}\in\mathcal{E}_{\boldsymbol{u}}} c_{\boldsymbol{\alpha}} \boldsymbol{x}^{\boldsymbol{\alpha}}$.*

For $n > 0$ and $\boldsymbol{u} \in \mathbb{K}^{\mathbb{N}^n}$ C-recursive, we define the $\mathbb{K}$-linear subspace $\mathrm{L}_{\boldsymbol{u}} := \{h \star \boldsymbol{u} \mid h \in \mathbb{K}[\boldsymbol{x}]\} \subset \mathbb{K}^{\mathbb{N}^n}$ and consider the linear application $\phi(h) = h \star \boldsymbol{u}$ from $\mathbb{K}[\boldsymbol{x}]$ to $\mathrm{L}_{\boldsymbol{u}}$. By construction, ϕ is surjective. As $\ker\phi = I(\boldsymbol{u})$, we can define the isomorphism $\bar{\phi} : \mathbb{K}[\boldsymbol{x}]/I(\boldsymbol{u}) \to \mathrm{L}_{\boldsymbol{u}}$ from ϕ. We define $\mathcal{F} = \{e_{\boldsymbol{i}}\}_{\boldsymbol{i}\in\mathcal{E}_{\boldsymbol{u}}} \subset \mathbb{K}^{\mathbb{N}^n}$ with $e_{\boldsymbol{i}}$ defined for $\boldsymbol{j} \in \mathcal{E}_{\boldsymbol{u}}$ such that $(e_{\boldsymbol{i}})_{\boldsymbol{j}} = 0$ if $\boldsymbol{j} \neq \boldsymbol{i}$ and $(e_{\boldsymbol{i}})_{\boldsymbol{i}} = 1$ and outside $\mathcal{E}_{\boldsymbol{u}}$ we extend the terms of $e_{\boldsymbol{i}}$ in $\mathcal{E}_{\boldsymbol{u}}$ by the relations in $I(\boldsymbol{u})$.

Lemma 2.3.2. *If $I(\boldsymbol{u}) \subset I(\boldsymbol{v})$ then $v \in \operatorname{span}_{\mathbb{K}}(\mathcal{F})$.*

Proof. Let $\boldsymbol{w} = \boldsymbol{v} - \sum_{\boldsymbol{i}\in\mathcal{E}_{\boldsymbol{u}}} v_{\boldsymbol{i}} e_{\boldsymbol{i}}$. For $\boldsymbol{j} \in \mathcal{E}_{\boldsymbol{u}}$, we have by construction $w_{\boldsymbol{j}} = 0$. From Lm. 2.3.1, we have $I(\boldsymbol{u}) \subset I(e_{\boldsymbol{i}})$ for any $\boldsymbol{i} \in \mathcal{E}_{\boldsymbol{u}}$. Since $f \in I(\boldsymbol{u})$ is in $I(\boldsymbol{v})$ and all $I(e_{\boldsymbol{i}})$, we deduce that $I(\boldsymbol{u}) \subset I(\boldsymbol{w})$. Hence, $\boldsymbol{w} = \boldsymbol{0}$ and $\boldsymbol{v} = \sum_{\boldsymbol{i}\in\mathcal{E}_{\boldsymbol{u}}} v_{\boldsymbol{i}} e_{\boldsymbol{i}}$. ◻

Lemma 2.3.3. *The family $\mathcal{F}$ is a basis of $\mathrm{L}_{\boldsymbol{u}}$.*

Proof. By construction, $\mathcal{F}$ is linearly independent. Let $h \star \boldsymbol{u} \in \mathrm{L}_{\boldsymbol{u}}$, since for $f \in I(\boldsymbol{u})$, $(fh) \star \boldsymbol{u} = f \star (h \star \boldsymbol{u}) = \boldsymbol{0}$, we have $I(\boldsymbol{u}) \subset I(h \star \boldsymbol{u})$. So we apply Lm. 2.3.2 and show that $\mathrm{L}_{\boldsymbol{u}} \subset \operatorname{span}_{\mathbb{K}}(\mathcal{F})$. Since $\dim_{\mathbb{K}}(\mathrm{L}_{\boldsymbol{u}}) = \dim_{\mathbb{K}}(\mathbb{K}[\boldsymbol{x}]/I(\boldsymbol{u})) = |\mathcal{S}_{\boldsymbol{u}}|$, we conclude that $\mathcal{F}$ is a basis of $\mathrm{L}_{\boldsymbol{u}}$. ◻

We note $\mathcal{H}_{\mathcal{S}_{\boldsymbol{u}}}$ the matrix associated to $\bar{\phi}$, with the basis $\mathcal{S}_{\boldsymbol{u}}$ for $\mathbb{K}[\boldsymbol{x}]/I(\boldsymbol{u})$ and $\mathcal{F}$ for $\mathrm{L}_{\boldsymbol{u}}$ both ordered w.r.t. $\prec$. The application $\overline{\phi}$ is an isomorphism so the matrix $\mathcal{H}_{\mathcal{S}_{\boldsymbol{u}}}$ is invertible.

Theorem 2.3.4. *Let $\boldsymbol{u}$ and $\boldsymbol{v}$ be two C-recursive sequences. The following statements are equivalent:*

(a) $\exists! h \in \mathbb{K}[\boldsymbol{x}]$ with support in $\mathcal{S}_{\boldsymbol{u}}$ such that $\boldsymbol{v} = h \star \boldsymbol{u}$;
(b) $\exists h \in \mathbb{K}[\boldsymbol{x}]$ such that $I(\boldsymbol{v}) = I(\boldsymbol{u}) : \langle h \rangle$;
(c) $I(\boldsymbol{u}) \subset I(\boldsymbol{v})$.

Proof. For $(a) \Rightarrow (b)$, we have $g \in I(\boldsymbol{v}) \Leftrightarrow 0 = g \star \boldsymbol{v} = (gh) \star \boldsymbol{u} \Leftrightarrow g \in I(\boldsymbol{u}) : \langle h \rangle$. For $(b) \Rightarrow (c)$, it is direct by definition. For $(c) \Rightarrow (a)$, since $I(\boldsymbol{u}) \subset I(\boldsymbol{v})$ we can write $\boldsymbol{v} = \sum_{\boldsymbol{i}\in\mathcal{E}_{\boldsymbol{u}}} v_{\boldsymbol{i}} e_{\boldsymbol{i}}$ so $\boldsymbol{v} \in \mathrm{L}_{\boldsymbol{u}}$ by Lms. 2.3.2 and 2.3.3. For uniqueness, let $h' \in \mathbb{K}[\boldsymbol{x}]$ s.t. $\boldsymbol{v} = h' \star \boldsymbol{u}$ and $\operatorname{supp}(h') \subset \mathcal{S}_{\boldsymbol{u}}$. We get $(h-h') \star \boldsymbol{u} = \boldsymbol{0}$ so $h - h' \in I(\boldsymbol{u})$ and $h - h' \operatorname{rem}(\mathcal{G}_{\boldsymbol{u}}) = 0$. Since $\operatorname{supp}(h), \operatorname{supp}(h') \subset \mathcal{S}_{\boldsymbol{u}}$ by the linearity of the reduction we obtain $h = h \operatorname{rem}(\mathcal{G}_{\boldsymbol{u}}) = h' \operatorname{rem}(\mathcal{G}_{\boldsymbol{u}}) = h'$. ◻

3 BI-INDEXED SEQUENCES

In this section, we restrict ourselves to C-recursive bi-indexed sequences $\boldsymbol{v} = (v_{i,j})_{i,j\in\mathbb{N}}$. We denote by $d_x, d_y \in \mathbb{N}$ the exponents satisfying $x^{d_x}, y^{d_y} \in \operatorname{lm}(\mathcal{G}_{\boldsymbol{v}})$.

3.1 Hankel matrix and LU decomposition

For a bi-indexed sequence $\boldsymbol{v}$ and $j \in \mathbb{N}$, we note the sub-sequences $\boldsymbol{v}_{*,j} = (v_{i,j})_{i\in\mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$. Sub-sequences does not necessarily contain enough information to recover the ideal $I(\boldsymbol{v}) \cap \mathbb{K}[x]$.

Example 3.1.1. *Let $\boldsymbol{v} = ((-1)^{ij})_{i,j\in\mathbb{N}}$, then $I(\boldsymbol{v}_{*,j}) = \langle x - (-1)^j \rangle$, but $I(\boldsymbol{v}) \cap \mathbb{K}[x] = \langle x^2 - 1 \rangle$.*

To overcome the problem posed by Ex. 3.1.1, we make the following assumption on the sequence $\boldsymbol{v}$.

Assumption A. *The matrix $\mathcal{H}_{\mathcal{S}_{\boldsymbol{v}}}$ defined in §2.3 for the bi-indexed sequence $\boldsymbol{v}$ admits a LU decomposition.*

For a matrix $\mathcal{M} \in \mathbb{K}^{n\times n}$, the *principal $r\times r$ submatrix* $\mathcal{M}_r \in \mathbb{K}^{r\times r}$ is the matrix built from the first r rows and columns of $\mathcal{M}$. Recall that an invertible matrix $\mathcal{M} \in \mathbb{K}^{n\times n}$ admits a LU decomposition iff for $1 \le r \le n$, the submatrix $\mathcal{M}_r$ is invertible.

Consider $\mathcal{H}_{\mathcal{S}_{\boldsymbol{v}}} = LU$ with L a lower triangular matrix with ones on the diagonal and U an upper triangular matrix. We note the rows of $L^{-1} = [\ell_m]_{m\in\mathcal{S}_{\boldsymbol{v}}}$ with $\ell_m \in \mathbb{K}^{1\times|\mathcal{S}_{\boldsymbol{v}}|}$. We note $p_m \in \mathbb{K}[x,y]$ the polynomial representing ℓ_m in the basis $\mathcal{S}_{\boldsymbol{v}}$. The matrix L^{-1} is lower triangular with ones on its diagonal, so $\operatorname{lt}(p_m) = m$ for all $m \in \mathcal{S}_{\boldsymbol{v}}$. For $y^j \in \mathcal{S}_{\boldsymbol{v}}$, we denote by $\boldsymbol{v}^{(j)}$ the sequence $p_{y^j} \star \boldsymbol{v}$.

Lemma 3.1.2. *For $0 \le j < d_y$, $\boldsymbol{v}^{(j)}$ satisfies $\boldsymbol{v}^{(j)}_{*,k} = \boldsymbol{0}$, for $0 \le k < j$.*

Proof. Let $i \in \mathbb{N}$, $k < j$ and consider the term $\boldsymbol{v}^{(j)}_{i,k}$ of $\boldsymbol{v}^{(j)}$. By construction, the row of U indexed by y^j contains terms of $\boldsymbol{v}^{(j)}$ and in particular $(\boldsymbol{v}^{(j)})_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},\prec(0,j)}$. Now, since $\boldsymbol{v}^{(j)}_{i,k} = (x^i y^k \star \boldsymbol{v}^{(j)})_{0,0} = ((x^i y^k \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})) \star \boldsymbol{v}^{(j)})_{0,0}$, we express $\boldsymbol{v}^{(j)}_{i,k}$ as a linear combination of $\boldsymbol{v}^{(j)}_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},\prec(0,j)}$. ◻

Lemma 3.1.3. *Let $j \in \mathbb{N}$ and $t \in \mathbb{K}[x,y]$ such that $(t \star \boldsymbol{v})_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},\prec(0,j)}$. If $\deg_y(t) < j$, then $t \in I(\boldsymbol{v})$. Otherwise, if $\operatorname{lt}(t) = y^j$ for $0 \le j < d_y$, then $p_{y^j} = t \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$.*

Proof. Let $\mathcal{H}_{\mathcal{S}_{\boldsymbol{v},\prec y^j}}$ be the principal submatrix of $\mathcal{H}_{\mathcal{S}_{\boldsymbol{v}}}$ with rows indexed by $\mathcal{S}_{\boldsymbol{v},\prec y^j}$ and columns by $(e_{\boldsymbol{i}})_{\boldsymbol{i}\in\mathcal{E}_{\boldsymbol{v},\prec(0,j)}}$. If $\deg_y(t) < j$, we can represent the polynomial $\tilde{t} := t \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$ by a vector ℓ in the basis $\mathcal{S}_{\boldsymbol{v},\prec y^j}$. Since $(\tilde{t} \star \boldsymbol{v})_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},\prec(0,j)}$, ℓ satisfies $\ell\mathcal{H}_{\mathcal{S}_{\boldsymbol{v},\prec y^j}} = 0$. As $\boldsymbol{v}$ satisfies Asm. A, $\mathcal{H}_{\mathcal{S}_{\boldsymbol{v},\prec y^j}}$ is invertible so $\ell = 0$, and $t \in I(\boldsymbol{v})$. Now, if $\operatorname{lt}(t) = y^j$ for $0 \le j < d_y$, then $\bar{t} := t - p_{y^j}$ satisfies the hypotheses and $\deg_y(\bar{t}) < j$, so $\bar{t} \in I(u)$ and $p_{y^j} = p_{y^j} \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}}) = t \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$. ◻

Theorem 3.1.4. *The family $\mathcal{P} = \{x^i p_{y^j} \mid x^i y^j \in \mathcal{S}_{\boldsymbol{v}}\}$ is a basis of $\mathbb{K}[x,y]/I(\boldsymbol{v})$ as $\mathbb{K}$-vector space.*

Proof. Let $x^i y^j \in \mathcal{S}_{\boldsymbol{v}}$ and consider $g = x^i p_{y^j} \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$. Since $\operatorname{lt}(x^i p_{y^j}) = x^i y^j \in \mathcal{S}_{\boldsymbol{v}}$, we have $g = x^i y^j + \sum_{(r,s)\in\mathcal{E}_{\boldsymbol{v},<(i,j)}} c_{r,s} x^r y^s$. Hence, the change-of-basis matrix between the bases $\mathcal{S}_{\boldsymbol{v}}$ and $\mathcal{P}$ is lower triangular with ones on its diagonal. □

We define the matrix $\mathcal{H}_{\mathcal{P}}$ representing the application $\overline{\phi}$ (see §2.3) with row basis $\mathcal{P}$ and column basis $\mathcal{F}$ defined in §2.3.

Lemma 3.1.5. *The matrix $\mathcal{H}_{\mathcal{P}}$ is block upper triangular and its diagonal blocks are invertible,* i.e.

$$\mathcal{H}_{\mathcal{P}} = \left[\begin{array}{c|c|c|c} \mathcal{H}_0 & \mathcal{H}_1 & \cdots & \mathcal{H}_{d_y-1} \\ \hline 0 & \mathcal{H}_1^{(1)} & \cdots & \mathcal{H}_{d_y-1}^{(1)} \\ \hline \vdots & \ddots & \ddots & \vdots \\ \hline 0 & 0 & \cdots & \mathcal{H}_{d_y-1}^{(d_y-1)} \end{array}\right]$$

Proof. For $0 \le j < d_y$, the jth row block starts with j zero matrices since $\boldsymbol{v}_{*,k}^{(j)} = \boldsymbol{0}$ for $0 \le k < j$ from Lm. 3.1.2 thus the matrix $\mathcal{H}_{\mathcal{P}}$ is block upper triangular matrix. The matrix $\mathcal{H}_{\mathcal{P}}$ is invertible since the linear application $\overline{\phi}$ is an isomorphism, hence the block diagonal matrices $\mathcal{H}_j^{(j)}$ are invertible. □

Theorem 3.1.6. *For $0 \le j < d_y$ and $d_j \in \mathbb{N}$, there exists $g \in I(\boldsymbol{v})$ s.t. $\operatorname{lm}(g) = x^{d_j} y^j$ iff there exists $f_j \in I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x]$ s.t. $\operatorname{lm}(f_j) = x^{d_j}$.*

Proof. Let $f_j \in I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x]$ with $\operatorname{lm}(f_j) = x^{d_j}$, by definition $\boldsymbol{0} = f_j \star \boldsymbol{v}^{(j)} = (f_j p_{y^j}) \star \boldsymbol{v}$ so $g = f_j p_{y^j} \in I(\boldsymbol{v})$ and $\operatorname{lm}(g) = x^{d_j} y^j$.

Let $g \in I(\boldsymbol{v})$ with $\operatorname{lm}(g) = x^{d_j} y^j \notin \mathcal{S}_{\boldsymbol{v}}$ by definition. Consider the sequence $(x^{d_j} p_{y^j}) \star \boldsymbol{v} = x^{d_j} \star \boldsymbol{v}^{(j)}$ from Lm. 3.1.2 we have for $k < j$, $(x^{d_j} \star \boldsymbol{v}^{(j)})_{*,k} = \boldsymbol{0}$. From Lm. 3.1.5, the matrix $\mathcal{H}_j^{(j)}$ is invertible, so there exists a polynomial $f \in \mathbb{K}[x]$ with $\operatorname{supp}(f y^j) \subset \mathcal{S}_{\boldsymbol{v}}$ satisfying $(f \star \boldsymbol{v}^{(j)})_{r,j} = (x^{d_j} \star \boldsymbol{v}^{(j)})_{r,j}$ for $(r,j) \in \mathcal{E}_{\boldsymbol{v}}$. By construction, the polynomial $t = (x^{d_j} - f) p_{y^j}$ is such that $(t \star \boldsymbol{v})_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},<(0,j+1)}$ and $\deg_y(t) = j$. So by Lm. 3.1.3, $t \in I(\boldsymbol{v})$ and $f_j = x^{d_j} - f \in I(\boldsymbol{v}^{(j)})$. Note that $x^{d_j} y^j \notin \mathcal{S}_{\boldsymbol{v}}$ and $\operatorname{supp}(f y^j) \subset \mathcal{S}_{\boldsymbol{v}}$, so $\operatorname{lm}((x^{d_j} - f) p_{y^j}) = \operatorname{lm}(x^{d_j} p_{y^j}) = x^{d_j} y^j$ and $\operatorname{lm}(f_j) = x^{d_j}$. □

Theorem 3.1.7. *For $0 \le j < d_y$, the sequence $\boldsymbol{v}_{*,j}^{(j)} \in \mathbb{K}^{\mathbb{N}}$ is such that $I(\boldsymbol{v}_{*,j}^{(j)}) = \bigcap_{k \ge j} I(\boldsymbol{v}_{*,k}^{(j)})$* i.e. $\boldsymbol{v}_{*,k}^{(j)} \in \mathrm{L}_{\boldsymbol{v}_{*,j}^{(j)}}$ *for $k \ge j$.*

Proof. The inclusion $\bigcap_{k \ge j} I(\boldsymbol{v}_{*,k}^{(j)}) \subset I(\boldsymbol{v}_{*,j}^{(j)})$ is direct. For the reverse inclusion, let $g \in I(\boldsymbol{v}_{*,j}^{(j)})$. The polynomial $t = g p_{y^j}$ is such that $(t \star \boldsymbol{v})_{r,s} = 0$ for $(r,s) \in \mathcal{E}_{\boldsymbol{v},<(0,j+1)}$, since it is zero for $s < j$ by Lm. 3.1.2, and for $s = j$ by definition of g. Since $\deg_y(t) \le j$ (as $\operatorname{lt}(p_{y^j}) = y^j$), we have $t \in I(\boldsymbol{v})$ using Lm. 3.1.3, and thus $g \star \boldsymbol{v}^{(j)} = t \star \boldsymbol{v} = \boldsymbol{0}$ so $g \in \bigcap_{k \ge j} I(\boldsymbol{v}_{*,k}^{(j)})$. □

From this property, we can find a relation between the sequences $(\boldsymbol{v}^{(j)})_{0 \le j \le d_y}$ with $\boldsymbol{v}^{(d_y)} = \boldsymbol{0}$.

Theorem 3.1.8. *For $0 \le j < d_y$, we have $\boldsymbol{v}_{*,j+1}^{(j+1)} \in \mathrm{L}_{\boldsymbol{v}_{*,j}^{(j)}}$ and there exists $(\overline{a}_j, \overline{b}_j) \in \mathbb{K}[x]^2$ with $\operatorname{supp}(\overline{a}_j) \subset \mathcal{S}_{\boldsymbol{v}_{*,j-1}^{(j-1)}}$ and $\operatorname{supp}(\overline{b}_j) \subset \mathcal{S}_{\boldsymbol{v}_{*,j}^{(j)}}$ satisfying $\boldsymbol{v}^{(j+1)} = \overline{a}_j \star \boldsymbol{v}^{(j-1)} + (y - \overline{b}_j) \star \boldsymbol{v}^{(j)}$ if $j \ne 0$ and $\boldsymbol{v}^{(1)} = (y - \overline{b}_0) \star \boldsymbol{v}$ if $j = 0$.*

Proof. We prove the statement by induction on j. For $j = 0$, we have by definition $\boldsymbol{v}^{(1)} = p_y \star \boldsymbol{v}$ with $\operatorname{lt}(p_y) = y$ and $\operatorname{supp}(p_y) \subset \mathcal{S}_{\boldsymbol{v}}$ so $p_y = y - \overline{b}_0$ with $\operatorname{supp}(\overline{b}_0) \subset \mathcal{S}_{\boldsymbol{v}_{*,0}}$. From this relation, we deduce that $\boldsymbol{v}_{*,1}^{(1)} = \boldsymbol{v}_{*,0} - \overline{b}_0 \star \boldsymbol{v}_{*,1}$ and by Thm. 3.1.7 it results that $\boldsymbol{v}_{*,1}^{(1)} \in \mathrm{L}_{\boldsymbol{v}_{*,0}}$. For $1 \le j < d_y - 1$, we suppose that the statement is true at step $j-1$ and prove that it holds at step j. Consider $(\overline{a}_j, \overline{b}_j) \in \mathbb{K}[x]^2$ with $\operatorname{supp}(\overline{a}_j) \subset \mathcal{S}_{\boldsymbol{v}_{*,j-1}^{(j-1)}}$ and $\operatorname{supp}(\overline{b}_j) \subset \mathcal{S}_{\boldsymbol{v}_{*,j}^{(j)}}$ satisfying $\overline{a}_j \star \boldsymbol{v}_{*,j-1}^{(j-1)} = -\boldsymbol{v}_{*,j}^{(j)}$ and $\overline{a}_j \star \boldsymbol{v}_{*,j}^{(j-1)} + \boldsymbol{v}_{*,j+1}^{(j)} = \overline{b}_j \star \boldsymbol{v}_{*,j}^{(j)}$. There exists $\overline{a}_j$ satisfying the first equality by the induction hypothesis $\boldsymbol{v}_{*,j}^{(j)} \in \mathrm{L}_{\boldsymbol{v}_{*,j-1}^{(j-1)}}$. For $\overline{b}_j$, by Thm. 3.1.7 we have $\overline{a}_j \star \boldsymbol{v}_{*,j}^{(j-1)} \in \mathrm{L}_{\overline{a}_j \star \boldsymbol{v}_{*,j-1}^{(j-1)}} = \mathrm{L}_{\boldsymbol{v}_{*,j}^{(j)}}$ hence from Thm. 2.3.4 we can find $\overline{b}_j$ satisfying the conditions. Let $\boldsymbol{w} = \overline{a}_j \star \boldsymbol{v}^{(j-1)} + (y - \overline{b}_j) \star \boldsymbol{v}^{(j)}$. By construction of $\boldsymbol{w}$, we have $\boldsymbol{w}_{*,k} = \boldsymbol{0}$ for $k < j+1$ and $\boldsymbol{w} = t \star \boldsymbol{v}$ with $t = (\overline{a}_j p_{y^{j-1}} + (y - \overline{b}_j) p_{y^j})$. If $j \ne d_y - 1$ then by Lm. 3.1.3 since $\operatorname{lt}(t) = y^{j+1}$ we deduce that $p_{y^{j+1}} = t \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$ and $\boldsymbol{v}^{(j+1)} = \boldsymbol{w}$, otherwise if $j = d_y - 1$ then $\boldsymbol{w}_{*,k} = \boldsymbol{0}$ for $k \le d_y$ so $\boldsymbol{w} = \boldsymbol{0} = \boldsymbol{v}^{(d_y)}$. Finally, the relation $\boldsymbol{v}_{*,j+1}^{(j+1)} = \overline{a}_j \star \boldsymbol{v}_{*,j+1}^{(j-1)} + \boldsymbol{v}_{*,j}^{(j)} - \overline{b}_j \star \boldsymbol{v}_{*,j+1}^{(j)}$ gives $\boldsymbol{v}_{*,j+1}^{(j+1)} \in \mathrm{L}_{\boldsymbol{v}_{*,j}^{(j)}}$ with the same arguments used to prove the existence of $\overline{b}_j$. □

Lemma 3.1.9. *For $0 \le j < d_y$, if we define $\begin{bmatrix} \overline{s}_j & \overline{t}_j \\ \overline{s}_{j+1} & \overline{t}_{j+1} \end{bmatrix} = \overline{Q}_j \cdots \overline{Q}_0$ with $\overline{Q}_k = \begin{bmatrix} 0 & 1 \\ \overline{a}_k & y - \overline{b}_k \end{bmatrix}$ then $p_{y^j} = \overline{t}_j \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$ and $\overline{t}_{d_y} \in I(\boldsymbol{v})$.*

Proof. For $0 \le j < d_y$, we have $\begin{bmatrix} \boldsymbol{v}^{(j)} \\ \boldsymbol{v}^{(j+1)} \end{bmatrix} = \overline{Q}_j \cdots \overline{Q}_1 \begin{bmatrix} \boldsymbol{v}^{(0)} \\ \boldsymbol{v}^{(1)} \end{bmatrix}$. If we note $R_j = \overline{Q}_j \cdots \overline{Q}_1 = \begin{bmatrix} \alpha_j & \beta_j \\ \gamma_j & \delta_j \end{bmatrix}$ then $\begin{bmatrix} \overline{s}_j & \overline{t}_j \\ \overline{s}_{j+1} & \overline{t}_{j+1} \end{bmatrix} = R_j \begin{bmatrix} 0 & 1 \\ \overline{a}_0 & (y - \overline{b}_0) \end{bmatrix}$ and $\overline{t}_j = \alpha_j + (y - \overline{b}_0)\beta_j$. From Thm. 3.1.8, we have $\boldsymbol{v}^{(1)} = (y - \overline{b}_0) \star \boldsymbol{v}^{(0)}$ so $\overline{t}_j \star \boldsymbol{v} = \alpha_j \star \boldsymbol{v} + \beta_j \star \boldsymbol{v}^{(1)} = \boldsymbol{v}^{(j)}$. By the same reasoning, we obtain $\overline{t}_{j+1} \star \boldsymbol{v} = \boldsymbol{v}^{(j+1)}$. Therefore, $(p_{y^j} - \overline{t}_j) \star \boldsymbol{v} = \boldsymbol{0}$ so $(p_{y^j} - \overline{t}_j \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})) = 0$ and by linearity of the reduction we get $p_{y^j} = p_{y^j} \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}}) = \overline{t}_j \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$. For $j = d_y$, we have $\boldsymbol{v}^{(d_y)} = \boldsymbol{0} = \overline{t}_{d_y} \star \boldsymbol{v}$ so $\overline{t}_{d_y} \in I(\boldsymbol{v})$. □

3.2 Pseudo-Euclidean division

In this subsection, following [11, Sec. 6], we work with polynomials in $\mathbb{K}^{\mathbb{N}}[y]$, the set $\mathbb{K}^{\mathbb{N}}$ is not a ring but is a $\mathbb{K}$-vector space. We define an arithmetic on $\mathbb{K}^{\mathbb{N}}[y]$ that mimics the action $\star$ on sequences.

Definition 3.2.1. *Let $r = \sum_{j=0}^{D} r_j y^j \in \mathbb{K}^{\mathbb{N}}[y]$. We define two operations: for $g \in \mathbb{K}[x]$, $g \cdot r = \sum_{j=0}^{D} (g \star r_j) y^j$ and $y^d \cdot r = \sum_{j=0}^{D} r_j y^{j+d}$ and extend linearly the operation $\cdot$ for polynomials in $\mathbb{K}[x,y]$.*

As in the uni-indexed case, our goal is to reduce the guessing problem to the computation of successive remainders for that we define a pseudo-Euclidean division in $\mathbb{K}^{\mathbb{N}}[y]$.

Theorem 3.2.2. *Let $f = \sum_{j=0}^{d} f_j y^j$ and $g = \sum_{j=0}^{d-1} g_j y^j$ be two polynomials in $\mathbb{K}^{\mathbb{N}}[y]$ of respective degree d and $d-1$ with $d \ge 1$.*

If (i) $g_{d-1} \in \mathrm{L}_{f_d}$, (ii) $f_{d-1} \in \mathrm{L}_{f_d}$, (iii) $g_{d-2} \in \mathrm{L}_{g_{d-1}}$ with f_d C-recursive then $\exists!(a,b) \in \mathbb{K}[x]^2$ with $\operatorname{supp}(a) \subset \mathcal{S}_{f_d}$ and $\operatorname{supp}(b) \subset \mathcal{S}_{g_{d-1}}$ satisfying $a \cdot f = (-y + b) \cdot g + r$ with $\deg_y(r) < \deg_y(g)$.

When the conditions $(i), (ii), (iii)$ of the previous theorem are satisfied, we say that the pseudo-Euclidean division of f by g is well-defined and that its result is (a, b, r).

Proof. Consider such polynomials $f, g \in \mathbb{K}^{\mathbb{N}}[y]$, since $g_{d-1} \in \mathrm{L}_{f_d}$ from Thm. 2.3.4 there exists a unique polynomial $a \in \mathbb{K}[x]$ with $\mathrm{supp}(a) \subset \mathcal{S}_{f_d}$ such that $g_{d-1} = -a \star f_d$. We can construct $\tilde{g} = a \cdot f + y \cdot g = \sum_{j=1}^{d-1}(a \star f_j + g_{j-1})y^j + a \star f_0$. If $\deg_y(\tilde{g}) < d-1$, then $\tilde{g} = r$ and the pair $(a, b) = (a, 0)$ satisfies the conditions. Otherwise, we have $\mathrm{lc}(\tilde{g}) = a \star f_{d-1} + g_{d-2}$ since $a \star f_{d-1} \in \mathrm{L}_{a \star f_d} = \mathrm{L}_{g_{d-1}}$ and $g_{d-2} \in \mathrm{L}_{g_{d-1}}$ we deduce that $\mathrm{lc}(\tilde{g}) \in \mathrm{L}_{g_{d-1}}$. From Thm. 2.3.4, there exists a unique polynomial $b \in \mathbb{K}[x]$ with $\mathrm{supp}(b) \subset \mathcal{S}_{g_{d-1}}$ such that $\mathrm{lc}(\tilde{g}) = b \star g_{d-1}$. Hence, by construction $r = a \cdot f + (y - b) \cdot g$ has degree $< \deg_y(g)$. For the uniqueness of (a, b), consider (a', b') another pair, which gives $\deg_y((a - a') \cdot f + (b' - b) \cdot g) < \deg_y(g)$. So, $(a - a') \star f_d = 0$ and $a = a'$ by Thm. 2.3.4. Finally, we must have $(b - b') \star g_{d-1} = 0$, so $b = b'$ again by Thm. 2.3.4. □

Definition 3.2.3. *For $0 \le j < d_y$, we consider the reverse truncated formal power series $S_j = \sum_{k=j}^{D_y} \boldsymbol{v}_{*,k}^{(j)} y^{D_y - k}$ representing the sequence $\boldsymbol{v}^{(j)}$ at precision D_y with $D_y \ge 2d_y$. Also, we note $S_{-1} = \boldsymbol{v}_{*,0}^{(0)} y^{D_y+1}$.*

Lemma 3.2.4. *For $0 \le j < d_y$, the pseudo-Euclidean division of S_{j-1} by S_j is well-defined.*

Proof. For $1 \le j < d_y$, from Thms. 3.1.7 and 3.1.8 and the construction of S_{j-1} and S_j we deduce that the hypotheses of Thm. 3.2.2 are satisfied. For $j = 0$, by construction of S_{-1} the hypotheses of Thm. 3.2.2 are also satisfied. Hence for $0 \le j < d_y$, the pseudo-Euclidean division of S_{j-1} by S_j is well-defined. □

The remainder of the pseudo-Euclidean division of S_{j-1} by S_j is not exactly S_{j+1} but has the same leading terms.

Definition 3.2.5 ([22, §11.1]). *For a polynomial $p = \sum_{j=0}^{d} p_j y^j \in \mathbb{K}^{\mathbb{N}}[y]$ of degree d in y and $k \le d$, we note $p\upharpoonright_k = \sum_{j=0}^{k} p_{d-j} y^{k-j}$ and $p\upharpoonright_k = y^{k-d}p$ when $k > d$.*

Lemma 3.2.6. *Let $k \ge 1$. For $g \in \mathbb{K}[x, y]$ with $\deg_y(g) = d \le k \le \deg_y(S_0) = D_y$, we have $g \cdot S_0\upharpoonright_k = f_{<d} + \sum_{j=0}^{k-d} \boldsymbol{w}_{*,j} y^{k-j} + f_{>k}$ with $\deg_y(f_{<d}) < d$ and y^{k+1} divides $f_{>k}$.*

Proof. Let $p = g \cdot S_0\upharpoonright_k \in \mathbb{K}^{\mathbb{N}}[y]$. If we note $g_{*,\ell}$ the polynomial in $\mathbb{K}[x]$ associated to the monomial y^ℓ then from the arithmetic on $\mathbb{K}^{\mathbb{N}}[y]$ defined in Def. 3.2.1, we have $p_{k-j} = \sum_{\ell=0}^{d} g_{*,\ell} \star v_{*,j+\ell} = (g \star v)_{*,j}$ for $0 \le j \le k - d$. □

Lemma 3.2.7. *For $0 \le j < d_y - 1$, if the pseudo-Euclidean division of S_{j-1} by S_j is $(c_j, d_j, \tilde{S}_{j+1})$ then we have $c_j = \overline{a}_j, d_j = \overline{b}_j$ with $(\overline{a}_j, \overline{b}_j)$ defined in Thm. 3.1.8 and $\tilde{S}_{j+1}\upharpoonright_{D_y-(j+1)-1} = S_{j+1}\upharpoonright_{D_y-(j+1)-1}$.*

Proof. For $j \ne 0$, the leading terms of S_{j-1} are $\boldsymbol{v}_{*,j-1}^{(j-1)} y^{D_y-j+1} + \boldsymbol{v}_{*,j-2}^{(j-1)} y^{D_y-j}$ and similarly for S_j we deduce from the proof of Thm. 3.2.2 that $c_j = \overline{a}_j$ and $d_j = \overline{b}_j$. For $j = 0$, we have $S_{-1} = \boldsymbol{v}_{*,0} y^{D_y+1}$ and S_0 has leading terms $\boldsymbol{v}_{*,0} y^{D_y} + \boldsymbol{v}_{*,1} y^{D_y-1}$ so we deduce that $c_0 = \overline{a}_0$ and $d_0 = \overline{b}_0$.

For $1 \le j < d_y - 1$, we have on the one hand the relation $\boldsymbol{v}_{*,k}^{(j+1)} = \overline{a}_j \star \boldsymbol{v}_{*,k}^{(j-1)} + \boldsymbol{v}_{*,k-1}^{(j)} - \overline{b}_j \star \boldsymbol{v}_{*,k}^{(j)}$ for $k > 0$ from Thm. 3.1.8. On the other hand, we have $\tilde{S}_{j+1} = \overline{a}_j S_{j-1} + (y - \overline{b}_j) S_j$ which gives $\tilde{S}_{j+1} = (\overline{a}_j \star \boldsymbol{v}_{*,j-1}^{(j-1)} + \boldsymbol{v}_{*,j}^{(j)}) y^{D_y-j+1} + \sum_{k=j}^{D_y-1} (\overline{a}_j \star \boldsymbol{v}_{*,k}^{(j-1)} + \boldsymbol{v}_{*,k-1}^{(j)} - \overline{b}_j \star \boldsymbol{v}_{*,k}^{(j)}) y^{D_y-k} + (\overline{a}_j \star \boldsymbol{v}_{*,D_y}^{(j-1)} - \overline{b}_j \star \boldsymbol{v}_{*,D_y}^{(j)})$. By definition of $\overline{a}_j$ and from Thm. 3.1.8, we deduce that $\deg_y(\tilde{S}_{j+1}) = D_y - j - 1$ thus $\tilde{S}_{j+1}\upharpoonright_{D_y-(j+1)-1} = S_{j+1}\upharpoonright_{D_y-(j+1)-1}$. For $j = 0$, we apply the same arguments and obtain $\tilde{S}_1\upharpoonright_{D_y-2} = S_1\upharpoonright_{D_y-2}$. □

For the purposes of Lms. 3.2.8 and 3.2.9, let $r_0, r_1, r_0', r_1' \in \mathbb{K}^{\mathbb{N}}[y]$ and $k \ge 1$ such that $r_0\upharpoonright_{2k} = r_0'\upharpoonright_{2k}$ and $r_1\upharpoonright_{2k-1} = r_1'\upharpoonright_{2k-1}$. Assume that $d := \deg_y(r_0) = \deg_y(r_1)+1$ and $d' := \deg_y(r_0') = \deg_y(r_1')+1$.

Lemma 3.2.8. *Suppose that the pseudo-Euclidean division (a_1, b_1, r_2) of r_0 by r_1 is well-defined, and that $\deg_y(r_2) = d-2$. Then, the pseudo-Euclidean division (a_1', b_1', r_2') of r_0' by r_1' is also well-defined, and satisfies $a_1 = a_1'$, $b_1 = b_1'$, and $r_2\upharpoonright_{2(k-1)-1} = r_2'\upharpoonright_{2(k-1)-1}$. Moreover, $\deg_y(r_2') = d' - 2$ provided that $k \ge 2$.*

Proof. By assumption, the two leading terms of r_0 and r_0' match, and the same for r_1 and r_1'. Yet, the conditions $(i), (ii), (iii)$ of Thm. 3.2.2 which determine if a pseudo-Euclidean division is well-defined only depends on the two leading terms of the dividend and the divisor. In fact, a_1, b_1 only depend on those same two leading terms. As a consequence, the pseudo-Euclidean division of r_0' by r_1' is well-defined, and $a_1 = a_1'$, $b_1 = b_1'$.

Assume w.l.o.g. $d' \le d$. The hypothesis $r_0\upharpoonright_{2k} = r_0'\upharpoonright_{2k}$ can be rewritten as $\deg_y(r_0 - r_0' y^{d-d'}) \le d - 2k - 1$. Likewise, $\deg_y(r_1 - r_1' y^{d-d'}) \le d - 2k - 1$. Considering that $r_2 = a_1 r_0 + (y - b_1) r_1$ and similarly for r_2', we obtain that $\deg_y(r_2 - r_2' y^{d-d'}) \le d - 2k$. Whenever $k \ge 2$, $\deg_y(r_2) = d - 2 > d - 2k \ge \deg_y(r_2 - r_2' y^{d-d'})$, which can only happen when $\deg_y(r_2) = \deg_y(r_2') + d - d'$, *i.e.* $\deg_y(r_2') = d' - 2$, and $r_2\upharpoonright_{2(k-1)-1} = r_2'\upharpoonright_{2(k-1)-1}$. □

Lemma 3.2.9. *Suppose that the first k pseudo-Euclidean divisions $(a_j, b_j, r_{j+1})_{1 \le j \le k}$ starting from r_0 and r_1 are well-defined, and that $\deg_y(r_j) = d - j$ for $1 \le j \le k$.*

Then the first k pseudo-Euclidean divisions $(a_j', b_j', r_{j+1}')_{1 \le j \le k}$ starting from r_0' and r_1' are also well-defined, and $a_j = a_j'$, $b_j = b_j'$, $\deg_y(r_j') = d' - j$ for $1 \le j \le k$. Moreover, $r_{j+1}\upharpoonright_{2(k-j)-1} = r_{j+1}'\upharpoonright_{2(k-j)-1}$ for $1 \le j < k$.

Proof. Let us prove this statement by induction on k. The base case $k = 1$ is a direct consequence of Lm. 3.2.8. For the induction step, suppose that $k \ge 2$ and that the lemma holds for $k-1$. Lm. 3.2.8 states that the first pseudo-Euclidean divisions (a_1', b_1', r_2') starting from r_0' and r_1' is well-defined, $\deg_y(r_2') = d' - 2$, $a_1' = a_1$, $b_1' = b_1$, and $r_2\upharpoonright_{2(k-1)-1} = r_2'\upharpoonright_{2(k-1)-1}$. It remains to apply our induction hypothesis to $k - 1$ and r_1, r_2, r_1', r_2' to conclude. □

If the k pseudo-Euclidean divisions $(a_j, b_j, r_{j+1})_{0 \le j < k}$ starting from r_{-1} and r_0 are well-defined then we have for $0 \le j < k$ the matrix relations $\begin{bmatrix} r_j \\ r_{j+1} \end{bmatrix} = Q_j \begin{bmatrix} r_{j-1} \\ r_j \end{bmatrix}$ where $Q_j := \begin{bmatrix} 0 & 1 \\ a_j & y - b_j \end{bmatrix}$. Thus,

$\begin{bmatrix} r_j \\ r_{j+1} \end{bmatrix} = Q_j \cdots Q_0 \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix}$ and by defining $\begin{bmatrix} s_j & t_j \\ s_{j+1} & t_{j+1} \end{bmatrix} = Q_j \cdots Q_0$, we have $s_j r_{-1} + t_j r_0 = r_j$ for $0 \le j \le k$.

Theorem 3.2.10. *Let $k \ge 1$, $2k-1 \le D_y$ and $r_{-1}, r_0 \in \mathbb{K}^{\mathbb{N}}[y]$ such that $r_{-1} = S_{-1}\upharpoonright_{2k}$ and $r_0 = S_0\upharpoonright_{2k-1}$. Then, for all $0 \le j < \min(k, d_y) - 1$, the pseudo-Euclidean division (a_j, b_j, r_{j+1}) of r_{j-1} by r_j is well-defined, $a_j = \overline{a}_j$ and $b_j = \overline{b}_j$ defined in Thm. 3.1.8, and also $r_j\upharpoonright_{2(k-j-1)} = S_j\upharpoonright_{2(k-j-1)}$ and $r_{j+1}\upharpoonright_{2(k-j-1)-1} = S_{j+1}\upharpoonright_{2(k-j-1)-1}$ with $\deg_y(r_{j+1}) = \deg_y(r_0) - (j+1)$. When $j = d_y - 1$ and $2k-1 \ge 2d_y$, the pseudo-Euclidean division $(a_{d_y-1}, b_{d_y-1}, r_{d_y})$ on r_{d_y-2} by r_{d_y-1} is well-defined and $\deg_y(r_{d_y}) < \deg_y(r_0) - d_y$.*

Proof. We prove by induction for $0 \le j < \min(k, d_y) - 1$ that the pseudo-Euclidean division (a_j, b_j, r_{j+1}) of r_{j-1} by r_j is well-defined and $r_j\upharpoonright_{2(k-j-1)} = S_j\upharpoonright_{2(k-j-1)}$ and $r_{j+1}\upharpoonright_{2(k-j-1)-1} = S_{j+1}\upharpoonright_{2(k-j-1)-1}$. For $j > 0$, we suppose that the statement is true at step $j-1$ and we prove that it holds at step j. For every j, we have that $r_{j-1}\upharpoonright_{2(k-j)} = S_{j-1}\upharpoonright_{2(k-j)}$ and $r_j\upharpoonright_{2(k-j)-1} = S_j\upharpoonright_{2(k-j)-1}$ also from Lm. 3.2.7 the pseudo-Euclidean division $(\overline{a}_j, \overline{b}_j, \tilde{S}_{j+1})$ of S_{j-1} and S_j is well-defined. Since $j < k-1$, we have $k - j \ge 2$ also by construction $\deg_y(S_j) = \deg_y(S_{j-1}) - 1$ so we can apply Lm. 3.2.8 and get that the pseudo-Euclidean (a_j, b_j, r_{j+1}) division of r_{j-1} by r_j is well-defined. On the one hand from Lm. 3.2.8, we have $r_{j+1}\upharpoonright_{2(k-j-1)-1} = \tilde{S}_{j+1}\upharpoonright_{2(k-j-1)-1}$. On the other hand from Lm. 3.2.7, we have the equality $\tilde{S}_{j+1}\upharpoonright_{D_y-(j+1)-1} = S_{j+1}\upharpoonright_{D_y-(j+1)-1}$. Since $2k-1 \le D_y$ and $j \ge 0$, we have $2k-1-2j-2 \le D_y - j - 2$ so we conclude that $r_{j+1}\upharpoonright_{2(k-j-1)-1} = S_{j+1}\upharpoonright_{2(k-j-1)-1}$. Also from Lm. 3.2.8, we get $a_j = \overline{a}_j$ and $b_j = \overline{b}_j$ and $\deg_y(r_{j+1}) = \deg_y(r_0) - (j+1)$.

When $j = d_y - 1$ and $2k-1 \ge 2d_y$ and the pseudo-Euclidean division $(\overline{a}_{d_y-1}, \overline{b}_{d_y-1}, r_{d_y})$ of r_{d_y-2} by r_{d_y-1} is well-defined by the same arguments so we have the relation $\overline{s}_{d_y} r_{-1} + \overline{t}_{d_y} r_0 = r_{d_y}$. By hypothesis, we have $r_0 = S_0\upharpoonright_{2k}$ so from Lm. 3.2.6 we can rewrite $\overline{t}_{d_y} r_0 = f_{<d_y} + \sum_{j=0}^{2k-1-d_y} \boldsymbol{v}_{*,j}^{(d_y)} y^{2k-1-j} + f_{>2k-1}$ with $\deg_y(f_{<d_y}) < d_y$ and y^{2k} divides $f_{>2k-1}$. We deduce from the division property that $\deg_y(r_{d_y}) \le \deg_y(r_{d_y-1}) - 1 = 2k-1-d_y$ so by identification on the monomial basis we deduce that $\overline{s}_j r_{-1} = f_{>2k-1}$ also since $\boldsymbol{v}^{(d_y)} = \mathbf{0}$ we have $\deg_y(r_{d_y}) < \deg_y(f_{<d_y}) < d_y$. Since $2k-1 \ge 2d_y$, it implies that $d_y \le 2k-1-d_y = \deg_y(r_0) - d_y$ hence $\deg_y(r_{d_y}) < \deg_y(r_0) - d_y$. ◻

3.3 From successive remainders to C-relations

Let $r_{-1} = S_{-1}$ and $r_0 = S_0$. The definition of S_{-1} is motivated by Thm. 3.2.2 and Lm. 3.2.6. Consider the successive remainders $(r_{-1}, r_0, \ldots, r_{d_y})$ and relations $r_j = s_j r_{-1} + t_j r_0$.

Lemma 3.3.1. *For $0 \le j < d_y$, we have $I(\mathrm{lc}(r_j)) = (I(\boldsymbol{v}) : \langle t_j \rangle) \cap \mathbb{K}[x]$ and $\langle 1 \rangle = \mathbb{K}[x] = (I(\boldsymbol{v}) : \langle t_{d_y} \rangle) \cap \mathbb{K}[x]$.*

Proof. Let $0 \le j < d_y$, from Lm. 3.1.9 and Thm. 3.2.10 we have $\boldsymbol{v}^{(j)} = t_j \star \boldsymbol{v}$ and $\mathrm{lc}(r_j) = \boldsymbol{v}_{*,j}^{(j)}$. From Thm. 3.1.7, we deduce that $I(\mathrm{lc}(r_j)) = I(\boldsymbol{v}_{*,j}^{(j)}) = I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x] = (I(\boldsymbol{v}) : \langle t_j \rangle) \cap \mathbb{K}[x]$. Also from Lm. 3.1.9, since $t_{d_y} \in I(\boldsymbol{v})$ we deduce the equality. ◻

For $0 \le j < d_y$, we note f_j be s.t. $\langle f_j \rangle = I(\mathrm{lc}(r_j))$ and $f_{d_y} = 1$.

Theorem 3.3.2. *The set $\{f_j t_j\}_{0 \le j \le d_y}$ is a Gröbner basis of $I(\boldsymbol{v})$.*

Proof. We verify that $f_j t_j \in I(\boldsymbol{v})$ and $\langle \mathrm{lm}(f_j t_j) \rangle_j = \mathrm{lm}(I(\boldsymbol{v}))$. For $0 \le j \le d_y$, from Lm. 3.3.1 the polynomial $f_j t_j \in I(\boldsymbol{v})$. For $x^r y^s \in \mathrm{lm}(I(\boldsymbol{v}))$, if $s \ge d_y$ then $x^r y^s = \mathrm{lm}(x^r y^{s-d_y} t_{d_y})$. Otherwise, if $s < d_y$, by Thm. 3.1.6 we can find $f_s \in \mathbb{K}[x]$ such that $f_s p_{y^s} \in I(\boldsymbol{v})$ and $\mathrm{lm}(f_s p_{y^s}) = x^r y^s$. Since $p_{y^s} = t_s \operatorname{rem}(\mathcal{G}_{\boldsymbol{v}})$ by Thm. 3.2.10, we deduce that $f_s t_s \in I(\boldsymbol{v})$. Note that since $\mathrm{lm}(t_s) = y^s = \mathrm{lm}(p_{y^s})$, $f_s t_s$ still has leading term $x^r y^s$. ◻

From a Gröbner basis of $I(\boldsymbol{v})$, one can compute a minimal Gröbner basis of $I(\boldsymbol{v})$ with the following corollary.

Corollary 3.3.3. *For $1 \le j \le d_y$, either $\mathrm{lm}(f_j t_j) \in \mathrm{lm}(\mathcal{G}_{\boldsymbol{v}})$ or $\deg(f_{j-1}) = \deg(f_j)$.*

Proof. From the definition of minimal Gröbner basis, if $\ell \ne j$ and $\mathrm{lm}(f_\ell t_\ell)$ divides $\mathrm{lm}(f_j t_j)$ then $\ell \le j$ and $\deg(f_\ell) \le \deg(f_j)$. If $(\deg(f_j))_j$ is a decreasing sequence then it proves the claim.

First, we prove that $\deg(f_j) = \min(\{r \mid x^r y^j \in \mathrm{lm}(I(\boldsymbol{v}))\})$. By definition $\langle f_j \rangle = I(\mathrm{lc}(r_j)) = (I(\boldsymbol{v}) : \langle t_j \rangle) \cap \mathbb{K}[x]$ by Lm. 3.3.1 so $\langle f_j \rangle = I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x]$ from Thm. 2.3.4 and $\boldsymbol{v}^{(j)} = t_j \star \boldsymbol{v}$. Finally by Thm. 3.1.6, we can deduce that $I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x] = \{r \mid x^r y^j \in \mathrm{lm}(I(\boldsymbol{v}))\}$. To conclude, if $x^{d_j} = \deg(f_j)$ then we have $\mathrm{lm}(f_j t_j) = (x^{d_j} y^j) y = x^{d_j} y^{j+1} \in \mathrm{lm}(I(\boldsymbol{v}))$ so $\deg(f_{j+1}) \le \deg(f_j)$. ◻

4 ALGORITHMS

In the previous sections, we have considered bi-indexed sequences either as plain sequences $\boldsymbol{v} = (v_{i,j})_{i,j \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}^2}$, or as polynomials with sequence coefficients $\mathbb{K}^{\mathbb{N}}[y]$ in order to get relations out of a pseudo-Euclidean algorithm. At the moment, with the aim of fully describing our algorithms, we need to specify how the operations in $\mathbb{K}^{\mathbb{N}}[y]$ are to be performed. Finite exact representations of univariate sequence include the representation by the initial d_x terms and the minimal relation, or the representation with the first $D_x \ge 2d_x$ terms, so that we can recover the relation. We choose the latter representation, and map these first D_x terms in a reverse truncated formal power series as in [4, 5]. Doing so, the action $t \star \boldsymbol{v}$ can be computed using bivariate polynomial multiplication, which allows us to design efficient algorithms.

4.1 A finite polynomial representation

Let $\boldsymbol{v} = (v_{i,j})_{i,j \in \mathbb{N}}$ be a C-recursive sequence s.t. $x^{d_x}, y^{d_y} \in \mathrm{lm}(\mathcal{G}_{\boldsymbol{v}})$ and consider bounds $D_x \ge 2d_x$ and $D_y \ge 2d_y$.

Definition 4.1.1. *Fix $D_x \ge 2d_x$ and $D_y \ge 2d_y$. A polynomial $r \in \mathbb{K}[x,y]$ is a representation of $\boldsymbol{v}$ at precision (d, δ) if $r \in \mathbb{K}[x,y]_{\le (D_x, D_y)}$ and $r_{D_x - i, D_y - j} = v_{i,j}$ for $0 \le i \le d$ and $0 \le j \le \delta$.*

For a representation q of $\boldsymbol{u}$ at precision (D_x, Δ), the addition term by term gives $q + r$, a representation of $\boldsymbol{u} + \boldsymbol{v}$ at precision $(D_x, \min(\delta, \Delta))$. However, for the multiplication by polynomial in $\mathbb{K}[x,y]$, we have to handle the same problem as in $\mathbb{K}^{\mathbb{N}}[y]$ described in Lm. 3.2.6.

Lemma 4.1.2. *Let r be a representation of $\boldsymbol{v}$ at precision (d, δ) and $t \in \mathbb{K}[x,y]_{\le (e,f)}$. The polynomial $p = tr \operatorname{rem}(\{x^{D_x+1}, y^{D_y+1}\})$ is a representation of $t \star \boldsymbol{v}$ at precision $(d - e, \delta - f)$.*

Proof. For $0 \le i \le d - e$ and $0 \le j \le \delta - f$, we have

$$p_{D_x-i,D_y-j} = \sum_{0\le k\le e} \sum_{0\le \ell \le f} t_{k,\ell}\, r_{D_x-i-k,D_y-j-\ell}$$

and $r_{D_x-i-k,D_y-j-\ell} = v_{i+k,j+\ell}$ by definition of a representation, so $p_{D_x-i,D_y-j} = (t \star \boldsymbol{v})_{i,j}$. By construction, $p \in \mathbb{K}[x,y]_{\le (D_x,D_y)}$. ◻

To handle the problem of decreasing precision in x, we can use fast univariate algorithmic to recover precision in x when the C-relation $f_0 \in \mathcal{G}_{\boldsymbol{v}} \cap \mathbb{K}[x]$ is known.

Theorem 4.1.3. *Let r be a representation of $\boldsymbol{v}$ at precision (D_x, δ) and $t \in \mathbb{K}[x,y]_{\le(e,f)}$ with $e \le D_x$ and $f \le \delta$. From r, t and f_0, one can compute a representation p, also denoted $t \cdot_{f_0} r$, of $\boldsymbol{w} := t \star \boldsymbol{v}$ at precision $(D_x, \delta - f)$ in $\tilde{O}(D_x\delta)$ operations in $\mathbb{K}$.*

Proof. Let $\bar{t} = t \operatorname{rem}(f_0)$ with $\deg_x(\bar{t}) < d_x$. Since $f_0 \in I(\boldsymbol{v})$, we deduce that $\boldsymbol{w} = \bar{t} \star \boldsymbol{v}$. The reduction of t by f_0 requires $\tilde{O}(D_x\delta)$ operations by Lm. 2.1.2. Then, computing a representation p of $\boldsymbol{w}$ at precision $(D_x - d_x, \delta - f)$ has complexity in $\tilde{O}(D_x\delta)$ using $\bar{t}$ and r. Since $D_x - d_x \ge d_x$, we can extend p with f_0 from the univariate extension of Lm. 2.1.2 in $\tilde{O}(D_x\delta)$ operations. ◻

We extend this definition of $\cdot_{f_0}$ to matrix-vector multiplication with entries in $\mathbb{K}[x,y]$. With this new operations on representation in $\mathbb{K}[x,y]$, we can mimic the $\mathbb{K}[x,y]$ action on $\mathbb{K}^{\mathbb{N}}[y]$ and apply a pseudo-Euclidean algorithm to solve the guessing problem on $\boldsymbol{v}$.

4.2 Quotient algorithm

We now define the quotient algorithm of our pseudo-Euclidean division. For that, we need two subroutines for C-recursive uni-indexed sequences. The first one, GuessingUnivar(r) takes a representation $r \in \mathbb{K}[x]$ of a C-recursive sequence $\boldsymbol{u}$ at precision D_x with $D_x \ge 2d_x$ and outputs the C-relation $f \in \mathbb{K}[x]_{\le d_x}$ satisfying $\langle f\rangle = I(\boldsymbol{u})$. The other one, HankelSolver(q, r, f), takes a representation $q \in \mathbb{K}[x]$ of a C-recursive sequence $\boldsymbol{u}$ at precision $D_x \ge 2(d_x - 1)$; a representation $r \in \mathbb{K}[x]$ of $\boldsymbol{v} \in \mathrm{L}_{\boldsymbol{u}}$ at precision $d \ge d_x - 1$ and a C-relation $f \in \mathbb{K}[x]_{\le d_x}$ s.t. $\langle f\rangle = I(\boldsymbol{u})$, and outputs $b \in \mathbb{K}[x]_{<d_x}$ satisfying $b \star \boldsymbol{u} = \boldsymbol{v}$. Both subroutines have complexities $\tilde{O}(D_x)$ (see §2.1).

Algorithm 1 QuoBivar(f, g)

Input: Polynomials $f = \sum_{j=0}^{d} f_j(x)y^j$ and $g = \sum_{j=0}^{d-1} g_j(x)y^j$ satisfying the hypotheses of Thm. 3.2.2 when viewed in $\mathbb{K}^{\mathbb{N}}[y]$ using the representation of $D_x + 1$ initial terms.

Output: $Q \in \mathbb{K}[x,y]^{2\times 2}, \{p_1\} \subset \mathbb{K}[x]$ be s.t. $\begin{bmatrix} g \\ r \end{bmatrix} = Q \cdot_{p_0} \begin{bmatrix} f \\ g \end{bmatrix}$ with $\deg_y(r) < \deg_y(g)$ and $\langle p_1 \rangle = I(g_{d-1})$.

$p_0 \leftarrow$ GuessingUnivar($f_d(x)$)
$a \leftarrow$ HankelSolver($-f_d(x), g_{d-1}(x), p_0$)
$h(x) \leftarrow a \cdot_{p_0} f_{d-1}(x) + g_{d-2}(x)$
$p_1 \leftarrow$ GuessingUnivar($g_{d-1}(x)$)
$b \leftarrow$ HankelSolver($g_{d-1}(x), h(x), p_1$)
return $\begin{bmatrix} 0 & 1 \\ a & y-b \end{bmatrix}, \{p_1\}$

Lemma 4.2.1. *QuoBivar is correct and has complexity in $\tilde{O}(D_x)$.*

Proof. The polynomials f, g viewed in $\mathbb{K}^{\mathbb{N}}[y]$ satisfy the hypotheses of Thm. 3.2.2 so we consider $f_d, f_{d-1}, g_{d-1}, g_{d-2} \in \mathbb{K}^{\mathbb{N}}$ the sequences represented by $f_d(x), f_{d-1}(x), g_d(x), g_{d-1}(x) \in \mathbb{K}[x]$. Thm. 3.2.2 shows that there exists $a \in \mathbb{K}[x]_{<\deg(p_0)}$ such that $-a\star f_d = g_{d-1}$, that the call to HankelSolver($-f_d(x), g_{d-1}(x), p_0$) computes. The update polynomial $h(x)$ represents the sequence $a \star f_{d-1} + g_{d-2}$. From Thm. 3.2.2, we can compute $b \in \mathbb{K}[x]_{<\deg(p_1)}$ such that $b \star g_{d-1} = a \star f_{d-1} + g_{d-2}$ also computed by the call to HankelSolver($g_{d-1}(x), h(x), p_1$). By hypothesis of Thm. 3.2.2, p_0 is a C-relation on $f_d, f_{d-1}, g_{d-1}, g_{d-2}$, which ensures that $\deg_y(r) < \deg_y(g)$ by construction of the quotient matrix Q. Also, $\langle p_1 \rangle = I(g_{d-1})$ from the correctness of GuessingUnivar.

Computing $p_0, p_1 \in \mathbb{K}[x]_{\le d_x}$ and $a, b \in \mathbb{K}[x]_{<d_x}$ have complexity in $\tilde{O}(D_x)$. The computation of $h(x)$ corresponds to univariate polynomial multiplication and addition of degree at most D_x so it requires $\tilde{O}(D_x)$. Hence, we can bound the complexity of QuoBivar(f, g) in $\tilde{O}(D_x)$. ◻

4.3 Recursive pseudo-Euclidean algorithm

Based on the half-gcd algorithm, we build a divide and conquer pseudo-Euclidean algorithm, following the exposition of [22, Alg. 11.4]. Since our pseudo-Euclidean division has specific hypotheses, we define an assumption on the input of our algorithm.

Assumption B. *For the input (r_{-1}, r_0, f_0, k), $f_0 \in \mathbb{K}[x]$ is a C-relation on the sequences represented by r_{-1} and r_0, and there exists $0 \le \ell \le k$ such that the ℓ firsts pseudo-Euclidean division of r_{-1} by r_0 are well-defined, and $\deg_y(r_{\ell-1}) - 1 > \deg_y(r_\ell)$ if $\ell < k$.*

Algorithm 2 half-gcd-seq(r_{-1}, r_0, f_0, k)

Input: Representations $r_{-1}, r_0 \in \mathbb{K}[x,y]$, a C-relation $f_0 \in \mathbb{K}[x]$ and $k \in \mathbb{N}$ satisfying Asm. B.

Output: $R \in \mathbb{K}[x,y]^{2\times 2}$ s.t. $\begin{bmatrix} r_{\ell-1} \\ r_\ell \end{bmatrix} = R \cdot_{f_0} \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix}$, $T = [Q_0, \dots, Q_{\ell-1}] \in (\mathbb{K}[x,y]^{2\times 2})^\ell$ s.t. $R = Q_{\ell-1} \cdots Q_0 \operatorname{rem}(f_0)$ and $\mathcal{F} = [f_0, \dots, f_{\ell-1}] \subset \mathbb{K}[x]$ s.t. $\langle f_j \rangle = I(\boldsymbol{w}^{(j)}_{*,j})$ with $\boldsymbol{w}^{(j)}$ corresponds to the sequence represented by r_j.

if $k = 0$ **then return** $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, [], []
$d \leftarrow \lceil k/2 \rceil, d^* \leftarrow k - d$
$R, T, \mathcal{F}_0 \leftarrow$ half-gcd-seq($r_{-1}\restriction_{2(d-1)}, r_0\restriction_{2(d-1)-1}, f_0, d-1$)
$\begin{bmatrix} r_{d-2} \\ r_{d-1} \end{bmatrix} \leftarrow R \cdot_{f_0} \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix}$
if $\deg_y(r_{d-2}) - 1 > \deg_y(r_{d-1})$ **then return** $R, T, \mathcal{F}_0$
$Q_{d-1}, \{f_{d-1}\} \leftarrow$ QuoBivar($r_{d-2}\restriction_2, r_{d-1}\restriction_1$)
$\begin{bmatrix} r_{d-1} \\ r_d \end{bmatrix} \leftarrow Q_{d-1} \cdot_{f_0} \begin{bmatrix} r_{d-2} \\ r_{d-1} \end{bmatrix}$
$S, U, \mathcal{F}_1 \leftarrow$ half-gcd-seq($r_{d-1}\restriction_{2d^*}, r_d\restriction_{2d^*-1}, f_0, d^*$)
return $(SQ_{d-1}R) \operatorname{rem}(f_0)$, $[T, Q_{d-1}, U]$, $[\mathcal{F}_0, f_{d-1}, \mathcal{F}_1]$

Theorem 4.3.1. *half-gcd-seq is correct. If D_x (resp. $D_y + 1$) is the maximum degree in x (resp. y) of r_{-1}, r_0 and $\lfloor D_y/2 \rfloor \le k \le D_y$ then half-gcd-seq(r_{-1}, r_0, f_0, k) requires $\tilde{O}(D_x D_y)$ operations in $\mathbb{K}$.*

Proof. We prove by induction on j, for any input (r_{-1}, r_0, f_0, j) satisfying Asm. B, half-gcd-seq is correct. For any input $(r_{-1}, r_0, f_0, 0)$ satisfying Asm. B, the algorithm outputs $(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, [], [])$ which satisfies all the conditions of the algorithm output.

For $j \in \mathbb{N}$, we suppose the induction hypothesis at each step $i < j$ and we prove that the algorithm is correct for the input

(r_{-1}, r_0, f_0, j) satisfying Asm. B. Consider the first ℓ pseudo-Euclidean divisions $(a_i, b_i, r_{i+1})_{0\le i\le \ell-1}$ of r_{-1} by r_0 with $0 \le \ell \le j$. Lm. 3.2.9 ensures that $(r_{-1}\upharpoonright_{2(d-1)}, r_0\upharpoonright_{2(d-1)-1}, f_0, d-1)$ satisfies Asm. B so by the induction hypothesis we have the same quotient matrices $Q_i = \begin{bmatrix} 0 & 1 \\ a_i & y-b_i \end{bmatrix}$ for $0 \le i < \min(d-1, \ell)$. Since, f_0 is a C-relation on the sequences represented by r_{-1} and r_0, it is a C-relation on r_i due to $r_i = s_i r_{-1} + t_i r_0$ for $0 \le i < \min(d, \ell+1)$. If $\ell \le d-1$ then $R \cdot_{f_0} \begin{bmatrix} r_{-1} \\ r_0 \end{bmatrix} = \begin{bmatrix} r_{\ell-1} \\ r_\ell \end{bmatrix}$ at Step 4 and $(R, T, \mathcal{F}_0)$ is the correct output. Otherwise, r_{d-2} and r_{d-1} are correctly computed at Step 4 from r_{-1}, r_0 and R at precision D_x in x. So, we can compute the quotient matrix Q_d from $r_{d-2}\upharpoonright_2$ and $r_{d-1}\upharpoonright_1$ since the quotient algorithm only need the first two leading terms of each polynomial. The computation of r_d from r_{d-2}, r_{d-1} and f_0 is computed at full precision in x. From Lm. 3.2.9, since $j \ge \ell$, we have $d^* \ge \ell - d$, so the $(\ell-d)$ first pseudo-Euclidean division of $r_{d-1}\upharpoonright_{2d^*}$ by $r_d\upharpoonright_{2d^*-1}$ give the same results as the ones of r_{d-1} and r_d. The second recursive call gives $S = Q_{\ell-1}\cdots Q_d \operatorname{rem}(f_0)$, $U = [Q_d, \dots, Q_{\ell-1}]$ and $\mathcal{F} = [f_d, \dots, f_{\ell-1}]$. Therefore, HALF-GCD-SEQ is correct.

For the complexity analysis, we suppose that k is a power of 2 and we note $\mathrm{C}(k)$ the cost of the computation. The base case requires $O(1)$ operations in $\mathbb{K}$. In the others cases due to the condition $k \in \Theta(D_y)$, the costs of the matrix multiplication $\cdot_{f_0}$ is in $\tilde{O}(D_x k)$ and the call to QuoBivar is in $\tilde{O}(D_x)$ by Lm. 4.2.1. Finally, since the quotient matrices have all degree 1 in y, we deduce that $\deg_y(S)$ and $\deg_y(R)$ are less or equal to $k/2$ and the degree in x is bounded by $O(D_x)$ since the matrices are reduced by the relation f_0. Hence, the last matrix multiplication is in $\tilde{O}(D_x k)$. Note that the recursive calls continue to verify the condition $\lfloor D_y/2\rfloor \le k \le D_y$. Thus, the cost $\mathrm{C}(k)$ follows the recurrence $\mathrm{C}(k) = 2\mathrm{C}(k/2) + \tilde{O}(D_x k)$ and by the Master theorem we conclude that $\mathrm{C}(k) = \tilde{O}(D_x D_y)$. ◻

4.4 Guessing of bi-indexed sequences

From the result of Thm. 4.3.1, it remains to compute the cofactors t_j from the quotient matrices to obtain a Gröbner basis of $I(\boldsymbol{v})$.

The product of matrices can be done recursively, we define RecursiveMatrixProduct(T, k, f_0) with $T = [Q_0, \dots, Q_{\ell-1}] \in \mathbb{K}[x,y]^{2\times 2}$ s.t. $\deg_y(Q_j) = 1$, $0 \le k < \ell$ and $f_0 \in \mathbb{K}[x]_{\le d_x}$ which computes the matrix $R = Q_k \cdots Q_0 \operatorname{rem}(f_0)$. A call to RecursiveMatrixProduct(T, k, f_0) requires $\tilde{O}(d_x k)$ operations.

By combining the algorithms HALF-GCD-SEQ and RecursiveMatrixProduct, we obtain a quasi-linear guessing algorithm for C-recursive bi-indexed sequences w.r.t. the lexicographic ordering.

Theorem 4.4.1. *GuessingBivar is correct and has complexity in* $\tilde{O}(D_x D_y + |\mathcal{G}_{\boldsymbol{v}}| d_x d_y)$.

Proof. For the correctness, the polynomial f_0 computed from the call to GuessingOnevar is in $\mathcal{G}_{\boldsymbol{v}} \cap \mathbb{K}[x]$ since $I(v_{*,0}) = I(\boldsymbol{v}) \cap \mathbb{K}[x]$ by Thm. 3.1.7. From Thm. 3.2.10, we have that (r_{-1}, r_0, f_0, k) satisfies Asm. B with $\ell = d_y$ and by Thm. 4.3.1, we deduce that $R = Q_{d_y-1}\cdots Q_0 \operatorname{rem}(f_0)$, $T = [Q_0, \dots, Q_{d_y-1}]$ and $\mathcal{G}_x = [f_0, \dots, f_{d_y-1}]$ with $f_j \in I(\boldsymbol{v}_{*,j}^{(j)}) = I(\boldsymbol{v}^{(j)}) \cap \mathbb{K}[x]$ by Thm. 3.1.7. From Cor. 3.3.3, we only have to compute the relations which are not divisible by a previous one. For that, we distinguish them by the degree of f_j and compute the corresponding cofactor t_j when $\deg(f_{j-1}) \ne \deg(f_j)$. Finally, we get t_{d_y} from the matrix R. Hence, GuessingBivar outputs a minimal Gröbner basis of $I(\boldsymbol{v})$ in $\mathcal{G}$.

Algorithm 3 GuessingBivar$(\boldsymbol{v})$

Input: The initial terms $(v_{i,j})_{0\le i\le D_x, 0\le j\le D_y}$ of a C-recursive sequence $\boldsymbol{v}$ satisfying Asm. A with $D_x \ge 2d_x$ and $D_y \ge 2d_y$.
Output: $\mathcal{G}$ a minimal Gröbner basis of $I(\boldsymbol{v})$ w.r.t. the order $\prec$.

$k \leftarrow \lfloor D_y/2 \rfloor$
$r_{-1} \leftarrow \sum_{i=0}^{D_x} v_{i,0} x^{D_x-i} y^{D_y+1}$, $r_0 \leftarrow \sum_{j=0}^{D_y}\sum_{i=0}^{D_x} v_{i,j} x^{D_x-i} y^{D_y-j}$
$f_0 \leftarrow$ GuessingUnivar$(\sum_{i=0}^{D_x} v_{i,0} x^{D_x-i})$
$R, T, \mathcal{G}_x \leftarrow$ HALF-GCD-SEQ(r_{-1}, r_0, f_0, k)
$d \leftarrow D_x + 1$, $\mathcal{G} \leftarrow \{\}$, $j \leftarrow 0$
for $f \in \mathcal{G}_x$ **do**
  if $\deg(f) < d$ **then**
    $\begin{bmatrix} s_j & t_j \\ s_{j+1} & t_{j+1} \end{bmatrix} \leftarrow$ RecursiveMatrixProduct(T, j, f_0)
    $\mathcal{G} \leftarrow \mathcal{G} \cup \{(t_j f) \operatorname{rem}(f_0)\}$, $d \leftarrow \deg(f)$
  $j \leftarrow j+1$
$\mathcal{G} \leftarrow \mathcal{G} \cup \{t_{d_y}\}$ ▷ $R = \begin{bmatrix} s_{d_y-1} & t_{d_y-1} \\ s_{d_y} & t_{d_y} \end{bmatrix} \operatorname{rem}(f_0)$
return $\mathcal{G}$

For the complexity analysis, calling HALF-GCD-SEQ is in $\tilde{O}(D_x D_y)$ by Thm. 4.3.1. The loops on the polynomials of $\mathcal{G}_x$ add computations only if they compute a new polynomial in the minimal Gröbner basis and do at most $\tilde{O}(d_x d_y)$ operations. Finally, all the others instructions of the algorithm are in $\tilde{O}(D_x D_y)$. Hence, the complexity of GuessingBivar is in $\tilde{O}(D_x D_y + |\mathcal{G}_{\boldsymbol{v}}| d_x d_y)$. ◻

5 BENCHMARKS

The quasi-linearity of our guessing algorithm can be observed in practice from our implementation in Maple (https://github.com/ktran11/CrecbiseqGuessing). We compare the timings of our implementation also in Maple of guessing algorithms from [3, 16, 19]. For some we have to specialize the implementation for the lexicographic ordering with weighted degree ordering. For [3], we consider the adaptive version of the algorithms. We do not compare with [5], as under Asm. A, the computations are the same as in [3].

In our examples, we consider different shapes of staircase using Lazard's structure theorem [13] to build $\operatorname{lm}(\mathcal{G}_{\boldsymbol{v}})$. We distinguish two particular shapes: *simplex* with $\operatorname{lm}(\mathcal{G}_{\boldsymbol{v}}) = \{x^{d_x-j} y^j\}_{0\le j\le d_x}$ and *L-shape* with $\operatorname{lm}(\mathcal{G}_{\boldsymbol{v}}) = \{x^{d_x}, xy, y^{d_y}\}$.

To begin with, we consider that we know d_x, d_y and give exactly $D_x = 2d_x$ and $D_y = 2d_y$ in order to compute a minimal Gröbner basis of $I(\boldsymbol{v})$. The quantity $\operatorname{size}(\mathcal{G}_{\boldsymbol{v}})$ corresponds to the number of coefficients in $\mathbb{K} = \mathbb{F}_{2^{16}+1}$ to represents $\mathcal{G}_{\boldsymbol{v}}$. The timings are in seconds, if the timing is greater than one day we use the symbol ∞.

For *simplex*, Fig. 1 shows a quasi-linear growth on the timings of Alg. 3 following the growth of the quantity $|\mathcal{G}_{\boldsymbol{v}}| d_x d_y$.

For *L-shape*, the timings of Alg. 3 also follow the complexity found following the growth of the quantity $D_x D_y$. But it is outperformed by the adaptive version of the different algorithms.

Next, for the second row of the Fig. 1 we now consider more initial terms of the sequence $\boldsymbol{v}$ than $D_x = 2d_x$ and $D_y = 2d_y$ by taking $(D_x, D_y) = (kd_x, kd_y)$ with $k \in \{10, 20, \dots, 50\}$.

On Fig. 2 when $k \ge 30$, there is a crossover point on which the adaptive algorithm performs better, it is explained by the fact that these adaptive versions do not depend on the number of initial terms $D_x D_y$.

	$\lvert\mathcal{G}_v\rvert d_x d_y$	$D_x D_y$	size($\mathcal{G}_v$)	[19]	[3]	[16]	Alg. 3
simplex	27900	3600	9951	287.8	20.5	4	4.2
	127500	10000	44250	4530	777.2	22.1	14.6
	347900	19600	119348	>10h	17857.2	79.1	35.6
	737100	32400	251248	∞	∞	206.6	71.7
	1343100	48400	455937	∞	∞	455.6	136.8
	2213900	67600	749439	∞	∞	922.9	231.6
	3397500	90000	1147735	∞	∞	1696.2	381.5
	4941900	115600	1666819	∞	∞	2871	650.5
L-shape	21600	28800	250	∞	1.2	489.5	37.184
	117600	156800	570	∞	12.8	34739.9	389.5
	290400	387200	890	∞	67.5	∞	1825.8
	540000	720000	1210	∞	209.8	∞	3666.9
	866400	1155200	1530	∞	534.6	∞	6113.2
	1269600	1692800	1850	∞	1201.9	∞	11422.7

Figure 1: Maple implementation of several examples with initial terms $(D_x, D_y) = (2d_x, 2d_y)$, timings in seconds.

	$\lvert\mathcal{G}_v\rvert d_x d_y$	$D_x D_y$	k	[19]	[3]	[16]	Alg. 3
simplex	127500	2500	2	4530	777.2	22.1	14.6
	127500	250000	10	∞	777.2	5675.9	43.3
	127500	1000000	20	∞	777.2	∞	202.7
	127500	2250000	30	∞	777.2	∞	491.1
	127500	4000000	40	∞	777.2	∞	924.2
	127500	6250000	50	∞	777.2	∞	1870.8

Figure 2: Maple implementation of one example with initial terms $(D_x, D_y) = (kd_x, kd_y)$, timings in seconds.

REFERENCES

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

[2] J. Berthomieu, B. Boyer, and J.-Ch. Faugère. 2015. Linear Algebra for Computing Gröbner Bases of Linear Recursive Multidimensional Sequences. In *Proceedings of the 2015 ACM on International Symposium on Symbolic and Algebraic Computation* (Bath, United Kingdom) *(ISSAC '15)*. ACM, New York, NY, USA, 61–68. https://doi.org/10.1145/2755996.2756673

[3] J. Berthomieu, B. Boyer, and J.-Ch. Faugère. 2017. Linear algebra for computing Gröbner bases of linear recursive multidimensional sequences. *Journal of Symbolic Computation* 83 (2017), 36–67. https://doi.org/10.1016/j.jsc.2016.11.005 Special issue on the conference ISSAC 2015.

[4] J. Berthomieu and J.-Ch. Faugère. 2018. A Polynomial-Division-Based Algorithm for Computing Linear Recurrence Relations. In *Proceedings of the 2018 ACM International Symposium on Symbolic and Algebraic Computation* (New York, NY, USA) *(ISSAC '18)*. ACM, New York, NY, USA, 79–86. https://doi.org/10.1145/3208976.3209017

[5] J. Berthomieu and J.-Ch. Faugère. 2022. Polynomial-division-based algorithms for computing linear recurrence relations. *Journal of Symbolic Computation* 109 (2022), 1–30. https://doi.org/10.1016/j.jsc.2021.07.002

[6] A. Bostan, G. Lecerf, and É. Schost. 2003. Tellegen's principle into practice. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation* (Philadelphia, PA, USA) *(ISSAC '03)*. Association for Computing Machinery, New York, NY, USA, 37–44. https://doi.org/10.1145/860854.860870

[7] R. P. Brent, F. G. Gustavson, and D. Y. Y. Yun. 1980. Fast solution of toeplitz systems of equations and computation of Padé approximants. *Journal of Algorithms* 1, 3 (1980), 259–295. https://doi.org/10.1016/0196-6774(80)90013-9

[8] D. A. Cox, J. Little, and D. O'Shea. 2015. *Ideals, Varieties, and Algorithms* (4 ed.). Springer Cham. https://doi.org/10.1007/978-3-319-16721-3

[9] J-Ch. Faugère, P. Gianni, D. Lazard, and T. Mora. 1993. Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. *Journal of Symbolic Computation* 16, 4 (1993), 329–344. https://doi.org/10.1006/jsco.1993.1051

[10] J.-Ch. Faugère and Ch. Mou. 2017. Sparse FGLM Algorithms. *Journal of Symbolic Computation* 80 (2017), 538–569. https://doi.org/10.1016/j.jsc.2016.07.025

[11] S. G. Hyun, V. Neiger, and É. Schost. 2021. Algorithms for Linearly Recurrent Sequences of Truncated Polynomials. In *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation* (Virtual Event, Russian Federation) *(ISSAC '21)*. Association for Computing Machinery, New York, NY, USA, 201–208. https://doi.org/10.1145/3452143.3465533

[12] D. E Knuth. 1970. The analysis of algorithms. In *Actes du Congres International des Mathématiciens (Nice, 1970)*, Vol. 3. 269–274.

[13] D. Lazard. 1985. Ideal Bases and Primary Decomposition: Case of Two Variables. *J. Symb. Comput.* 1, 3 (1985), 261–270. https://doi.org/10.1016/S0747-7171(85)80035-3

[14] J. Massey. 1969. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theor.* 15, 1 (1969), 122–127. https://doi.org/10.1109/TIT.1969.1054260

[15] R. T. Moenck. 1973. Fast Computation of GCDs. In *Proceedings of the Fifth Annual ACM Symposium on Theory of Computing* (Austin, Texas, USA) *(STOC '73)*. Association for Computing Machinery, New York, NY, USA, 142–151. https://doi.org/10.1145/800125.804045

[16] B. Mourrain. 2017. Fast Algorithm for Border Bases of Artinian Gorenstein Algebras. In *Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation* (Kaiserslautern, Germany) *(ISSAC '17)*. Association for Computing Machinery, New York, NY, USA, 333–340. https://doi.org/10.1145/3087604.3087632

[17] S. Naldi and V. Neiger. 2020. A divide-and-conquer algorithm for computing gröbner bases of syzygies in finite dimension. In *Proceedings of the 45th International Symposium on Symbolic and Algebraic Computation* (Kalamata, Greece) *(ISSAC '20)*. Association for Computing Machinery, New York, NY, USA, 380–387. https://doi.org/10.1145/3373207.3404059

[18] Sh. Sakata. 1988. Finding a minimal set of linear recurring relations capable of generating a given finite two-dimensional array. *J. Symbolic Comput.* 5, 3 (1988), 321–337. https://doi.org/10.1016/S0747-7171(88)80033-6

[19] Sh. Sakata. 1990. Extension of the Berlekamp-Massey Algorithm to N Dimensions. *Inform. and Comput.* 84, 2 (1990), 207–239. https://doi.org/10.1016/0890-5401(90)90039-K

[20] Sh. Sakata. 2009. The BMS Algorithm. In *Gröbner Bases, Coding, and Cryptography*, Massimiliano Sala, Shojiro Sakata, Teo Mora, Carlo Traverso, and Ludovic Perret (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 143–163. https://doi.org/10.1007/978-3-540-93806-4_9

[21] A. Schönhage. 1971. Schnelle Berechnung von Kettenbruchentwicklungen. *Acta Informatica* 1, 2 (1971), 139–144. https://doi.org/10.1007/BF00289520

[22] J. von zur Gathen and J. Gerhard. 2013. *Modern Computer Algebra* (3 ed.). Cambridge University Press. https://doi.org/10.1017/CBO9781139856065

[23] D. Wiedemann. 1986. Solving sparse linear equations over finite fields. *IEEE Trans. Inf. Theory* 32, 1 (1986), 54–62.